

1.1. ✓Электронная подпись. Требования, алгоритмы.

Электронная подпись (ЭП) — реквизит **электронного документа**, полученный в результате криптографического преобразования **информации** с использованием **закрытого ключа** подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу **сертификата ключа подписи** (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Принятый ещё в апреле 2011 года Федеральный закон N 63-ФЗ «Об электронной подписи» определил следующие два вида электронной подписи (ЭП): простая ЭП и усиленная ЭП, из которых вторая в свою очередь бывает невалифицированной и квалифицированной.

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

Усиленная же электронная подпись обязательно использует криптографические преобразования. Вот требования для усиленной невалифицированной ЭП:

- 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.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам невалифицированной 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, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Существует несколько схем построения цифровой подписи:

- На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью ЭП.

1.2. ✓Идентификация и аутентификация. Требования, сравнение основных методов.

Для защиты от НСД, как правило, используется идентификация, аутентификация и управление доступом. В дополнение к перечисленным, могут применяться и другие методы.

Идентификация – присвоение пользователям идентификаторов (уникальных имен или меток), под которыми система «знает» пользователя. Кроме идентификации пользователей, может проводиться идентификация групп пользователей, ресурсов АС и т. д. В большинстве случаев идентификация сопровождается аутентификацией. **Аутентификация** – установление подлинности – проверка принадлежности пользователю предъявленного им идентификатора. Например, в начале сеанса работы в АС пользователь вводит имя и пароль. На основании этих данных система проводит идентификацию (по имени пользователя) и аутентификацию (сопоставляя имя пользователя и введенный пароль). Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Обычно выделяют 3 группы методов аутентификации.

1. Аутентификация по наличию у пользователя уникального объекта заданного типа. Иногда этот класс методов аутентификации называют по-английски —I have || («у меня есть»). В качестве примера можно привести аутентификацию с помощью смарт-карт или электронных USB-ключей.

2. Аутентификация, основанная на том, что пользователю известна некоторая конфиденциальная информация – —I know || («я знаю»). Например, аутентификация по паролю.

3. Аутентификация пользователя по его собственным уникальным характеристикам – —I am || («я есть»).

Биометрические методы аутентификации делят на статические и динамические. Примеры аутентификации по статическим признакам – это проверка отпечатка пальца, рисунка радужной оболочки глаз, геометрии кисти руки, сравнение с фотографией и т. д. Достоинством этих методов является достаточно высокая точность. Но надо отметить, что подобные методы, как правило, требуют наличия специализированного оборудования (например, специальные сканеры) и имеют ограниченную область применения (например, при аутентификации по отпечатку пальца, из-за грязи на руке человек может не пройти аутентификацию, т. е. подобные методы неприменимы на стройках и на многих производствах). Примеры динамической аутентификации – аутентификация по голосу (при произнесении заранее определенной фразы или произвольного текста), аутентификация по «клавиатурному почерку» (проверяются особенности работы пользователя на клавиатуре, такие как время задержки при нажатии клавиш в различных сочетаниях) и т. д. Нередко используются комбинированные схемы аутентификации, объединяющие методы разных классов. Например, двухфакторная аутентификация – пользователь предъявляет системе смарт-карту и вводит пин-код для ее активации. Аутентификация может быть односторонней, когда одна сторона аутентифицирует другую (например, сервер проверяет подлинность клиентов), и двусторонней, когда стороны проводят взаимную проверку подлинности.

Также аутентификация может быть непосредственной, когда в процедуре аутентификации участвуют только две стороны, или с участием доверенной стороны.

2.1. ✓ Конфиденциальная информация, классификация.

Конфиденциальная информация — информация, являющаяся конфиденциальной, то есть «доверительной, не подлежащей огласке, секретной»; это понятие равнозначно с понятиями тайны или секрета

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации[10].

Коммерческая тайна — режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Все виды сведений, сохранность которых защищается на законодательном уровне, перечислены в одноименном перечне, утвержденном Указом Президента России от 06.03.1997 № 188. Так, в соответствии с документом, к категории конфиденциальной информации относятся:

-персональные данные гражданина

– любые сведения о событиях, фактах и обстоятельствах его частной жизни;

-сведения, составляющие служебную тайну – данные, доступ к которым ограничен уполномоченными государственными органами в соответствии с нормами гражданского законодательства (к этой категории отнесена в том числе информация, составляющая налоговую тайну);

-информация, охраняемая Конституцией России и известная ограниченному кругу лиц в связи с исполнением ими профессионального долга (профессиональная тайна);

-данные, сохранность которых устанавливается с целью извлечения дохода, защиты от конкуренции или получения иной выгоды (коммерческая тайна);

-содержание личных дел лиц, осужденных за совершение преступлений;

-информация об исполнении судебных решений в рамках исполнительного производства;

-информация, составляющая тайну судопроизводства и следствия, в том числе данные о свидетелях и потерпевших, подлежащих государственной защите, а также о судьях и должностных лицах следственных и правоохранительных органов.

2.2. Вредоносные программы, классификация. Основные способы проникновения, тенденции. Антивирусные средства, принципы работы, основные требования

Вирус-самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя. Вирусы можно разделить по типу объектов, которые они заражают, по методам заражения и выбора жертв. Вирусы можно подцепить разными способами: от нажатия вредоносной ссылки или файла в неизвестном письме до заражения на вредоносном сайте. При этом вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда операционной системе.

Червь. Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ. Однако черви не могут заражать существующие файлы. Вместо этого червь поселяется в компьютер отдельным файлом и ищет уязвимости в Сети или системе для дальнейшего распространения себя. Черви также могут подразделяться по способу заражения (электронная почта, мессенджеры, обмен файлами и пр.). Некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые поселяются лишь в оперативной памяти компьютера.

Троян. По своему действию является противоположностью вирусам и червям. Его предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности он делает то, что нужно злоумышленникам. Троянцы получили свое название от одноименного печально известного мифологического коня, так как под видом какой-либо полезной программы или утилиты в систему проникает деструктивный элемент. Трояны не самовоспроизводятся и не распространяются сами по себе. Однако с увеличением вала информации и файлов в Интернете трояна стало довольно легко подцепить. Нынешние трояны эволюционировали до таких сложных форм, как, например, бэкдор (троян, пытающийся взять на себя администрирование компьютера) и троян-загрузчик (устанавливает на компьютер жертвы вредоносный код).

Руткит. В современном мире руткит представляет собой особую часть вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного

защитного программного обеспечения. Это возможно благодаря тесной интеграции руткита с операционной системой. А некоторые руткиты могут начать свою работу прежде, чем загрузится операционная система. Таких называют буткитами. Однако, как бы ни развивался этот тип вредоносных, [сложные современные антивирусные программы](#) в состоянии [обнаружить и обезвредить](#) практически все существующие разновидности руткитов.

Бэкдор (средство удаленного администрирования). Бэкдор, или RAT (remote administration tool), — это приложение, которое позволяет честному системному администратору или злобному злоумышленнику управлять вашим компьютером на расстоянии. В зависимости от функциональных особенностей конкретного бэкдора, хакер может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру. Словом, брать на себя контроль за компьютером и информацией жертвы.

Загрузчик. Эта зараза является небольшой частью кода, используемой для дальнейшей загрузки и установки полной версии вредоноса. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь вредонос.

Антивирусная программа — специализированная [программа](#) для обнаружения компьютерных [вирусов](#), а также нежелательных (считающихся [вредоносными](#)) программ и восстановления заражённых (модифицированных) такими программами [файлов](#), а также для профилактики — предотвращения заражения (модификации) файлов или [операционной системы](#) вредоносным кодом.

Для защиты от вирусов используют три группы методов¹:

1. Методы, основанные на *анализе содержимого файлов* (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.
2. Методы, основанные на *отслеживании поведения программ* при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.
3. Методы *регламентации порядка работы* с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности

Метод сканирования сигнатур - смотрим на известные вирусы в базе данных

Метод контроля целостности - смотрим изменение файлов

Метод сканирования подозрительных команд ([эвристическое сканирование](#)) - смотрим использование подозрительных команд в файле

Метод отслеживания поведения программ -смотрим подозрительное поведение уже в запущенной программе

3.1. ✓ Классификация ресурсов. Категорирование информации

Присвоение категорий безопасности информации и информационным системам производится на основе оценки ущерба, который может быть нанесен нарушениями безопасности. Категории безопасности используются совместно с данными об уязвимостях и угрозах в процессе анализа рисков, которым подвержена организация. Существуют три основных аспекта ИБ: доступность; конфиденциальность; целостность. Целесообразно оценивать возможный ущерб отдельно для нарушений доступности, конфиденциальности и целостности, а при необходимости можно получить интегральную оценку.

