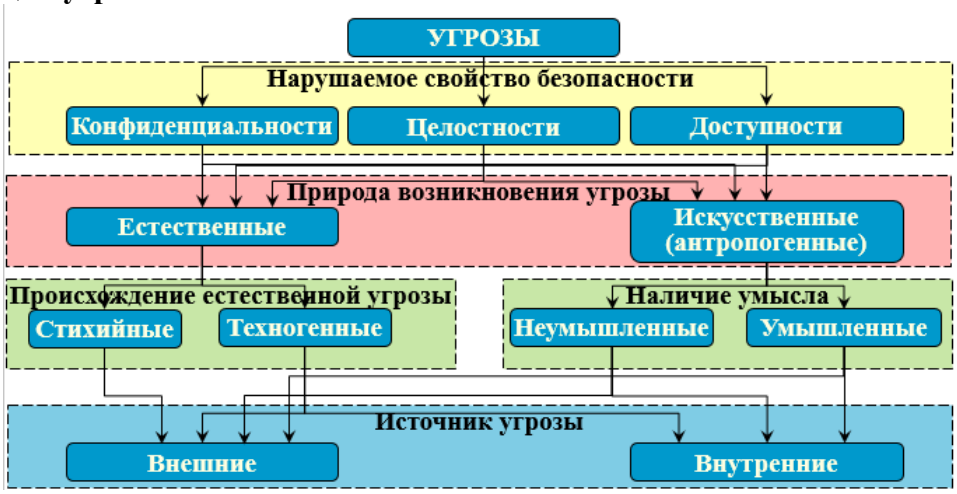
1. Классификация угроз ИБ



2. Уязвимости компьютерных систем

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Известная уязвимость – уязвимость, опубликованная в общедоступных источниках с описанием соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.

Уязвимость нулевого дня – уязвимость, которая становится известной до момента *выпуска* разработчиком компонента информационной системы соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений.

Впервые выявленная уязвимость – уязвимость, не опубликованная в общедоступных источниках.

3. Классификация атак на основе эталонной модели OSI

1. Физический уровень
   - прослушивание сетевого трафика
   - отказ в обслуживании путем «глушения» канала
   - отказ в обслуживании путем добавления шумов
   - нарушение физической целостности кабелей и оборудования
2. Канальный уровень
   - MAC Spoofing - подделка MAC-адреса в отправляемых пакетах
   - переполнение CAM–таблицы (Content Address Memory);
   - VLAN hopping
   - ARP spoofing
   - DoS
3. Сетевой уровень
   - IP Spoofing
   - ICPM attack
   - Smurf attack
4. Транспортный уровень
   - Подмена TCP-соединения (hijacking);
   - UDP Flood;
   - SYN Flood.
   - Сканирование сети;
5. Сеансовый (Перехват сессии, MITM, Blind attack, Man-in-the-browser, SSH Sniffing)
6. Представления (SSL Hijacking, понижение уровня шифрования)
7. Прикладной уровень (DDoS, HTTP Flood, SQLi, XSS, DNS Spoofing, др.)

4. Современные тенденции в развитии компьютерных технологий

Современные тенденции:

- *Открытость* порождена сложностью надежной физической защиты каналов передачи данных, а также подключением компьютерных систем к глобальным сетям, прежде всего к сети Internet.
- *Неоднородность* (гетерогенность) – современные вычислительные сети объединяют в себе, как правило, разнотипные компьютеры с различным программным обеспечением
- *Масштабность* определяется широтой ее территориального распределения, а также количеством входящих в ее состав рабочих станций, серверов и коммуникационных устройств.
- *Динамичность* – постоянное изменение структуры, технологических схем и условий функционирования любой компьютерной сети приводит к ошибкам в конфигурировании, настройке и использовании средств защиты

5. Концепция многоуровневой защиты компьютерных ресурсов

Уровни защиты:

- Охрана по территории объекта;
- Защита аппаратных средств;
- Защита программных средств;
- Защита информации

