Содержание.

Введение.

Жизнь современного общества не мыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями.

Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Однако, именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной и т. п.). Доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

Тому есть много примеров. Так имеют место широкомасштабные атаки вредоносного программного обеспечения, как на информационные ресурсы кредитных организаций, так и на информационные ресурсы клиентов кредитных организаций. По информации Лаборатории Касперского, только в третьем квартале 2014 года инциденты, связанные с вредоносными программами, относящимися к категории банковских «троянцев», произошли на компьютерах более 67 000 пользователей. По информации территориальных учреждений Банка России. В 2015 году у3частилисьслучаицеленаправленных спам - рассылок с вложением вредоносного программного обеспечения на адреса региональных банков и филиалов. Потери от хищений или повреждений компьютерных сетей составляют сотни миллионов рублей в год.

Субъекты производственно – хозяйственных отношений вступают друг с другом в информационные отношения (отношения по поводу получения, хранения, обработки, распределения и использования информации) для выполнения своих производственно – хозяйственных и экономических задач.

Поэтому обеспечение информационной безопасности – это гарантия удовлетворения законных прав и интересов субъектов информационных отношений.

Исходя из выше изложенного, в данной работе будут рассмотрены такие вопросы как:

- понятие информационной безопасности:
- проблемы обеспечения безопасности операционных систем (ОС) от несанкционированного доступа (НСД):
- способы защиты ОС от НСД;
- обеспечение безопасности данных криптографическими методами;
- сетевые атаки и способы защиты от них;
- требования по защите информации от НСД, в том числе, изложенные в документах ФСТЭК и ФСБ;
- подтверждение защищенности информационных систем в соответствии с документами ФСТЭК.

Понятие информационной безопасности.

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, стихийные бедствия.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Основные типы угроз информационной безопасности:

1. Угрозы конфиденциальности – несанкционированный доступ к данным (например, получение посторонними лицами сведений о состоянии счетов клиентов банка).
2. Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных (например, внесение изменений в бухгалтерские проводки с целью хищения денежных средств).
3. Угрозы доступности – ограничение или блокирование доступа к данным (например, невозможность подключится к серверу с базой данных в результате DDoS-атаки).

Источники угроз:

1. Внутренние:

а) ошибки пользователей и системных администраторов;

б) ошибки в работе ПО;

в) сбои в работе компьютерного оборудования;

г) нарушение сотрудниками компании регламентов по работе с информацией.

2. Внешние угрозы:

а) несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лиц (промышленный шпионаж конкурентов, сбор информации спецслужбами, атаки хакеров и т.п.);

б) компьютерные вирусы и иные вредоносные программы;

в) стихийные бедствия и техногенные катастрофы (например, ураган может нарушить работу телекоммуникационной сети, а пожар уничтожить сервера с важной информацией).

Обеспечение безопасности операционных систем.

Под механизмами защиты ОС понимают все средства и механизмы защиты данных, функционирующие в составе ОС. Операционные системы, в составе которых функционируют средства и механизмы защиты данных, часто называют защищенными системами.

Под безопасностью ОС понимают такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы.

Адекватная политика безопасности.

Одной из наиболее важных задач администратора ОС являются выбор и поддержание адекватной политики безопасности. Если принятая в ОС политика безопасности неадекватна, то это может привести к НСД злоумышленника к ресурсам системы и к снижению надежности функционирования ОС.

Чем лучше защищена ОС, тем труднее с ней работать пользователям и администраторам. Это обусловлено следующими факторами:

1) система защиты не всегда способна определить, является ли некоторое действие пользователя злонамеренным. Поэтому система защиты либо не пресекает некоторые виды НСД, либо запрещает некоторые вполне легальные действия пользователей. Чем выше защищенность системы, тем шире класс тех легальных действий пользователей, которые рассматриваются подсистемой защиты как несанкционированные;

2) чем больше в ОС защитных функций, тем больше времени и средств нужно тратить на поддержание защиты;

3) подсистема защиты ОС, как и любой другой программный пакет, потребляет аппаратные ресурсы компьютера. Чем сложнее устроены защитные функции ОС, тем больше ресурсов компьютера (процессорного времени, оперативной памяти и др.) затрачивается на поддержание функционирования подсистемы защиты и тем меньше ресурсов остается на долю прикладных программ;

4) поддержание слишком жесткой политики безопасности может негативно сказаться на надежности функционирования ОС. Чрезмерно жесткая политика безопасности может привести к трудно выявляемым ошибкам и сбоям в процессе функционирования ОС и даже к ее краху.

Оптимальная адекватная политика безопасности — это такая политика безопасности, которая не только не позволяет злоумышленникам выполнять несанкционированные действия, но и не приводит к описанным выше негативным эффектам. Она определяется не только архитектурой ОС, но и ее конфигурацией, установленными прикладными программами и т. д. Формирование и поддержание адекватной политики безопасности ОС можно разделить на ряд этапов.

1. Анализ угроз. Администратор ОС рассматривает возможные угрозы безопасности данной ОС. Среди возможных угроз выделяются наиболее опасные, защите от которых нужно уделять максимум средств.

2. Формирование требований к политике безопасности. Администратор определяет, какие средства и методы будут применяться для защиты от тех или иных угроз. Например, защиту от НСД к некоторому объекту ОС можно решать либо средствами разграничения доступа, либо криптографическими средствами, либо используя некоторую комбинацию этих средств.

3. Формулируются необходимые требования к конфигурации ОС, а также требования к конфигурации дополнительных пакетов защиты, если установка таких пакетов необходима. В результате на этом этапе составляется развернутый перечень настроек конфигурации ОС и дополнительных пакетов защиты с указанием того, в каких ситуациях, какие настройки должны быть установлены.

4. Приведение конфигурации ОС и дополнительных пакетов защиты в соответствие с предыдущим этапом.

5. Контроль соблюдения политики безопасности администратором ОС и внесение в нее необходимых изменений по мере появления изменений в функционировании ОС.

Специальных стандартов защищенности ОС не существует. Для оценки защищенности ОС используются стандарты, разработанные для компьютерных систем вообще. Как правило, сертификация ОС по некоторому классу защиты сопровождается составлением требований к адекватной политике безопасности, при безусловном выполнении которой защищенность конкретного экземпляра ОС будет соответствовать требованиям соответствующего класса защиты.

Определяя адекватную политику безопасности, администратор ОС должен в первую очередь ориентироваться на защиту ОС от конкретных угроз ее безопасности.

1. Проблемы обеспечения безопасности ОС.

Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка ОС. Окружение, в котором функционирует ОС (доверенная вычислительная база), включает в себя полный набор элементов, обеспечивающих информационную безопасность: ОС, программы, сетевое оборудование, средства физической защиты.

Операционную систему называют защищенной, если она предусматривает средства защиты от основных классов угроз. Защищенная ОС обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с ОС. Кроме того, защищенная ОС должна содержать средства противодействия случайному или преднамеренному выводу ОС из строя.

Если ОС предусматривает защиту не от всех основных классов угроз, а только от некоторых, такую ОС называют частично защищенной.

Существуют два основных подхода к созданию защищенных ОС — фрагментарный и комплексный. При фрагментарном подходе вначале организуется защита от одной угрозы, затем от другой и т. д. Примером

фрагментарного подхода может служить ситуация, когда за основу берется незащищенная ОС, на нее устанавливаются: антивирусный пакет, система шифрования, система регистрации действий пользователей и т. д.

При применении фрагментарного подхода подсистема защиты ОС представляет собой набор разрозненных программных продуктов, как правило, от разных производителей. Эти программные средства работают независимо друг от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

При комплексном подходе защитные функции вносятся в ОС на этапе проектирования архитектуры ОС и являются ее неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации, поэтому конфликты между ее отдельными компонентами практически невозможны. Подсистема защиты, созданная на основе комплексного подхода, может быть устроена так, что при фатальных сбоях в функционировании ее ключевых элементов она вызывает крах ОС, что не позволяет злоумышленнику отключать защитные функции системы. При фрагментарном подходе такая организация подсистемы защиты невозможна.