Категорировать необходимо и пользовательскую, и системную информацию, представленную как в электронной форме, так и в виде "твердой" копии. Открытая информация может не иметь категории конфиденциальности. Например, сведения, содержащиеся на общедоступном web-сервере организации, не имеют категории конфиденциальности, а их доступность и целостность оцениваются как умеренные.

| Категория конфиденциальности информации | Категория целостности информации | Категория доступности информации | Тип информации |
|--|---|---|-------------------------------|
| Строго конфиденциальная информация | * | * | Наиболее критичная информация |
| * | Высокая | * | |
| * | * | Беспрепятственная доступность | |
| Конфиденциальная информация | * | * | Критичная информация |
| * | Низкая | * | |
| * | * | Высокая доступность | |
| Открытая информация | Нет требований | Средняя доступность | Некритичная информация |
| Открытая информация | Нет требований | Низкая доступность | |

1 Категории конфиденциальности защищаемой информации

Конфиденциальность информации – свойство информации, указывающее на необходимость введения ограничений на круг лиц, имеющих доступ к данной информации

вводятся следующие категории конфиденциальности информации:

- Строго конфиденциальная информация – информация, являющаяся конфиденциальной в соответствии с требованиями законодательства, а также информация, ограничения на распространение которой введены решениями руководства организации, разглашение которой может привести к нанесению значительного ущерба деятельности организации.
- Конфиденциальная информация – информация, не являющаяся строго конфиденциальной, ограничения на распространение которой вводятся только решением руководства организации, разглашение которой может привести к нанесению ущерба деятельности организации.
- Открытая информация – к данной категории относится информация, обеспечения конфиденциальности которой не требуется.

2. Категории целостности информации

целостность информации – свойство, при выполнении которого данные сохраняют заранее определенный вид и качество (остаются неизменными по отношению к некоторому фиксированному состоянию). вводятся следующие категории целостности информации: – Высокая – к данной категории относится информация, несанкционированная модификация или подделка которой может привести к нанесению значительного ущерба деятельности организации. М. М. Коптенков 118 – Низкая – к данной категории относится информация, несанкционированная модификация которой может привести к нанесению умеренного или незначительного ущерба деятельности организации. – Нет требований – к данной категории относится информация, к обеспечению целостности которой требований не предъявляется.

3. Категории доступности информации

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно. вводятся следующие категории доступности информации: – Беспрепятственная доступность – доступ к информации должен обеспечиваться в любое время (задержка получения доступа к информации не должна превышать нескольких секунд или минут). – Высокая доступность – доступ к информации должен

осуществляться без существенных временных задержек (задержка получения доступа к информации не должна превышать нескольких часов). – Средняя доступность – доступ к информации может обеспечиваться с существенными временными задержками (задержка получения информации не должна превышать нескольких дней). – Низкая доступность – временные задержки при доступе к информации практически не лимитированы (допустимая задержка получения доступа к информации – несколько недель). из вышеперечисленного видно, что категории конфиденциальности и целостности

3.2. ✓ Управление доступом, произвольное, принудительное, ролевое

Управление доступом на основе ролей ([англ. Role Based Access Control, RBAC](#)) — развитие политики [избирательного управления доступом](#), при этом права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя [роли](#)

Формирование ролей призвано определить чёткие и понятные для [пользователей](#) компьютерной системы правила разграничения [доступа](#).

Такое разграничение доступа является составляющей многих современных компьютерных систем. Как правило, данный подход применяется в системах защиты [СУБД](#), а отдельные элементы реализуются в сетевых [операционных системах](#). Ролевой подход часто используется в системах, для пользователей которых чётко определён круг их должностных полномочий и обязанностей.

Несмотря на то, что *Роль* является совокупностью прав доступа на объекты компьютерной системы, ролевое управление доступом отнюдь не является частным случаем избирательного управления доступом, так как его правила определяют порядок предоставления доступа субъектам компьютерной системы в зависимости от имеющихся (или отсутствующих) у него ролей в каждый момент времени, что является характерным для систем [мандатного управления доступом](#). С другой стороны, правила ролевого разграничения доступа являются более гибкими, чем при мандатном подходе к разграничению.

Так как привилегии не назначаются пользователям непосредственно и приобретаются ими только через свою роль (или роли), управление индивидуальными правами пользователя по сути сводится к назначению ему ролей. Это упрощает такие операции, как добавление пользователя или смена подразделения пользователем.

Избирательное управление доступом ([англ. discretionary access control, DAC](#)) — управление доступом субъектов к [объектам](#) на основе [списков управления доступом](#) или матрицы доступа. Также используются названия «*дискреционное управление доступом*», «*контролируемое управление доступом*» или «*разграничительное управление доступом*».

Субъект доступа «Пользователь № 1» имеет право доступа только к объекту доступа № 3, поэтому его запрос к объекту доступа № 2 отклоняется. Субъект «Пользователь № 2» имеет право доступа как к объекту доступа № 1, так и к объекту доступа № 2, поэтому его запросы к данным объектам не отклоняются.

Для каждой пары (субъект — объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту)^[2].

Возможны несколько подходов к построению дискреционного управления доступом:

- Каждый объект системы имеет привязанного к нему субъекта, называемого **владельцем**. Именно владелец устанавливает права доступа к объекту.
- Система имеет одного выделенного субъекта — [суперпользователя](#), который имеет право устанавливать права владения для всех остальных субъектов системы.
- Субъект с определённым правом доступа может передать это право любому другому субъекту^[2].

Мандатное управление доступом ([англ. Mandatory access control, MAC](#)) — разграничение [доступа](#) субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как **Принудительный контроль доступа**. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования.

Мандатная модель управления доступом, помимо [дискреционной](#) и [ролевой](#), является основой реализации разграничительной политики доступа к ресурсам при защите информации ограниченного доступа. При этом данная модель доступа практически не используется «в чистом виде», обычно на практике она дополняется элементами других моделей доступа.

4.2. ✓ Криптографическая хеш-функция, свойства, алгоритмы, применение

Криптографические хэш-функции используются обычно для генерации дайджеста сообщения при создании цифровой подписи. Хэш-функции отображают сообщение в имеющее фиксированный размер хэш-значение (hash value) таким образом, что все множество возможных сообщений распределяется равномерно по множеству хэш-значений. При этом криптографическая хэш-функция делает это таким образом, что практически невозможно подогнать документ к заданному хэш-значению.

Криптографические хэш-функции обычно производят значения длиной в 128 и более бит. Это число значительно больше, чем количество сообщений, которые когда-либо будут существовать в мире.

Много хороших криптографических хэш-функций доступно бесплатно. Широко известные включают MD5 и SHA. Отечественный стандарт хэш-функций ГОСТ Р 34.11-94 предусматривает хэш размером 256 бит.

Среди множества существующих хэш-функций принято выделять криптографически стойкие, применяемые в криптографии. Криптостойкая хэш-функция прежде всего должна обладать стойкостью к коллизиям двух типов:

- Стойкость к коллизиям первого рода: для заданного сообщения должно быть практически невозможно подобрать другое сообщение, имеющее такой же хэш. Это свойство также называется необратимостью хэш-функции.
- Стойкость к коллизиям второго рода: должно быть практически невозможно подобрать пару сообщений, имеющих одинаковый хэш.

Согласно парадоксу о днях рождения, нахождение коллизии для хэш-функции с длиной значений n бит требует в среднем перебора около $2n / 2$ операций. Поэтому n -битная хэш-функция считается криптостойкой, если вычислительная сложность нахождения коллизий для нее близка к $2n / 2$.

Простейшим (хотя и не всегда приемлемым) способом усложнения поиска коллизий является увеличение разрядности хэша, например, путем параллельного использования двух или более различных хэш-функций.

Для криптографических хэш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно менялось. В частности, значение хэша не должно давать утечки информации даже об отдельных битах аргумента. Это требование является залогом криптостойкости алгоритмов шифрования, хеширующих пользовательский пароль для получения ключа.

К криптографическим хэш-функциям предъявляются следующие требования:

1. **Стойкость к поиску первого прообраза** — отсутствие эффективного полиномиального алгоритма вычисления обратной функции, т.е. нельзя восстановить текст m по известной его свертке $H(m)$ за реальное время (необратимость). Это свойство эквивалентно тому, что хэш-функция является односторонней функцией.
2. **Стойкость к поиску второго прообраза** — вычислительно невозможно, зная сообщение m и его свертку $H(m)$, найти такое другое сообщение $m' \neq m$, чтобы $H(m) = H(m')$.

3. Стойкость к коллизиям

5.1. ✓ Системы DLP, принципы работы.

Предотвращение утечек (англ. Data Leak Prevention, DLP) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются.

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста. Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п. Хостовые компоненты также стараются отслеживать изменение сетевых настроек, установку программ для туннелирования, стеганографии и другие возможные методы для обхода контроля. DLP-система должна иметь компоненты обоих указанных типов плюс модуль для централизованного управления.