Слои многоуровневой системы ЗИ:

- *защита данных* подразумевает управление доступом к обрабатывающимся и хранящимся в системе данным, шифрование и резервное копирование
- *защита приложений* отвечает за защиту от атак, направленных на конкретные приложения и сервисы (установка обновлений, средств АВЗ)
- *защита узлов сети* рассматривает атаки на отдельные узлы сети, с учетом функциональности узла (механизмы защиты, предоставляемые операционной системой узла: аутентификация и контроль доступа пользователей, настройка параметров безопасности, МЭ, HIDS)
- *защита внутренней сети* обеспечивает безопасность передаваемого внутри сети трафика и сетевой инфраструктуры (сегментация сети, использование защищенных сетевых протоколов передачи данных)
- *защита периметра сети* подразумевает обеспечение ИБ в «точках входа» в защищаемую сеть из внешней, потенциально опасной среды

Многоуровневая СЗИ позволяет:

- снизить вероятность успешного осуществления атак и затруднить несанкционированный доступ к защищаемой информации;
- повысить вероятность обнаружения нарушителя;
- выиграть время для определения несанкционированных действий и для реакции на атаку, а вследствие этого смягчить возможные негативные последствия.

6. Концепция комплексной защиты компьютерных ресурсов

Подходы к обеспечению ИБ:

1. *Фрагментарный* – направлен на противодействие четко определенным угрозам в заданных условиях
2. *Комплексный* – ориентирован на создание защищенной среды обработки информации, объединяющий в единый комплекс разнородные меры противодействия всем угрозам. Основан на построении системы обеспечения безопасности информации

Меры обеспечения ИБ:

- *правовые* (законодательные) – действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил
- *морально-этические* – нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе
- *организационные* (административные) – меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой
- *физические* – основаны на применении устройств и сооружений, предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации
- *технические* – основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих функции защиты

7. Комплекс работ по созданию СЗИ

Комплекс работ:

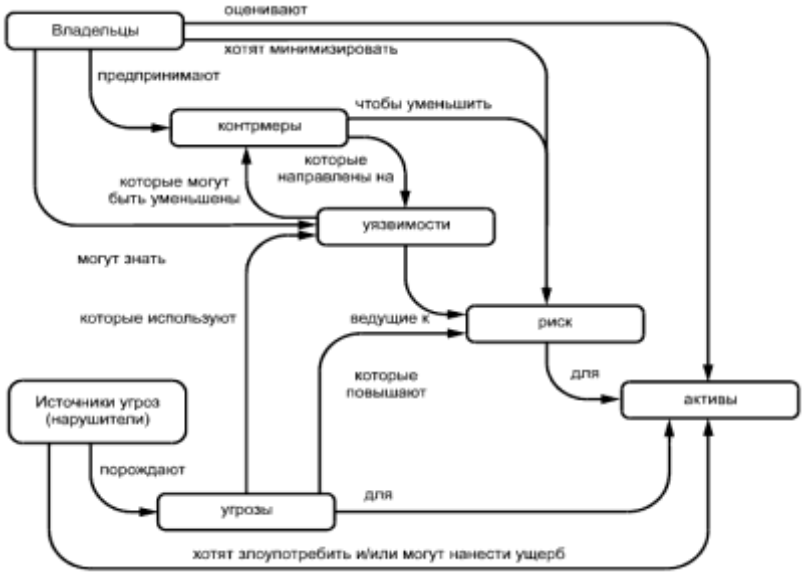
- формирование требований к системе защиты информации АС;
  - проведение обследования и сбор исходных сведений об АС;
  - классификация АС по требованиям защиты информации;
  - разработка модели нарушителя и угроз безопасности информации АС;
  - определение перечня мер обеспечения безопасности, которые должны быть реализованы.
- разработка (проектирование) системы защиты информации АС;
- внедрение системы защиты информации АС;
- аттестация АС по требованиям безопасности информации и ввод в действие;
- сопровождение системы защиты информации в ходе эксплуатации АС.

