**Обучающий курс по информационной безопасности для администраторов безопасности компаний, организаций и учреждений**

Об этом курсе

1. Введение
   1. Актуальность проблемы информационной безопасности
   2. Основные понятия
   3. Правовые основы обеспечения информационной безопасности. Государственная система защиты информации
   4. Электронная подпись
   5. Виды мер и основные принципы обеспечения информационной безопасности
   6. Тест
2. Средства Защиты Информации
   1. Межсетевые экраны
   2. Средства анализа защищенности
   3. Средства обнаружения атак
   4. Средства доверенной загрузки
   5. Средства контроля съёмных носителей
   6. Тест
3. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы
   1. Управление(администрирование) системой защиты информации информационной системы
      1. Действия администратора в ходе управления доступом субъектов доступа к объектам доступа
      2. Действия администратора в ходе управления СЗИ в ИС
      3. Действия администратора по управлению компонентами ПО и регистрации, анализу событий безопасности
      4. Методы по информированию пользователей
   2. Управление инцидентами информационной безопасности
      1. Реагирование на инциденты ИБ
      2. Рекомендуемые инструменты
   3. Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
      1. Использование отказоуйстчивых тех средств
      2. резервное копирование ИС и информации на резервные машинные носители
      3. Восстановление работоспособности СЗИ
   4. Тест
4. Итог
   1. Инструкции по организации парольной защиты
   2. Итоговый Тест

Оглавление

[Об этом курсе 4](#_Toc41582652)

[Глава 1: Введение 5](#_Toc41582653)

[Термины и определения 6](#_Toc41582654)

[Актуальность проблемы информационной безопасности 8](#_Toc41582655)

[Основные понятия информационной безопасности 11](#_Toc41582656)

[Правовые основы обеспечения информационной безопасности. Государственная система защиты информации 16](#_Toc41582657)

[Государственная система защиты информации 17](#_Toc41582658)

[Юридическая значимость ЭП 18](#_Toc41582659)

[Организационные и технические меры, и основные принципы обеспечения информационной безопасности 26](#_Toc41582660)

[ТЕСТ ПО 1 ГЛАВЕ 29](#_Toc41582661)

[Глава 2: Средства Защиты Информации 30](#_Toc41582662)

[Межсетевые экраны 33](#_Toc41582663)

[Средства анализа защищенности 38](#_Toc41582664)

[Средства обнаружения атак 40](#_Toc41582665)

[Средства доверенной загрузки 42](#_Toc41582666)

[Средства контроля съёмных носителей 46](#_Toc41582667)

[Тест по 2 главе 50](#_Toc41582668)

[Глава 3: Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы 51](#_Toc41582669)

[Управление(администрирование) системой защиты информации информационной системы 51](#_Toc41582670)

[Действия администратора в ходе управления доступом субъектов доступа к объектам доступа 52](#_Toc41582671)

[Управление устройствами 53](#_Toc41582672)

[Действия администратора в ходе управления средствами защиты информации в ИС 55](#_Toc41582673)

[Действия администратора по управлению компонентами ПО и регистрации, анализу событий безопасности. 60](#_Toc41582674)

[Методы администратора по информированию пользователей 62](#_Toc41582675)

[Управление инцидентами информационной безопасности 63](#_Toc41582676)

[Реагирование на инциденты 64](#_Toc41582677)

[Подготовительный этап 64](#_Toc41582680)

[Рекомендуемые инструменты 73](#_Toc41582681)

[Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций 75](#_Toc41582682)

[Использование отказоустойчивых технических средств 76](#_Toc41582683)

[Резервное копирование компонентов ИС и информации на резервные машинные носители 77](#_Toc41582684)

[Восстановление работоспособности средств защиты информации 79](#_Toc41582685)

[Тест по итогам 3 главы 79](#_Toc41582686)

[Глава 4: Итоги курса 80](#_Toc41582687)

[Инструкции сотрудника по работе в информационных системах компании. 80](#_Toc41582688)

[Итоговый тест по 4 Главе 80](#_Toc41582689)

[Список используемых источников 81](#_Toc41582690)

[Приложение 82](#_Toc41582691)

# Об этом курсе

Целью курса является направлен на повторение и расширение знаний администраторов безопасности с основными понятиями защиты информации, принципами построения систем защиты информации, администрированием системой защиты информации информационной системы, а также основными категориями мер защиты информации, их возможностями с точки зрения защиты информации, сильными и слабыми сторонами, средствами защиты информации.

В процессе освоения курса ученики получат углубленные знания в сфере защиты информации, изучат тему обеспечения работоспособности систем защиты информации при возникновении нештатных ситуаций. Курс направлен развитие критического мышления по отношению к информации, а также на понимание о важности информационной безопасности и данных, которые распростятся в компании.

Для освоения материала курса будут обязательны профильное образование в сфере информационной безопасности, а также будут полезны знания из общего курса информационных технологий, основы работы с ПК. Их наличие позволит понять принципы различных угроз безопасности данных, а также терминологию, используемую в сфере информационной безопасности.

В качестве эксперта в курсе участвует Никитин Виктор Николаевич, доцент кафедры Информационные технологии и система, а так же директор ДВУНЦ (Дальневосточный Учебно-научный центр по информационной безопасности), который в настоящее время занимает одну из лидирующих позиций на территории Хабаровского края и Дальневосточного федерального округа в области услуг по обеспечению информационной безопасности объектов информатизации и автоматизированных систем, а также в области обучения, переподготовки и повышения квалификации специалистов по защите персональных данных, конфиденциальной информации и государственной тайны.

# Глава 1: Введение

Здравствуйте, и добро пожаловать в специальный курс по информационной безопасности для администраторов безопасности. В ходе данного курса мы повторим основные аспекты связанные с защитой информации, которые вы могли забыть или не изучить, изучим различную документацию регламентирующую работу обычных пользователей в компании, нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. Наиболее важным навыком после прохождения курса будет умение грамотно управлять системой защиты информационной системы, предпринимать быстрые и действенные методы при возникновении нештатных ситуаций. А также в конце курса вы получите полезные инструкции по организации парольной политике и антивирусной защиты в компании.

Сперва для полного понимания курса мы должны повторить основные сокращения и термины, используемые в курсе.

**Сокращения**

– ВТСС – вспомогательные технические средства и системы;

– ЗИ – защита информации;

– ИБ – информационная безопасность

– ИС – информационная система;

– КЗ – контролируемая зона;

–МНИ – машинный носитель информации;

– НСД – несанкционированный доступ;

– ОС – операционная система;

– ОРД – организационно – распорядительная документация;

– ОТСС – основные технические средства и системы

– ПД – персональные данные;

– ПО – программное обеспечение;

– СЗИ – средства защиты информации.

# Термины и определения

|  |  |
| --- | --- |
| Термин | Определение |
| Информационная безопасность  (ИБ) | Сфера науки и техники, охватывающая совокупность проблем, связанных с обеспечением защищенности объектов информационной сферы в условиях существования угроз. Под ИБ также понимают защищенность информации от несанкционированного ознакомления, преобразования и уничтожения, защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. |
| Событие ИБ | Любое идентифицированное явление в системе или сети. |
| Инцидент ИБ | Нарушение или угроза нарушения ИБ компании. |
| Угроза ИБ | Потенциально возможное событие, действие (воздействие), процесс или явление, создающее опасность возникновения инцидента ИБ. |
| Уязвимость ИС | Недостаток в ИС, используя который злоумышленник может намеренно реализовать угрозу ИБ. |
| Реагирование на инцидент ИБ | Структурированная совокупность действий, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения инцидента ИБ. |
| APT-атака | Сложная, продолжительная, хорошо спланированная многоходовая атака, использующая сложное вредоносное ПО, методы социальной инженерии и данные об информационной инфраструктуре атакуемого. |
| Жизненный цикл атаки | Последовательность шагов осуществления атаки |
| SIEM – система | Система, которая обеспечивает анализ событий ИБ, исходящих от сетевых устройств и приложений, в реальном времени. |
| Индикаторы компрометации | Наблюдаемая в компьютерной сети или на одном из компьютеров сущность, наличие которой может свидетельствовать о компрометации ИС. Обычно под такими индикаторами понимают IP-адреса, URL-адреса, хеши файлов. |
| Атака типа  WATERING HOLE | Watering hole – одна из разновидностей многоуровневых  целенаправленных кибератак. Атака заключается в том, что злоумышленники заражают вредоносным ПО веб-сайты, часто посещаемые их потенциальными жертвами. Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений. |

## **Актуальность проблемы информационной безопасности**

Добро пожаловать в самый первый урок нашего курса для администраторов безопасности. В данной лекции мы рассмотрим актуальность проблемы информационной безопасности, ответим на вопросы почему нужна защита информации. Рассмотрим новый подход к обработке информации и как глобальная информатизация повлияла на работу компаний.

Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых, так называемых, информационных технологий.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

• обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование

• расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи

• повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности

• вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса

• концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях

• количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам

• отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем

• многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации

• ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации

• увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов)

• развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин.

Прежде всего — это расширение сферы применения средств вычислительной техники и возросший уровень доверия к автоматизированным системам управления и обработки информации. Компьютерным системам доверяют самую ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, управляют движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию.

Изменился подход и к самому понятию "информация". Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в рамках которой он существует. Осуществляется переход к рыночным отношениям в области создания и предоставления информационных услуг, с присущей этим отношениям конкуренцией и промышленным шпионажем.

Особую опасность для компьютерных систем представляют злоумышленники, специалисты - профессионалы в области вычислительной техники и программирования, досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией и самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты.

Трудности решения практических задач обеспечения безопасности конкретных АС связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

## **Основные понятия информационной безопасности**

Добро пожаловать во второй урок курса для администраторов безопасности. В данной лекции мы повторим основные понятия, связанные с информационной безопасностью, вспомним главные цели защиты автоматизированной системы. Понимание этого занятия влияет на успешное изучение всего курса, так что отнеситесь к нему с должным усердием.

Прежде всего необходимо разобраться, что такое безопасность информационных технологий, определить, ***что (кого), от чего (от кого), почему (зачем) и как (в какой степени и какими средствами) надо защищать.***Только получив четкие ответы на данные вопросы, можно правильно сформулировать общие требования к системе обеспечения безопасности и переходить к обсуждению вопросов построения соответствующих систем зашиты.

**Информация и информационные отношения. Субъекты информационных отношений, их безопасность**

Под *автоматизированной системой*(АС) обработки информации будем понимать организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов:

• технических средств обработки и передачи данных (средств вычислительной техники и связи)

• методов и алгоритмов обработки в виде соответствующего программного обеспечения

• информации (массивов, наборов, баз данных) на различных носителях

• обслуживающего персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Под *обработкой информации*в АС будем понимать любую совокупность операций (прием, накопление, хранение, преобразование, отображение, передача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

В дальнейшем *субъектами*будем называть:

• *государство*(в целом или отдельные его органы и организации)

• общественные или коммерческие организации (объединения) и предприятия *(юридических лиц)*

*•*отдельных граждан *(физических лиц).*

В процессе своей деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе, касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие отношения между субъектами будем называть *информационными отношениями,*а самих участвующих в них субъектов - *субъектами информационных отношений.*

Различные субъекты по отношению к определенной информации могут (возможно одновременно) выступать в качестве (в роли):

• источников (поставщиков) информации

• потребителей (пользователей) информации

• собственников, владельцев, распорядителей информации

• физических и юридических лиц, о которых собирается информация

• владельцев систем обработки информации

• участников процессов обработки и передачи информации и т.д.

Будучи заинтересованным в обеспечении требований связанных с защитой информации, субъект информационных отношений является *уязвимым,*то есть потенциально подверженным нанесению *ему ущерба*(прямого или косвенного, материального или морального) посредством воздействия на критичную для него информацию, ее носители и процессы обработки либо посредством неправомерного использования такой информации. Поэтому все субъекты информационных отношений в той или иной степени (в зависимости от размеров ущерба, который им может быть нанесен) заинтересованы в обеспечении своей информационной безопасности.

Для обеспечения законных прав и удовлетворения перечисленных выше интересов субъектов (т.е. обеспечения их информационной безопасности) необходимо постоянно поддерживать следующие свойства информации и систем ее обработки:

• *доступность информации*- такое свойство системы (инфраструктуры, средств и технологии обработки, в которой циркулирует информация), которое характеризует ее способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам (готовность к обслуживанию поступающих от субъектов) запросов всегда, когда в обращении к ним возникает необходимость;

• *целостность информации -*такое свойство информации, которое заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

• *конфиденциальность информации -*такую субъективно определяемую (приписываемую) характеристику (свойство) информации, которая указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих прав на доступ к ней.

В качестве *объектов, подлежащих защите*в целях обеспечения безопасности субъектов информационных отношений, должны рассматриваться: информация, любые ее носители (отдельные компоненты АС и АС в целом) и процессы обработки (передачи).

Однако, всегда следует помнить, что уязвимыми в конечном счете являются именно заинтересованные в обеспечении определенных свойств информации и систем ее обработки субъекты (информация, равно как и средства ее обработки, не имеют своих интересов, которые можно было бы ущемить). Поэтому, говоря об обеспечении безопасности АС или циркулирующей в системе информации, всегда следует понимать под этим косвенное обеспечение безопасности соответствующих субъектов, участвующих в процессах автоматизированного информационного взаимодействия.

Следовательно, термин *«безопасность информации»*нужно понимать как *защищенность*информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения или утраты (нарушения целостности, фальсификации) или снижения степени доступности информации, а также незаконного ее тиражирования (неправомерного использования).

Поэтому под *«безопасностью автоматизированной системы»*(системы обработки информации, компьютерной системы) следует понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных, пользователей и персонала) от разного рода нежелательных для соответствующих субъектов воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

**Цель защиты АС и циркулирующей в ней информации**

При рассмотрении проблемы обеспечения компьютерной, информационной безопасности следует всегда исходить из того, что защита информации и вычислительной системы ее обработки не является самоцелью.

*Конечной целью создания системы компьютерной безопасности АС*является защита всех категорий субъектов, прямо или косвенно участвующих в процессах информационного взаимодействия, от нанесения им ощутимого материального, морального или иного ущерба в результате случайных или преднамеренных нежелательных воздействий на информацию и системы ее обработки и передачи.

В качестве защищаемых объектов должны рассматриваться информация, все ее носители (отдельные компоненты и автоматизированная система обработки информации в целом) и процессы обработки.

*Целью защиты, циркулирующей в АС информации*является предотвращение разглашения (утечки), искажения (модификации), утраты, блокирования (снижения степени доступности) или незаконного тиражирования информации.

Обеспечение безопасности вычислительной системы предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также для попыток хищения, модификации, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов системы: оборудования, программного обеспечения, данных (информации) и ее персонала.