DLP-система должна уметь отличать конфиденциальную информацию от неконфиденциальной. DLP работает в основном «в связке» с ответственным специалистом, который не только «учит» систему корректно работать, вносит новые и удаляет неактуальные правила, но и проводит мониторинг текущих, заблокированных или подозрительных событий в информационной системе.

Функциональность DLP-системы строится вокруг «ядра» – программного алгоритма, который отвечает за обнаружение и категоризацию информации, нуждающейся в защите от утечек. В ядре большинства DLP-решений заложены две технологии: лингвистического анализа и технология, основанная на статистических методах. Также в ядре могут использоваться менее распространенные техники, например, применение меток или формальные методы анализа.

5.2. Виртуальные частные сети (VPN). Принципы организации, режимы работы, используемые протоколы

VPN (англ. Virtual Private Network - виртуальная частная сеть) - логическая сеть, создаваемая поверх другой сети, например Internet. Несмотря на то, что коммуникации осуществляются по публичным сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые от посторонних каналы обмена информацией. VPN позволяет объединить, например, несколько офисов организации в единую сеть с использованием для связи между ними неподконтрольных каналов.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

Работает VPN в нескольких режимах:

- узел-сеть;
- сеть-сеть;
- узел-узел.

Организация частной виртуальной сети на сетевых уровнях позволяет использовать TCP и UDP протоколы. Все данные, которые проходят через компьютеры, шифруются. Это дополнительная защита для вашего подключения.

Наиболее универсальным способом построения VPN является использование технологии инкапсуляции, или туннелирования. В общем случае туннелирование применяется для того, чтобы передавать пакеты одной сети (первичной) по каналам связи другой (вторичной), протоколы которых не совместимы. Для этого пакет первичной сети (данные и протоколы) инкапсулируется в пакет вторичной сети и становится виден как данные. Таким образом, пакет продвигается маршрутизаторами ядра сети только на основании внешнего заголовка, без инспекции содержимого

Под политикой безопасности организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет технические требования к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности. Эта конфигурация будет оказывать влияние на пользователей, и некоторые требования, установленные в политике, связаны со всем коллективом пользователей. Главная ответственность за развертывание этой политики ложится на системных и сетевых администраторов при поддержке руководства.

Политика безопасности определяет требования, выполнение которых должно быть обеспечено на каждой системе. Однако политика сама по себе не определяет конкретную конфигурацию различных операционных систем. Это устанавливается в отдельных процедурах по настройке. Такие процедуры могут быть размещены в приложении к политике.

Идентификация и аутентификация, Управление доступом, Аудит

Для каждого типа соединений в сети политика безопасности описывает правила установки сетевых соединений и используемые механизмы защиты.

Политика безопасности должна определять приемлемые алгоритмы шифрования для применения внутри организации и ссылаться на информационную политику для указания соответствующих алгоритмов для защиты секретной информации. В такой политике совершенно не обязательно указывать какой-либо один конкретный алгоритм. Политика безопасности также определяет процедуры управления ключами.

Одним из принципов является предоставление каждому сотруднику предприятия того минимального уровня привилегий на доступ к данным, который необходим ему для выполнения его должностных обязанностей. использование многоуровневого подхода к обеспечению безопасности. Система защиты с многократным резервированием средств безопасности увеличивает вероятность сохранности данных. Так, например, физические средства защиты (закрытые помещения, блокировочные ключи), ограничивающие непосредственный контакт пользователя только приписанным ему компьютером, дополняют и усиливают эффективность централизованной системы авторизации пользователей.

6.2. Основы криптографической защиты информации. Симметричное шифрование, основные алгоритмы. Асимметричное шифрование, открытый и закрытый ключи, распределение ключей

Симметричные криптосистемы - способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический **ключ**. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями. Главным принципом в них является условие, что передатчик и приемник заранее знают алгоритм шифрования, а также ключ к сообщению, без которых информация представляет собой всего лишь набор символов, не имеющих смысла.

Требования Полная утрата всех статистических закономерностей исходного сообщения является важным требованием к симметричному шифру. Для этого шифр должен иметь «эффект лавины» — должно происходить сильное изменение шифроблока при 1-битном изменении входных данных (в идеале должны меняться значения 1/2 бит шифроблока). Также важным требованием является отсутствие линейности (то есть условия $f(a \oplus b) = f(a) \oplus f(b)$), в противном случае облегчается применение дифференциального криптоанализа к шифру.

Блочные шифры. Обработывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

Поточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования.

Параметры алгоритмов: Стойкость, длина ключа, число раундов, длина обрабатываемого блока, сложность аппаратной/программной реализации, сложность преобразования

Блочные шифры [AES](#), [ГОСТ 28147-89](#), [DES](#), [3DES](#), [RC2](#) **IDEA** **Потоковые шифры** [RC4](#), [SEAL](#), [WAKE](#)

Асимметричное шифрование при которой *открытый ключ* передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ

Преимущества асимметричных шифров перед симметричными: не нужно предварительно передавать секретный ключ по надёжному каналу; только одной стороне известен ключ дешифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обоим сторонам и должен держаться в секрете

обеими); в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки алгоритма несимметричного шифрования в сравнении с симметричным: в алгоритм сложнее внести изменения; более длинные ключи; шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом;

Алгоритмы RSA DSA Elgamal

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица. В централизованных системах сертификатов (например PKI) используются центры сертификации, поддерживаемые доверенными организациями. В децентрализованных системах (например PGP) путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия.

7.1. ФСТЭК, основные руководящие документы. Система лицензирования и сертификации (не оч)

Сертификат соответствия ФСТЭК

Сертификат соответствия ФСТЭК – это дословно документ, выданный федеральной структурой ФСТЭК, подтверждающий соответствие сертифицируемого объекта требованиям нормативных российских актов. Попробуем это расшифровать на понятийном уровне, и определиться, с чем это связано и о чем идет речь.

ФСТЭК России — Федеральная служба по техническому и экспортному контролю, в функции которой включен специальный контроль в некоторых областях. ФСТЭК в настоящее время подчинена Министерству обороны РФ. До августа 2004 года данная служба имела другое название и подчинение. Это была Государственная техническая комиссия при Президенте РФ. Одна из функций, которые определены ФСТЭК государством, является техническая защита информации.

К сфере деятельности сертификата соответствия ФСТЭК относятся средства защиты информации (СЗИ) без использования средств криптографии и не составляющих государственную тайну. Т.е. обеспечение защиты информационной безопасности некриптографическими методами.

Продукция, подлежащая сертификации ФСТЭК

К объектам, для которых оформляется сертификат соответствия ФСТЭК, относятся следующие:

антивирусные программы массового использования для реализации на российском рынке;
межсетевые экраны;
средства защиты системного и сетевого уровня (сканеры безопасности, средства мониторинга безопасности, средства защиты от несанкционированного доступа);
операционные системы;
системы управления базами данных;
прикладные информационные системы;
системы генерации паролей для доступа к информационным ресурсам;
электронные системы документооборота и другие.

В органах государственной власти, а также в государственных корпорациях могут применяться только программные средства, имеющие требуемые по закону лицензии и сертификаты безопасности информации, включая сертификаты соответствия ФСТЭК.

Основным законом, который регулирует сертификацию в сфере СЗИ является Постановление Правительства РФ № 608 «О сертификации СЗИ», введенное в действие в 1995 году. Этот закон предписывает: обязательная сертификация и оформление сертификата соответствия ФСТЭК предусмотрено только для продукции, относящейся к средствам защиты информации для предохранения сведений, являющимися государственной тайной.

Для защиты от несанкционированного доступа к конфиденциальным данным не требуется обязательный сертификат соответствия ФСТЭК или Декларация соответствия на СЗИ. В этом случае оценка соответствия СЗИ является добровольной.

Система сертификации ФСТЭК

ФСТЭК (ранее Правительственная комиссия) создала Систему сертификации средств защиты информации по требованиям безопасности информации, которая имеет Свидетельство № РОСС RU.0001.01БИ00 и зарегистрирована в Государственном реестре в 1995 году.

Органы сертификации данной системы производят оценку соответствия СЗИ на основе Руководящих документов (РД) «Защита от несанкционированного доступа к информации». Данные документы разработаны на разные группы продуктов, относящихся к программному, техническому обеспечению, к автоматизированным системам в целом.

Во всех документах имеется показатель — Оценочный уровень доверия (ОУД). Он введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187. ОУД характеризует уровень доверия к практическому исполнению требований по защите информации.

Классы защищенности изделий

Для защиты информации, значимость которой определяется градацией «секретность/конфиденциальность», установлены следующие классы защищенности изделий Информационных Технологий (ИТ):

четвертый класс защищенности изделий ИТ является достаточным для защиты конфиденциальной информации; третий класс защищенности используется для защиты информации с грифом «Секретно»; второй класс — с грифом «Совершенно секретно»; первый класс используется для защиты информации с грифом «Особой важности».