8. Классификация автоматизированных систем в соответствии с РД

9. Разработка СЗИ в контексте анализа информационных рисков

Риск информационной безопасности - возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.
Угрозы - потенциальные возможности нарушения безопасности информации.
Уязвимости - слабые места (слабости) в системе защиты, которые делают возможной реализацию угроз
Контрмеры – меры, направленные на уменьшение уязвимостей.
Риски - факторы, отражающие опасность возникновения ущерба в результате реализации угроз.
Методы оценки риска ИБ АС:

- качественные (OCTAVE, COBRA) – определяют последствия, вероятность и уровень риска по шкале «*высокий*», «*средний*» и «*низкий*».
- количественные (RiskWatch) – определяют практическую значимость и стоимость последствий, их вероятности и получают значение уровня риска в *определенных единицах*, установленных при разработке области применения менеджмента риска
- смешанные (CRAMM, ГРИФ) – любому качественному уровню *соответствуют* определенные диапазоны количественных величин



10. Модель защищаемых ресурсов
Уровни архитектуры систем и сетей, на которых определяются объекты воздействия:

- пользователей
- прикладной
- системный
- сетевой

Объекты воздействия:

- информация
- программно-аппаратные средства обработки и хранения информации;
- программные средства;
- машинные носители информации;
- телекоммуникационное оборудование;
- средства защиты информации;
- привилегированные и непривилегированные пользователи систем и сетей;
- обеспечивающие системы.

Виды воздействия на защищаемые ресурсы:

- утечка конфиденциальной информации или отдельных данных;
- отказ в обслуживании компонентов;

- НСД к компонентам, ЗИ, системным, конфигурационным, иным служебным данным;
- несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных;
- несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
- нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации;

11. Модель нарушителя

Виды нарушителей:

1. Внешний – не имеющий прав доступа в контролируемую зону и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации.
    - специальные службы иностранных государств;
    - террористические, экстремистские группировки;
    - преступные группы (криминальные структуры);
    - отдельные физические лица (хакеры);
    - конкурирующие организации;
    - лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
2. Внутренний – имеющий права доступа в контролируемую зону и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.
    - бывшие (уволенные) работники (пользователи);
    - разработчики программных, программно-аппаратных средств;
    - поставщики услуг связи, вычислительных услуг;
    - лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
    - лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
    - авторизованные пользователи систем и сетей;
    - системные администраторы и администраторы безопасности.

В зависимости от уровня возможностей по реализации угроз безопасности информации:

- базовые (Н1): индивидуальные хакеры, поставщики, сисадмины, бывшие работники
- базовыми повышенные (Н2): конкуренты, преступные группы, поставщики вычислительных услуг связи, администраторы безопасности
- средние (Н3): террористы, экстремисты, разработчики ПО
- высокие (Н4): специальные службы

12. Концепция контроля доступа в компьютерную систему

Контроль и управление доступом (КУД) **–** комплекс мероприятий, направленных на предотвращения несанкционированного доступа.

Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью, осуществляет:

- Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- Аутентификация – действия по проверке подлинности субъекта доступа или объекта доступа, а также по проверке принадлежности субъекту доступа или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

- Авторизация – предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом.

См. лекцию 5

13. Проверка подлинности на основе статического и динамического пароля

Проверка подлинности на основе *статического пароля* производится путём сверки пароля, введённого пользователем, с уже имеющимся в хранилище паролем.

Методы парольной защиты, основанные на динамическом пароле:

- метод модификации схемы простых паролей;
  - При **случайной выборке символов пароля** каждому пользователю выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только некоторая его часть.
  - При **одноразовом использовании паролей** каждому пользователю выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки
- метод «запрос-ответ» - заблаговременно создается и особо защищается массив вопросов, включающий в себя как вопросы общего характера, так и персональные вопросы, относящиеся к конкретному пользователю
- функциональный метод: методы функционального преобразования, методы «рукопожатия»

14. Проверка подлинности на основе биометрической идентификации

Биометрическая идентификация — это предъявление пользователем своего уникального биометрического параметра и процесс сравнения его со всей базой имеющихся данных. Для извлечения такого рода персональных данных используются биометрические считыватели.