Как правило, подсистему защиты ОС, созданную на основе комплексного подхода, проектируют так, чтобы отдельные ее элементы были заменяемы. Соответствующие программные модули могут быть заменены другими модулями.

2. Классификация угроз безопасности ОС.

Организация эффективной и надежной защиты ОС невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности ОС существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т. д. Например, если ОС используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же ОС используется как платформа провайдера Internet-услуг, очень опасны атаки на сетевое программное обеспечение ОС.

Угрозы безопасности ОС можно классифицировать:

1. По цели атаки:

а) несанкционированное чтение информации;

б) несанкционированное изменение информации;

в) несанкционированное уничтожение информации;

г) полное или частичное разрушение ОС.

2. По принципу воздействия на операционную систему:

а) использование известных (легальных) каналов получения информации; например угроза несанкционированного чтения файла, доступ

пользователей к которому определен некорректно, т. е. разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;

б) использование скрытых каналов получения информации; например угроза использования злоумышленником недокументированных возможностей ОС;

в) создание новых каналов получения информации с помощью программных закладок.

3. По типу используемой злоумышленником уязвимости защиты:

а) неадекватная политика безопасности, в том числе и ошибки администратора системы;

б) ошибки и недокументированные возможности программного обеспечения ОС, в том числе и так называемые люки — случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;

в) ранее внедренная программная закладка.

4. По характеру воздействия на операционную систему:

а) активное воздействие — несанкционированные действия злоумышленника в системе;

б) пассивное воздействие — несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Угрозы безопасности ОС можно также классифицировать по таким признакам, как: способ действий злоумышленника, используемые средства атаки, объект атаки, способ воздействия на объект атаки, состояние атакуемого объекта ОС на момент атаки.

3. Типичные атаки ОС.

ОС может подвергнуться следующим типичным атакам:

а) сканированию файловой системы. Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, который должен быть ему запрещен;

б) подбору пароля. Существуют несколько методов подбора паролей пользователей:

- тотальный перебор;
- тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;
- подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);

в) угрозы получения НСД путем подмены доверенного объекта (краже ключевой информации). Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой

информацией (смарт-карта, Touch Memory и т. д.) может быть просто украден;

г) сборке мусора. Во многих ОС информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Злоумышленник восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;

д) превышению полномочий. Злоумышленник, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя;

е) программным закладкам. Программные закладки, внедряемые в ОС, не имеют существенных отличий от других классов программных закладок;

ж) жадным программам. Это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху ОС;

з) модификация BIOS;

и) несанкционированный доступ с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т. п.);

к) угрозы сканирования, направленные на выявление типа операционной системы, информационной системы персональных данных, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.

4. Способы защиты ОС.

а) механизм аутентификации.

В защищенной ОС любой пользователь перед тем, как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию.

Идентификация заключается в том, что пользователь сообщает ОС идентификационную информацию о себе. Это может быть имя. Учетный номер и т. п. Для того, чтобы установить, что пользователь именно тот, за кого себя выдает, в информационных системах предусмотрена процедура аутентификации. Задача этой процедуры заключается в предотвращении доступа к системе нежелательных лиц. Пользователь предоставляет системе, помимо идентифицирующей информации, аутентифицирующую. (Например, пароль или шифр). То есть он должен подтвердить, что он именно тот пользователь, к которому относится идентификационная информация. После успешной идентификации и аутентификации происходит авторизация пользователя. При авторизации пользователя ОС

выполняет действия, необходимые для того, чтобы пользователь мог работать в системе. Например. Авторизация в операционной системе UNIX включает в себя создание процесса, являющегося операционной оболочкой, с которой в дальнейшем будет работать пользователь.

Для обеспечения безопасности ОС процедуры идентификации и аутентификации очень важны, так как если злоумышленник вошел в систему от имени другого пользователя, он легко получает доступ ко всем объектам ОС, к которым имел доступ этот пользователь.

Наиболее распространенными методами идентификации и аутентификации являются идентификация и аутентификация с помощью имени и пароля, с помощью внешних носителей ключевой информации, с помощью биометрических характеристик пользователя.

Значительно повысить надежность парольной защиты могут следующие меры: наложение технических ограничений (например, пароль не должен быть коротким, содержать различные символы, цифры, знаки пунктуации и т. д.), пароль должен периодически меняться, должно быть ограничено число попыток неудачных попыток входа в систему, ограничение доступа к файлу паролей.

б) управление доступом к объектам.

Средства управления доступом к объектам ОС позволяют контролировать действия, которые пользователи и процессы могут выполнять над объектами (информацией и другими компьютерными ресурсами). Основной механизм многопользовательских систем, призванный обеспечить конфиденциальность, целостность объектов и их доступность (путем запрещения обслуживания неавторизованных пользователей) - логическое управление доступом, которое реализуется с помощью программных средств.

Правила разграничения доступа, действующие в ОС, устанавливаются администраторами системы при определении текущей политики безопасности. За соблюдением этих правил следит монитор ссылок — часть подсистемы защиты ОС.

Выделяют следующие методы разграничения доступа: разграничение доступа по спискам, использование матрицы установления полномочий, по уровням секретности и категориям, парольное разграничение доступа.

Списки позволяют установить права с точностью до пользователя. Они используются в большинстве ОС и СУБД.

Матрица установления полномочий или матрица доступа (таблица полномочий). В ней строками являются идентификаторы субъектов, имеющих доступ к объектам, а столбцами – объекты (информационные ресурсы). Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

При **разграничении по уровню секретности** выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен.

Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем он имеет. При **разграничении по категориям** задается и контролируется ранг категории, соответствующей пользователю. Все ресурсы разграничивают по уровню важности, причем определенному уровню соответствует некоторый ранг персонала (руководитель, администратор, пользователь).

Парольное разграничение представляет собой использование методов доступа к объектам по паролю. При этом используются все методы парольной защиты.

На практике обычно сочетают различные методы разграничения доступа.

Программно-аппаратные средства защиты ОС обязательно должны дополняться административными мерами защиты. Основные административные меры защиты:

1. Постоянный контроль корректности функционирования ОС, особенно ее подсистемы защиты. Такой контроль удобно организовать, если ОС поддерживает автоматическую регистрацию наиболее важных событий (event logging) в специальном журнале.

2. Организация и поддержание адекватной политики безопасности. Политики безопасности ОС должна постоянно корректироваться, оперативно реагируя на попытки злоумышленников преодолеть защиту ОС, а также на изменения в конфигурации ОС, установку и удаление прикладных программ.

3. Инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с ОС и контроль соблюдения этих мер.

4. Регулярное создание и обновление резервных копий программ и данных ОС.

5. Постоянный контроль изменений в конфигурационных данных и политике безопасности ОС. Информацию об этих изменениях целесообразно хранить на неэлектронных носителях информации, для того чтобы злоумышленнику, преодолевшему защиту ОС, было труднее замаскировать свои несанкционированные действия.

В конкретных ОС могут потребоваться и другие административные меры защиты информации.

в) шифрующая файловая система.

На персональном компьютере операционную систему можно загрузить не с жесткого диска, а с других устройств (например, CD ROM, USB-носитель, гибкий диск, и др.). Это позволяет обойти проблемы, связанные с отказом жесткого диска и разрушением загрузочных разделов. Однако, поскольку с помощью гибкого диска можно загружать различные операционные системы, любой пользователь, получивший физический доступ к компьютеру, может обойти встроенную систему управления доступом файловой системы и с помощью определенных инструментов прочесть информацию жесткого диска.

Назначение шифрующей файловой системы - защита данных, хранящихся на диске, от несанкционированного доступа путем их шифрования.

Система шифрования файлов Encrypting File System (EFS) позволяет шифровать файлы и папки для защиты от несанкционированного доступа. Она полностью встроена в файловую систему NTFS и совершенно прозрачна для приложений. Когда пользователь или программа обращаются к зашифрованному файлу, операционная система автоматически пытается получить ключ расшифрования, после чего выполняет шифрование и расшифрование от имени пользователя. Пользователи, имеющие доступ к ключам, могут работать с зашифрованными файлами так, как будто они не зашифрованы, в то время как остальным пользователям доступ будет запрещен.