Сертификат соответствия ФСТЭК содержит сведения: на основе каких нормативных документов происходило изготовление продукции, содержащей СЗИ и соответствует ли конечный товар требованиям, изложенным в указанном нормативном акте. Здесь же указывается класс защищенности продукта по классификации уровня контроля отсутствия недекларированных возможностей.

Сертификат соответствия ФСТЭК также содержит сведения о сертификационных испытаниях, об экспертном заключении и о лаборатории, где проходили лабораторные исследования с указанием, когда и кем был выполнен инспекционный контроль данной сертификационной лаборатории.

Процедура получения сертификата соответствия ФСТЭК

Сертификационные лаборатории для оформления сертификата соответствия ФСТЭК могут проводить целый ряд различных испытаний:

на соответствие требованиям, связанным с защитой от неразрешенного доступа к информации;
на соответствие требованиям Технических условий;
на соответствие функциональных возможностей, которые реально имеются у исследуемого продукта описаниям, указанным в документации на эксплуатацию;
на соответствие декларируемой безопасности исследуемого товара;
на отсутствие возможностей, которые не указаны в документации, и связанные с безопасностью информации будущего пользователя;
на соответствие требованиям стандартов предприятий, международным стандартам в сфере СЗИ;
исследование датчиков случайных чисел на соответствие криптографическим требованиям и другие исследования.

Закон "О лицензировании отдельных видов деятельности"

от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года, последняя учтенная редакция от 30.12.2008 номер 309-ФЗ, с изменением, внесенным Федеральным Законом от 22.12.2008 номер 272-ФЗ).

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

7.2. Межсетевые экраны, классификация, принципы работы, используемые технологии (пакетный фильтр, nat, proxy)

Межсетевой экран (МЭ): комплекс аппаратных и/или программных средств, осуществляющий анализ проходящих через него сетевых пакетов на предмет соответствия заданным правилам фильтрации. Фильтрует (не пропускает) пакеты, не соответствующие определённой политике безопасности. Основная задача: защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Альтернативные названия: брандмауэр (нем. Brandmauer), файрвол (англ. Firewall), сетевой экран, фильтр пакетов. Дополнительные функции:

(NAT), редирект, контроль корректности функционирования сетевых протоколов, организация VPN.

Преимущества использования межсетевого экрана

- Управляемый доступ к внешним сетевым ресурсам
- Защита внутренних сетевых ресурсов от внешних угроз
- Обнаружение и защита от типовых атак отказа в обслуживании
- Скрытие структуры внутренней сети
- Конфиденциальность внешних сетевых соединений
- Аудит событий безопасности
- Управление сетевым трафиком

От чего не может защитить межсетевой экран?

- Внутренние угрозы
- Атаки через разрешенные соединения

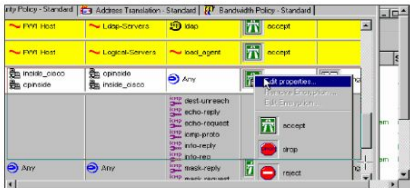
Классификация межсетевых экранов

1. По способу реализации

- Программный
- Аппаратно-программный

Межсетевые экраны: классификация по способу реализации

Программные межсетевые экраны




Плюсы:

- Возможность интеграции с другими продуктами
- Простота наращивания мощности аппаратного обеспечения
- Возможность быстрого проведения апгрейдов и латания дыр программного обеспечения МЭ

Минусы:

- Уязвимость управляющей ОС может стать причиной нарушений информационной безопасности
- Администратор должен хорошо знать как сам МЭ, так и управляющую ОС

Программно-аппаратные межсетевые экраны



Плюсы:

- Простота эксплуатации
- Высокая производительность
- Высокая надежность

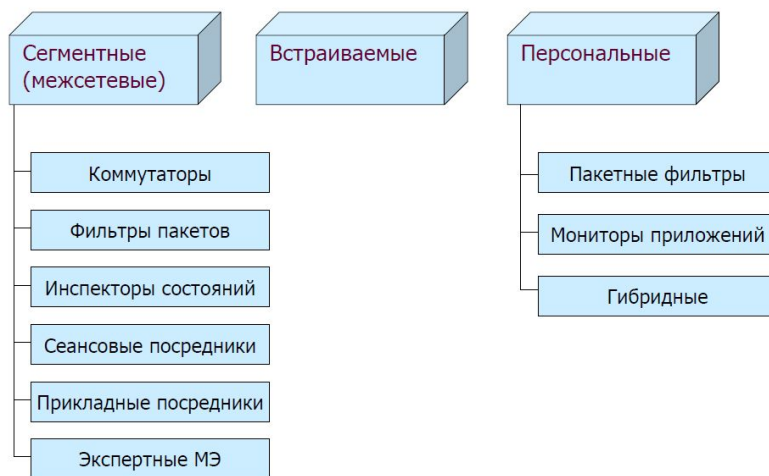
Минусы:

- Плохая программная и аппаратная масштабируемость

2. По типу защищаемых объектов

- Сегментные (межсетевые)
- Встраиваемые
- Персональные

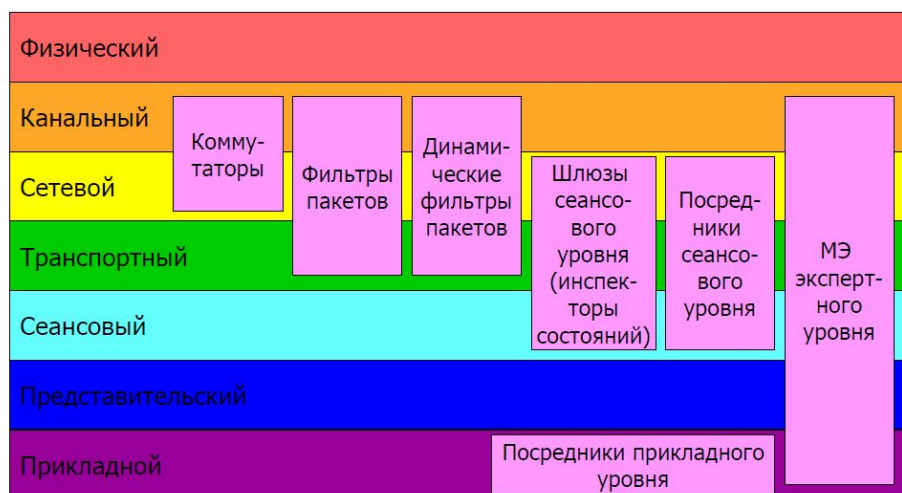
Межсетевые экраны: классификация по типу защищаемых объектов



3. По уровням модели OSI/ISO

- Коммутаторы
- Фильтры пакетов
- Динамические фильтры пакетов
- Инспекторы состояний (шлюзы сеансового уровня)
- Посредники сеансового уровня
- Посредники прикладного уровня
- Межсетевые экраны экспертного уровня

Межсетевые экраны: классификация по уровням модели OSI/ISO



Пакетные фильтры

Пакетные фильтры функционируют на сетевом уровне и контролируют прохождение трафика на основе информации, содержащейся в заголовке пакетов. Многие межсетевые экраны данного типа могут оперировать заголовками протоколов и более высокого, транспортного, уровня (например, TCP или UDP). Пакетные фильтры одними из первых появились на рынке межсетевых экранов и по сей день остаются самым распространённым их типом. Данная технология реализована в подавляющем большинстве маршрутизаторов и даже в некоторых коммутаторах^[16].

При анализе заголовка сетевого пакета могут использоваться следующие параметры^[10]:

- IP-адреса источника и получателя;
- тип транспортного протокола;

- поля служебных заголовков протоколов сетевого и транспортного уровней;
- [порт](#) источника и получателя.

Достаточно часто приходится фильтровать фрагментированные пакеты, что затрудняет определение некоторых [атак](#). Многие сетевые атаки используют данную уязвимость межсетевых экранов, выдавая пакеты, содержащие запрещённые данные, за фрагменты другого, доверенного пакета. Одним из способов борьбы с данным типом атак является конфигурирование межсетевого экрана таким образом, чтобы блокировать фрагментированные пакеты^[17]. Некоторые межсетевые экраны могут дефрагментировать пакеты перед пересылкой во внутреннюю сеть, но это требует дополнительных ресурсов самого межсетевого экрана, особенно памяти. Дефрагментация должна использоваться очень обоснованно, иначе такой межсетевой экран легко может сам стать жертвой DoS-атак.

Пакетные фильтры могут быть реализованы в следующих компонентах сетевой инфраструктуры^[18]:

- пограничные маршрутизаторы;
- операционные системы;
- персональные межсетевые экраны.