Виды:

1. Статическая (отпечаток пальца, форма ладони, расположение вен на ладони, сетчатка глаза, радужная оболочка глаза, форма лица, термограмма лица, ДНК)
2. Динамическая (рукописный почерк, клавиатурный почерк, голос, походка)

15. Концепция и формальные модели разграничения доступа

Подсистема разграничения доступа к компьютерным ресурсам реализует концепцию единого диспетчера доступа, являющегося посредником при всех обращениях субъектов к объектам

Схема контроля доступа к компьютерным ресурсам:

БД защиты и Субъект доступа → Диспетчер → Объект доступа и Системный журнал

Функции диспетчера доступа:

- проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты (правил разграничения доступа);
- при необходимости регистрировать факт доступа и его параметры в системном журнале регистрации.

Требования к реализации диспетчера доступа:

- требование полноты контролируемых операций, согласно которому проверке должны подвергаться все операции всех субъектов над всеми объектами системы (обход диспетчера предполагается невозможным);
- требование изолированности, то есть защищенности диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;
- требование формальной проверки правильности функционирования;
- минимизация используемых диспетчером ресурсов

16. Произвольное разграничение

Произвольное или, как его еще называют, дискреционное управление доступом — это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую

субъект входит. С концептуальной точки зрения, текущее состояние прав доступа при произвольном управлении описывается *матрицей (таблицей) доступа*, каждая ячейка которой для заданного субъекта и объекта содержит следующую информацию:

- размер предоставляемого ресурса, например, размер области внешней памяти;
- имя компонента предоставляемого ресурса, например, имя каталога или логического диска;
- код, определяющий права доступа к ресурсу, например, 012 - только чтение, 102 - чтение и запись и т.д.;
- ссылку на другую информационную структуру, задающую права доступа к ресурсу, например, ссылку на другую матрицу доступа;
- ссылку на программу, регулирующую права доступа к ресурсу.

17. Принудительное разграничение

При *принудительном разграничении* доступа компьютерные ресурсы разделяются на группы в соответствии с уровнями секретности и категориями информации, к которым они относятся. В качестве уровней секретности могут быть выделены следующие:

- «несекретно»;
- «для служебного использования»;
- «секретно»;
- «совершенно секретно».

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются *метки безопасности*. Метка субъекта, называемая еще мандатом, описывает его благонадежность и задает:

- максимальный уровень секретности информации, доступ к которой ему разрешен;
- категории информации, к которой он допущен

Метка объекта определяет степень закрытости и категории содержащейся в нем информации. Принудительное разграничение доступа к компьютерным ресурсам основано на сопоставлении меток безопасности субъекта и объекта.

18. Использование криптографических систем для разграничения доступа к информации

Криптографические системы (криптосистемы) выполняют обратимое преобразование информации на основе секретного ключа, известного только санкционированному пользователю, и делающем эту информацию зашифрованной, т.е. недоступной для злоумышленника. Отдельный класс таких подсистем образует *подсистема специального преобразования содержимого носителей* информации в режиме реального времени, обеспечивающая разграничение доступа к информации, хранящихся на различных носителях – для защиты от НСД к содержимому носителей информации за счет специального преобразования в режиме реального времени информации.

Задачи:

- Двухуровневое "прозрачное" кодирование информации на жестких дисках АРМ.
- Одноуровневое "прозрачное" кодирование информации на съемных информационных носителях (FDD-, ZIP-, Flash-, CD-, DVD-дисках).
- Логическая привязка съемных носителей к заданной группе автономных АРМ за счет "прозрачного" кодирования информации на этих съемных носителях по секретному ключу.