В этом смысле защита информации от несанкционированного доступа (НСД) является только частью общей проблемы обеспечения безопасности компьютерных систем и защиты законных интересов субъектов информационных отношений, а сам термин НСД было бы правильнее трактовать не как "несанкционированный доступ" (к информации), а шире, - как "несанкционированные (неправомерные) действия", наносящие ущерб субъектам информационных отношений.

## **Правовые основы обеспечения информационной безопасности. Государственная система защиты информации**

Здравствуйте, в нашей третьей лекции курса для администратора мы изучим правовые основные некоторых сфер информационной безопасности, например положение о государственной системы защиты информации и юридическое основание электронных подписей. Все очевидным становится то, что современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных.

Федеральные законы и другие нормативные акты предусматривают:

• разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется на:

* отнесенную к государственной тайне
* отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн)
* и другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

• правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:

* + в отношении сведений, отнесенных к государственной тайне, -уполномоченными государственными органами на основании Закона Российской Федерации "О государственной тайне" (от 21.07.93 г. N 5485-1);
  + в отношении конфиденциальной документированной информации -собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации "Об информации, информационных технологиях и защите информации" (от 27.07.06 г. N 149-ФЗ);
  + в отношении персональных данных - отдельным федеральным законом;
  + лицензирование деятельности предприятий, учреждений и организаций в области защиты информации;
  + аттестацию автоматизированных и информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);
  + сертификацию средств защиты информации и средств контроля эффективности защиты, используемых в АС и ИС;
  + возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;
  + создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;
  + определение прав и обязанностей субъектов в области защиты информации.

### **Государственная система защиты информации**

Структура и основные функции государственной системы защиты информации от ее утечки по техническим каналам и организация работ по защите информации определены в *«Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам",*утвержденном Постановлением Правительства от 15 сентября 1993 г. № 912-51.

Этим Положением предусматривается, что мероприятия по защите информации, обрабатываемой техническими средствами, являются составной частью управленческой, научной и производственной деятельности учреждений и предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению установленного федеральными законами *"Об информации, информатизации и защите информации"*и *"О государственной тайне"*комплекса мер по защите сведений, составляющих государственную и служебную тайну.

Основные задачи государственной системы защиты информации:

• проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

• исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных специальных программно-технических воздействий на информацию с целью ее разрушения, уничтожения, искажения или блокирования в процессе обработки, передачи и хранения;

• принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;

• общая организация сил, создание средств защиты информации и средств контроля эффективности ее защиты;

• контроль за проведением работ по защите информации в органах государственного управления, объединениях, на предприятиях, в организациях и учреждениях (независимо от форм собственности).

### **Юридическая значимость ЭП**

За последние годы достигнут существенный прогресс в развитии методов решения задачи дискретного логарифмирования, что послужило причиной разработки государственного стандарта ЭП. Новый стандарт основан на математическом аппарате эллиптических кривых. Внедрение схемы ЭП на базе данного стандарта повышает, по сравнению с действующей схемой, уровень защищенности передаваемых сообщений от подделок и искажений.

ГОСТ 34.10-2018 (полное название: «ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи») — действующий межгосударственный криптографический стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Стандарт использует схему формирования электронной цифровой подписи. Новые стандарты с 2012 года отличается наличием дополнительного варианта параметров схем, соответствующего длине секретного ключа порядка 512 бит.

После подписывания сообщения *М* к нему дописывается цифровая подпись размером 512 или 1024 бит, и текстовое поле. В текстовом поле могут содержаться, например, дата и время отправки или различные данные об отправителе:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | Сообщение М | | + | |  |  | | --- | --- | | Цифровая подпись | Текст | |
|  |  | Дополнение |

Данный алгоритм не описывает механизм генерации параметров, необходимых для формирования подписи, а только определяет, каким образом на основании таких параметров получить цифровую подпись. Механизм генерации параметров определяется на месте в зависимости от разрабатываемой системы.

Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-Ф определяет основные понятия, связанные с ЭП следующим образом:

Для целей настоящего Федерального закона используются следующие основные понятия:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию;

2) сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Примечание автора:

С 01.07.2020 в п. 3 ст. 2 вносятся изменения ([ФЗ](http://www.consultant.ru/document/cons_doc_LAW_341757/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100011) от 27.12.2019 N 476-ФЗ).

3) квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

(п. 3 в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_191492/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100011) от 30.12.2015 N 445-ФЗ)

(см. текст в предыдущей редакции)

4) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_191492/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100013) от 30.12.2015 N 445-ФЗ)

(см. текст в предыдущей редакции)

Примечание автора:

С 01.07.2020 в п. 8 ст. 2 вносятся изменения ([ФЗ](http://www.consultant.ru/document/cons_doc_LAW_341757/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100012) от 27.12.2019 N 476-ФЗ).

8) аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

Примечание автора:

С 01.07.2020 ст. 2 дополняется п. 8.1 ([ФЗ](http://www.consultant.ru/document/cons_doc_LAW_341757/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100013) от 27.12.2019 N 476-ФЗ).

9) средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

Примечание автора:

С 01.07.2020 в п. 11 ст. 2 вносятся изменения ([ФЗ](http://www.consultant.ru/document/cons_doc_LAW_341757/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100015) от 27.12.2019 N 476-ФЗ).

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

12) корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

Примечание автора:

С 01.07.2020 в п. 14 ст. 2 вносятся изменения ([ФЗ](http://www.consultant.ru/document/cons_doc_LAW_341757/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100016) от 27.12.2019 N 476-ФЗ).

14) вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра, изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

(п. 14 введен Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_191492/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100014) от 30.12.2015 N 445-ФЗ)

15) подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

(п. 15 введен Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_191492/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100016) от 30.12.2015 N 445-ФЗ)

#### **Виды электронных подписей**

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

2. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3. Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

4. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_191492/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100017) от 30.12.2015 N 445-ФЗ)

(см. текст в предыдущей редакции)

5. При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

#### **Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью**

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_191492/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100018) от 30.12.2015 N 445-ФЗ)

(см. текст в предыдущей редакции)

Примечание автора:

С 01.07.2020 в ч. 2 ст. 6 вносятся изменения ([ФЗ](http://www.consultant.ru/document/cons_doc_LAW_341757/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100022) от 27.12.2019 N 476-ФЗ).

2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям [статьи 9](http://www.consultant.ru/document/cons_doc_LAW_220806/051b5d07ff06df5b020f6414689eda4bf3119b7f/#dst100073) настоящего Федерального закона.

3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

3.1. Если федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами предусмотрено, что документ должен подписываться несколькими лицами, электронный документ должен быть подписан лицами (уполномоченными должностными лицами органа, организации), изготовившими этот документ, тем видом подписи, который установлен законодательством Российской Федерации для подписания изготовленного электронного документа электронной подписью.

(часть 3.1 введена Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_200008/bdb2754392763f4c0afbdb3bc7ea77ef6a5287c4/#dst100159) от 23.06.2016 N 220-ФЗ)

4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов. Исключение составляют случаи, когда в состав пакета электронных документов лицом, подписавшим пакет, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные ими тем видом электронной подписи, который установлен законодательством Российской Федерации для подписания таких документов. В этих случаях электронный документ, входящий в пакет, считается подписанным лицом, первоначально создавшим такой электронный документ, тем видом электронной подписи, которым этот документ был подписан при создании, вне зависимости от того, каким видом электронной подписи подписан пакет электронных документов.

Организационные и технические меры, и основные принципы обеспечения информационной безопасности  
Здравствуйте, мы переходим к заключительному уроку в первой главе нашего курса. Здесь мы обсудим основные принципы по обеспечению защиты информации и какие виды мер противодействия угрозам безопасности существуют. А также целью рассмотрения данной темы является обзор видов известных мер противодействия угрозам безопасности АС (контрмер), а также основных принципов построения систем защиты информации.

**Виды мер противодействия угрозам безопасности**

* По способам осуществления все меры защиты информации, ее носителей и систем ее обработки подразделяются на:
* правовые (законодательные);
* морально-этические;
* технологические;
* организационные (административные и процедурные);
* физические;
* технические (аппаратурные и программные).

**Правовые (законодательные)**

К правовым мерам защиты относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

**Морально-этические**

К морально-этическим мерам защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако, их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т.п.) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АС.

**Технологические**

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии разрешений от нескольких должностных лиц, процедур проверки соответствия реквизитов исходящих и входящих сообщении в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т.п.

**Организационные**

Организационные меры зашиты - это меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

**Меры физической защиты**

Физические меры защиты основаны на применении разного рода механических, электро-или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т.п.).

**Технические**

Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Взаимосвязь рассмотренных выше мер обеспечения безопасности приведена на рисунке 1.6.1.

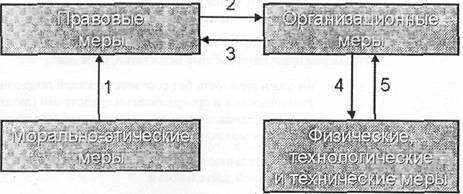


Рис. 1.6.1 Взаимосвязь мер обеспечения информационной безопасности

1. Нормативные и организационно-распорядительные документы составляются с учетом и на основе существующих норм морали и этики.
2. Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации
3. Воплощение организационных мер требует разработки соответствующих нормативных и организационно-распорядительных документов
4. Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами
5. Применение и использование технических средств защиты требует соответствующей организационной поддержки.

## **ТЕСТ ПО 1 ГЛАВЕ**

Правильный ответ помечен\*

Выбери правильный ответ

**Что означает термин №Правовые меры защиты информации»?**

* Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения. \*
* Это традиционно слоившиеся в стране или обществе нормы поведения и правила обращения с информацией.
* Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.

Выбери правильный ответ

**Что означает термин «Морально-этические меры защиты информации»?**

* Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.\*
* Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
* Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

Выбери правильный ответ

**Что означает термин «Организационные меры по защите информации»?**

* Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а так же порядок взаимодействия пользователей с системой.\*
* Это действующие в стране законы, указы и другие нормативные акты.
* Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.

Выбери правильный ответ

**Что означает термин «Физические меры защиты информации»?**

* Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.\*
* Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
* Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

Выбери правильный ответ

**Что означает термин Аутентификация?**

* Это проверка подлинности объекта или субъекта\*
* Это проверка целостности информации, программы, документа
* Это присвоение имени субъекту или объекту

Выбери правильный ответ

**Что означает термин Верификация?**

* Это проверка целостности информации, программы, документа.\*
* Это проверка подлинности субъекта или объекта.
* Это присвоение имени субъекту или объекту.

Выбери правильный ответ

**Что означает термин Идентификация?**

* Это присвоение имени субъекту или объекту.\*
* Это проверка подлинности субъекта или объекта.
* Это проверка целостности информации, программы, документа.

Выбери правильный ответ

**Что означает термин Криптография?**

* Это метод специального преобразования информации с целью сокрытия от посторонних лиц\*
* Это преобразование информации в виде условных сигналов с целью автоматизации её хранения, обработки, передачи и ввода-вывода
* Это преобразование информации при её передаче по каналам связи от одного элемента вычислительной сети к другому

Выберите несколько из 5 вариантов ответа

**К аспектам ИБ относятся:**

1) дискретность

2) целостность\*

3) конфиденциальность\*

4) актуальность

5) доступность\*

Выберите один из 5 вариантов ответа:

**Что такое несанкционированный доступ (НСД)?**

* Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа\*
* Создание резервных копий в организации
* Правила и положения, выработанные в организации для обхода парольной защиты
* Вход в систему без согласования с руководителем организации
* Удаление не нужной информации

Выберите один из 4 вариантов ответа:

**Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется**

* кодируемой
* шифруемой
* недостоверной
* защищаемой\*

Выберите несколько из 4 вариантов ответа:

**К видам защиты информации относятся:**

* правовые и законодательные:\*
* морально-этические;\*
* юридические;
* административно-организационные;\*

Выберите несколько из 5 вариантов ответа:

**К методам защиты от НСД относятся**

* разделение доступа;\*
* разграничение доступа;\*
* увеличение доступа;
* ограничение доступа.\*
* аутентификация и идентификация\*

**Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …**

* **с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды\***
* с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
* способна противостоять только информационным угрозам, как внешним так и внутренним способна противостоять только внешним информационным угрозам

# Глава 2: Средства Защиты Информации

Добро пожаловать во вторую главу нашего обучающего курса. Если вы это читаете, значит вы успешно справились с вводной главой, освежили свои знания в области защиты информации и готовы изучать новые темы, которые помогут вам в будущем более оптимально затрачивать все ресурсы автоматизированной системы, а также молниеносно реагировать в критических ситуациях. В данной главе мы коснемся основные средства защиты информации, с которыми администраторы безопасности сталкиваются чаще всего.

Сегодня вопросы обеспечения информационной безопасности являются предметом пристального внимания, поскольку внедряемые повсеместно технологии без обеспечения информационной безопасности становятся источником новых серьезных проблем. О серьезности ситуации сообщает ФСБ России: сумма ущерба, нанесенная злоумышленниками за несколько лет по всему миру, составила от $300 млрд до $1 трлн. По сведениям, представленным Генеральным прокурором РФ, только за первое полугодие 2019 г. в России количество преступлений в сфере высоких технологий увеличилось в шесть раз, общая сумма ущерба превысила $ 18 млн. Рост целевых атак в промышленном секторе в 2019 г. отмечен по всему миру. В частности, в России прирост числа атак по отношению к 2018 г. составил 22 %. На территории Российской Федерации обладатели информации и операторы информационных систем обязаны блокировать попытки несанкционированного доступа к информации, а также осуществлять мониторинг состояния защищенности ИТ-инфраструктуры на постоянной основе. При этом защита информации обеспечивается за счет принятия различных мер, включая технические. Средства защиты информации, или СЗИ обеспечивают защиту информации в информационных системах, по сути представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Для современных информационных систем характерно использование различных аппаратно-программных платформ, территориальная распределенность компонентов, а также взаимодействие с открытыми сетями передачи данных.

Как защитить информацию в таких условиях? Соответствующие требования предъявляют уполномоченные органы, в частности, ФСТЭК и ФСБ России. В рамках главы постараемся отразить основные подходы к классификации СЗИ с учетом требований указанных регуляторов. Иные способы описания классификации СЗИ, отраженные в нормативных документах российских ведомств. Глава может быть полезна начинающим специалистам в области информационной безопасности в качестве источника структурированной информации о способах классификации СЗИ на основании требований ФСТЭК России (в большей степени) и, кратко, ФСБ России.

Структурой, определяющей порядок и координирующей действия обеспечения не криптографическими методами ИБ, является ФСТЭК России (ранее — Государственная техническая комиссия при Президенте Российской Федерации, Гостехкомиссия). Если читателю приходилось видеть Государственный реестр сертифицированных средств защиты информации, который формирует ФСТЭК России, то он безусловно обращал внимание на наличие в описательной части предназначения СЗИ таких фраз, как «класс РД СВТ», «уровень отсутствия НДВ» и пр.