Так как пакетные фильтры обычно проверяют данные только в заголовках сетевого и транспортного уровней, они могут выполнять это достаточно быстро. Поэтому пакетные фильтры, встроенные в пограничные маршрутизаторы, идеальны для размещения на границе с сетью с низкой степенью доверия. Однако в пакетных фильтрах отсутствует возможность анализа протоколов более высоких уровней сетевой модели OSI. Кроме того, пакетные фильтры обычно уязвимы для атак, которые используют подделку сетевого адреса. Такие атаки обычно выполняются для обхода управления доступом, осуществляемого межсетевым экраном.

Механизм NAT определён в [RFC 1631](#), [RFC 3022](#).

Управляемые коммутаторы иногда причисляют к классу межсетевых экранов, так как они осуществляют фильтрацию трафика между сетями или узлами сети. Однако они работают на канальном уровне и разделяют трафик в рамках локальной сети, а значит не могут быть использованы для обработки трафика из внешних сетей (например, из Интернета).

Преимущества

NAT выполняет две важных функции.

1. Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).
2. Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.

Недостатки

1. Не все протоколы могут «преодолеть» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протоколов [FTP](#) или [H.323](#)). См. [Application-level gateway](#).
2. Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.
3. [DoS](#) со стороны узла, осуществляющего NAT — если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT'ом приводит к проблеме подключения некоторых пользователей из-за превышения допустимой скорости коннектов к серверу. Частичным решением проблемы является использование *пула адресов* (группы адресов), для которых осуществляется трансляция.

Шлюзы сеансового уровня (*proxy*)

Межсетевой экран сеансового уровня исключает прямое взаимодействие внешних хостов с узлом, расположенным в локальной сети, выступая в качестве посредника (англ. *proxy*), который реагирует на все входящие пакеты и проверяет их допустимость на основании текущей фазы соединения. Шлюз сеансового уровня гарантирует, что ни

один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению. Как только приходит запрос на установление соединения, в специальную таблицу помещается соответствующая информация (адреса отправителя и получателя, используемые протоколы сетевого и транспортного уровня, состояние соединения и т. д.). В случае, если соединение установлено, пакеты, передаваемые в рамках данной сессии, будут просто копироваться в локальную сеть без дополнительной фильтрации. Когда сеанс связи завершается, сведения о нём удаляются из данной таблицы. Поэтому все последующие пакеты, «притворяющиеся» пакетами уже завершённого соединения, отбрасываются.

Так как межсетевой экран данного типа исключает прямое взаимодействие между двумя узлами, шлюз сеансового уровня является единственным связующим элементом между внешней сетью и внутренними ресурсами. Это создаёт видимость того, что на все запросы из внешней сети отвечает шлюз, и делает практически невозможным определение топологии защищаемой сети. Кроме того, так как контакт между узлами устанавливается только при условии его допустимости, шлюз сеансового уровня предотвращает возможность реализации DoS-атаки, присущей пакетным фильтра.

Несмотря на эффективность этой технологии, она обладает серьёзным недостатком: как и у всех вышеперечисленных классов межсетевых экранов, у шлюзов сеансового уровня отсутствует возможность проверки содержания поля данных, что позволяет злоумышленнику передавать «тройных коней» в защищаемую сеть.

8.1. **PKI, сертификаты, система удостоверяющих центров**

Инфраструктура открытых ключей (ИОК, [англ. PKI - Public Key Infrastructure](#)) — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей. В основе PKI лежит использование [криптографической системы с открытым ключом](#) и несколько основных принципов:

1. закрытый ключ (private key) известен только его владельцу;
2. удостоверяющий центр создает электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передается в сертификате;
3. никто не доверяет друг другу, но все доверяют удостоверяющему центру;
4. удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

PKI реализуется в модели [клиент-сервер](#), то есть проверка какой-либо информации, предоставляемой инфраструктурой, может происходить только по инициативе клиента.

Основные компоненты PKI:

- [Удостоверяющий центр](#) (УЦ) является основной структурой, формирующей цифровые сертификаты подчиненных центров сертификации и конечных пользователей. УЦ является главным компонентом PKI:
 1. он является [доверенной третьей стороной](#) (trusted third party)
 2. это сервер, который осуществляет управление жизненным циклом сертификатов (но не их непосредственным использованием).
- [Сертификат открытого ключа](#) (чаще всего просто *сертификат*) — это данные пользователя и его открытый ключ, скрепленные электронной подписью удостоверяющего центра. Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет закрытым ключом, который соответствует этому открытому ключу.
- Регистрационный центр (РЦ) — необязательный компонент системы, предназначенный для регистрации пользователей. Для этих целей РЦ обычно предоставляет веб-интерфейс. Удостоверяющий центр доверяет регистрационному центру проверку информации о субъекте. Регистрационный центр, проверив правильность информации, подписывает её своим ключом и передает удостоверяющему центру, который, проверив ключ регистрационного центра, выписывает сертификат. Один регистрационный центр может работать с несколькими удостоверяющими центрами (то есть состоять в нескольких PKI), один удостоверяющий центр может работать с несколькими регистрационными центрами. Иногда, удостоверяющий центр выполняет функции регистрационного центра.
- Репозиторий — хранилище, содержащее сертификаты и [списки отозванных сертификатов](#) (COC) и служащее для распространения этих объектов среди пользователей. В Федеральном Законе РФ № 63 «Об электронной подписи» он называется *реестр сертификатов ключей подписей*.
- Архив сертификатов — хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком действия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы.
- Центр запросов — необязательный компонент системы, где конечные пользователи могут запросить или отозвать сертификат.
- Конечные пользователи — пользователи, приложения или системы, являющиеся владельцами сертификата и использующие инфраструктуру управления открытыми ключами.

Основные задачи системы информационной безопасности, которые решает инфраструктура управления открытыми ключами:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи;
- обеспечение возможности подтверждения совершенных пользователями действий с информацией (неотказуемость, неотречаемость, апеллируемость) — [англ. non-repudiation](#)).

Упрощенно, PKI представляет собой систему, основным компонентом которой является удостоверяющий центр и пользователи, взаимодействующие между собой используя сертификаты, выданные этим удостоверяющим центром. Деятельность инфраструктуры управления открытыми ключами осуществляется на основе регламента системы. Инфраструктура открытых ключей основывается на использовании принципов [криптографической системы с открытым ключом](#). Инфраструктура управления открытыми ключами состоит из [центра сертификации](#)

([удостоверяющего центра](#) — УЦ), конечных пользователей и опциональных компонентов: центра регистрации и сетевого справочника.

8.2. Системы обнаружения вторжений, классификация, принципы работы.

9.1. ✓ Управление рисками

При разработке концепции Информационной Безопасности организации необходимо выработать стратегию управления рисками различных классов. Возможно несколько подходов.

Уклонение от риска. Например, вынесение Web-сервера за пределы локальной сети организации позволит избежать несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Уменьшение риска. Например, грамотное использование средств аутентификации снижает вероятность несанкционированного доступа.

Изменение характера риска. Если не удастся уклониться от риска или уменьшить степень его воздействия, можно применить некоторые меры страховки.

Принятие риска. На практике многие риски не могут быть уменьшены до пренебрежимо малой величины.

Необходимо знать остаточную величину риска

Модель анализа угроз и уязвимостей

Для оценки рисков информационной системы организации защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

В результате работы алгоритма программа представляет следующие данные:

1. Инвентаризация;
2. Значения риска для каждого ценного ресурса организации;
3. Перечень всех уязвимостей, которые стали причиной полученного значения риска;
4. Значения риска для ресурсов после задания контрмер (остаточный риск);
5. Эффективность контрмер.

Введение в модель

Данная модель основана на построении модели угроз и уязвимостей.

Для того, чтобы оценить риск информации, необходимо проанализировать все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз.

Исходя из введенных владельцем информационной системы данных, можно построить модель угроз и уязвимостей, актуальных для информационной системы компании. На основе полученной модели будет проведен анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитаны риски.

Процесс управления рисками безопасности, предлагаемый Майкрософт, включает следующие четыре этапа (рис.4.1):

1. Оценка рисков.

Планирование сбора данных. Обсуждение основных условий успешной реализации и подготовка рекомендаций.

Сбор данных о рисках. Описание процесса сбора и анализа данных.

Приоритезация рисков. Подробное описание шагов по качественной и количественной оценке рисков.

2. Поддержка принятия решений.

Определение функциональных требований. Определение функциональных требований для снижения рисков.

Выбор возможных решений для контроля. Описание подхода к выбору решений по нейтрализации риска.

Экспертиза решения. Проверка предложенных элементов контроля на соответствие функциональным требованиям.

Оценка снижения риска. Оценка снижения подверженности воздействию или вероятности рисков.

Оценка стоимости решения. Оценка прямых и косвенных затрат, связанных с решениями по нейтрализации риска.