19. Криптографическое закрытие данных

В подсистеме специального преобразования содержимого носителей информации исходный секретный ключ не используется для непосредственного кодирования, а служит для порождения рабочих ключей, которые и применяются в качестве параметров криптографических преобразований.

Базовая схема прозрачного кодирования включает следующие шаги:

- по исходному секретному ключу генерируется (настраивается) алгоритм вычисления рабочих ключей;

- формируются рабочие ключи шифрования;
- на основе полученных рабочих ключей генерируется (настраивается) алгоритм криптографических преобразований;
- выполняются криптографические преобразования

Базовая схема прозрачного кодирования в ПАК включает два этапа:

1. на этапе предвычислений выполняется настройка криптосистемы под исходный секретный ключ, в процессе которой:
   - генерируется алгоритм порождения рабочих ключей;
   - вычисляются сами рабочие ключи;
   - генерируется алгоритм криптографических преобразований;
2. на этапе криптографических преобразований выполняется непосредственное наложение и/или снятие криптозащиты.

20. Контроль целостности информации

Контроль эталонного состояния информационно-программного обеспечения предполагает динамическое формирование и обновление эталонных характеристик информационных объектов компьютерной системы, а также динамическую проверку на соответствие текущих характеристик эталонным.

Действия при непосредственном контроле эталонного состояния информационного объекта:

1. определение текущей характеристики объекта по тому же способу, по которому формировалась его эталонная характеристика;
2. сравнение текущей и эталонной характеристики;
3. принятие решения о целостности и подлинности проверяемого объекта по результатам сравнения - если текущая и эталонная характеристики совпадают, то считается, что контролируемый объект является целостным и подлинным.

21. Использование секретных виртуальных дисков (Алиев)

Секретный диск – файловый контейнер, в котором хранятся закодированные данные.

Схема работы с виртуальными секретными дисками основана на применении драйвера прозрачного кодирования, эмулирующего кодирующий дисковод, и файловых контейнеров, заменяющих собой реальные диски разных объемов.

Для подключения и организации доступа к виртуальному секретному диску драйвер прозрачного кодирования виртуальных дисков использует *закрытый ключ.*

При кодировании ключа виртуального секретного диска драйвер прозрачного кодирования виртуальных дисков использует:

- пароль (PIN-код) пользователя;
- личный ключ пользователя.

Двухэтапный процесс кодирования:

1) на этапе инициализации криптосистемы (монтирования виртуального секретного диска) осуществляются:
   - выбор модуля аутентификации и криптографического модуля в зависимости от параметров указанного файлового контейнера;
   - запрос пароля и личного ключа пользователя;
   - считывание пароля и личного ключа пользователя;
   - аутентификация пользователя на основе его пароля и ключа; в случае отрицательных результатов аутентификации процесс инициализации прерывается, и дальнейший доступ к секретному диску блокируется;
   - раскодирование ключа секретного диска и генерация рабочих ключей кодирования;
2) на этапе криптографических преобразований выполняется автоматическое кодирование информации при ее записи на секретный диск, а также автоматическое раскодирование при ее считывании с секретного диска.

По окончании работы с виртуальным секретным диском этот диск демонтируется, что предотвращает возможность несанкционированного доступа к хранящейся на нем информации.

22. Классификация компьютерных вирусов и программных закладок (Воронецкий)

Программная закладка – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Компьютерный вирус – вредоносная программа, способная создавать свои копии и другие вредоносные программы.