Рисунок 1. Фрагмент реестра сертифицированных СЗИ



Аналогичный перечень сертифицированных СЗИ поддерживает и ФСБ России в рамках своей компетенции. В нем фигурируют такие понятия, как «антивирусные средства класса Б2», «средства обнаружения атак класса Б» и пр. Далее постараемся разобраться в терминах, основываясь в первую очередь на нормативных актах отечественных регуляторов сферы информационной безопасности.

Проникая в систему, злоумышленник преодолевает выстроенную систему защиты информации, осуществляет несанкционированный доступ. НСД. ФСТЭК России под системой защиты информации от НСД понимает совокупность мер организационного характера и программно-технических СЗИ от НСД. Функциональность СЗИ от НСД должна предотвращать или существенно затруднять несанкционированное проникновение в обход правил разграничения доступа, реализованных штатными средствами. Эти средства входят в состав средств вычислительной техники и автоматизированных систем в виде совокупности программного и технического обеспечения. При этом, регулятор полагает, что средства вычислительной техники являются элементами, из которых строятся автоматизированные системы. Поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. Совокупность требований в части защиты СВТ и АС образуют т. н. класс защищенности. В качестве СЗИ регулятором рассматриваются т.н. межсетевые экраны — средства, реализующее контроль за информацией, направленной в АС или исходящей из нее. Межсетевые экраны выполняют фильтрацию информации по заданным критериям. К СЗИ также относят т.н. средства обнаружения вторжений. Они представляют собой средства, автоматизирующие процесс контроля событий в системе (сети) с проведением анализа этих событий с целью поисках признаков инцидента ИБ. Антивирусные СЗИ должны выявлять и соответствующим образом реагировать на средства несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации СЗИ. В рамках реализации мер по управлению доступом предусмотрено обеспечение так называемой доверенной загрузки. Для этого применяются также соответствующие СЗИ. Меры по защите машинных носителей информации в части обеспечения контроля за их использованием реализуются с помощью средств контроля съемных носителей. Далее мы разберем все эти средства более подробно.

## **Межсетевые экраны**

Здравствуйте, вы открыли первый урок второй главы «Средства защиты информации», посвященный межсетевому экранированию. Данная мера одна из важнейших в организации защиты автоматизированной системы.

Межсетевые экраны (МЭ) обеспечивают безопасность при осуществлении электронного обмена информацией с другими взаимодействующими автоматизированными системами и внешними сетями, разграничение доступа между сегментами корпоративной сети, а также защиту от проникновения и вмешательства в работу АС нарушителей из внешних систем.

Согласно Руководящему документу ФСТЭК при Президенте РФ «межсетевым экраном называется локальное (однокомпонентное) или функционально-распределённое средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т.е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе». Однако такое определение имеет общий характер и подразумевает слишком расширенное толкование.

**Основные сведения**

Межсетевой экран (МЭ) — это специализированное программное или аппаратное (или программно-аппаратное) средство, позволяющее разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения сетевых пакетов из одной части в другую.

МЭ, установленные в точках соединения с сетью Интернет, обеспечивают защиту внешнего периметра сети предприятия и защиту собственных Internet серверов, открытых для общего пользования, от несанкционированного доступа.

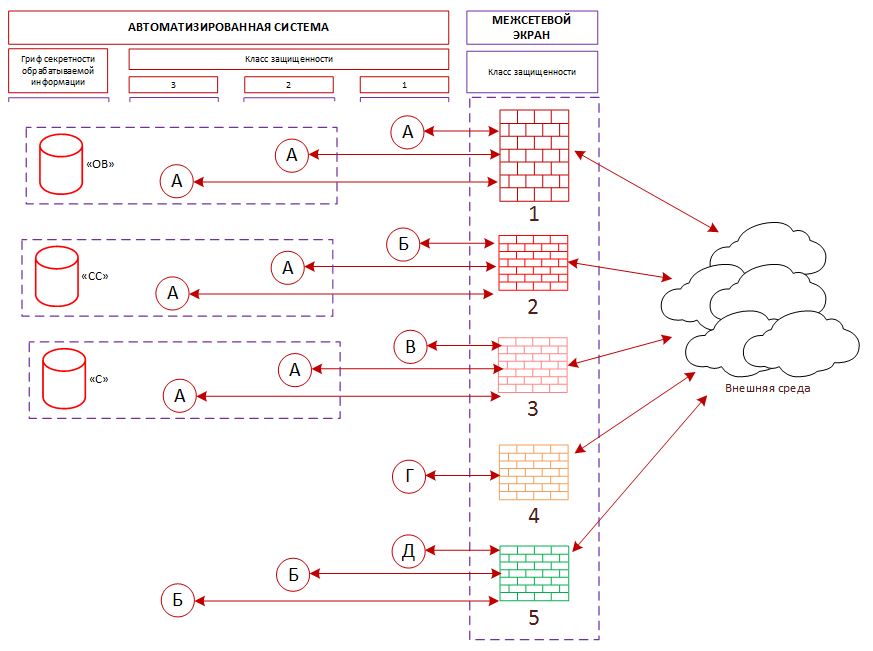
Механизмы защиты, реализуемые МЭ:

* Фильтрация сетевого трафика
* Шифрование (создание VPN)
* Трансляция адресов
* Аутентификация (дополнительная)
* Противодействие некоторым сетевым атакам (наиболее  
  распространённым)
* Управление списками доступа на маршрутизаторах (необязательно)

Основная функция МЭ - фильтрация сетевого трафика Она может осуществляться на любом уровне модели OSI. В качестве критериев может выступать информация с разных уровней: адреса отправителя/получателя, номера портов, содержимое поля данных.

В основе классификации заложено деление по уровням контроля межсетевых информационных потоков (рисунок 5).

Рисунок 5. Классы защищенности межсетевых экранов



Самый высокий — 1-й класс. Он применим, когда требуется обеспечить безопасное взаимодействие автоматизированных систем класса 1А с внешней средой. Если в автоматизированных системах классов 3А, 2А обрабатывается информация с грифом «особой важности», то требуется использовать межсетевой экран не ниже 1 класса. Для защиты взаимодействия с внешним миром систем класса 1Б предназначены межсетевые экраны 2 класса. Если в системах классов 3А, 2А обрабатывается информация с грифом «совершенно секретно», необходимо использовать межсетевые экраны не ниже указанного класса. Защита взаимодействия систем класса 1В обеспечивается межсетевыми экранами 3 класса. Если в автоматизированных системах классов 3А, 2А происходит обработка информации с грифом «секретно», потребуется межсетевой экран не ниже 3 класса. Межсетевые экраны 4 класса требуются в случае защиты взаимодействия автоматизированных систем класса 1Г с внешней средой. Взаимодействие систем класса 1Д должны обеспечивать межсетевые экраны 5 класса. Также требуется использовать их не ниже указанного класса для автоматизированных систем класса 3Б и 2Б. Классы защиты межсетевых экранов В 2016 г. введена шестиуровневая классификация межсетевых экранов (рисунок 6).

Рисунок 6. Классификация межсетевых экранов по классам защиты



По такому подходу, в информационных системах защита информации, содержащей сведения, отнесенные к государственной тайне, должна обеспечиваться с помощью межсетевых экранов 3, 2 и 1 классов защиты. Что касается остальных случаев, то в государственных информационных системах (ГИС) 1, 2, 3 и 4 классов защиты должны использоваться межсетевые экраны 4, 5 и 6 классов соответственно. Аналогичная ситуация в отношении автоматизированных систем управления производственными и технологическими процессами (далее — АСУ). Для обеспечения 1 и 2 уровней защищенности персональных данных в информационных системах персональных данных (ИСПДн) потребуется устанавливать межсетевые экраны 4 и 5 классов соответственно. Если же требуется обеспечить 3 или 4 уровень защищенности персональных данных, то достаточно 6 класса защиты. Регулятор также определил необходимость использования межсетевых экранов 4 класса для защиты информации в информационных системах общего пользования II класса. Типы межсетевых экранов ФСТЭК выделяет межсетевые экраны уровня: сети (тип «А»); логических границ сети (тип «Б»); узла (тип «В»); веб-сервера (тип «Г»); промышленной сети (тип «Д»). Межсетевые экраны типа «А» реализуется только в программно-техническом исполнении. «Б», «Г» и «Д» могут быть как в виде программного продукта, так и в ПТИ. Исключительно в виде программного продукта реализуется межсетевые экраны типа «В». Межсетевые экраны типа «А» устанавливают на физическом периметре информационных систем. Если в них есть несколько физических сегментов, то такой межсетевой экран может устанавливаться между ними (рисунок 7).

Рисунок 7. Пример размещения межсетевых экранов типа «А»



Межсетевые экраны типа «Б» устанавливаются на логической границе информационных систем. Если в них выделяются логические сегменты, то между ними также может быть установлен межсетевой экран данного типа (рисунок 8).

Рисунок 8. Пример размещения межсетевого экрана класса «Б»



Для размещения на мобильных или стационарных узлах информационных систем предназначены межсетевые экраны типа «В». Разбор http(s)-трафика между веб-сервером и клиентом осуществляют межсетевые экраны типа «Г». Они устанавливаются на сервере, обслуживающем веб-сайты (службы, приложения). Возможна установка на физической границе сегмента таких серверов. С промышленными протоколами передачи данных работают межсетевые экраны типа «Д». Именно они устанавливаются в АСУ.

## **Средства анализа защищенности**

Добро пожаловать во вторую лекцию по средствам защиты информации. В данном уроке мы расскажем вам о средствах анализа защищенности, как они влияют на уровень защиты автоматизированной системы и как они помогают в аналитике защищённости АС.

Анализ защищенности — это процесс проверки инфраструктуры организации на наличие возможных уязвимостей сетевого периметра, виртуальной инфраструктуры, вызванных в том числе ошибками конфигурации, а также программного обеспечения и исходного кода приложений. Другими словами, при анализе защищенности проверяется безопасность различных информационных систем, как внутренних, так и внешних. Анализ защищенности проводится с целью определения незакрытых уязвимостей в инфраструктуре и поиска слабых мест, которые могут быть использованы злоумышленниками для получения доступа во внутреннюю сеть организации из интернета. Одной из причин такой проверки могут служить требования регуляторов (например, ФСТЭК России) по проведению анализа защищенности государственных информационных систем и систем персональных данных. Такой анализ должен быть проведен на момент формирования требований к защищенности инфраструктуры и выполняться периодически уже после проведения мероприятий по защите и использования сертифицированных средств защиты.  Для анализа защищенности чаще всего используются сканеры защищенности, а также проводятся тесты на проникновение с привлечением сторонних специалистов. Результатом работы сканеров защищенности являются подробные отчеты с описаниями найденных уязвимостей и возможных путей их устранения, что позволяет повысить уровень защищенности инфраструктуры организации. В то же время использование сканера защищенности предоставляет следующие преимущества: Определение возможных действий злоумышленников при их намерении осуществления несанкционированного доступа во внутреннюю сеть компании. Получение экспертной оценки эффективности применяемых мер по защищенности инфраструктуры. Контроль качества работ, проведенных в процессе внедрения программно-аппаратных средств, а также средств защиты информации. Получение экспертной оценки рисков в созданной инфраструктуре организации. Проверка разрабатываемых приложений на наличие уязвимостей. Повышение общего уровня защищенности собственной инфраструктуры. Проведение инвентаризации в процессе сканирования и получение полного списка доступных сервисов, протоколов и возможностей для осуществления несанкционированного доступа.

При этом при проверке сканеры защищенности способны выявлять уязвимости следующих объектов: Сетевого периметра и внутренних сетевые корпоративных ресурсов. Беспроводной инфраструктуры. Программного обеспечения. Интернет-приложений и веб-сайтов. Технологических сетей предприятия и АСУ ТП.

Сканеры защищенности могут работать в двух режимах: Режим статического сканирования. Позволяет проводить пассивный анализ инфраструктуры. В данном случае проверка на наличие уязвимостей происходит по косвенным признакам — проверяются заголовки портов, обнаруженные на сетевых устройствах, после чего сравниваются с базой данных уязвимостей. В случае совпадения сканер защищенности сигнализирует о найденной уязвимости. Режим динамического сканирования. Позволяет проводить активный анализ инфраструктуры. При таком режиме работы сканер уязвимостей действует как злоумышленник и имитирует атаки, проверяя реакцию системы. Исходя из возможностей этого режима, он является более медленным, однако считается более точным при выявлении уязвимостей.

Принцип работы сканеров уязвимостей заключается в последовательном прохождении следующих шагов: 1. Сбор данных об инфраструктуре. 2. Поиск потенциальных уязвимостей методом сканирования. 3. Подтверждение найденных уязвимостей динамическими методами. 4. Создание отчетов на основе результатов анализа. 5. Автоматические исправление найденных уязвимостей (при наличии данной функциональности у выбранного сканера защищенности).

## **Средства обнаружения атак**

Здравствуйте, стремительно мы переходим к 3 уроку в нашей главе о СЗИ. Сегодня мы изучим работу средств обнаружения атак, проанализируем их вклад в защищенность автоматизированной системы и узнаем о том, как работает архитектура системы обнаружения атак.

В последнее время сообщения о проникновении в корпоративные сети и атаках на Web, FTP, почтовые и другие сервера появляются с ужасающей частотой. Злоумышленники преодолевают установленные в организациях защитные средства (системы аутентификации, межсетевые экраны и т.д.), установленные для разграничения доступа к ресурсам корпоративной сети. С ростом квалификации злоумышленники становятся более изощренными в разработке и применении методов проникновения за защитную преграду. Обнаружить таких злоумышленников очень трудно. Они маскируются под авторизованных пользователей, используют промежуточные узлы для сокрытия своего истинного адреса, осуществляют атаки, распределенные во времени (в течение нескольких часов) и пространстве (одновременно с нескольких узлов) и т.д. Многие атаки осуществляются за очень короткое время (минуты и даже секунды), что также не позволяет обнаружить и предотвратить их стандартными защитными средствами. Необходимы динамические методы, позволяющие обнаруживать, оперативно реагировать и предотвращать нарушения безопасности.

Одной из технологий, которая может быть применена для обнаружения нарушений, является технология обнаружения атак (intrusion detection).

Средства обнаружения атак (Intrusion Detection Tools) в сетях предназначены для осуществления оперативного (в реальном времени) контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирования при обнаружении признаков атак (нападений на узлы и устройства корпоративной сети).

Архитектура систем обнаружения атак

Система обнаружения атак должна фиксировать попытки нарушения безопасности. Очевидно, она должна иметь распределённую архитектуру. Обычно в состав системы обнаружения атак входят два типа компонентов:

Модули слежения (сенсоры, датчики, детекторы) - программы, занимающиеся сбором данных.