Выбор стратегии нейтрализации риска. Определение наиболее экономически эффективного решения по нейтрализации риска путем анализа выгод и затрат.

3. Реализация контроля. Развертывание и использование решений для контроля, снижающих риск для организации.

Поиск целостного подхода. Включение персонала, процессов и технологий в решение по нейтрализации риска.

Организация по принципу многоуровневой защиты. Упорядочение решений по нейтрализации риска в рамках предприятия.

4. Оценка эффективности программы. Анализ эффективности процесса управления рисками и проверка того, обеспечивают ли элементы контроля надлежащий уровень безопасности.

Разработка системы показателей рисков. Оценка уровня и изменения риска.

Оценка эффективности программы. Оценка программы управления рисками для выявления возможностей совершенствования.

9.2. ✓Протоколирование и аудит

Под **протоколированием (логи, журналы)** понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). **(не желательно до его вопросов про активный аудит) Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.**

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Подотчетность служит больше психологическим барьером для администраторов и прочих (как камеры в магазинах, чтобы не пиздили).

Какие события протоколировать? Согласно “оранжевой книге” (критерии определения безопасности компьютерных систем - стандарт МО США (от автора: там штук 30 книг “радужной серии” с разными стандартами)):

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

Что должно содержать сообщение протоколирования? Рекомендуются хотя бы (тоже по “оранжевой книги”) это:

- дата и время события;
- уникальный идентификатор пользователя – инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Еще одно важное понятие, фигурирующее в "Оранжевой книге", – **выборочное протоколирование**, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

От автора: насколько я помню, гелич не особо углублялся в активный аудит, лучше это до его вопросов вообще не использовать. А вот во что он углублялся, так это

Под **подозрительной активностью** понимается поведение пользователя или компонента информационной системы, являющееся **злоумышленным** (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Задача активного аудита – оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

10.1. ✓Классификация угроз.

При разработке алгоритма оценки информационных рисков, основанного на анализе угроз и уязвимостей информационной системы, специалистами Digital Security были рассмотрены и проанализированы различные существующие классификации угроз информационной безопасности. Попытки использования данных классификаций для описания по возможности большего количества угроз показали, что во многих случаях реальные угрозы либо не подходили ни под один из классификационных признаков, либо, наоборот, удовлетворяли нескольким.

Таким образом, основная цель создания специалистами Digital Security классификации угроз - наиболее полная, детальная классификация, которая описывает все существующие угрозы информационной безопасности, по которой каждая из угроз попадает только под один классификационный признак, и которая, таким образом, наиболее применима для анализа рисков реальных информационных систем.

Описание классификации:

По характеру угрозы информационной безопасности можно разделить на технологические и организационные. Соответственно, получим верхний уровень классификации:

1. Угрозы технологического характера

2. Угрозы организационного характера

Рассмотрим технологические угрозы информационной безопасности, которые по виду воздействия делятся на:

1.1. Физические

1.2. Программные (логические)

Следующая ступень классификации - причина угрозы.

Причинами реализации физических угроз могут быть:

1.1.1. Действия нарушителя (человека)

1.1.2. Форс-мажорные обстоятельства

1.1.3. Отказ оборудования и внутренних систем жизнеобеспечения

Независимо от причины физические угрозы воздействуют:

1.1.1.1. На ресурс

1.1.1.2. На канал связи

Далее перейдем к рассмотрению программных угроз.

Программные угрозы по причине воздействия можно разделить на:

1.2.1. Угрозы, исходящие от локального нарушителя;

1.2.2. Угрозы, исходящие от удаленного нарушителя.

Объектом локального нарушителя может быть только ресурс.

При этом, на ресурсе локальный нарушитель может реализовать угрозы, направленные:

1.2.1.1. На операционную систему;

1.2.1.2. На прикладное программное обеспечение;

1.2.1.3. На информацию.

Угрозы, исходящие от удаленного нарушителя, могут воздействовать:

1.2.2.1. На ресурс;

1.2.2.2. На канал связи.

При доступе к ресурсу удаленный нарушитель может воздействовать:

1.2.2.1.1. На операционную систему;

1.2.2.1.2. На сетевые службы;

1.2.2.1.3. На информацию.

При воздействии на канал связи удаленный нарушитель может реализовать угрозы, направленные:

1.2.2.2.1. На сетевое оборудование;

1.2.2.2.2. На протоколы связи.

Рассмотрим организационные угрозы.

Организационные угрозы по характеру воздействия разделим на:

2.1. Воздействие на персонал;

2.2. Действия персонала.

Воздействие на персонал может быть:

2.1.1. Физическим;

2.1.2. Психологическим.

Как физическое, так и психологическое воздействие на персонал направлено на сотрудников компании с целью:

2.1.1.1. Получения информации;

2.1.1.2. Нарушения непрерывности ведения бизнеса.

Причинами действий персонала, способных вызвать угрозы информационной безопасности, могут быть:

2.2.1. Умышленные действия;

2.2.2. Неумышленные действия.

Угрозы, вызванные умышленными действиями персонала, могут быть направлены:

2.2.1.1. На информацию;

2.2.1.2. На непрерывность ведения бизнеса.

Угрозы, вызванные неумышленными действиями персонала, могут быть направлены:

2.2.2.1. На информацию;

2.2.2.2. На непрерывность ведения бизнеса.

Таким образом, классификация угроз информационной безопасности разделяется по характеру угрозы, виды воздействия, причине и объекту угрозы.

10.2. ✓VPN на базе SSL/TLS

VPN, или Virtual Private Network, что в переводе означает Виртуальная Частная Сеть - это криптосистема, позволяющая защитить данные при передаче их по незащищенной сети, такой как Интернет. Несмотря на то, что данное описание подходит и для криптосистемы SSH, VPN имеет другое предназначение. **Цель VPN** - прозрачный доступ к ресурсам сети, где пользователь может делать всё то, что он делает обычно независимо от того, насколько он удалён.

VPN соединение всегда состоит из канала типа точка-точка, также известного под названием *туннель*. Туннель создаётся в незащищённой сети, в качестве которой чаще всего выступает Интернет. Соединение точка-точка подразумевает, что оно всегда устанавливается между двумя компьютерами, которые называются узлами или *peers*. Каждый реер отвечает за шифрование данных до того, как они попадут в туннель и расшифровке этих данных после того, как они туннель покинут.

Хотя VPN туннель всегда устанавливается между двумя точками, каждый реер может устанавливать дополнительные туннели с другими узлами. Для примера, когда трём удалённым станциям необходимо связаться с одним и тем же офисом, будет создано три отдельных VPN туннеля к этому офису. Для всех туннелей реер на стороне офиса может быть одним и тем же. Это возможно благодаря тому, что узел может шифровать и расшифровывать данные от имени всей сети, как это показано на рисунке 1:

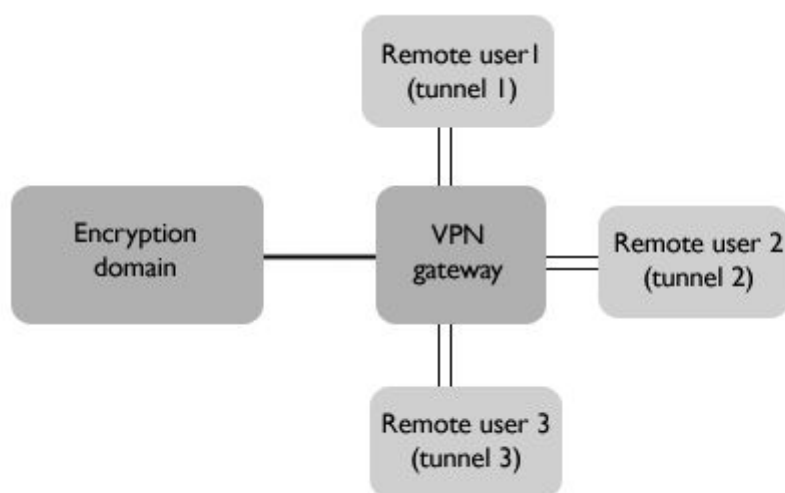


Рисунок 1 -- VPN шлюз к сети

В этом случае VPN узел называется *VPN шлюзом*, а сеть за ним - *доменом шифрования (encryption domain)*.

Использование шлюзов удобно по нескольким причинам. Во-первых, все пользователи должны пройти через одно устройство, которое облегчает задачу управления политикой безопасности и контроля входящего и исходящего трафика сети. Во-вторых, персональные туннели к каждой рабочей станции, к которой пользователю надо получить доступ, очень быстро станут неуправляемыми (т.к. туннель - это канал типа точка-точка). При наличии шлюза, пользователь устанавливает соединение с ним, после чего пользователю открывается доступ к сети (домену шифрования).