г) инфраструктура открытых ключей.

Инфраструктура открытых ключей (PKI - Public Key Infrastructure) — это система управления криптографической защитой, совокупность цифровых сертификатов открытых ключей и служб управления сертификатами. Основная задача PKI - распространение ключей и управление их жизненным циклом.

В задачи PKI входит определение политики цифровых сертификатов, выдача их и аннулирование, а так же хранение информации для последующей проверки правильности и актуальности сертификатов. Приложениями, которые поддерживает PKI, как правило, является защищенная электронная почта, протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом IP, электронные формы и документы с электронной цифровой подписью (ЭЦП).

Фактически, PKI представляет собой систему, основными компонентами которой являются Удостоверяющий центр и пользователи, взаимодействующие между собой посредством Удостоверяющего центра.

Идея PKI основана на том, что каждый узел имеет открытый и секретный ключ (SSL). SSL использует PKI для аутентификации OpenVPN узлов перед передачей шифрованных данных. Секретный ключ должен держаться в секрете, а открытый ключ должен распространяться через Сертификаты. Цель сертификата заверить, что открытый ключ принадлежит тому, кто утверждает, что это его ключ (т.е. владеет соответствующим секретным ключом).

Первоначально пользователь зашифровывает данные с помощью открытого ключа, далее сообщение передается адресату через сеть, и расшифровывается при получении с помощью личного ключа. Аутентификация зашифрованного сообщения происходит при помощи подписи отправителем сообщения личным ключом.

Центр сертификации (Certification Authority, CA) подписывает сертификаты своим секретным ключом и публикует свой открытый ключ в виде сертификата. CA сертификат подписывается собственным секретным ключом.

д) защита коммуникаций и средств удаленного доступа.

Защита коммуникаций подразумевает наличие защищенных, безопасных соединений типа клиент-клиент или клиент-сервер. Аутентификацию и защиту данных при связи через публичные сети помогают обеспечить такие протоколы, как Secure Sockets Layer (SSL), Transport Layer Security (TLS), Private Communication Technology (PCT).

После того, как клиенты установили защищенное соединение, они договариваются о том, какие криптографические алгоритмы будут использоваться в сеансе связи (RSA – при обмене ключами, RC4 – для шифрования данных, SHA и MD5 – для хеширования). Далее пользователи взаимно аутентифицируют друг друга с помощью сертификатов и генерируют ключи для шифрования и хеширования.

Защищенное соединение клиент-сервер реализуется средствами протоколов SSL/TLS. Последовательность алгоритма взаимодействия клиента с сервером имеет следующий вид:

Клиент посылает на сервер сообщение «ClientHello». Сервер отвечает клиенту откликом «ServerHello» и передает клиенту свой сертификат с открытым ключом. Клиент зашифровывает данные необходимые для передачи открытым ключом и отправляет на сервер. Сервер при получении зашифрованных данных расшифровывает их при помощи своего закрытого ключа.

Для удаленного доступа или связи клиент-клиент используется защищенное подключение по протоколу Point-to-Point Protocol (PPP), который имеет два уровня аутентификации: аутентификация средствами PPP и аутентификация в домене.

Кроме этого для передачи защищаемых данных используются виртуальные частные сети (VPN). VPN – это защищенное подключение клиента к серверу удаленного доступа через виртуальный туннель, созданный в открытой сети. Данные инкапсулируются и шифруются.

Для подключения клиент-сервер используется протокол PPTP (Point-to-point tunneling protocol - туннельный протокол типа точка-точка, устанавливающий между компьютерами защищённое соединение за счёт создания специального туннеля в незащищённой сети). Для шифрования данных использует модифицированный протокол MPPE.

е) IP Security.

IP Security – это набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

Фундаментальной единицей коммуникации в IP – сетях является IP – пакет. IP – пакет содержит адрес источника и адрес получателя сообщения, транспортный заголовок, информацию о типе данных, переносимых в этом пакете, а также сами данные. Пользователь воспринимает сеть как надежно защищенную только в том случае, если уверен, что его партнер по обмену именно тот, за кого он себя выдает (аутентификация сторон), что передаваемые данные не просматриваются другими пользователями (конфиденциальность связи) и, что получаемые данные не подверглись изменению в процессе передачи (целостность данных). Для того чтобы это

обеспечить, стек протоколов IPSec построен на базе ряда стандартизованных криптографических технологий.

IPSec представлен следующими компонентами: IPSec Driver - обеспечивает обработку пакетов; IPSec Filter, - указывает, какие пакеты и как нужно обрабатывать; IPSec Policy - отвечает за определение параметров IP Security для компьютеров; Internet Key Exchange (IKE) - организует переговоры между хостами при помощи протокола ISAKMP/Oakley.

IPsec может работать в транспортном режиме и туннельном.

В транспортном режиме зашифровывается (подписывается) информативная часть IP-пакета. Так как заголовок IP пакета не изменяется, не меняется и его маршрутизация. Транспортный режим используется в основном для установления соединения между рабочими станциями, но так же может использоваться между шлюзами, для защиты туннелей.

В туннельном режиме IP-пакет шифруется полностью. После этого он помещается в другой IP-пакет для передачи по сети, образуя защищённый туннель. Этот режим используется для подключения удалённых компьютеров к виртуальной частной сети или для безопасной передачи данных по сетям общего доступа (Интернет).

ж) аппаратно-программный модуль доверенной загрузки (АПМДЗ).

Под доверенной загрузкой обычно понимается загрузка операционной системы с внутреннего жесткого диска компьютера, которая происходит только после выполнения процедур идентификации и аутентификации пользователя, а также проверки целостности программной и аппаратной среды рабочего места, в том числе целостности объектов загружаемой ОС. При этом должна обеспечиваться невозможность загрузки пользователем другой ОС (с внешних носителей информации и др.).

Модуль доверенной загрузки представляет собой комплекс аппаратно-программных средств, устанавливаемый в рабочее место вычислительной системы (персональный компьютер, сервер, ноутбук, специализированный компьютер и др.) и обеспечивающий контроль доступа пользователя к рабочему месту и контроль целостности программной среды рабочего места.

Модули доверенной загрузки обеспечивают выполнение следующих основных функций:

а) идентификация и аутентификация пользователей до загрузки ОС с помощью персональных электронных идентификаторов;

б) блокировка несанкционированной загрузки ОС с внешних съемных носителей;

в) контроль целостности объектов системы, объектов пользователя и программного обеспечения МДЗ до загрузки ОС;

г) регистрация действий пользователей и программ;

д) предоставление возможностей для внешних приложений (работа с датчиком случайных чисел, работа с электронными идентификаторами и т.д.).

При первичной настройке МДЗ назначается администратор модуля, который обладает привилегиями на регистрацию и удаление пользователей,

управление параметрами работы модуля, просмотр журнала событий и управление списком объектов, целостность которых должна контролироваться до загрузки операционной системы. В случае появления нарушений при проверке целостности объектов возможность работы на компьютере для обычных пользователей блокируется. В некоторых МДЗ реализована поддержка возможности удаленного управления параметрами работы.