Управляющие модули (консоли, менеджеры) - программы, отвечающие за обработку собранных сведений и конфигурирование модулей слежения.

Кроме того, в состав системы могут входить и другие вспомогательные компоненты (СУБД для хранения различных данных, связанных с работой системы и т. п.).

Классификация средств защиты систем обнаружения вторжений С 2011 г. используется шестиуровневая классификация систем обнаружения вторжений (рисунок 9).

Рисунок 9. Классы защиты систем обнаружения вторжений



По этому подходу, защита информационных систем, в которых обрабатывается информация, содержащая сведения, отнесенные к государственной тайне, обеспечивается средствами обнаружения вторжений 3, 2 и 1 классов защиты. В ИСПДн для обеспечения 3 и 4 уровней защищенности персональных данных устанавливаются системы обнаружения вторжений 6 и 5 класса. Обеспечение 1 и 2 уровней защищенности персональных данных обеспечивается применением систем 4 и 5 классов защиты соответственно. Защиту государственных систем при отсутствии сведений, составляющих государственную тайну, обеспечивают системы обнаружения вторжений 4 класса защиты. В случае информационных систем общего пользования II класса надлежит применять системы обнаружения вторжений 4 класса.

Типы систем обнаружения вторжений Требования к функциям систем обнаружения вторжений отражены в разработанных ФСТЭК России профилях защиты. В спецификации профилей защиты выделяют системы обнаружения вторжений уровней сети и узла. Система уровня сети подключается к коммуникационному оборудованию (например, коммутатору) и контролирует сетевой трафик, наблюдая за несколькими сетевыми узлами. Система уровня узла устанавливается на узел и проводит анализ системных вызовов, журналов работы приложений и прочих источников узла.

## **Средства доверенной загрузки**

Добро пожаловать, в 4 урок третьей главы нашего обучающего курса для администраторов безопасности. В данной лекции вы узнаете о средствах доверенной загрузки, повторите свои знания в области их работы. А также изучите классы средств доверенной загрузки.

Средства или модули доверенной загрузки (МДЗ, СДЗ) — это программные или программно-аппаратные средства, позволяющие осуществлять запуск операционной системы исключительно с доверенных носителей информации (например, жестких дисков). При этом такие устройства могут производить контроль целостности программного обеспечения (системные файлы и каталоги операционной системы) и технических параметров (сравнивать конфигурации компьютера при запуске с теми, которые были предопределены администратором при инициализации), и выступать в роли средств идентификации и аутентификации (с применением паролей и токенов). Средства доверенной загрузки позволяют решать такие проблемы, как:

- Запуск операционной системы в обход жесткого диска.

Если злоумышленник не знает учетных данных легитимных сотрудников, но имеет физический доступ к пользовательскому компьютеру или серверу, он может загрузить операционную систему с заранее подготовленного флеш-накопителя и тем самым получить доступ к хранящейся на жестком диске информации. Однако одной из возможностей средств доверенной загрузки является наличие механизма сторожевого таймера. Так как для загрузки операционной системы с внешнего носителя необходимо зайти в BIOS (или базовую систему ввода вывода) компьютера и вручную выбрать средство для загрузки, на это может уйти достаточно много времени. Если выставить перезапуск компьютера, в случае, когда операционная система загружается дольше обычного, злоумышленник не успеет изменить настройки BIOS и загрузиться со своего устройства.

- Кража учетных данных пользователей. Даже если злоумышленник узнает логин и пароль сотрудника для входа в систему, его сдержит отсутствие персонального идентификатора. Для того чтобы загрузить операционную систему, когда на компьютере установлен модуль доверенной загрузки, пользователю необходимо прикладывать персональный идентификатор или токен. Без него загрузка осуществляться не будет.

- Соответствие требованиям регуляторов. Для государственных информационных систем и систем, в которых обрабатываются персональные данные, требуется проходить аттестацию на соответствие требованиям. В требования включена обязательная защита информационных систем средствами защиты от несанкционированного доступа. При необходимости более высокого уровня защищенности хранящихся в системе данных в мерах обеспечения безопасности предписано применение аппаратных средств доверенной загрузки.

Средства доверенной загрузки могут быть:

* Программно-аппаратные модули доверенной загрузки уровня платы расширения. Такие устройства встраиваются в корпус компьютера, подключаясь к материнской плате через PCI-разъем.
* Программные. Они делятся на средства доверенной загрузки BIOS и уровня загрузочной записи. Первые встраиваются в BIOS, что позволяет выполнять свои функции до загрузки операционной системы. Другие заменяют загрузочную запись на жестком диске и действуют до того, как управление перешло на уровень операционной системы

Классы защиты средств доверенной загрузки С 2013 г. введена 6-уровневая классификация средств доверенной загрузки.

При организации защиты ГИС 3 класса защищенности рассматривают случаи наличия доступа к сетям международного обмена и его отсутствия. При наличии взаимодействия должны средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса. В информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса. В информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса.

Типы средств доверенной загрузки Регулятор выделил средства доверенной загрузки уровней:

* базовой системы ввода-вывода;
* платы расширения;
* загрузочной записи.

Требования к усилению УПД.17:

1) в ИСПДн должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения;

2) в ИСПДн должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения, реализованные на основе программно-аппаратного модуля;

3) в ИСПДн должна осуществляться доверенная загрузка программного обеспечения телекоммуникационного оборудования;

Содержание базовой меры УПД.17:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных | | | |
| 4 | 3 | 2 | 1 |
| УПД.17 |  |  | + | + |
| Усиление УПД.17 |  |  | 1 | 2 |

**Средства контроля съёмных носителей**

Добро пожаловать в заключительный урок по третьей главе нашего обучающего курса. В данном занятии мы рассмотрим средства контроля съемных носителей, определим их значимость среди средств защиты информации. Посмотрим на изменения внесенные ФСТЭК в 2017 году, касающиеся средств контря съемных носителей и как эти перемены повлияли на сферу информационной безопасности.

Объект оценки представляет собой программное или программнотехническое средство, которое предназначено для обеспечения контроля использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации. Объект оценки должен обеспечивать нейтрализацию угроз безопасности информации, связанных с подключением к информационной системе внутренними и внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы или загрузкой в информационную систему с этих съемных машинных носителей информации вредоносного программного обеспечения. В состав средства контроля подключения съемных машинных носителей информации входят следующие компоненты:

* программное обеспечение, устанавливаемое на средствах вычислительной техники и обеспечивающее взаимодействие с подключаемыми съемными машинными носителями информации;
* программное обеспечение управления (локального и (или) централизованного) средствами контроля подключения съемных машинных носителей информации.

Классы защиты средств контроля съемных машинных носителей.

С 2014 г. введена 6-уровневая классификация средств контроля съемных машинных носителей. Она в полной мере аналогична рассмотренному выше случаю классификации средств доверенной загрузки (рисунок 10). Так же, при организации защиты ГИС 3 класса защищенности рассматривают случаи наличия доступа к сетям международного обмена и его отсутствия. При наличии взаимодействия должны применяться средства контроля носителей 4 класса защиты. Средства этого же класса должны использоваться в ГИС 1 и 2 классов защищенности. При отсутствии взаимодействия с сетями международного информационного обмена в ГИС 3 класса защищенности достаточно устанавливать средства контроля съемных носителей 5 класса.

Этот же класс рассматриваемых СЗИ достаточен в случае защиты ИСПДн, когда необходимо обеспечить 4 уровень защищенности персональных данных или 3-й — при отсутствии взаимодействия с сетями международного информационного обмена. Для обеспечения 1 и 2 уровней защищенности персональных данных, а также 3-го — при наличии указанного сетевого взаимодействия или при актуальности угроз 2 типа потребуется установка средств контроля съемных носителей 4 класса. Применение средств контроля носителей 4 класса достаточно для защиты информационных систем общего пользования II класса. Шестой класс рассматриваемых СЗИ устанавливается, если они не относятся к ГИС, ИСПДн и ИС общего пользования, а также в них отсутствует обработка информации, содержащей сведения, отнесенные к государственной тайне. Если же они «причастны» к гостайне — потребуется установка средств контроля носителей 3, 2 или 1 класса защиты.

Типы средств контроля съемных машинных носителей информации

В отношении них различают средства контроля: подключения съемных носителей информации; отчуждения (переноса) информации со съемных машинных носителей.

Приказом ФСТЭК России от 23.03.2017 №49 внесены изменения в приказ ФСТЭК России от 18.02.2013 №21 в части касающегося технических мер защиты персональных данных. Технические меры защиты персональных данных реализуются посредством применения средств реализующим функции по предотвращению несанкционированного доступа к информации с использованием съемных машинных носителей персональных данных, подключаемых к информационной системе персональных данных (ИСПДн), и (или) по предотвращению несанкционированного отчуждения (переноса) персональных данных с зарегистрированных (учтенных) съемных машинных носителей персональных данных (средства контроля съемных носителей), в том числе программных (программно-аппаратных), в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в ИСПДн сертифицированных по требованиям безопасности информации средств контроля съемных носителей:

* в ИСПДн 1 уровня защищенности персональных данных применяются средства контроля съемных носителей не ниже 4 класса;
* в ИСПДн 2 уровня защищенности персональных данных применяются средства контроля съемных носителей не ниже 5 класса;
* в ИСПДн 3 уровня защищенности персональных данных применяются средства контроля съемных носителей 6 класса;
* в ИСПДн 4 уровня защищенности персональных данных применяются средства контроля съемных носителей 6 класса.

Для дифференциации требований к функциям безопасности средств контроля съемных носителей установлено шесть классов защиты средств контроля съемных носителей. Самый низкий класс – шестой, самый высокий – первый.

Выделены следующие типы средств контроля съемных носителей:

* средства контроля подключения съемных машинных носителей информации;
* средства контроля отчуждения (переноса) информации со съемных машинных носителей информации.

Спецификация профилей средств контроля съемных носителей для каждого типа средства контроля съемных носителей и класса защиты средства контроля съемных носителей для обеспечения защиты персональных данных приведена в таблице.

|  |  |  |  |
| --- | --- | --- | --- |
| Класс защиты  Тип средства контроля съемных носителей | 6 | 5 | 4 |
| Средство контроля подключения съемных машинных носителей информации | ИТ.СКН.П6.ПЗ | ИТ.СКН.П5.ПЗ | ИТ.СКН.П4.ПЗ |
| Средство контроля отчуждения (переноса) информации со съемных машинных носителей информации | - | - | ИТ.СКН.Н4.ПЗ |

## 

## **Тест по 2 главе**

Правильный ответ помечен\*

Выберите один верный ответ

**К видам системы обнаружения атак относятся :**

системы, обнаружения атаки на ОС

системы, обнаружения атаки на конкретные приложения

системы, обнаружения атаки на удаленных БД

все варианты верны\*

Выберите один верный ответ

**Защита информации обеспечивается применением антивирусных средств**

да\*

нет

не всегда

Выберите пропущенное слово

**Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза**

активная

пассивная\*

Выберите один верный ответ

**Устройство, защищающее сеть от несанкционированного внешнего доступа:**

мост

шлюз

брандмауэр\*

Выберите правильный ответ

**На чем основан принцип работы антивирусных мониторов?**

* На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю\*
* На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
* На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.
* На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

Выберите правильный ответ

**Может ли межсетевой экран защитить от DoS-атаки?**

* может
* может, если он совмещён с системой обнаружения атак
* может, если он типа statefull
* может, если он производит трансляцию адресов (NAT)
* может, лишь от некоторых видов DoS-атак\*
* не может

Выберите правильный ответ

**В системе обнаружения атак вероятности ошибок первого и второго рода...**

* равны
* коррелированы\*
* составляют в сумме 1
* независимы

Выберите правильный ответ

**Какой пароль невозможно подобрать методом прямого перебора?**

* включающий прописные буквы
* включающий символы кириллицы
* включающий пробел
* включающий символы пунктуации
* никакой (то есть, любой пароль можно подобрать)\*

**Методы противодействия вредоносным программам следующие. Укажите лишнее.**

использование антивирусов

устранение уязвимостей ПО

преследование создателей и распространителей вредоносных программ

обучение пользователей

разделение полномочий (привилегий)

запрет на пересылку исполняемых файлов по электронной почте

запрет на доступ в Интернет\*

резервирование данных

Выберите один верный ответ

**Какой класс защиты межсетевых экранов рекомендуют для защиты ГИС 3,4 класса защищенности, 3 класса АСУ ТП и 3,4 уровня ИСПДн?**

* 6\*
* 5
* 4
* 2

Заполните пробелы в предложении

**В информационных системах 1 класса защищенности применяются средства защиты информации не ниже … класса, а также средства вычислительной техники не ниже … класса.**

* 5,4
* 4,4
* 3,4
* 4,5\*

Выберите правильный ответ

**Какой класс защиты средств обнаружения вторжений должен быть использова для «ГИС, в которых обрабатывается информация ограниченного доступа, не содержащая сведения составляющие гос тайну», «ИСПДн», «ИС оющего пользования»**

* 4\*
* 3
* 5
* 6

# Глава 3: Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

Здравствуйте, поздравляем вас, вы прошли половину обучающего курса для администраторов безопасности. Теперь вас ждет самая важная глава в нашем обучении. В этой главе мы собрали для вас необходимые методические рекомендации по обеспечению защиты информации в ходе эксплуатации аттестованной информационной системы. Настоящие методические рекомендации описывают действия администратора безопасности в ходе реализации одного из мероприятий для обеспечения ЗИ, содержащейся в ИС обеспечения ЗИ в ходе эксплуатации аттестованной ИС.

Обеспечение ЗИ в ходе эксплуатации аттестованной ИС включает: управление системой ЗИ ИС, управление инцидентами ИБ, управление конфигурацией аттестованной ИС и ее системы защиты информации, контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС, обеспечение работоспособности системы ЗИ при возникновении нештатных ситуаций.

В данных методических рекомендациях вопросы, связанные с защитой информации при применении средств криптографической защиты не рассматриваются. Данный вопрос – отдельное направление исследования функций, решаемых органом криптографической защиты информации.

## **Управление(администрирование) системой защиты информации информационной системы**

Доброй пожаловать на первое занятие по обеспечению защиты информации в ходе работы с информационной системой. В данном уроке мы рассмотрим главные аспекты администрирования системы защиты информации информационной системы. Изучим технологию управления учетными записями пользователей, действия администратора в ходе управления доступом субъектов доступа к объектам доступа, а также в процессе управления СЗИ в ИС. Внимательно рассмотрим методы по информированию пользователей.