Интересно отметить, что внутри домена шифрования самого шифрования не происходит. Причина в том, что эта часть сети считается безопасной и находящейся под непосредственным контролем в противоположность Интернет. Это справедливо и при соединении офисов с помощью VPN шлюзов. Таким образом гарантируется шифрование только той информации, которая передаётся по небезопасному каналу между офисами.

Всякий раз, когда соединение сетей обслуживают два VPN шлюза, они используют *режим туннеля*. Это означает, что шифруется весь пакет IP, после чего к нему добавляется новый IP заголовок. Новый заголовок содержит IP адреса двух VPN шлюзов, которые и увидит пакетный сниффер при перехвате. Невозможно определить компьютер-источник в первом домене шифрования и компьютер-получатель во втором домене.

Посмотрите на рисунок 1, иллюстрирующий типичное использование VPN, которая позволяет удаленным пользователям с переносными компьютерами и пользователям, работающим из дома, иметь доступ к офисной сети. Чтобы эта схема заработала, пользователь должен иметь установленное ПО - *VPN клиент*, который обеспечит создание VPN туннеля к удаленному VPN шлюзу. По сценарию используется режим туннеля, т.к. пользователь хочет получить доступ к ресурсам домена, а не самого шлюза. Единственным случаем, когда включается *режим транспорта* - это если одному компьютеру нужно получить доступ к другому непосредственно.

Независимо от используемого ПО, все VPN работают по следующим принципам:

1. Каждый из узлов идентифицирует друг друга перед созданием туннеля, чтобы удостовериться, что зашифрованные данные будут отправлены на нужный узел
2. Оба узла требуют заранее настроенной политики, указывающей какие протоколы могут использоваться для шифрования и обеспечения целостности данных
3. Узлы сверяют политики, чтобы договориться об используемых алгоритмах; если это не получается, то туннель не устанавливается
4. Как только достигнуто соглашение по алгоритмам, создается ключ, который будет использован в симметричном алгоритме для шифрования/расшифровки данных

Есть несколько стандартов регламентирующих вышеописанное взаимодействие. Вы, должно быть, слышали о некоторых из них: L2TP, PPTP, и IPSec.

SSL (Secure Socket Layer) протокол защищенных сокетов, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создается защищенное соединение между клиентом и сервером.

SSL использует защиту данных с открытым ключом для подтверждения подлинности передатчика и получателя. Поддерживает надёжность передачи данных за счёт использования корректирующих кодов и безопасных хэш-функций.

SSL использует RC4, MD5, RSA и другие алгоритмы защиты данных.

SSL использует два ключа для защиты данных - открытый ключ и закрытый или частный ключ известный только получателю сообщения.

На сегодняшний день, в сети Интернет можно встретить множество сайтов на которых используется протокол SSL для обеспечения безопасности пользовательских данных (например, веб-сайты предоставляющие коммерческие и банковские сервисы). Практически все самые популярные браузеры, почтовые клиенты и интернет-приложения поддерживают работу с протоколом SSL. Для доступа к страницам, защищённым протоколом SSL, в URL вместо обычного префикса http, как правило, применяется префикс https (порт 443), указывающий на то, что будет использоваться SSL-соединение.

SSL также может обеспечить защиту протоколов прикладного уровня (уровень 7 модели OSI), например, таких как POP3 или FTP. Для работы SSL требуется, чтобы на сервере имелся SSL-сертификат.

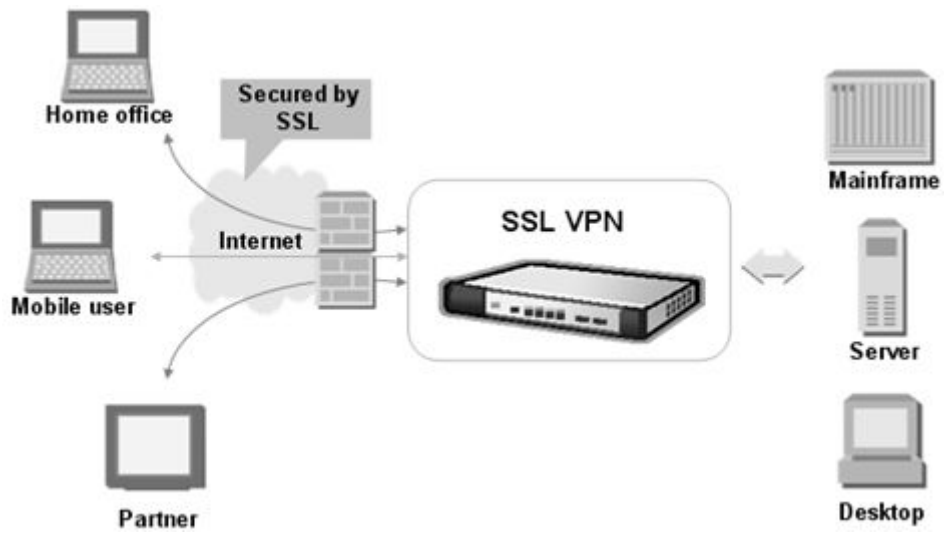
Безопасное соединение между клиентом и сервером при использовании SSL выполняет две функции - аутентификацию и защиту данных.

SSL состоит из двух уровней. На нижних уровнях (уровни 4-5) многоуровневого транспортного протокола (например, TCP) он является протоколом записи и используется для инкапсуляции (то есть формирования пакета) различных протоколов. Для каждого инкапсулированного протокола он обеспечивает условия, при которых сервер и клиент могут подтверждать друг другу свою подлинность, выполнять защиту передаваемых данных и производить обмен ключами, прежде чем протокол прикладной программы начнет передавать и получать данные.

Преимущества протокола SSL:

- Простота использования
- Нет необходимости в дополнительном программном обеспечении
- Безопасный удаленный доступ

SSL VPN оптимален для подключения удаленных пользователей к ресурсам локальной сети офиса через Интернет.



11.1. ✓ Информационные системы Персональных Данных (ИСПДн), требования по защите, классификация

В соответствии с Постановлением Правительства № 1119 от 1 ноября 2012г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн установлено 4 уровня защищенности.

Для определения уровня защищенности необходимо определить тип информационной системы и актуальные угрозы.

По типам информационные системы делятся на:

- · Обрабатывающие специальные категории персональных данных;
- · Обрабатывающие биометрические персональные данные;
- · Обрабатывающие общедоступные персональные данные;
- · Обрабатывающие иные категории персональных данных;
- · Обрабатывающие персональные данные сотрудников оператора.

Актуальные угрозы делятся на следующие типы:

- Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;
- Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;
- Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе;

Итоговое определение уровня защищенности информационной системы персональных данных производится на основании следующей таблицы:

| Тип ИСПДн | Категории субъектов | Количество субъектов | Тип актуальных угроз | | |
|--------------------------|---------------------|----------------------|----------------------|-------------------|-----------------|
| | | | 1 тип (НДВ в СПО) | 2 тип (НДВ в ППО) | 3 тип (нет НДВ) |
| ИСПДн-С (специальные) | Не сотрудников | Более 100 000 | УЗ 1 | УЗ 1 | УЗ 2 |
| | | Менее чем 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | Сотрудников | Любое | УЗ 1 | УЗ 2 | УЗ 3 |
| ИСПДн-Б (биометрические) | Любых | Любое | УЗ 1 | УЗ 2 | УЗ 3 |
| ИСПДн-И (иные) | Не сотрудников | Более 100 000 | УЗ 1 | УЗ 2 | УЗ 3 |
| | | Менее чем 100 000 | УЗ 1 | УЗ 3 | УЗ 4 |
| | Сотрудников | Любое | УЗ 1 | УЗ 3 | УЗ 4 |
| ИСПДн-О (общедоступные) | Не сотрудников | Более 100 000 | УЗ 2 | УЗ 2 | УЗ 4 |
| | | Менее чем 100 000 | УЗ 2 | УЗ 3 | УЗ 4 |

| | | | | | |
|--|-------------|-------|------|------|------|
| | Сотрудников | Любое | УЗ 2 | УЗ 3 | УЗ 4 |
|--|-------------|-------|------|------|------|

11.2. ✓ ФСТЭК. классификация средств ВТ, АС и МЭ.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

Классификация ВТ

СВТ – средства вычислительной техники

Устанавливается семь классов защищенности СВТ от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- - первая группа содержит только один седьмой класс;
- - вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- - третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- - четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Перечень показателей по классам защищенности СВТ приведен в таблице. Обозначения:

- - "-" – нет требований к данному классу;
- - "+" – новые или дополнительные требования,
- - "=" – требования совпадают с требованиями к СВТ предыдущего класса.

| Наименование показателя | Класс защищенности | | | | | |
|---|--------------------|---|---|---|---|---|
| | 6 | 5 | 4 | 3 | 2 | 1 |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчуждаемый физический носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство для пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Тестовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |

Классификация МЭ

В Требованиях выделены следующие типы межсетевых экранов:

- межсетевой экран уровня сети (тип «А») – межсетевой экран, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы. Межсетевые экраны типа «А» могут иметь только программно-техническое исполнение;
- межсетевой экран уровня логических границ сети (тип «Б») – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы. Межсетевые экраны типа «Б» могут иметь программное или программно-техническое исполнение;
- межсетевой экран уровня узла (тип «В») – межсетевой экран, применяемый на узле (хосте) информационной системы. Межсетевые экраны типа «В» могут иметь только программное исполнение и устанавливаются на мобильных или стационарных технических средствах конкретного узла информационной системы;
- межсетевой экран уровня веб-сервера (тип «Г») – межсетевой экран, применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера;
- межсетевой экран уровня промышленной сети (тип «Д») – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами. Межсетевые экраны типа «Д» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, IndustrialEthernet и (или) иные протоколы).