Модули доверенной загрузки, как правило, реализуются на базе плат с системными шинами PCI, PCI-X, PCI Express, mini-PCI, mini-PCI Express, которые могут включать следующие компоненты:

- программируемая логическая интегральная схема (для реализации интерфейса по шине и выполнения функций по работе с другими компонентами платы) и микросхема памяти для хранения кода загрузчика интегральной схемы;
- микросхема flash-памяти с программным расширением BIOS компьютера, которое получает управление до старта операционной системы и обеспечивает выполнение основных функций МДЗ. Код программного расширения BIOS выполняется в центральном процессоре компьютера;
- микросхема микроконтроллера для защищенной реализации специальных функций МДЗ (например, для взаимодействия с некоторыми компонентами платы или для кода, выполнение которого не в центральном процессоре компьютера повышает его защищенность от перехвата и модификации злонамеренными программами);
- знергонезависимая память, предназначенная для хранения настроек МДЗ, журналов событий и других данных;
- блок управления сторожевым таймером (watch dog), который не позволяет работать с компьютером в случае, если программное расширение BIOS модуля не получило управления. Данный механизм не позволит получить доступ к компьютеру посредством специальной настройки параметров BIOS или в случае системного сбоя;
- блок датчика случайных чисел, необходимый для аппаратной выработки последовательностей случайных величин;
- блок часов реального времени, предназначенный для независимого замера времени с целью обеспечения защищенной реализации механизмов периодического устаревания критичных данных, а также других функций МДЗ;
- разъемы различных типов для подключения электронных идентификаторов (iButton, USB);
- переключатели для изменения режимов работы МДЗ.

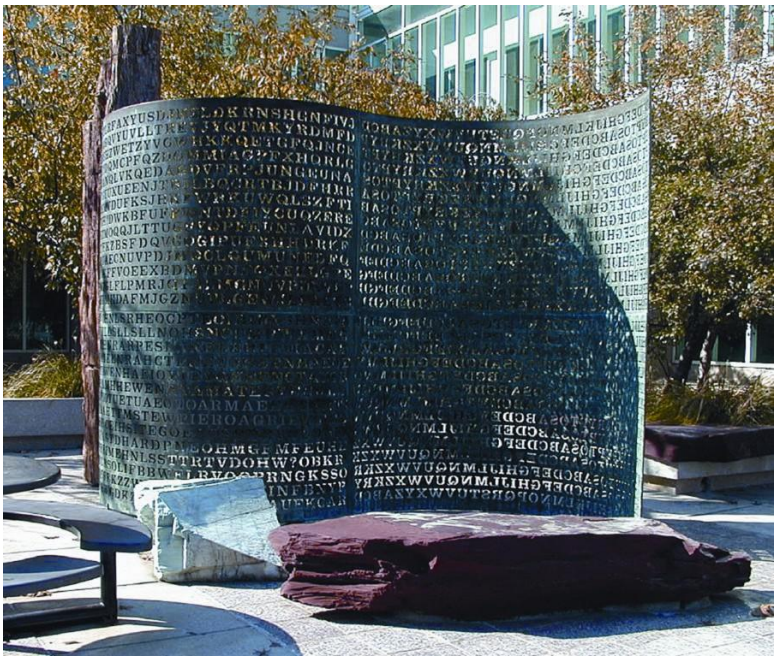
Кроме того, в состав МДЗ может входить программное обеспечение для поддерживаемых ОС, которое обычно включает драйвер, программу управления и интерфейсный модуль API для внешних приложений.

Современные МДЗ поддерживают работу на компьютерах как с ОС семейства MS Windows, так и с рядом ОС семейства UNIX/Linux.

Обеспечение безопасности данных.

1. Криптографическая защита информации.

Криптография появилась практически одновременно с письменностью. Письменность всегда была предназначена для того, чтобы фиксировать и передавать информацию. Далеко не всегда хотели, чтобы она попала в чужие руки. Официально история криптографии началась 4 тыс. лет назад. Первым известным применением криптографии принято считать использование специальных иероглифов около 4000 лет назад в Древнем Египте. С тех пор было придумано много способов шифрования информации.



У криптографии даже есть свои памятники – это статуя Криптос, у офиса ЦРУ в США. Она представляет собой 4 страницы с 4 зашифрованными посланиями, которые сделал американский художник Джеймс Санборн. На сегодняшний момент расшифрованы только 3 из 4 посланий.

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает «тайнопись») зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных.

Для обеспечения безопасности данных необходимо поддерживать три основные функции: защиту конфиденциальности передаваемых или хранимых в памяти данных, подтверждение целостности и подлинности данных, аутентификацию абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

а) системы шифрования.

Существует множество различных алгоритмов шифрования. Некоторые, например, DES, используют секретный, или закрытый ключ. Другие, например, RSA, используют открытый и отдельный закрытый ключи.

Шифрование с закрытым ключом основано на том, что доступ к ключу имеет только авторизованный персонал. Этот ключ должен держаться в секрете. Если ключ попадет к постороннему, то он может получить несанкционированный доступ к зашифрованной информации.

Наиболее широко используемым алгоритмом с закрытым ключом является стандарт Data Encryption Standard (DES). Этот алгоритм, разработанный компанией IBM в семидесятых годах прошлого века, принят в качестве американского стандарта для коммерческих и несекретных правительственных коммуникаций. Современные скорости вычислений на порядок превышают скорости вычислений в семидесятых годах, поэтому алгоритм DES считается устаревшим как минимум с 1998 года.

Другие известные системы шифрования с закрытым ключом — это RC2, RC4, RC5, тройной DES (triple DES) и IDEA. Тройной DES-алгоритм обеспечивает достаточную степень защиты. Этот алгоритм использует тот же метод шифрования, что и DES, но применяет его трижды, используя при этом до трех разных ключей. Открытый текст шифруется с использованием первого ключа, дешифруется при помощи второго ключа, а затем шифруется с применением третьего ключа.

Явный недостаток алгоритмов с закрытым ключом состоит в том, что для отправки кому-то защищенного сообщения необходимо располагать безопасным способом передачи этому лицу закрытого ключа. А если у нас есть безопасный метод передачи ключа, то этим же методом можно воспользоваться и для передачи сообщений.

Шифрование с открытым ключом базируется на двух различных ключах - открытом и закрытом.

В 1976 году Уитфилд Диффи и Мартин Хеллман опубликовали работу «Новые направления в криптографии» (англ. «New Directions in Cryptography»). Это был первый алгоритм шифрования с открытым ключом. Он позволял сторонам сгенерировать общий секретный ключ, используя только открытый канал. Одним из результатов публикации стал значительный рост числа людей, занимающихся криптографией.

Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов — Rivest, Shamir и Adleman). Опубликованная в августе 1977 года работа позволила сторонам обмениваться секретной информацией, не имея заранее выбранного секретного ключа. Опасаясь распространения системы в негосударственных структурах, АНБ безуспешно требовало прекращения распространения системы. RSA используется во всём мире и, на 1996 год, являлся стандартом де-факто для шифрования с открытым ключом. Черновики стандарта ISO для цифровой подписи и банковского стандарта ANSI основаны на RSA, также он служит информационным дополнением для ISO 9796, принят в качестве стандарта во Французском банковском сообществе и в Австралии. В США, из-за давления АНБ, стандарты на шифрование с открытым ключом или цифровую подпись отсутствуют, хотя большинство компаний использует стандарт PKCS #1, основанный на RSA.

RSA, и алгоритм Диффи — Хеллмана были впервые открыты в английских спецслужбах в обратном порядке, но не были ни опубликованы, ни запатентованы из-за секретности

В России для шифрования с открытым ключом стандарт отсутствует, однако для электронной цифровой подписи (органически связанной с шифрованием с открытым ключом) принят стандарт ГОСТ Р 34.10-2001, использующий криптографию на эллиптических кривых.

В августе 2015 года в США АНБ опубликовало заявление о необходимости разработки новых стандартов для постквантовой криптографии, или PQC.

Для всех широко применяемых ныне алгоритмов и протоколов криптографии с открытым ключом (построенных на базе схем RSA и ECC, то есть криптографии на эллиптических кривых) стойкость выстроена на основе двух трудных в решении задач математики – разложения большого целого числа на пару простых сомножителей (что именуют факторизацией) и вычисления дискретного логарифма. Для обычных – классических – компьютеров обе задачи решить за приемлемое время считается невозможным. Таких методов решения пока никто не продемонстрировал.

В начале 1990-х ученые вплотную занялись теорией создания компьютеров существенно новых, «квантовых» (работающих на основе принципов квантовой механики). Очень быстро обнаружились квантовые методы для быстрого решения именно этих двух задач криптографии – факторизации и дискретного логарифмирования. То есть большая проблема с надежностью засекречивания коммуникаций обозначилась уже весьма давно, более 20 лет назад.