Классификация компьютерных вирусов:

1. по типу ОС (Windows, Linux, MacOS, Android, iOS)
2. по способу заражения среды обитания
   - *Резидентные вирусы*. Загружают в оперативную память резидентную часть вируса, которая впоследствии может отслеживать открываемые пользователем файлы и заражать их
   - *Нерезидентные вирусы***.** Не оставляющие своих резидентных частей в оперативной памяти компьютера и активны непродолжительное время
3. по среде обитания (файловые, загрузочные, макровирусы, сетевые)
4. по особенностям алгоритма вируса (черви, стелс, полиморфные, метаморфные)

Классификация программных закладок:

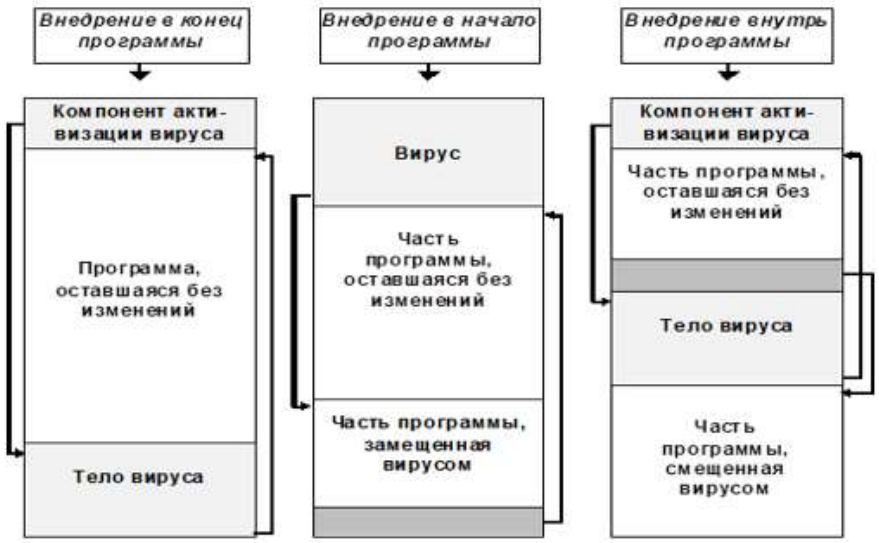
1. по методу внедрения
   - программно-аппаратные закладки;
   - загрузочные закладки;
   - драйверные закладки;
   - прикладные закладки;
   - закладки-имитаторы
2. по назначению
   - копирование информации пользователя компьютерной системы;
   - изменение алгоритмов функционирования системных, прикладных и служебных программ;
   - навязывание определенных режимов работы

23. Схемы заражения и способы маскировки, используемые вредоносными программами

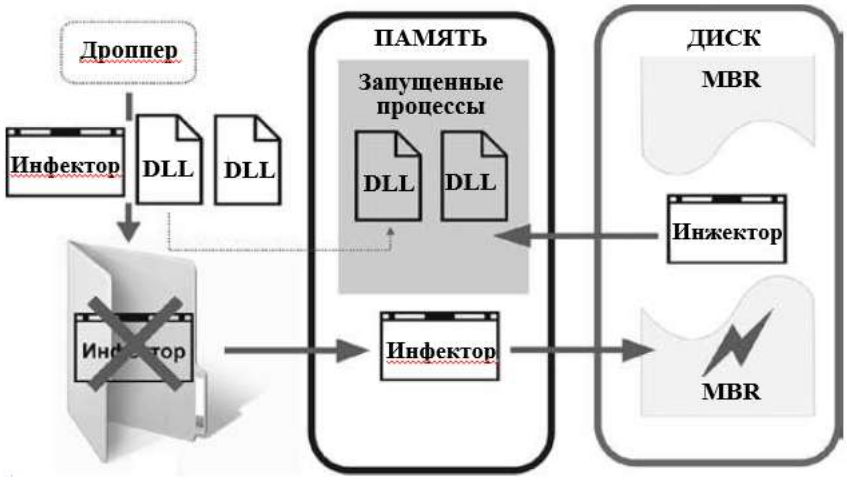
Дроппер – это объект, осуществляющий извлечение содержащихся в нем основных модулей вируса или троянца, их распаковку и установку в операционной системе.

Инфектор – это модуль, осуществляющий заражение файловых объектов либо загрузочной записи компьютера путем изменения их внутренней структуры.