Для дифференциации требований к функциям безопасности межсетевых экранов выделяются шесть классов защиты межсетевых экранов. Самый низкий класс – шестой, самый высокий – первый.

- Межсетевые экраны, соответствующие 6 классу защиты, применяются в государственных информационных системах 3 и 4 классов защищенности*, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности**, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровней защищенности персональных данных***.
- Межсетевые экраны, соответствующие 5 классу защиты, применяются в государственных информационных системах 2 класса защищенности*, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности***, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных**.
- Межсетевые экраны, соответствующие 4 классу защиты, применяются в государственных информационных системах 1 класса защищенности*, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности**, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных***, в информационных системах общего пользования II класса****.
- Межсетевые экраны, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Классификация АС

РД предусматривает следующие этапы классификации АС:

разработка и анализ исходных данных;

выявление основных признаков АС, необходимых для классификации;

сравнение выявленных признаков АС с классифицируемыми;

присвоение АС соответствующего класса защиты информации от НСД.

Для проведения классификации конкретной АС необходимо провести анализ следующих данных:

перечень защищаемых [информационных ресурсов](#) АС и их уровень конфиденциальности;

перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

матрицу доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

режим обработки данных в АС.

Определяющими признаками, по которым производится группировка АС в различные классы, являются:

наличие в АС информации различного уровня конфиденциальности; уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС — коллективный или индивидуальный.

Указанным РД установлено девять классов защищенности Автоматизированных систем от НСД к информации. Каждый класс характеризуется определённой минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса — 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

Классы 1А, 2А, 3А включают АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом "особой важности".

Класс 1Б включает АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом "совершенно секретно".

Класс 1В включает АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом "секретно".

Классы 1Г, 2Б, 3Б включают АС, на которых обрабатываются сведения, составляющие конфиденциальную информацию - служебная тайна.

Классы 1Г, 1Д, 2Б, 3Б включают АС, на которых обрабатываются сведения, составляющие конфиденциальную информацию - персональные данные, коммерческая тайна.

| | ГТ | | | КИ | | |
|------------|----|----|----|-----|----|---|
| | С | | | ПДн | | |
| | СС | | | | | |
| | ОВ | | | СТ | | |
| I | 1А | 1Б | 1В | 1Г | 1Д | многопользовательская с разными правами |
| II | 2А | | | 2Б | | многопользовательская с одинаковыми правами |
| III | 3А | | | 3Б | | однопользовательская |

НАЧАЛО в 10.2 Т.к. IPsec - наиболее широко поддерживаемый стандарт, который имеет в арсенале наибольшее количество сокращений, оставшуюся часть статьи стоит посвятить именно ему.

Рассмотрим архитектуру семейства протоколов **IPsec**. Цель данного семейства протоколов состоит в том, чтобы обеспечить различные сервисы безопасности на уровне IP для протоколов IPv4 и IPv6. Стандарт IPsec был разработан для повышения безопасности IP протокола. Это достигается за счёт дополнительных протоколов, добавляющих к IP пакету собственные заголовки, которые называются инкапсуляциями. Т.к. IPsec - стандарт Интернет, то для него существуют RFC (Requests For Comments).

AH (Authentication Header) - протокол заголовка идентификации. Обеспечивает целостность путём проверки того, что ни один бит в защищаемой части пакета не был изменён во время передачи. Использование AH может вызвать проблемы, например, при прохождении пакета через NAT устройство. NAT меняет IP адрес пакета, чтобы разрешить доступ в Интернет с закрытого локального адреса. Т.к. пакет в таком случае изменится, то контрольная сумма AH станет неверной. Также стоит отметить, что AH разрабатывался только для обеспечения целостности. Он не гарантирует конфиденциальности путём шифрования содержимого пакета.

ESP (Encapsulating Security Protocol) - инкапсулирующий протокол безопасности, который обеспечивает и целостность и конфиденциальность. В режиме транспорта ESP заголовок находится между оригинальным IP заголовком и заголовком TCP или UDP. В режиме туннеля заголовок ESP размещается между новым IP заголовком и полностью зашифрованным оригинальным IP пакетом.

Т.к. оба протокола - AH и ESP добавляют собственные заголовки, они имеют свой ID протокола, по которому можно определить что последует за заголовком IP.

Третий протокол, используемый IPsec - это IKE или Internet Key Exchange protocol. Он предназначен для обмена ключами между двумя узлами VPN. Несмотря на то, что генерировать ключи можно вручную, лучшим и более масштабируемым вариантом будет автоматизация этого процесса с помощью IKE. Помните, что ключи должны часто меняться, и вам наверняка не хочется полагаться на свою память, чтобы найти время для совершения этой операции вручную. Главное - не забудьте настроить правило на файрволе для UDP порта с номером 500, т.к. именно этот порт используется IKE.

SA (Security Association), что можно приближённо перевести как "связь или ассоциация безопасности" - это термин IPsec для обозначения соединения. При настроенном VPN, для каждого используемого протокола создается одна SA пара (т.е. одна для AH и одна для ESP). SA создаются парами, т.к. каждая SA - это однонаправленное соединение, а данные необходимо передавать в двух направлениях. Полученные SA пары хранятся на каждом узле. Если ваш узел имеет SA, значит VPN туннель был установлен успешно. Т.к. каждый узел способен устанавливать несколько туннелей с другими узлами, каждый SA имеет уникальный номер, позволяющий определить к какому узлу он относится. Это номер называется **SPI (Security Parameter Index)** или индекс параметра безопасности.

SA хранятся в базе данных **SAD (Security Association Database)** или БД ассоциаций безопасности. Каждый узел IPsec также имеет вторую БД - **SPD или Security Policy Database** (БД политики безопасности). Она содержит настроенную вами политику узла.

12.2. ✓Коммерческая тайна, признаки, требования по защите.

Коммерческая тайна — режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Под режимом конфиденциальности информации понимается введение и поддержание особых мер по защите информации.

Также под коммерческой тайной могут подразумевать саму информацию, которая составляет коммерческую тайну, то есть, научно-техническую, технологическую, производственную, финансово-экономическую или иную информацию, в том числе составляющую секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны.

Основные признаки коммерческой тайны

- Коммерческая ценность информации и её неизвестность третьим лицам. Неизвестность третьим лицам означает, что информация не должна быть общеизвестна.

- Отсутствие доступа к информации на законном основании. В данном контексте под доступом понимается возможность получения сведений, составляющих [коммерческую тайну](#), на основе законодательных или договорных норм для использования в целях, оговоренных в этих нормах.
- Меры по охране конфиденциальности информации.

Сведения должны иметь для предприятия действительную или потенциальную коммерческую ценность. Должны быть неизвестны третьим лицам. В отношении них предприятие должно ввести режим КТ.

Чтобы информация получила статус коммерческой тайны, её обладатель должен исполнить установленные процедуры (составление перечня, нанесение грифа и некоторые другие):

1. Нанесение на документы соответствующего грифа (пометки). Например, «Секретно», или «Коммерческая тайна».
2. Назначение сотрудников, которые будут нести личную ответственность за сохранность ценной информации; подписание договора о неразглашении информации.
3. Составление и введение в действие документа «Положение о коммерческой тайне».
4. Обозначение круга сотрудников, которые имеют открытый доступ к секретной информации.
5. Внесение в трудовой договор пункта об ответственности за разглашение коммерческой тайны.

Разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

За разглашение (умышленное или неосторожное), а также за незаконное использование информации, составляющей коммерческую тайну, предусмотрена ответственность — дисциплинарная, гражданско-правовая, административная, уголовная и материальная. Материальная ответственность наступает независимо от других форм ответственности.

Меры по поддержанию секретности информации

- Техническая защита - комплекс мероприятий и (или) услуг по защите её от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на неё в целях уничтожения, искажения или блокирования доступа к ней.
- Организационные меры - меры по ограничению доступа к секретной информации работников организации и третьих лиц.
- Юридические (правовые) меры - федеральное законодательство в сфере [информационной безопасности](#) и различные правовые акты.