Однако никаких конкретных шагов по решению этой проблемы никто все эти годы не предпринимал, так как задача построения реального квантового компьютера для решения подобных задач сама по себе представляет гигантскую научно-техническую проблему. До сих пор как эффективно решить данную проблему неизвестно. Шаги по созданию квантовых компьютеров предприняты в таких условиях, когда мировая криптографическая наука все еще не нашла тех самых трудных математических задач, которые окажутся гарантированно не по зубам для этих компьютеров.

Как и многие из других сторон, участвующих в этом процессе, АНБ заявило, что считает настоящий момент наиболее подходящим временем для того, чтобы вплотную заняться разработкой новых протоколов для криптографии с открытым ключом. Такой криптографии, где стойкость также будет зависеть от трудных задач математики, но только теперь это должны быть иные трудные задачи – не поддающиеся эффективному решению с помощью квантовых компьютеров.

Американский математик и криптограф Нил Коблиц является (наряду с Виктором Миллером) одним из тех двух человек, которые в 1985 году одновременно и независимо друг от друга придумали новую криптосхему с открытым ключом, получившую название ECC (Elliptic Curve Cryptography, то есть «криптография на эллиптических кривых»).

б) электронная цифровая подпись.

Цифровые подписи относятся к криптографическим алгоритмам с открытым ключом, но с измененными ролями открытого и закрытого ключей. Отправитель может зашифровать и подписать сообщение своим закрытым ключом. Когда сообщение получено, получатель может дешифровать его, используя открытый ключ отправителя. Ввиду того, что отправитель — это единственное лицо, обладающее доступом к закрытому ключу, то получатель достаточно точно знает, от кого получено сообщение, а также может быть уверен, что сообщение не было изменено.

Цифровые подписи гарантируют получателю, что сообщение не подделано, а также не позволяют отправителю отказаться от обязательств, отрицая факт отправки сообщения. Хотя сообщения шифруются, их может прочитать любой обладатель открытого ключа. Назначением шифрования является не запретить чтение, а предотвратить подделку и отказ от обязательств. Так как алгоритмы с открытым ключом работают достаточно медленно с большими сообщениями, для повышения производительности обычно используется алгоритм другого типа, называемый хеш-функцией.

Хэширование - преобразование массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины, называемой хэш-кодом, проверочной суммой или цифровым отпечатком, которое выполняется по определённому алгоритму. Функция, реализующая алгоритм и выполняющая преобразование, называется «хэш-функцией» или «функцией свёртки».

Хэш-функция вычисляет дайджест, или хэш-значение, для каждого указанного сообщения. Совершенно не важно, какое значение генерирует алгоритм. Важно, что результат этой функции будет одним и тем же каждый раз, когда на вход передаются одни и те же данные. Кроме того, важно, что результат имеет небольшой размер, и алгоритм быстро работает. Располагая сообщением и его дайджестом, можно убедиться, не подделывалось ли сообщение, но только в том случае, если дайджест не был подделан вместе с ним. Особенностью хэш-функций является то, что они не допускают обратного преобразования – получить исходное сообщения по его дайджесту невозможно. Поэтому их называют еще односторонними функциями шифрования.

Блоки данных, которые могут быть подписаны непосредственно, ограничены по размеру: они не могут выходить за пределы используемой при работе алгоритмов разрядной сетки. В то же время может возникнуть потребность разработки ЭЦП для документа произвольного размера. Чтобы преодолеть данное ограничение, в схемах ЭЦП принято подписывать не непосредственно электронный документ, а результат его преобразования к блоку данных фиксированного размера, называемого хэшем (hash) сообщения.

Алгоритм выработки хэша должен обладать следующими свойствами:

- для входного массива данных произвольного размера результатом должен быть блок данных фиксированного размера;

- для заданного хэша не должно быть способа подбора массива данных под него более эффективным способом, чем перебор по возможным значениям массива данных;

- не должно существовать вычислительно эффективного способа поиска двух массивов данных с одинаковым значением хэша.

в) криптоключи.

Криптосистема основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами очевиден, то в информационных системах, где количество пользователей составляет десятки и сотни, управление ключами - серьезная проблема. Если не обеспечено достаточно надежное управление ключевой информацией, то завладев ею, злоумышленник получает неограниченный доступ ко всей информации. Управление ключами включает в себя: **генерацию ключей**, **накопление ключей**, **распределение ключей**.

В серьезных информационных системах используются специальные аппаратные и программные методы **генерации случайных ключей**. Степень случайности их генерации должна быть достаточно высокой. Идеальным генераторами являются устройства на основе “натуральных” случайных процессов. Например, случайным математическим объектом являются десятичные знаки иррациональных чисел, которые вычисляются с помощью стандартных математических методов.

Под **накоплением ключей** понимается организация их хранения, учета и удаления. Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей уделяют особое внимание. Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован. В достаточно сложной информационной системе один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей. Каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию, называются мастер - ключами. Очень важным условием безопасности информации является периодическое обновление ключевой информации в информационной системе.

Распределение ключей - самый ответственный процесс в управлении ключами. К нему предъявляются два требования: оперативность и точность распределения, скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения ключей отпадает.

2. Аудентификация, авторизация и администрирование действий пользователя.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности.

Идентификация позволяет субъекту - пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова "аутентификация" иногда используют сочетание "проверка подлинности".

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть. Пароль можно угадать методом грубой силы, используя, быть может, словарь. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Пароли уязвимы по отношению к электронному перехвату - это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход - использование криптографии для шифрования паролей перед передачей по линиям связи.

Следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему, что затруднит применение метода грубой силы;
- обучение и воспитание пользователей;
- использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации, основанные, например, на применении токенов.

Токен - это предмет или устройство, владение которым подтверждает подлинность пользователя. Различают токены с памятью (пассивные, которые только хранят, но не обрабатывают информацию) и интеллектуальные токены (активные).

Самой распространенной разновидностью токенов с памятью являются карточки с магнитной полосой. Для использования подобных токенов необходимо устройство чтения, снабженное также клавиатурой и процессором. Обычно пользователь набирает на этой клавиатуре свой личный идентификационный номер, после чего процессор проверяет его совпадение с тем, что записано на карточке, а также подлинность самой

карточки. Таким образом, здесь фактически применяется комбинация двух способов защиты, что существенно затрудняет действия злоумышленника.

Интеллектуальные токены характеризуются наличием собственной вычислительной мощности. Они подразделяются на интеллектуальные карты, стандартизованные ISO и прочие токены. Карты нуждаются в интерфейсном устройстве, прочие токены обычно обладают ручным интерфейсом (дисплеем и клавиатурой) и по внешнему виду напоминают калькуляторы. Чтобы токен начал работать, пользователь должен ввести свой личный идентификационный номер.

По принципу действия интеллектуальные токены можно разделить на следующие категории:

Статический обмен паролями, когда пользователь обычным образом доказывает токену свою подлинность, затем токен проверяется компьютерной системой;

Динамическая генерация паролей: токен генерирует пароли, периодически изменяя их. Компьютерная система должна иметь синхронизированный генератор паролей. Информация от токена поступает по электронному интерфейсу или набирается пользователем на клавиатуре терминала;

Запросно-ответные системы: компьютер выдает случайное число, которое преобразуется криптографическим механизмом, встроенным в токен, после чего результат возвращается в компьютер для проверки. Здесь также возможно использование электронного или ручного интерфейса. В последнем случае пользователь читает запрос с экрана терминала, набирает его на клавиатуре токена (возможно, в это время вводится и личный номер), а на дисплее токена видит ответ и переносит его на клавиатуру терминала.

Сетевая безопасность.