Создание системы ЗИ осуществляется с целью обеспечения надежной ЗИ ИС. Максимально эффективной ЗИ будет лишь в том случае, если созданы надежные механизмы защиты, а в процессе функционирования системы осуществляется непрерывное управление этими механизмами. В системе ЗИ ИС в ходе ее эксплуатации должно осуществляться непрерывное и оптимальное управление механизмами защиты, спроектированными на этапе разработки системы защиты ИС.

Администрирование системы ЗИ – это комплекс мероприятий, направленных на обеспечение стабильной и безопасной работы программной и аппаратной составляющей ИС. Администрирование включает в себя планирование, установку и поддержание работоспособности ИС. Задачи администрирования системы ЗИ можно разделить на две группы: методическое руководство пользователями и управление ИС.

### Действия администратора в ходе управления доступом субъектов доступа к объектам доступа

Управление учетными записями пользователей

Администратором безопасности информации должен быть определен список учетных записей пользователей. Пересмотр и, при необходимости, корректировка списка учетных записей пользователей с периодичностью не менее один раз в год. Корректировка списка учетных записей пользователей, а именно заведение, активация, блокирование и уничтожение производится администратором после оповещения администратора в письменной форме руководителями структурных подразделений об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях, после внесения соответствующих изменений в списки работников, допущенных к обработке информации в ИС для данных подразделений.

Администратор безопасности осуществляет:

1. заведение учетной записи пользователя:

* определение типа учетной записи [2 ИАФ.1];
* объединение учетных записей пользователей с равными правами на доступ к ресурсам ИС в группы, для упрощения процедуры управления доступом;
* осуществление верификации пользователя в соответствии со списком работников, допущенных к обработке информации в ИС;
* предоставление пользователям прав доступа к объектам доступа ИС;

1. блокирование учетных записей пользователей в случаях:

* временных учетных записей пользователей по окончании установленного периода времени для их использования;
* неактивных (неиспользуемых) учетных записей пользователей  
  после периода времени неиспользования [2 УПД.1];
* учетной записи пользователя, при превышении установленного числа неуспешных попыток аутентификации пользователя [2 ИАФ.4];
* учетной записи пользователя, при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены к событиям нарушения безопасности информации [2 РСБ.1];

1. уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС.

Управление устройствами

Администратором безопасности информации должен быть определен перечень типов устройств (Приложение таблица 2), используемых в ИС и подлежащих идентификации и аутентификации до начала информационного взаимодействия. Для каждого устройства должен быть определен способ идентификации (по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, МАС-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства).

Пересмотр и, при необходимости, корректировка перечня типов устройств осуществляется с периодичностью не менее один раз в год.

Поддержание правил разграничения доступа в ИС

Правила разграничения доступа реализуются на основе списков доступа или матриц доступа, которые регламентированы в ОРД. Корректировку списка или матрицы доступа осуществляет администратор при внесении изменений в список пользователей ИС.

Администратором должен быть определен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень действий, разрешенных до прохождения ими процедур идентификации и аутентификации [2 УПД.11].

При модернизации правил разграничения доступа необходимо:

1. уточнить метод управления доступом (дискреционный, ролевой, мандатный, комбинация перечисленных методов);
2. уточнить типы доступа субъектов к объектам доступа (чтение, запись, удаление, выполнение и иные операции).

При реализации удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети и необходимости внесения изменений в списки пользователей или его уточнении:

1. установить пользователей, которым необходимо предоставить возможность удаленного доступа к объектам ИС [2 УПД.2];
2. установить (уточнить) объекты доступа;
3. определить (уточнить) вид доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа).

Управление полномочиями пользователей ИС

В ходе управления доступом должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, в соответствии с их должностными обязанностями, зафиксированными в ОРД.

При необходимости изменения полномочий пользователей администратору безопасности необходимо:

1. уточнить определенные роли пользователей, администраторов и лиц, обеспечивающих функционирование ИС;
2. в соответствии с назначенной ролью присвоить пользователям минимально необходимые права и привилегии.

Доступ к объектам доступа с учетом разделения полномочий (ролей) и минимально необходимых прав и привилегий обеспечивается в соответствии с правилами разграничения доступа.

При взаимодействии с ИС сторонних организаций и необходимости внесения изменения в списки пользователей или его уточнении:

1) определить (уточнить) учетные записи, используемые для взаимодействия с внешними ИС;

2) назначить внешним пользователям ИС права доступа [2 УПД.2].

### Действия администратора в ходе управления средствами защиты информации в ИС

Управление средствами аутентификации

Администратор обязан обновлять аутентификационную информацию с периодичностью, определяемой в зависимости от класса ИС [2 ИАФ.4].

При использовании в ИС механизмов аутентификации на основе пароля и изменении характеристик пароля необходимо [2 ИАФ.4]:

* изменить минимальную сложность пароля;
* изменить минимальное количество измененных символов при создании новых паролей;
* изменить максимальное время действия;
* изменить минимальное время действия;

Администратор осуществляет блокирование и замену утерянных, скомпрометированных или поврежденных средств аутентификации.

Управление идентификаторами

Администратор безопасности в ходе управления идентификаторами:

1. формирует идентификатор, который однозначно идентифицирует пользователя или устройство;
2. присваивает идентификатор пользователю или устройству;
3. предотвращает повторное использование идентификатора пользователя и (устройства) в течение установленного периода времени [2 ИАФ.3];
4. блокирует идентификатор пользователя после установленного времени неиспользования [2 ИАФ.3].

Управление средствами антивирусной защиты

Действия администратора в ходе управления средствами антивирусной защиты:

1. проверка компонентов ИС на наличие вредоносных компьютерных программ не менее одного раза в неделю;
2. проверка при загрузке, открытии или исполнении объектов (файлов) из внешних источников во времени, близкому к реальному;
3. проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты с периодичностью не менее один раз в месяц;
4. определение и выполнение действий по реагированию на обнаружение в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

Управление средствами доверенной загрузки

В ИС должно обеспечиваться исключение НСД к программным и (или) техническим ресурсам средств вычислительной техники ИС на этапе его загрузки. Доверенная загрузка должна обеспечивать обязательную идентификацию и аутентификацию пользователей ИС до выполнения действий при загрузке ОС, что включает корректировку перечня действий, разрешенных до прохождения идентификации и аутентификации [2 УПД.11].

Управление системами обнаружения вторжений

Действия администратора по управлению системами обнаружения вторжений включают обновление базы решающих правил системы обнаружения вторжений, применяемой в ИС [2 СОВ.2].

Порядок обновления базы решающих правил:

1. получение уведомления о необходимости обновлений базы решающих правил;
2. установка обновлений базы решающих правил из доверенных источников;
3. регистрация в журнале обновлений;
4. контроль целостности обновлений базы решающих правил.

В случае редактирования базы решающих правил запись об этом событии с указанием произведенных изменений фиксируется в соответствующем журнале регистрации событий безопасности (раздел 1.4).

Управление средствами анализа защищенности

На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью не реже одного раза в три месяца.

Управление средствами контроля носителей

Действия администратора безопасности в ходе управления средствами контроля носителей:

1. учет МНИ, используемых в ИС для хранения и обработки информации и контроль их подключения:

* определение или уточнение типов машинных носителей информации;

Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации (Приложение таблица 3). Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств;

* определение или уточнение пользователей ИС, уполномоченных на подключение машинных носителей;

1. определение и поддержание в актуальном состоянии списка пользователей, уполномоченных на доступ к МНИ;
2. определение и поддержание в актуальном состоянии списка пользователей, имеющих права на перемещение МНИ за пределы КЗ;
3. периодическая проверка наличия МНИ;
4. определение типов МНИ, подлежащих хранению в хранилище машинных носителей информации;
5. проверка информации, хранящейся на съемных машинных носителях, на отсутствие вредоносного ПО;
6. контроль использования интерфейсов ввода (вывода):

* определение или уточнение разрешенные для ввода (вывода) информации интерфейсы;
* определение или уточнение пользователей, уполномоченных на доступ к интерфейсам ввода (вывода);

1. контроль ввода (вывода) информации на машинные носители информации:

* определение или уточнение машинные носители информации, подлежащие контролю ввода (вывода) информации;
* определение или уточнение пользователей ИС, уполномоченных на ввод (вывод) информации на машинные носители;

1. уничтожение (стирание) информации на машинных носителях производится комиссионно с составлением акта при их передаче между пользователями, в сторонние организации для ремонта или утилизации.

Управление межсетевыми экранами

При передаче информации между устройствами, сегментами ИС администратор осуществляет:

* контроль за передачей и фильтрацией информационных потоков в соответствии с правилами управления потоками;
* запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи.

Управление информационными потоками должно обеспечивать разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИС, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

### Действия администратора по управлению компонентами ПО и регистрации, анализу событий безопасности.

Администратором безопасности в ходе управления компонентами ПО должны быть определены:

1. компоненты ПО, подлежащие установке в ИС после загрузки ОС;
2. компоненты ПО, запускаемые автоматически при загрузке ОС;
3. компоненты ПО, обновляемые автоматически при загрузке ОС.

Определённые компоненты ПО формируются в перечень компонентов, подлежащие установке в ИС после загрузки ОС (Приложение таблица 4).

Пересмотр перечней проводится с периодичностью не реже одного раза в шесть месяцев.

При установке ПО администратору необходимо:

1. скорректировать перечень компонентов ПО, подлежащих установке в ИС после загрузки ОС;
2. установить разрешенные к автоматическому запуску компоненты ПО;
3. установить разрешенные к автоматическому обновлению компоненты ПО;
4. осуществить контроль за установкой компонентов ПО в соответствие с данным перечнем;
5. применить параметров настройки компонентов, определенных в ОРД.

При установке обновлений ПО администратору необходимо:

1. осуществить проверку наличия отметок в эксплуатационной документации (формуляр или паспорт) об установке обновлений ПО;
2. осуществить проверку соответствия версий общесистемного, прикладного и специального ПО;
3. установить необходимые обновления;
4. зафиксировать сведения об обновлениях в соответствующем журнале.

Контроль установки обновлений проводится еженедельно. В ИС регистрации подлежат события безопасности, определенные в перечне событий безопасности (Приложение таблица 5), фиксируемом в ОРД.

Пересмотр перечня событий безопасности, подлежащих регистрации, производится не менее чем один раз в год. Администратор должен обеспечить срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев.

Состав и содержание информации о событиях безопасности определяется в зависимости от типа события [2 РСБ.2].

Таблица 1 – Минимальный состав и содержание событий

|  |  |
| --- | --- |
| Событие | Состав |
| Регистрация входа (выхода) субъектов доступа в ИС и загрузки (останова) ОС | Дата и время входа в ИС или загрузки ОС, результат попытки входа (успешная или неуспешная), результат попытки загрузки ОС (успешная или неуспешная), идентификатор, предъявленный при попытке доступа |
| Регистрация подключения МНИ | Дата и время подключения МНИ и вывода информации на МНИ, логическое имя подключаемого МНИ, идентификатор субъекта доступа, осуществляющего вывод информации на МНИ |
| Регистрация запуска (завершения) программ и процессов | Дата и время запуска, имя (идентификатор) программы, идентификатор субъекта доступа, запросившего программу, результат запуска (успешный, неуспешный) |
| Регистрация попыток доступа программных средств к защищаемым файлам | Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа, спецификация защищаемого файла (логическое имя, тип). |
| Регистрации попыток доступа программных средств к защищаемым объектам доступа | Дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа, спецификация защищаемого объекта доступа (логическое имя (номер). |
| При регистрации попыток удаленного доступа к информационной системе | Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (используемый протокол доступа, используемый интерфейс доступа |

Возможные действия администратора при сбоях при регистрации событий безопасности (например, переполнение объема памяти):

* изменение параметров сбора, записи и хранения информации о событиях безопасности;
* отключение записи информации о событиях безопасности от части компонентов ИС;
* запись поверх устаревших хранимых записей событий безопасности.

### Методы администратора по информированию пользователей

Информирование пользователей о правилах эксплуатации ИС с учетом требований по ЗИ и проведение занятий с персоналом по работе с системой защиты ИС производится администратором безопасности в виде инструктажа.

Инструктаж проводят на рабочем месте до начала производственной деятельности со всеми новыми пользователями ИС. Повторный инструктаж проводится с целью проверки и повышения уровня знаний пользователями правил эксплуатации ИС не реже чем через шесть месяцев после проведения очередного инструктажа или в следующих случаях:

* при введении в действие новых правил эксплуатации ИС или её системы защиты;
* при замене или модернизации компонентов ИС или средств защиты ИС;
* при нарушении правил эксплуатации ИС;
* по требованию органов надзора.

В инструктаж следует включать:

* ознакомление с должностной инструкцией и правилами политики ИБ предприятия;
* ознакомление с эксплуатационной документацией на ИС;
* ознакомление с правилами эксплуатации средств защиты ИС (Например, средств идентификации и аутентификации, включая правила хранения и использования паролей и идентификаторов);
* ознакомление с обязанностями пользователей ИС;
* ознакомление с последствиями нарушения правил эксплуатации ИС и её системы защиты.

Проведение всех видов инструктажей регистрируется в соответствующих журналах проведения инструктажей (Приложение таблица 6).

## **Управление инцидентами информационной безопасности**

Здравствуйте, мы снова приветствуем вас в нашем курсе для администраторов безопасности. Сегодня мы изучим одну из основных тем обучающего материала, которая поможет вам понять последовательность действий при управлении инцидентами информационной безопасности. Расскажем вам как правильно реагировать на инциденты ИБ и посоветуем важный инструментарий для подобных ситуаций.

Работа с инцидентами в области ИБ помогает определить наиболее актуальные угрозы ИБ и создает обратную связь в системе обеспечения ИБ, что способствует повышению общего уровня защиты информационных ресурсов и ИС.

Менеджмент инцидентов ИБ должен основываться на результатах мониторинга ИБ. Примерный перечень инцидентов ИБ приведен в Приложении таблица 7.

В целях организации работы с инцидентами ИБ на предприятии разрабатывается регламент или инструкция выявления инцидентов ИБ и реагирования на них. Учет инцидентов осуществляется администратором безопасности предприятия, в соответствии с формой журнала учета инцидентов ИБ (Приложение таблица 8). Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Хранение электронных журналов регистрации и учета событий безопасности ОС, СУБД, системного и прикладного ПО, СЗИ, а также специализированных средств анализа защищенности ИС должно осуществляться в течение срока, достаточного для проведения анализа инцидента, но не менее 3 месяцев.

В срок не более трех рабочих дней с момента поступления информации об инциденте, администратор ИС определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий. Меры по устранению включают в себя технические мероприятия, обеспечивающие целостность значимых данных, а также организационные мероприятия, которые позволяют снизить ущерб и составить необходимые документы.