Движущая сила и главный объект всех отраслей человеческой деятельности в наше время - информация. Состояние каналов, сетей и безопасность серверов становятся основой экономического развития. Сложные сетевые технологии достаточно уязвимы для целенаправленных атак. Такие атаки могут производиться удаленно, в том числе и из-за пределов национальных границ. Все это ставит новые проблемы перед разработчиками и строителями информационной инфраструктуры. Некоторые современные формы бизнеса полностью базируются на сетевых технологиях (электронная торговля, IP-телефония, сетевое провайдерство и т.д.) и по этой причине особенно уязвимы.

Основным источником сетевых уязвимостей являются дефекты программ и особенности каналов связи.

1.Виды атак. (DDos атаки, сканирование портов, атаки-вторжения).

DoS (от англ. Denial of Service — отказ в обслуживании) — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам

(серверам), либо этот доступ затруднён**.** В общем потоке атак DoS-атаки занимают до 27%.

Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS**-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). В первом полугодии 2016 года регистрировались до 2000 DDoS-атак ежедневно. Если в 2008 году мощность DDoS-атак достигала 40Гбит/с, то в 2014-ом превысила 400 Гбит/с. Ущерб от этих атак в 2012 году составил 1 млн. долларов в день (США).

DoS и DDoS атаки предназначены для нарушения нормального функционирования системы, которое обычно дополняется нехваткой ресурсов, необходимых для работы сети, операционной системы или приложений.

Классификация DDoS-атак.

Сетевой флуд – атака, которая заключается в отправке большого количества бессмысленных или неправильно сформированных запросов к компьютерной системе или сетевому оборудованию с целью отказа оборудования из-за исчерпания системных ресурсов (процессора, памяти или каналов связи).

Атака на исчерпание системных ресурсов. Атакующие прибегают к данному виду атаки для захвата таких ресурсов как оперативная и физическая память, процессорное время и т.д.

Недостаточная проверка данных пользователя. Может приводить к бесконечному или длительному циклу, что приводит к повышенному и продолжительному потреблению процессорных ресурсов либо выделению больших объемов памяти, вплоть до ее исчерпания.

Атаки второго рода. Это атаки, которые приводят к ложным срабатываниям систем защиты, тем самым приводят к недоступности определенных ресурсов.

HTTP-флуд. Атакующий отсылает небольшие http-пакеты, которые заставляют в свою очередь отвечать сервер пакетами, размеры которых значительно больше. Тем самым злоумышленник имеет большой шанс насытить полосу пропускания жертвы и вызвать отказ в работе сервисов. Для того, чтобы ответные пакеты не вызывали отказ в обслуживании у атакующего, он подменяет свой сетевой адрес на адреса узлов в сети.

Smurf-атака (ICMP-флуд). Данный тип атаки является одним из самых опасных. В ней по широковещательному адресу злоумышленник отправляет поддельный ICMP-пакет, в котором адрес атакующего меняется на адрес жертвы. Все узлы присылают ответ на данный ping-запрос. Для такого вида атаки обычно используют большую сеть, чтобы у компьютера-жертвы не было никаких шансов. Таким образом, запрос, отправленный через сеть в 1000 компьютеров, будет усилен в 1000 раз.

Fraggle (UDP-флуд). Данный тип атаки является аналогом ICMP флуда, но вместо ICMP пакетов используются UDP пакеты. На седьмой порт жертвы отправляются ECHO-команды по широковещательному запросу. После чего подменяется IP-адрес злоумышленника на IP-адрес

жертвы, которая получает множество ответных сообщений, что приводит к насыщению полосы пропускания и отказу в обслуживании жертвы.

SYN-флуд. Данный вид атаки основан на попытке запуска большого числа одновременных TCP-соединений через посылку SYN-пакета с несуществующим обратным адресом. После нескольких попыток отослать в ответ ACK-пакет на недоступный адрес большинство операционных систем ставят неустановленное соединение в очередь. И только после n-ой попытки закрывают соединение. Поскольку поток ACK-пакетов очень большой, вскоре очередь оказывается заполненной, и ядро дает отказ на попытки открыть новое соединение.

Отправка «тяжелых пакетов». Атакующий отсылает пакеты серверу, которые не насыщают полосу пропускания, а тратят все его процессорное время. Соответственно, в системе может пройти сбой и легальные пользователи не смогут получить доступ к необходимым ресурсам.

Переполнение сервера лог - файлами. При неправильной системе ротации лог - файлов и неправильно установленной системе квотирования злоумышленник может отправлять большие по объему пакеты, которые вскоре займут все свободное место на жестком диске сервера.

Ошибки программного кода. Опытные реализаторы DDoS-атак, полностью разобравшись в структуре жертвы, пишут программы-эксплоиты, которые позволяют атаковать сложные системы коммерческих предприятий и организаций. В основном это ошибки в программном коде, которые позволяют выполниться недопустимой инструкции или исключительной ситуации, которая может привести к аварийному завершению службы.

Недостатки в программном коде. Злоумышленники ищут ошибки в программном коде каких-либо программ либо операционных систем и заставляют их обрабатывать исключительные ситуации, которые они обрабатывать не умеют, что приводит к падению ядра или краху всей системы в целом.

Сканирование портов – данные угрозы сами по себе атакой не являются, но, как правило, ей предшествуют, так как это один из способов получить информацию об удаленном компьютере. Суть данного способа заключается в сканировании UDP/TCP-портов, которые используются сетевыми сервисами на нужном компьютере для выявления их состояния. Такой процесс помогает понять, какие атаки на данную систему могут быть удачными, а какие нет. Более того, сканирование дает злоумышленнику необходимые сведения об операционной системе, что позволяет подобрать еще более подходящие типы атак.

Атаки-вторжения. Их цель – «захват» системы. Такой тип атак самый опасный, так как при успешном их выполнении злоумышленник получает максимально полную информацию о системе. Атаки-вторжения применяются в тех случаях, когда есть необходимость в получении конфиденциальных данных с удаленного компьютера, такие как пароли и доступ к кредитным картам. Также целью таких атак может быть закрепление в системе для того, чтобы впоследствии в целях

злоумышленника использовать ее вычислительные ресурсы. К данной группе относится самое большое количество атак.

Более распространенные виды атак, которые используют сетевые сервисы операционной системы:

- Атаки на переполнение буфера. Этот тип уязвимостей в программном обеспечении, который возникает из-за отсутствия или недостаточной меры контроля при работе с массивами данных.

- Атаки, основанные на ошибках форматных строк. Такой тип возникает из-за недостаточной степени контроля значений входных параметров функций форматного ввода-вывода. В том случае, если такая уязвимость находится в программном обеспечении, то злоумышленник может получить абсолютный контроль над системой.

Все меры противодействия DDoS-атакам можно разделить на пассивные, запускаемые один раз и действующие сами по себе, и активные, для нормального функционирования которых необходимо присутствие и контроль со стороны человека. Также их можно разделить на превентивные, используемые для того, чтобы предупредить возникновение DDoS-атак, и реакционные, используемые при возникновении угрозы или устранения последствий DDoS-атаки.

Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки. В число анализируемых шаблонов нестандартного трафика входят все известные на сегодняшний день методы атак, в том числе реализуемые и при помощи распределённых бот-сетей.

2. Способы защиты от основных видов атак.

Методологической основой стандартизации в компьютерных сетях является многоуровневый подход к разработке средств сетевого взаимодействия. На основе предложений Международного института стандартов ISO (International Standards Organization) в начале 1980-х годов была разработана стандартная модель взаимодействия открытых систем OSI (Open System Interconnection).

В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представительный, транспортный, сетевой, канальный и физический. Самый верхний уровень – прикладной. На этом уровне пользователь взаимодействует с приложениями. Самый нижний уровень – физический. Этот уровень обеспечивает обмен сигналами между устройствами.

Обмен данных через каналы связи происходит путем перемещения данных с верхнего уровня на нижний. Затем транспортировке по линиям связи и обратным воспроизведением данных в компьютере клиента в результате их перемещения с нижнего уровня на верхний.

а) защита на прикладном уровне.

Прикладной уровень отвечает за доступ приложений в сеть. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и

управление сетью. Прикладной уровень – это в действительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message).

Существует очень большое разнообразие служб прикладного уровня.