### Реагирование на инциденты



Подготовительный этап

Для отслеживания и ведения статистики инцидентов ИБ администратору необходимо:

* выработать процедуру реагирования на инциденты ИБ;
* выбрать средство накопления и хранения экспертной информации и отчётов о произошедших ранее инцидентах ИБ;
* регулярно повышать свою квалификацию на различных тренингах и семинарах, следить за последними тенденциями ИБ и быть в курсе новейших программных и аппаратных решений в области ИБ, а также отслеживать появляющиеся новые типы угроз и сценарии атак.

Этап обнаружения инцидентов

Для обнаружения инцидентов ИБ администратору необходимо:

1. определить события ИБ, свидетельствующие о возможном инциденте ИБ.

К источникам событий ИБ относятся Anti-APT-системы, сетевые ловушки, системы обнаружения вторжений и многие другие решения для обеспечения ИБ. В рамках данного руководства область источников событий сужена до SIEM-систем и систем централизованного управления антивирусами.

Соответственно триггерами для начала реагирования на инцидент будут следующие события:

а) событие в SIEM, возникающее в результате сопоставления событий от устройств обеспечения ИБ с потоками данных об угрозах. Такое событие свидетельствует о наличии в исходном событии от устройства обеспечения ИБ (например, прокси-сервера) одного из индикаторов, содержащихся в потоках данных об угрозах.

б) некоторые срабатывания антивируса на компьютере (информация о срабатывании отображается в центре управления антивирусами). Не всякое срабатывание антивируса должно инициировать процесс реагирования на инциденты. Требующими расследования можно считать следующие срабатывания:

* обнаружение взаимодействия с сервером управления;
* безуспешное лечение зараженных объектов;
* неоднократное заражение одного и того же компьютера;
* ошибки в работе антивируса, которые приводят к снижению уровня защищённости.

Эти триггеры почти всегда свидетельствуют о наличии инцидента ИБ. О наличии инцидента так же могут свидетельствовать следующие события:

а) наличие неизвестного ПО в списках автозагрузки;

б) появление неизвестных сервисов в списке сервисов ОС;

в) запуск исполняемых файлов из папок, в которых ПО обычно не располагается (например, временные папки системы, системный кеш и другие);

г) загрузка динамических библиотек из папок, в которых обычно данные библиотеки не располагаются (например, загрузка системных библиотек из папки, в которой располагается загружающий их исполняемый файл);

д) непредвиденная или необычная сетевая активность;

е) непредвиденное повышение привилегий пользователя;

1. определить варианты приоритетов инцидентов.

Приоритет инцидента выставляется в зависимости от сегмента сети (определяется не только физическим положением компьютера в сети, но и ценностью данных, которые размещены на потенциально скомпрометированной машине), в котором произошел инцидент, типа и количества инцидентов, а также от показателя достоверности индикатора, по которому был выявлен инцидент. Определять, какие инциденты следует расследовать в первую очередь, следует исходя из специфики конкретной организации.

Пример. В качестве примера приоритизации можно привести подход, при котором в первую очередь должны быть расследованы инциденты, в которых есть подозрения на APT-угрозы (способы определения APT-угроз перечислены ниже), затем следует переключиться на инциденты, связанные с вредоносными ПО (в рамках «Лаборатории Касперского»).Для того чтобы определить, является ли APT-угрозой обнаруженная в рамках инцидента ИБ угроза, рекомендуется воспользоваться следующими критериями:

* наличие индикаторов компрометации, соответствующих обнаруженному образцу в аналитических отчётах об APT-угрозах;
* взаимодействие угрозы с серверами управления, которые ранее использовались APT-угрозами, выявляемое с использованием статического или динамического анализа угрозы.

Угрозы, индикаторы компрометации которых имеют значение популярности 2 и более в потоках данных об угрозах, относятся к массовому вредоносному ПО. Такие угрозы не могут считаться APT, и на них необходимо реагировать как на массовое вредоносное ПО. Если популярность индикатора компрометации (хеш-сумма, URL-адрес) низкая, возможно, индикатор относится к APT-угрозе;

1. проанализировать события в SIEM-системе.

Администратору безопасности при получении сообщения о детектировании угрозы в SIEM-системе рекомендуется выполнить следующую последовательность действий:

а) попытаться определить источник исходного события, которое было сопоставлено с потоками данных об угрозах, то есть установить событие, содержащее обнаруженный индикатор компрометации. Если доставка угрозы произошла через рассылку электронных писем с опасными вложениями, то это можно будет обнаружить по журналам корпоративной почтовой системы. В случае заражения в процессе серфинга сети Интернет – индикаторы компрометации обнаруживаются в журналах прокси-сервера (файрволла, шлюза безопасности UTM или других устройств).

б) определить, на каком этапе жизненного цикла находится обнаруженная атака.

Таблица 2 – Жизненный цикл атаки

|  |  |
| --- | --- |
| Этап жизненного цикла | Описание |
| Разведка и сбор данных | На этом этапе происходит сбор информации об организации, которая будет атакована, а также о её информационных активах. Разведка может быть пассивной и активной.Пассивная разведка заключается в получении информации без непосредственного воздействия на атакуемую ИС (например, просмотр DNS и Whois информации, связанной с ИС организации). Активная разведка включает в себя взаимодействие с атакуемой ИС: сканирование портов, поиск уязвимостей ИС и другие действия. |
| Этап жизненного цикла | Описание |
| Выбор способа атаки | Используя информацию, полученную на этапе разведки и сбора данных, злоумышленник определяет способ атаки. Злоумышленник внедряет ПО, которое будет использоваться при атаке, в файлы MS Office (.docx, .xlsx), PDF-документы, электронные письма или на съёмные носители. |
| Доставка | Атакующий должен обеспечить попадание разработанного на прошлом шаге вредоносного ПО в ИС атакуемой организации. Обычно для этого используются вложения электронной почты, вредоносные и фишинговые ссылки, watering hole-атаки (заражения сайтов, которые посещают сотрудники атакуемой организации) или зараженные USB-устройства. |
| Эксплуатация | После попадания в ИС атакуемой организации вредоносное ПО, используя уязвимости ИБ, распространяется по сети и закрепляется на зараженных машинах в ожидании команд, поступающих от злоумышленника. |
| Закрепление | Вредоносное ПО осуществляет заражение компьютера для того, чтобы не быть обнаруженным или удаленным после перезагрузки или установки обновления, блокирующего возможность использовать одну из уязвимостей ИС. |
| Исполнение атак | С помощью соединения, устанавливаемого изнутри ИС атакованной организации, вредоносное ПО реализует взаимодействие с сервером управления, подконтрольным злоумышленнику. |
| Достижение цели | Получив управление, злоумышленник может работать с данными на скомпрометированном компьютере, не только осуществляя НСД, но и изменяя или удаляя их. |

в) оценить важность информации на потенциально скомпрометированной машине и показатель достоверности индикатора, по которому был выявлен инцидент, скорректировать приоритет данного инцидента в зависимости от ценности затронутых информационных активов и информации об индикаторе.

Дальнейшие шаги зависят от типа угрозы, которая была обнаружена в потоках данных об угрозах. Приведем несколько примеров реакции в таблицах 3-5.

Таблица 3 – Обнаружен URL-адрес угрозы

|  |  |
| --- | --- |
| Категория угрозы | Необходимые шаги |
| PHISHING | 1. Исследовать исходный код web-страницы, на которую ведет опасный URL. Определить, какие данные пользователь мог передать злоумышленникам.  2. В SIEM проанализировать события, связанные с пользователем,  инициировавшим обращение на Phishing URL, в десятиминутном интервале.  2.1. Если были загружены или отправлены какие-либо файлы, повторить  этап обнаружения для их индикаторов.  2.2. В противном случае довести до сведения пользователя,  инициировавшего активность, информацию об инциденте.  3. Если есть угроза компрометации, следует сменить пароли данного  пользователя в ИС. |
| MALICIOUS | 1. По событиям Proxy-сервера проверить, было ли получено вредоносное ПО.  Если вредоносное ПО не было получено, значит заражения не произошло.  Такое событие не является инцидентом, и дальнейшее расследование не  проводится. URL при этом нужно занести в черный список.  2. Убедиться, что вредоносное ПО не было заблокировано какими-либо  средствами обеспечения ИБ (Proxy, Endpoint-антивирус). Если угроза была  заблокирована, значит заражения не было и дальнейшее расследование  не проводится. Исключением являются случаи повторного заражения – их  следует расследовать в любом случае.  3. Получить образцы вредоносного ПО по ссылке.  4. Исследовать исходный код web-страницы по ссылке. |
| Категория угрозы | Необходимые шаги |
|  | 5. Исследовать образец вредоносного ПО (см. Инструменты для анализа  потенциальных угроз).  6. Проверить, был ли запущен скачанный образец (если возможно).  7. Просканировать на наличие обнаруженных индикаторов диск компьютера,  на котором была обнаружена угроза (см. Инструменты для анализа образов  диска) и машины в сегменте сети. Затем перейти к этапу Сдерживание. |
| BOTNET C&C | Обращения к C&C-адресам свидетельствует о наличии  активного заражения.  1. Выявить ПО, инициировавшее запросы к C&C и исследовать его Инструменты для анализа потенциальных угроз).  2. Просканировать инициировавший активность компьютер на наличие  вредоносного ПО, которое могло быть загружено по командам от сервера  управления.  3. Исследовать URL (см. Инструменты для анализа потенциальных угроз).  4. Просканировать на наличие обнаруженных индикаторов (см.  Инструменты для анализа образов диска) и машины в сегменте сети.  Затем перейти к этапу Сдерживание. |

Таблица 4 – Обнаружен хеш вредоносного объекта

|  |  |
| --- | --- |
| КАТЕГОРИЯ  УГРОЗЫ | НЕОБХОДИМЫЕ ШАГИ |
| MALICIOUS, BOT | 1. Исследовать образец (см. Инструменты для анализа потенциальных угроз).  2. Просканировать на наличие обнаруженных индикаторов диск (см. Инструменты для анализа образов диска) и машины в сегменте сети. Затем перейти к этапу Сдерживание. |

Таблица 5 – Обнаружен IP-адрес вредоносного объекта

|  |  |
| --- | --- |
| КАТЕГОРИЯ  УГРОЗЫ | НЕОБХОДИМЫЕ ШАГИ |
| TOR EXIT NODE | 1. Запросить от пользователя подтверждение использования сети Tor  1.1. В случае, если пользователь подтверждает, что использует Tor, дальнейшее расследование не проводится, инцидент считается закрытым.  1.2. В противном случае просканировать машину пользователя  (см. Инструменты для первоначального реагирования) и машины в сегменте сети, а затем повторить этап обнаружения для детектированных файлов. |
| SPAM | Перейти к этапу «Выводы». |
| MALWARE | 1. Выявить ПО, инициировавшее запросы к детектированному IP-  адресу, исследовать его (см. Инструменты для анализа потенциальных угроз).  Дальнейшие шаги аналогичны обнаружению Malicious URL-адреса. |

Этап сдерживания инцидентов

Для реализации данного этапа администратору необходимо осуществить следующее:

1. изоляция инфицированных машин.

Рекомендуется вывести инфицированные компьютеры в отдельную сеть. В случае если есть подозрение на APT-атаку, не следует физически отключать компьютер от локальной сети (извлечением провода). Некоторые виды угроз отслеживают наличие сетевого соединения и могут начать уничтожение следов в случае, если сеть была отключена на длительное время. Вместо этого следует перенастроить правила маршрутизации таким образом, чтобы инфицированные машины не смогли коммуницировать с другими компьютерами организации.

1. снятие образов;

Снятие образов позволяет получить все компоненты вредоносного ПО. По результатам исследования этих компонентов можно определить, как следует бороться с заражением. Также анализ образов позволит определить вектор распространения угрозы, чтобы не допустить повторного заражения по аналогичному сценарию. При снятии образа диска записывается полный образ диска (в том числе с неиспользуемых секторов), а не только видимая пользователю часть, поэтому необходим носитель информации, превышающий общую емкость жесткого диска. Для снятия образа рекомендуется использовать средства, описанные в разделе 2.2.2 Инструменты для сбора данных.

1. перевод системы в режим работы без изолированных машин.

Проведение этапа восстановления займет некоторое время. На это время ИС должна быть сконфигурирована так, чтобы отсутствие пораженных машин минимально влияло на функционирование ИС.

Этап удаления угрозы

Существуют две стратегии проведения данного этапа – полное восстановление из образа рабочей станции или обнаружение и удаление угрозы и всех её артефактов. Для удаления угрозы с компьютера рекомендуется использовать утилиты, описанные в разделе 2.2.5 Инструменты для удаления угроз. В корпоративных сетях, где рабочее место пользователя стандартизовано, может оказаться, что эффективнее вместо этапов сдерживания, удаления и восстановления полностью переустановить ОС и ПО на скомпрометированных пользовательских рабочих станциях.

Этап восстановления системы

После успешного проведения этапа удаления администратору необходимо:

* ввести машины обратно в сеть;
* некоторое время внимательно наблюдать за состоянием сети и восстановленных машин, чтобы убедиться в том, что угроза была полностью устранена.

Этап формирования выводов

По результатам расследования инцидента администратор готовит отчет. Содержание отчета должно отвечать на вопросы:

* когда, кем, и с помощью каких инструментов был впервые обнаружен инцидент;
* что включал в себя инцидент;
* как проводилось сдерживание, удаление и восстановление;
* на каких этапах реагирования сотрудники, ответственные за ИБ, были наиболее эффективны;
* что необходимо улучшить в работе сотрудников, ответственных за ИБ.

Выводы также могут повлечь обновление ОРД. В таком случае новые правила должны быть доведены до сведения всех сотрудников предприятия.

### Рекомендуемые инструменты

Инструменты для первоначального реагирования

1. Sysinternals – это набор бесплатных программ для администрирования и мониторинга компьютеров под управлением ОС Windows.
2. PSTools – набор утилит командной строки для удаленного запуска приложений (PSExec), получения списка процессов на локальном или удаленном компьютере (PSList), принудительного завершения задач (Pskill), управления службами (PSService).
3. Process Monitor – программа для наблюдения в реальном времени за действиями различных процессов в среде ОС Windows. Утилита включает в себя возможности мониторинга обращений к реестру, обращений к файловой системе и дополнительно позволяет получать более подробную информацию о взаимодействии процессов, использовании ресурсов, сетевой активности и операциях ввода-вывода.
4. Process Explorer – программа для наблюдения в реальном масштабе времени за действиями различных процессов и управления ими в среде ОС Windows.
5. AutoRuns – утилита для 32 и 64-разрядных ОС Microsoft Windows, которая способна управлять автозагрузкой программ, сервисов, модулей, драйверов и других компонентов системы.

Инструменты для сбора данных

1. GRR – фреймворк для реагирования на инциденты ИБ.
2. Forensic Toolkit (FTK) – набор утилит для компьютерной криминалистики. FTK предусматривает сразу несколько вариантов просмотра образа диска.
3. DD – утилита UNIX, предназначенная для копирования и конвертации файлов. Данная утилита позволяет копировать любые секторы жесткого диска, в том числе секторы, которые не используются ОС.
4. Belkasoft RAM Capturer предназначен для помощи в проведении анализа оперативной памяти компьютера.

Инструменты для анализа потенциальных угроз

1. Kaspersky Threat Lookup позволяет получить информацию по каждому из следующих индикаторов: хеши файлов, URL-, IP-адреса, имя угрозы. При этом результаты поиска будут содержать не только информацию о самом объекте исследования (например, размер для файла, whois-информацию для URL-адреса или географическое положение для IP), но и описания связанных с ним объектов.
2. Kaspersky Threat Intelligence Portal (TIP) позволяет провести анализ объекта в Песочнице (Sandbox). В результате эмуляции действий объекта в защищенной среде становится возможным обнаружение ранее неизвестных угроз, а также получение ключевых индикаторов компрометации и подробных отчетов о поведении проанализированного объекта.

Инструменты для анализа образов диска

1. The Sleuth Kit (TSK) представляет собой библиотеку и набор инструментов командной строки, которые позволяют исследовать образы дисков, а также анализировать данные о файловой системе и содержимое файлов.
2. RegRipper – это написанная на Perl утилита, позволяющая извлекать и анализировать значения ветвей реестра Windows с возможностью сохранить полученную информацию в файл отчета.
3. Strings – стандартная утилита UNIX-подобных ОС, применяемая для поиска печатаемых строк, которые могут служить дополнительными индикаторами.

Инструменты для удаления угроз

1. Kaspersky Virus Removal Tool — бесплатная программа для проверки и лечения зараженных компьютеров под управлением операционных систем Windows.
2. Kaspersky Rescue Disk применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения (например, Kaspersky Virus Removal Tool), запускаемых под управлением ОС.

## **Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций**

Добро пожаловать, в заключительный урок нашей главы, посвященный обеспечению работоспособности систем защиты информации при возникновении нештатных ситуаций. В этой лекции мы рассмотрим варианты использования отказоустойчивых технических средств, их влияния на работу системы, а так же проанализируем пользу резервного копирования ИС.и информации на резервные носители. Рассмотрим этапы восстановления работоспособности СЗИ.

В ходе обеспечения работоспособности систем ЗИ при возникновении нештатных ситуаций разрабатывается инструкция по резервированию и восстановлению работоспособности технических средств, ПО, БД и СЗИ ИС, которая определяет действия, связанные с функционированием технических и программных средств ИС и системы ЗИ. Целью данной инструкции является превентивная защита элементов ИС и системы ЗИ от предотвращения потери защищаемой информации.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

* системы жизнеобеспечения ИС;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.

Системы жизнеобеспечения ИС включают:

* пожарные сигнализации и системы пожаротушения;
* системы вентиляции и кондиционирования;
* системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИС) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

### Использование отказоустойчивых технических средств

Администратором безопасности должны быть обеспечены:

1. определение и поддержание в актуальном состоянии перечня отказоустойчивых технических средств (Приложение таблица 11);
2. определение требуемых характеристик (коэффициентов) надежности и готовности исходя из требуемых условий обеспечения непрерывности функционирования ИС и доступности информации;
3. контроль с периодичностью не реже одного раза в месяц за значениями характеристик (коэффициентов) готовности и надежности технических средств, и реагирование на ухудшение значений данных характеристик;
4. замена технических средств, в случае достижения коэффициентов готовности и надежности предельного значения.

### Резервное копирование компонентов ИС и информации на резервные машинные носители

В ИС должно обеспечиваться резервирование технических средств, ПО, каналов передачи информации, средств обеспечения функционирования ИС.

Администратором безопасности при резервировании осуществляется:

1. актуализация сегментов ИС, в которых должно осуществляться резервирование;
2. определение и поддержание в актуальном состоянии перечня резервируемых средств (Приложение таблица 12);
3. актуализация типа резервирования технических средств;

* ненагруженное ("холодное");
* нагруженное ("горячее");
* комбинированное.

1. создание резервных копий общесистемного, специального и прикладного ПО с периодичностью;
2. актуализация каналов связи, резервирование которых обеспечивает снижение вероятности отказа в доступе к ИС;
3. обращение к провайдерам, при наличии у них планов по восстановлению связи при авариях и сбоях;
4. определение и поддержание в актуальном состоянии перечня энергозависимых технических средств.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

* локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
* источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
* дублированные системы электропитания в устройствах (серверы, активное сетевое оборудование и т. д.);
* резервные линии электропитания в пределах комплекса зданий;
* аварийные электрогенераторы.

Администратором безопасности при резервном копировании информации на резервные машинные носители информации должно обеспечиваться:

1. резервное копирование информации на резервные машинные носители информации с периодичностью не реже раза в неделю;
2. определение и поддержание в актуальном состоянии перечня информации (типов информации), подлежащей резервному копированию (Приложение таблица 13);
3. регистрация событий, связанных с резервным копированием;
4. принятие мер для защиты резервируемой информации.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Хранение резервных копий информации в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

Носители должны храниться не менее года для возможности восстановления данных.

При восстановлении информации с резервных машинных носителей информации (резервных копий) должно обеспечиваться:

1. восстановление информации в течение 4 часов, для обеспечения непрерывности функционирования ИС;
2. регистрация событий, связанных восстановлением информации.

### Восстановление работоспособности средств защиты информации

При обнаружении отказов функционирования осуществляется регистрация событий, связанных с отказами функционирования, в соответствующих журналах, принятие мер по восстановлению отказавших средств:

1. восстановление ПО из резервных копий (дистрибутивов) ПО;
2. возврат ИС в начальное состояние, обеспечивающее ее штатное функционирование.

## **Тест по итогам 3 главы**

Верные ответы помечены \*

Выберите правильный ответ

**Кем производится корректировка списка учетных записей пользователей (заведение, активация, блокирования, уничтожение)**

* Руководителем структурного подразделения
* Администратором безопасности\*
* Самим пользователем
* Сотрудником отдела кадров

Выберите правильные ответы

**В каких случаях производится блокирования учетных записей пользователей**

* временных учетных записей пользователей по окончании установленного периода времени для их использования;\*
* неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования [2 УПД.1];\*
* учетной записи пользователя, при превышении установленного числа неуспешных попыток аутентификации пользователя [2 ИАФ.4];\*
* учетной записи пользователя, при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены к событиям нарушения безопасности информации [2 РСБ.1];\*

Выберите правильный ответ

**Действия администратора в ходе управления средствами аутенфикации**

* изменить минимальную сложность пароля;\*
* присваивает идентификатор пользователю или устройству;
* проверка компонентов ИС на наличие вредоносных компьютерных программ не менее одного раза в неделю;
* получение уведомления о необходимости обновлений базы решающих правил;

Выберите правильный ответ

**Действия администратора в ходе управления системами обнаружения вторжения**

* изменить минимальное количество измененных символов при создании новых паролей;
* предотвращает повторное использование идентификатора пользователя и (устройства) в течение установленного периода времени [2 ИАФ.3];
* проверка при загрузке, открытии или исполнении объектов (файлов) из внешних источников во времени, близкому к реальному;
* установка обновлений базы решающих правил из доверенных источников\*

Выберите правильный ответ

**Действия администратора в ходе управления средствами контроля носителей**

* определение и выполнение действий по реагированию на обнаружение в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).
* формирует идентификатор, который однозначно идентифицирует пользователя или устройство;
* определение и поддержание в актуальном состоянии списка пользователей, уполномоченных на доступ к МНИ;\*
* запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи.

Выберите правильные ответы

**Действия администратора в ходе управления межсетевыми экранами**

* определение и выполнение действий по реагированию на обнаружение в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).
* контроль за передачей и фильтрацией информационных потоков в соответствии с правилами управления потоками;\*
* запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи.\*
* определение или уточнение пользователей ИС, уполномоченных на ввод (вывод) информации на машинные носители;
* определение или уточнение разрешенные для ввода (вывода) информации интерфейсы;

Выберите правильный ответ

**Соответствует ли содержание события и его минимальный состав**

|  |  |
| --- | --- |
| Событие | Состав |
| Регистрация входа (выхода) субъектов доступа в ИС и загрузки (останова) ОС | Дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа, спецификация защищаемого объекта доступа (логическое имя (номер). |

* Да
* Нет\*

Выберите правильные ответы

**На какие этапы подразделяется реагирование на инциденты информационной безопасности.**

* Подготовительный этап\*
* Этап уничтожения вирусов
* Этап резервного копирования ИС
* Этап обнаружения инцидентов\*
* Этап формирования выводов\*

Выберите правильный ответ

**Включает ли в себя этап сдержевания инцидентов изоляцию инф инфицированных машин.**

* Да\*
* Нет

Выберите правильный ответ

**При использовании отказоустойчивых тех средств администратором безопасности должны быть обеспечены следующие меры:**

1. определение и поддержание в актуальном состоянии перечня отказоустойчивых технических средств; \*
2. актуализация сегментов ИС, в которых должно осуществляться резервирование;
3. определение и поддержание в актуальном состоянии перечня резервируемых средств;

# Глава 4: Итоги курса

Здравствуйте, вот мы и подошли к завершающей главе нашего курса для администраторов безопасности. Вы уже на фашинной прямой все что вам нужно это пройти тест по итогам всего курса. А также специально для вас мы добавили инструкцию для сотрудника по работе в информационных системах компании. Удачи в прохождении теста.

## Инструкции сотрудника по работе в информационных системах компании.

Данная инструкция призвана

1. Общие сведения

Все сотрудники компании, при работе в информационных системах (т.е. на компьютерах) компании, должны руководствоваться требования настоящей инструкции, положений, приказов и иных нормативных документов по информационной безопасности компании. При возникновении затруднении в трактовке требований настоящей памятки, необходимо искать разъяснения в соответствующих положениях, регламентах и инструкциях уточнять информацию в отдел информационной безопасности.

1. Рабочее место и компьютер
   1. Нельзя самолично подключать к компьютеру дополнительное оборудование и устройства, за исключением съемных носителей информации
   2. При уходе со своего рабочего места, даже на непродолжительное время, необходимо блокировать компьютер нажатием клавиш «Windows + L» одновременно.
2. Пароли и доступ
   1. Необходимо использовать сложные пароли длинной не менее 8 символов. Они должны содержать минимум три из четырёх групп символов:
      * Строчные буквы (например: a, s, f, r, п, ь, ш, я)
      * Заглавные буквы (например: A, S, F, R, П, Ь, Ш, Я)
      * Цифры (например: 1, 5, 6, 3)
      * Специальные символы (например: %, №, \*)
   2. Запрещено раскрывать пароли, даже сотрудникам ИТ/ИБ/СБ подразделений и руководителям. Если ваш пароль кто-либо запрашивает, сообщите об этом в отдел безопасности.
   3. Запрещено предпринимать попытки узнать чужие пароли. Если по какой-то причине узнали чужой пароль, сообщите об этом в отдел безопасности
   4. Категорически запрещено использовать чужие пароли, даже если это распоряжение руководителя!
   5. Нельзя хранить записанные пароли н рабочем месте.
   6. Нельзя пытаться получить доступ к программам, компьютерам и ресурсам, доступ к которым не был разрешен.
3. Интернет
   1. Запрещено пользоваться интернетом в личных целях
   2. Запрещено совершать покупки и иные полаты с личных банковский карт и счетов с рабочего компьютера
   3. Нельзя пытаться получить доступ к заблокированным сайтам
   4. Запрещено посещать сайты порнографической или экстремистской направленности, а также доступ, к которым ограничен на территории РФ
4. Электронная почта
   1. При получении подозрительной почты (например, о неизвестного отправителя, со странными запросами или содержанием) не открывать ее, а направить вашему системному администратору. Особенно нельзя открывать вложения в подобных письмах, это грозит многомиллионными убытками
   2. При отправке писем и файлов с информацией «не для всех» (например, сведения, связанные с финансами, ценами, заработной платой, условиями контрактов, персональными данными и прочее) нужно использовать имеющиеся в компании средства защиты и шифрования. Если не знаете, как применять и использовать такие средства обратитесь в отдел безопасности.
5. Программы и вирусы
   1. Нельзя использовать программы кроме тех, которые вам установили специалисты ИТ
   2. При подозрении что что-то заражено вирусами, сразу обращайтесь в отдел безопасности
   3. Запрещено открывать любые файлы, скаченные из интернета, за исключение присланных от доверенных отправителей
   4. При появлении на экране надписей с требованиями выкупа, при произвольном открывании окон на экране или при появлении других признаков вирусного заражения, перестать пользоваться компьютером, ничего не нажимайте, не блокируйте и не выключайте компьютер, сразу сообщите системному администратору

# Итоговый тест по 4 Главе

Верные ответы помечены \*

Выбери правильный ответ

**Что означает термин Правовые меры защиты информации?**

* Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.\*
* Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией.
* Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов.

Выбери правильный ответ

**Что означает термин Физические меры защиты информации?**

* Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.\*
* Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.
* Это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов.

Выбери правильный ответ

**Какие угрозы информации относятся к случайным?**

* Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неумышленная порча носителей информации.\*
* Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.
* Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

Выбери правильный ответ

**Какие угрозы информации относятся к преднамеренным?**

* Проявление ошибок программно-аппаратных средств АС; некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности; неправомерное включение оборудования или изменение режимов работы устройств и программ.
* Несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.\*
* Пересылка данных по ошибочному адресу абонента; ввод ошибочных данных; несанкционированное уничтожение информации; полное или частичное разрушение операционной системы

Выберите один из 3 вариантов ответа

**Выделите группы, на которые делятся средства защиты информации:**

* физические, аппаратные, программные, криптографические, комбинированные;\*
* химические, аппаратные, программные, криптографические, комбинированные;
* физические, аппаратные, программные, этнографические, комбинированные;

Выбери правильный ответ

**Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)**

* **МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения\***
* МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
* МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

Выбери правильный ответ

**Информация, составляющая государственную тайну не может иметь гриф…**

* **«для служебного пользования»\***
* «секретно»
* «совершенно секретно»
* «особой важности»

Выбери правильный ответ

**В чем заключается метод защиты информации - разграничение доступа?**

* В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями\*
* В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
* В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
* В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду

Выбери правильный ответ

**В чем заключается целостность компонента системы?**

* В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.\*
* В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
* В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.

Выбери правильный ответ

**В чем заключается доступность компонента системы?**

* В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы.\*
* В том, что он доступен только тем субъектам доступа ( пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.
* В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

Выбери правильный ответ

**Какой из функциональных блоков должна содержать система разграничения доступа к информации:**

* блок криптографического преобразования информации при ее
* хранении и передаче;\*
* блок контроля среды размещения
* блок контроля среды выполнения.