К числу наиболее распространенных протоколов верхних уровней относятся: X.400 - электронная почта, Telnet, SMTP - простой протокол почтового обмена, CMIP - общий протокол управления информацией, SNMP - простой протокол управления сетью, NFS - сетевая файловая система, FTAM - метод доступа для переноса файлов.

Задача защиты на прикладном уровне состоит в выявлении и в фиксировании факта того, что несанкционированное событие произошло. Основой защиты на прикладном уровне должна являться непрерывная регистрация событий, происходящих в системе, и их контроль, посредством сравнения с заданным (эталонным) списком санкционированных событий. На любое зарегистрированное в системе несанкционированное событие соответствующий механизм прикладного уровня должен вырабатывать реакцию, призванную минимизировать последствия несанкционированного события, например, завершать несанкционированный процесс.

б) защита на представительном уровне.

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и EBCDIC. На этом уровне может выполняться сжатие, шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

в) защита на транспортном уровне.

Транспортный уровень обеспечивает приложениям или верхним уровням стека - прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное - способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней, а с другой стороны - насколько надежной является система транспортировки данных в сети, обеспечиваемая уровнями, расположенными ниже транспортного (сетевым, канальным и физическим).

Наиболее распространенные протоколы транспортного уровня включают: TCP (протокол управления передачей), NCP (Netware Core Protocol), SPX (упорядоченный обмен пакетами), TP4(протокол передачи класса 4).

Стек протоколов IPSec используется для аутентификации участников обмена, туннелирования трафика и шифрования IP-пакетов. Основное назначение протокола IPSec (Internet Protocol Security) — обеспечение безопасной передачи данных по сетям IP.

г) защита на сетевом уровне.

Радикальное устранение уязвимостей компьютерных сетей возможно при создании системы защиты не для отдельных классов приложений, а для сети в целом. Применительно к IP-сетям это означает, что системы защиты должны действовать на сетевом уровне модели OSI.

При формировании защищенных виртуальных каналов на сетевом уровне модели OSI достигается оптимальное соотношение между прозрачностью и качеством защиты. На сетевом уровне существует возможность достаточно полной реализации функций защиты трафика и управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений.

д) защита на канальном уровне.

Защита информации в процессе ее передачи по открытым каналам компьютерных сетей основана на построении виртуальных защищенных каналов связи, называемых криптозащищенными туннелями или туннелями. Каждый туннель представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты свободной виртуальной сети.

Протоколы PPTP (Point-to-Point Tunneling Protocol) и L2TP (Layer-2 Tunneling Protocol) являются протоколами туннелирования канального уровня модели OSI. Общим свойством этих протоколов является то, что они используются для организации защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через открытую сеть, например Интернет.

Оба протокола обычно относят к протоколам формирования защищенного канала, однако этому определению точно соответствует только протокол PPTP, который обеспечивает туннелирование и шифрование передаваемых данных. Протокол L2TP является протоколом туннелирования, так как поддерживает только функции туннелирования. Функции защиты данных (шифрование, целостность, аутентификация) в этом протоколе не поддерживается. Для защиты туннелируемых данных в

протоколе L2TP необходимо использовать дополнительный протокол, в частности IPSec.

е) защита на физическом уровне.

Защита на физическом уровне – это контроль электромагнитных излучений линий связи и устройств, поддержка коммутационного оборудования в рабочем состоянии. Защита обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

ж) межсетевое экранирование.

Межсетевой экран – аппаратные и программные средства защиты сетей. Межсетевой экран осуществляет контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданной политикой безопасности, блокирует нежелательную сетевую активность и уведомляет о попытках нарушения заданных правил.

з) защищенные сети VPN.

VPN-канал (virtual private network – частная виртуальная сеть) – это защищенный канал связи между удаленными компьютерами и/или подсетями через небезопасную среду (обычно через интернет). На практике VPN-каналы позволяют организовать компьютеры различных подразделений/филиалов компании в единую защищенную сеть, работающую через обычный интернет.

Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются туннелями VPN. Сеть VPN позволяет с помощью туннелей VPN соединить центральный офис, офисы филиалов, офисы бизнес - партнеров и удаленных пользователей и безопасно передавать информацию через Интернет.

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети. Защита информации в процессе ее передачи по туннелю VPN основана на аутентификации взаимодействующих сторон, криптографическом шифровании передаваемых данных и проверке подлинности и целостности доставляемой информации.

Для этих функций характерна взаимосвязь друг с другом. При их реализации используются криптографические методы защиты информации. Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, которая развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

Защита от вредоносных программ и спама.

Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузке.

В соответствии со способом распространения и вредоносной нагрузки все вредоносные программы можно разделить на четыре основных типа:

– **«компьютерные вирусы».** Вирус вносит свой код одну из программ, либо маскируется отдельной программой в том месте, куда обычно пользователи не заходят (папки с операционной системой, скрытые системные папки). Вирус не может запуститься сам, пока мы сами не запустим зараженную программу.

– **«черви».** Черви чаще всего проникают в систему сами, используя уязвимости ОС, браузера, определенной программы. Они могут проникать через чаты, программы для общения, такие как skype, могут распространяться через электронную почту. Так же они могут быть на сайтах, и, используя уязвимость браузера, проникнуть систему. Черви обладают способностью перемещаться в пределах системы или сети и размножаться аналогично вирусам. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке работы

Черви стараются писать под самые популярные программы. Например, сейчас самый популярный браузер «Chrome», поэтому мошенники будут стараться писать под него, и делать вредоносный код на сайты под него. Потому что часто интереснее заразить тысячи пользователей, которые используют популярную программу, чем сотню с непопулярной программой. Хотя Chrome и постоянно улучшает защиту.

– **«троянский конь»** — такие программы «скрываются» под видом полезного приложения, а, на самом деле, наносят вред компьютеру: разрушают программное обеспечение, копируют и пересылают злоумышленнику файлы с конфиденциальной информацией;

– другие программы.

Для того, чтобы обнаружить, удалить или защитить компьютер от вирусов, разрабатываются специальные программы. Эти программы называются антивирусными и представляют собой многофункциональный продукт, который сочетает в себе такие средства как: превентивные, профилактические, средства «лечения» или удаления, а также восстановления нарушенных или потерянных данных.

Антивирусные программы делятся на определенные типы:

Программы-детекторы – те, которые помогают найти вирусы в оперативной памяти или же на носителях информации, при этом программы-детекторы найденные вирусы не лечат.

Программы-доктора – программы, которые в отличие от предыдущего вида, не только находят вирус, но и лечат зараженный файл, возвращая его в исходное состояние.

Программы-ревизоры – такие программы имеют свойство запоминать файл или системную область диска в его исходном состоянии, и позже сравнивать текущее состояние с исходным. При сравнении файла учитываются многие параметры файла, поэтому скрыться вирусу такие программы не оставляют шанса.

Программы-фильтры – предназначены для выявления подозрительных действий в работе компьютера. При попытке активизации вируса программа может блокировать его работу.

Вакцины – такие программы, которые сразу предотвращают заражение различных файлов. Стоит применять такие программы, если программы-доктора отсутствуют. Но стоит учесть, что «вакцинация» возможна только против уже известных вирусов.

Абсолютной защиты от вредоносных программ не существует. Но с помощью некоторых мер можно существенно снизить риск заражения вредоносными программами.

Наиболее эффективные меры для повышения безопасности:

- использовать операционные системы, не дающие изменять важные файлы без ведома пользователя;
- своевременно устанавливать обновления;
- использовать антивирусные продукты;
- постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере и изменить системные настройки. Но это не защитит персональные данные от вредоносных (Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, ransomware шпионского ПО) и потенциально-нежелательных программ (Adware, Hoax), имеющих доступ к файлам пользователя, к которым ограниченная учетная запись имеет разрешение на запись и чтение (например, домашний каталог — подкаталоги /home в GNU/Linux, Documents and settings в Windows XP, папка «Пользователи» в Windows 7,8,8.1,10), к любым папкам, в которые разрешена запись и чтение файлов, или интерфейсу пользователя (как делают пользовательские программы для создания снимков экрана или изменения раскладки клавиатуры);
- ограничить физический доступ к компьютеру посторонних лиц;
- использовать внешние носители информации только от проверенных источников на рабочем компьютере;
- не открывать компьютерные файлы, полученные от ненадёжных источников, на рабочем компьютере;
- использовать межсетевой экран (аппаратный или программный), контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь;
- использовать второй компьютер (не для работы) для запуска программ из малонадежных источников, на котором нет ценной информации, представляющей интерес для третьих лиц;
- делать резервное копирование важной информации на внешние носители и отключать их от компьютера (вредоносное ПО может шифровать или ещё как-нибудь портить найденные им файлы).

6. Требования по защите информации от НСД для автоматизированных систем.

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

7. Подтверждение защищенности информационных систем.

Подтверждение защищенности той или иной системы от НСД осуществляется Федеральной службой по техническому и экспортному контролю России (ФСТЭК России). Требования по защите информации в государственных информационных системах утверждены приказом ФСТЭК России от 11 февраля 2013г. №17.

В соответствии с данным приказом в зависимости от значимости обрабатываемой в системе информации и масштаба информационной системы (федеральный, региональный, объектовый) проводится ее классификация. Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый. Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей). Требование к классу защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы.

Результаты классификации информационной системы оформляются актом классификации.

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие ее структуру и состав, физические, логические, функциональные и технологические взаимосвязи между ее сегментами и иными информационными системами, информационно-телекоммуникационными сетями. Учитываются режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

В соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. №17 для каждой государственной информационной системы должна разрабатываться модель угроз безопасности информации. Данная модель должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085. Модель угроз и нарушителя разрабатывается с учетом характеристик угроз безопасности информации (УБИ), представленных в «Банке данных угроз» ФСТЭК России (www.bdu.fstec.ru). В настоящее время в этом банке данных содержатся описания 194 угроз безопасности и 15176 уязвимостей программного обеспечения. На основе этих данных для конкретной системы создается актуальный перечень угроз информационной безопасности. В качестве метода оценки уязвимостей системы информационной безопасности (СИБ), возможностей и способов реализации УБИ, а также актуализации нарушителей безопасности используется метод экспертных оценок.

В состав экспертной группы включаются представители:

-организации-владельца СИБ, ответственные за обеспечение безопасности информации;

-организации-разработчика СИБ;

-организации-лицензиата, предоставляющего услуги в области разработки, внедрения и аттестации систем информационной безопасности.

В соответствии с принятой классификацией ФСБ России и ФСТЭК России определяются следующие виды нарушителей:

-администраторы безопасности СИБ;

-бывшие пользователи СИБ;

-взломщики компьютерных систем (сетевые хакеры);
-криминальные структуры;
-лица, привлекаемые к монтажу и вводу СИБ в эксплуатацию;
-недобросовестные организации-конкуренты;
-обслуживающий персонал СИБ;
-пользователи СИБ;
-разработчики, производители и поставщики ПО и ТС для СИБ;
-резиденты службы разведки иностранных государств или блоков государств;
-системные администраторы СИБ;
-службы разведки иностранных государств или блоков государств;
-сторонние физические лица;
-террористические и экстремистские группировки.

Под «сетевым хакером» понимается физическое лицо или группа лиц, осуществляющие атаки из ИТКС «Интернет» по линии используемых в СИБ информационных технологий. «Сетевым хакером» также может являться представитель сегмента «Физические лица», намеренно или неумышленно отправляющий вредоносные данные в виде кодов и файлов на сервисы СИБ, доступные из ИТКС «Интернет».

Для определения актуальных направлений реализации УБИ от каждого нарушителя в ИС представленных выше нарушителей разделяют на 2 типа:

-внешний нарушитель (тип 1) - лица, не имеющие штатных прав доступа к ресурсам СИБ и реализующие УБИ из-за границ контролируемой зоны (КЗ) СИБ;

-внутренний нарушитель (тип 2) - лица, имеющие штатные права доступа к ресурсам СИБ и реализующие УБИ из-за границ СИБ и изнутри СИБ.

Для оценки интеллектуальных, организационных, экономических и технологических возможностей нарушителей вводят понятие «потенциала» нарушителя следующим образом:

1) Нарушители с низким потенциалом. Владеют исключительно общедоступной информацией об уязвимостях, методах и средствах реализации УБИ. Разрабатывают методы и средства реализации УБИ с использованием исключительно личного интеллектуального, временного и финансового ресурса.

2) Нарушители со средним потенциалом. Обладают всеми возможностями нарушителей с низким потенциалом. Обладают частью информации об особенностях технологического процесса обработки информации и комплексной системе информационной безопасности в СИБ. Проводят самостоятельный анализ кода и аппаратных компонент системы защиты с использованием общедоступных/коммерческих средств анализа. Разрабатывают методы и средства реализации УБИ с привлечением стороннего интеллектуального, временного и финансового ресурса.

3) Нарушители с высоким потенциалом. Обладают всеми возможностями нарушителей со средним потенциала. Владеют доступом к выделенным сетям связи, в случае невыполнения организационных мер защиты. Способны внедрять не декларированные возможности (НДВ) 1 и 2

типа в ПО и аппаратные компоненты СИБ. Обладают полной информацией об особенностях технологического процесса обработки информации и подсистеме информационной безопасности (ПИБ) в СИБ. Разрабатывают методы и средства реализации УБИ с использованием практически неограниченного интеллектуального, временного и финансового ресурса.

Экспертная группа оценивает наличие у потенциальных нарушителей мотивов для реализации той или иной УБИ.

В соответствии с методическими документами ФСТЭК России на решение об отнесении возможностей реализации УБИ к одной из градаций влияют показатели «потенциала нарушителя», «исходной защищенности СИБ» и «существующих защитных мероприятий».

При этом актуальность каждой УБИ определяется при условии одновременного выполнения всех следующих правил:

-для УБИ определены мотивированные нарушители безопасности;

-для УБИ определен конечный объект воздействия из состава СИБ;

-для УБИ определен способ реализации;

-возможность реализации УБИ признана «средней» или «высокой» на основании сравнения «потенциала нарушителя» и «уровня исходной защищенности» СИБ.

Если в СИБ используются средства криптографической защиты информации (СКЗИ) для защиты каналов связи и передаваемой по сети информации, то в соответствии с методическими документами ФСБ России (Приказ ФСБ России №378 от 10.07.2014 г.) определяются актуальные группы нарушителей, способные оказывать влияние на компоненты СКЗИ в СИБ. Определение таких нарушителей производится в соответствии с методическими документами ФСБ России и перечнем актуальных нарушителей.

Для подтверждения соответствия СИБ требованиям ФСТЭК России проводится аттестация СИБ. Она организуется обладателем информации (заказчиком) или оператором системы и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний).

В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы. Используется проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы.

Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с

подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

Заключение.

В моей работе рассмотрены только некоторые вопросы из чрезвычайно широкой и сложной тематики защиты информации от НСД. В заключение я хотел бы обратить внимание на важность человеческого фактора в решении этой проблемы.

Дело в том. что большая часть пользователей компьютеров не осознает, что постоянно рискует своей безопасностью и личными тайнами. И лишь немногие хоть, каким либо образом, защищают свои данные. Пользователи компьютеров регулярно оставляют полностью незащищенными даже такие данные, как налоговая и банковская информация, деловая переписка и электронные таблицы. Проблемы значительно усложняются, когда они начинают работать или играть в сети, так ка хакеру намного легче в это время заполучить или уничтожить информацию, находящуюся на их компьютере.

Надо отметить также, что с развитием технологий количество угроз, направленных на несанкционированный доступ к информации, на ее искажение, удаление непрерывно увеличивается. В связи с этим нужно четко представлять, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в информационных системах. Но также следует помнить, что большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей, но и к тому, что у нее произойдет существенное снижение производительности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Поэтому главное при определении мер и принципов защиты информации – это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска в другом.