Выбери правильный ответ

**Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?**

* Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
* Когда риски не могут быть приняты во внимание по политическим соображениям
* Когда необходимые защитные меры слишком сложны
* Когда стоимость контрмер превышает ценность актива и потенциальные потери\*

Выбери правильный ответ

**Что из перечисленного не является целью проведения анализа рисков?**

* Делегирование полномочий\*
* Количественная оценка воздействия потенциальных угроз
* Выявление рисков
* Определение баланса между воздействием риска и стоимостью необходимых контрмер

Выберите верный ответ

**Инцидент информационной безопасности это**

* непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).\*
* часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.
* препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы.

Выберите правильный ответ

**Администратором безопасности при резервном копировании информации на резервные машинные носители информации должно обеспечиваться регистрация событий, не связанных с резервным копированием?**

Да

Нет\*

Выберите правильный ответ

**Что не стоит включать в инструктаж пользователей**

* ознакомление с должностной инструкцией и правилами политики ИБ предприятия;
* ознакомление с эксплуатационной документацией на ИС;
* ознакомление с уязвимостями системы защиты информации \*
* ознакомление с правилами эксплуатации средств защиты ИС (Например, средств идентификации и аутентификации, включая правила хранения и использования паролей и идентификаторов);
* ознакомление с обязанностями пользователей ИС;

Выбери правильный ответ

**Какую степень секретности имеют оперативные планы по всем направлениям деятельности предприятия и его структурных подразделений**

- коммерческая тайна \*

- для служебного пользования

- секретно

Выбери правильный ответ

**К объектам доступа относятся**

* персонал и все лица, которые имеют возможность доступа к средствам обработки информации, а также программные средства, посредством которых осуществляется доступ к объектам
* технические и программные средства вычислительной техники, средства и линии связи, предоставляющие возможности как для перемещения (копирования) информации между различными областями памяти и информационными носителями, различными средствами обработки, определенными для объекта ВТ, так и по выводу информации из установленной для нее сферы обращения.
* средства обработки и передачи информации, информационные носители на магнитной и бумажной основе, накопители и все виды памяти ЭВМ, в которых может находиться информация, отдельные документы и их архивы, используемые в технологическом процессе автоматизированной обработки информации, файлы, записи и другие единицы информационных ресурсов, доступ к которым необходимо регламентировать.\*

Выбери правильный ответ

**Что такое электронная подпись?**

* аналог собственноручной подписи, являющийся средством защиты информации, обеспечивающим возможность контроля целостности и подтверждения подлинности электронных документов.\*
* аналог собственноручной подписи, обеспечивающий возможность контроля целостности и подтверждения подлинности электронных документов.
* аналог собственноручной подписи и печати организации, обеспечивающий возможность контроля целостности и подтверждения подлинности электронных документов.

Выбери правильный ответ

**Что такое усиленная квалифицированная электронная подпись?**

* подпись, обязательно имеющая сертификат аккредитованного Удостоверяющего центра и заменяющая бумажные документы во всех случаях, за исключением тех, когда закон требует наличия исключительно документа на бумаге.\*
* подпись, которая создается с использованием криптографических средств и позволяет определить не только автора документа, но и проверить его на наличие изменений.
* подпись, которая создается с помощью кодов, паролей и других инструментов и позволяет идентифицировать автора подписанного документа.

Выбери правильный ответ

**Виды электронных подписей**

* простая, усиленная, усиленная квалифицированная.
* простая, усиленная неквалифицированная, усиленная квалифицированная.\*
* простая, квалифицированная, усиленная квалифицированная.

Выбери правильный ответ

**Юридически значимый электронный документооборот обеспечивает:**

* конфиденциальность, целостность, достоверность, аутентичность и юридическую значимость электронных документов.
* конфиденциальность, целостность, достоверность, аутентичность, неотказуемость и юридическую значимость электронных документов.\*
* конфиденциальность, достоверность, аутентичность и юридическую значимость электронных документов.

Выбери правильный ответ

**Юридически значимая электронная подпись:**

* электронная подпись признается в качестве реквизита электронного документа и лицо её сформировавшее или проверяющее при исполнении документа, несет правовые последствия за это действие.\*
* электронная подпись признается в качестве реквизита электронного документа и лицо её сформировавшее или проверяющее при исполнении документа, не несет правовых последствий за это действие.
* электронная подпись признается в качестве реквизита электронного документа и лицо её сформировавшее или проверяющее при исполнении документа, несет ответственность за обработку документа.

Выбери правильный ответ

**Согласно рекомендациям Технической спецификации X.800, усилия администратора безопасности должны распределяться по направлениям:**

* администрирование информационной системы в целом, администрирование сервисов безопасности.
* администрирование механизмов безопасности, администрирование информационной системы в целом, администрирование сервисов безопасности.\*
* обеспечение актуальности политики безопасности, администрирование информационной системы в целом, администрирование сервисов безопасности.

Выбери правильный ответ

**Средство защиты информации**

* техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.\*
* совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.
* совокупность органов и (или) исполнителей, используемой ими техники, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

**Список используемых источников**

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Текст] : приказ №17 : утв. ФСТЭК России 11 февраля 2013 : зарег. Минюстом России 31.05.2013 №28608. – М. : ФСТЭК, 2017– 2 с.
2. Меры защиты информации в государственных информационных системах [Текст] : метод. док. : утв. ФСТЭК России 11.02.2014 : – М.: ФСТЭК, 2014. – 78 с.
3. Специалист по защите информации в автоматизированных системах [Текст]: приказ: утв. приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. : зарег. Минюстом России 28.09.2016 г. № 43857 – М. : КонсультантПлюс, 2018. - 42 с.
4. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента Информационной безопасности. [Текст] : ГОСТ Р ИСО/МЭК 27001-2006. - Введ. 2002-12-27. - М. : Стандартинформ, 2006. - 26 с.
5. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности определения [Текст] : ГОСТ Р ИСО/МЭК 27002-2012. - Взамен ГОСТ Р ИСО/МЭК 17799-2005; Введ. 2014-09-24. - М. : Стандартинформ, 2012. - 97 с.

**Приложение**

Формы для заполнения при обеспечении ЗИ при эксплуатации ИС

Таблица 1 – Форма списка учетных записей пользователей

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Пользователь | Учетная запись | Тип пользователя | Идентификатор | Группа | Вид доступа |
|  |  | Внутренний |  | Администраторы |  |
|  |  |  |  |
|  |  | Внутренний |  | Пользователи | Проводной |
|  | Гость | Внешний |  | Беспроводной |

Таблица 2 – Перечень типов устройств, используемых в ИС

|  |  |  |  |
| --- | --- | --- | --- |
| Тип устройства | Наименование устройства | Идентификатор | Рабочая станция |
| Жесткие диски |  |  | АРМ 1 |
|  |  |  |
| ОЗУ |  |  | АРМ 2 |
|  |  |  |
| Съемные диски |  |  |  |
| Сетевые карты |  |  |  |

Таблица 3 – Форма для журнала учета МНИ

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Учетный номер | Дата  регистрации  МНИ | Вид | ФИО  работника,  получившего  МНИ | Дата  получения МНИ | Подпись работника,  получившего  МНИ | Дата  возврата МНИ | Подлежит хранению в хранилище МНИ | Дата окончания использования  МНИ |
|  |  | Съемный |  |  |  |  | **-** |  |
|  |  | Портативный |  |  |  |  | **+** |  |

Таблица 4 – Перечень компонентов ПО, подлежащие установке в ИС после загрузки ОС

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование ПО | Тип ПО | Компоненты ПО | Автозапуск при загрузке ОС | Автообновление при загрузке ОС |
| 1 | WinRar | Архиватор |  | **-** | **-** |
| 2 | Kaspersky Inetrnet Security | Антивирус | Почтовый антивирус, мониторинг активности | **+** | **+** |

Таблица 5 – Перечень событий безопасности, подлежащих регистрации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование события | Регистрационные данные | Объем памяти для хранения события | Сбои |
| 1 | Регистрация входа (выхода) субъектов доступа в ИС | Дата и время входа в ИС, результат попытки входа, идентификатор, предъявленный при попытке доступа |  |  |
| 2 | Регистрация подключения МНИ | Дата и время подключения, логическое имя подключаемого МНИ, идентификатор субъекта доступа, осуществляющего вывод информации на МНИ |  |  |

Таблица 6 – Форма журнала проведения инструктажей

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | ФИО  инструктируемого | Должность  инструктируемого | Вид инструктажа | Дата | ФИО  инструктирующего | Подпись  инструктирующего | Подпись  инструктируемого |
|  |  |  |  |  |  |  |  |

Таблица 7 – Примерный перечень инцидентов ИБ

| №  п/п | Описание инцидента ИБ |
| --- | --- |
| Инциденты категории 1 | |
|  | Однократные ошибки при регистрации пользователя ИС, связанные в вводом неверных регистрационных данных (пароля, имени пользователя и т.п.) более пяти раз подряд, приводящие к блокировке учетных данных пользователей |
|  | Однократные попытки неудачного доступа к объектам (серверам, телекоммуникационному оборудованию, СЗИ, компьютерам, принтерам, файлам) |
|  | Несанкционированный перевод времени на рабочей станции, либо на других элементах информационной инфраструктуры |
|  | Оставление работающего (включенного) компьютера без блокировки экрана в рабочее время (при отсутствии сотрудника на рабочем месте) |
|  | Перезагрузка рабочей станции при сбоях в работе технических или программных средств. |
|  | Нецелевое использование сотрудниками элементов информационной инфраструктуры (печать, сервисы сети Интернет, электронная почта, и т.п.) |
| Инциденты категории 2 | |
|  | Регулярные попытки неудачного доступа к объектам (серверам, телекоммуникационному оборудованию, СЗИ, компьютерам, принтерам, файлам) |
|  | Ошибки при регистрации администратора ИС, связанные с вводом неверных регистрационных данных (пароля, имени пользователя и т.п.) более пяти раз подряд, приводящие к блокировке учетных данных администратора |
|  | Многократные ошибки при регистрации пользователя в ИС (повторяющиеся случаи ввода неправильных регистрационных данных (пароля, имени пользователя и т.п.) более 5 раз подряд, приводящие к блокировке учетных данных пользователей) |
|  | Неоднократное оставление работающего (включенного) компьютера без блокировки экрана в рабочее время (при отсутствии сотрудника на рабочем месте) |
|  | Выход из строя или утрата носителя информации с резервной копией баз данных или учтенного носителя конфиденциальной информации |
|  | Неудачные попытки регистрации в ИС под чужими регистрационными данными (именем пользователя, паролем и т.п.) |
|  | Регистрация в ИС под чужими регистрационными данными (именем пользователя, паролем и т.п.) |
|  | Регистрация или попытки регистрации в ИС с учетными данными пользователя, которые не соответствуют штатным зарегистрированным техническим средствам и сетевым идентификационным данным (адресам) пользователя |
|  | Нерегламентированная очистка электронных журналов событий безопасности ИС и потеря их целостности |
|  | Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации |
|  | Нерегламентированное изменение аппаратной конфигурации серверного оборудования или технических средств рабочей станции |
|  | Перезагрузка сервера при сбоях в работе, которая может привести к нарушению работы системного или прикладного программного обеспечения или нарушению целостности и доступности информации (баз данных) |
|  | Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет |
|  | Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах |
|  | Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам ИС (повышение уровня прав доступа, получение прав на отладку программ и т.п.) |
|  | Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное) |
|  | Использование сканирующего (на различные уязвимости) программного обеспечения |
|  | Использование анализаторов протоколов (снифферов) |
|  | Попытки реализации сетевых атак на информационно-телекоммуникационную инфраструктуру и информационные ресурсы, совершаемых с использованием внешних информационно-телекоммуникационных сетей, в том числе атак типа «отказ в обслуживании» (DDoS-атака) |
|  | Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите) |
|  | Несанкционированное проведение обновления версий системного и прикладного программного обеспечения |
| **Инциденты категории 3** | |
|  | Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры |
|  | Несанкционированное изменение конфигурации элементов информационной инфраструктуры |
|  | Хищение носителей резервных копий баз данных |
|  | Утечка конфиденциальной информации (баз данных ИС и др.) |
|  | Подозрение в умышленном нарушении работоспособности информационной сети, элементов информационной инфраструктуры, системного и прикладного программного обеспечения |
|  | Несанкционированная передача (распространение) конфиденциальной информации |
|  | Несанкционированное внесение изменений в базы данных информационных систем |
|  | Несанкционированное уничтожение конфиденциальной информации |
|  | Проведение технического обслуживания (ремонт) или изменение характеристик и конфигурации информационных систем, повлекшее за собой потерю конфиденциальной информации |
|  | Намеренное заражение информационных систем вредоносным программным обеспечением |

Таблица 8 – Форма журнала учета инцидентов ИБ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Дата | Описание инцидента | Категория | Источник получения информации об инциденте | Принятые меры | ФИО ответственного за управление инцидентами | Подпись |
|  | Однократный ввод неверных регистрационных данных более пяти раз подряд | 1 | Пользователь | Восстановление работы системы |  |  |
|  | Попытки реализации сетевых атак с использованием внешних информационно-телекоммуникационных сетей | 2 | SIEM-система | Блокировка всех соединений |  |  |

Таблица 9 – Форма журнала регистрации изменений конфигурации

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  п/п | № заявки на внесение изменений | ФИО ответственного лица, внёсшего изменения | Подпись | Дата внесения изменений | № акта | Примечание |
|  |  |  |  |  |  |  |

Таблица 10 – Форма журнала учета мероприятий по контролю обеспечения ЗИ в ИС

| Мероприятие | Дата | Исполнитель | Результат/меры, необходимые для устранения нарушений |
| --- | --- | --- | --- |
| Контроль над выполнением антивирусной защиты |  |  | Соответствует требованиям |
| Контроль за обеспечением резервного копирования |  |  | Не соответствует требованиям. Резервное копирование информации осуществлять с периодичностью не реже раза в неделю |

Таблица 11 – Перечень отказоустойчивых средств

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование | Компоненты | Надежность, часов | Вероятность отказа в течение года | Сегмент ИС | Примечания |
| 1 | Сервер | Системная плата | 300 000 | 0,02920 |  |  |
| RAM | 1 000 000 | 0,00876 | 1 |  |

Таблица 12 – Перечень резервируемых средств

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Тип резервирования | Сегмент ИС |
| 1 | RAM | Горячее | 1 |
|  |  | Холодное |  |

Таблица 13 – Перечня информации, подлежащей резервному копированию

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Вид информации | Данные | Объем памяти для хранения | Примечания |
| 1 | Персональные данные | Данные о работниках | 1Гб | Копирование информации раз в три дня |
| 2 |  |  |  |  |