Инжектором – функциональный модуль вредоносной программы, реализующий встраивание вредоносных компонент в запущенный процесс другого приложения (инжект).



Схемы заражения



Обобщенный процесс заражения

24. Общая организация защиты от вредоносных программ (Кешев)

Подсистема защиты от компьютерных вирусов является одним из основных компонентов системы защиты информации и процесса ее обработки в вычислительных системах.

Уровни защиты от компьютерных вирусов:

- уровень защиты от проникновения в ВС вирусов известных типов;
- уровень углубленного анализа компьютерной системы на наличие вирусов как известных, так и неизвестных типов;
- уровень защиты от деструктивных действий и размножения вирусов.

Первый уровень защиты обеспечивает препятствие доступу в ВС вирусов известных типов. Основой реализации данного уровня является поиск и обезвреживание вирусов в компьютерной системе, а также во всех программах, поступающих в компьютерную систему извне. Обнаружение и обезвреживание вирусов осуществляется на основе поиска кодовых последовательностей (сигнатур), характерных для вирусов известных типов.

Второй уровень защиты обеспечивает обнаружение в компьютерной системе вирусов, которым удалось обойти первый уровень защиты. Это в основном касается вирусов незнакомых типов, для которых неизвестны характерные им кодовые последовательности (сигнатуры). Поиск вирусов на данном уровне осуществляется путем сравнения текущих характеристик элементов компьютерной системы с эталонными характеристиками, соответствующими их незараженному состоянию.

Третий уровень защиты обеспечивает защиту от деструктивных действий и размножения вирусов, которым удалось преодолеть первые два уровня. Данный уровень реализуется на основе перехвата характерных для вирусов функций (низкоуровневое форматирование дисков, модификация программ и т.д.).
Средства поиска и обезвреживания вирусов известных типов
Для поиска и обезвреживания вирусов перед установкой первого уровня антивирусной защиты, а также для непосредственной защиты от проникновения вирусов известных типов используют *антивирусные программные средства*, называемые *сканерами*.
Виды программ-сканеров:

- *транзитные*, которые загружаются в оперативную память только для поиска и обезвреживания вирусов;
- *резидентные*, которые после запуска остаются в оперативной памяти резидентно и проверяют программные файлы при возникновении с ними определенных событий (запуск, копирование, создание, переименование).

Наибольшая результативность достигается при совместном использовании транзитного и резидентного сканеров.
Углубленный анализ на наличие вирусов
Основная задача - обнаружение вирусов, которым удалось обойти уровень защиты от проникновения известных вирусных программ. Для реализации уровня углубленного анализа на наличие вирусов используют антивирусные программные средства, называемые ревизорами.
Защита от деструктивных действий и размножения вирусов
На данном уровне должно быть обеспечено блокирование всех действий вирусов, связанных с их саморазмножением и нанесением ущерба. Такое блокирование реализуется на основе перехвата выполнения функций, характерных для вирусов (модификация программ, низкоуровневое форматирование дисков и т.д.).

25. Поиск по сигнатурам, углубленный анализ, защита от деструктивных действий (Коновалов)
Поиск по сигнатурам характерен для антивирусных средств. По отношению к сетевым атакам этот метод заключается в мониторинге сетевого трафика в реальном или близком к реальному времени и использовании соответствующих алгоритмов обнаружения. Очень часто используется механизм поиска в трафике определенных строк, которые могут характеризовать несанкционированную деятельность.
Основная *задача углубленного анализа* – обнаружение вирусов, которым удалось обойти уровень защиты от проникновения известных вирусных программ.
Для реализации уровня углубленного анализа на наличие вирусов используют антивирусные программные средства, называемые *ревизорами*. При установке и поддержании данного уровня антивирусной защиты должны быть выдержаны следующие *этапы*:

1. Тщательный анализ вычислительной системы на наличие вирусов и полное обезвреживание обнаруженных вирусных программ с помощью обновленной версии транзитного сканера.
2. Формирование с помощью ревизора следующих эталонных характеристик незараженного компьютера:
    - содержимого загрузочных секторов жестких дисков;
    - контрольных сумм содержимого файлов конфигурирования и настройки;
    - контрольных сумм или описания структуры содержимого оперативной памяти компьютера
3. Периодическая проверка ревизором соответствия реальных характеристик элементов компьютерной системы их эталонным характеристикам, которые эти элементы имели при незараженном состоянии. Виды периодических проверок:
    - периодическая разовая (например, ежедневная или еженедельная), при которой после запуска ревизора проверяются все элементы компьютера, для которых созданы эталонные характеристики

- в режиме реального времени, при которой осуществляется проверка контролируемых элементов только при попытке их использования, например, при попытке запуска программ

На уровне *защиты от деструктивных действий* должно быть обеспечено блокирование всех действий вирусов, связанных с их саморазмножением и нанесением ущерба. Такое блокирование реализуется на основе перехвата выполнения функций, характерных для вирусов.
Уровень защиты от деструктивных действий и размножения вирусов реализуется путем использования встроенных аппаратных возможностей компьютера, а также специальных антивирусных программ, называемых *фильтрами*.
К *встроенным аппаратным* возможностям по блокированию действий вирусов относится аппаратный контроль изменения внесистемного загрузчика и таблицы разделов винчестера, находящихся в загрузочном секторе (MBR) каждого жесткого диска компьютера. Это позволяет блокировать действия вирусов пытающихся заразить внесистемный загрузчик или исказить таблицу разделов винчестера.
Если функция аппаратного антивирусного контроля является активной, то при любой попытке изменения внесистемного загрузчика или таблицы разделов жесткого диска будет выдано предупреждающее сообщение и запрос пользователю, ответом на который пользователь может запретить или разрешить модификацию загрузочного сектора.

26. Обзор логической сегментации сети (VLAN) (Красников)
Сеть может быть сегментирована в рамках одного коммутатора.
Логическая сегментация сети реализуется путем использования технологии виртуальной локальной компьютерной сети (Virtual Local Area Network, VLAN).
Способы организации виртуальных локальных сетей:
- виртуальная сеть на базе *порта*
- виртуальная сеть на базе *тега*

*Достоинства***:**
- гибкое разделение устройств на группы;
- уменьшение широковещательного трафика в сети;
- увеличение безопасности и управляемости сети;
- уменьшение количества оборудования и сетевого кабеля;

Недостатки:
- высокая стоимость реализации.

27. Обзор протоколов криптографического закрытия передаваемых данных (Лаврентьев)
Рассмотрю протоколы криптографического закрытия передаваемых данных на примере семейства протоколов криптографической защиты *IPSec* (Internet Protocol Security), соответствующих сетевому уровню модели OSI и входящих в состав новой версии протокола IP – IPv6.
В соответствии с протоколом IPSec архитектура средств безопасности информационного обмена разделяется на три уровня
На верхнем уровне расположены следующие *протоколы*:
- *протокол согласования параметров виртуального канала и управления ключами* (Internet Security Association Key Management Protocol - ISAKMP), обеспечивающий общее управление защищенным виртуальным соединением, включая согласование используемых алгоритмов криптозащиты, а также генерацию и распределение ключевой информации;
- *протокол аутентифицирующего заголовка* (Authentication Header - AH), предусматривающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;
- *протокол инкапсулирующей защиты содержимого* (Encapsulating Security Payload – ESP), обеспечивающий криптографическое закрытие передаваемых пакетов сообщений и

предусматривающий также выполнение всех функций протокола аутентифицирующего заголовка (AH).

28. Способы создания защищенных виртуальных каналов (Лысенко)

Любой из двух узлов виртуальной сети, между которыми формируется защищенный туннель, может принадлежать конечной или промежуточной точке защищаемого потока сообщений. Соответственно возможны различные способы образования защищенного виртуального канала. *Вариант*, когда конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений, является с точки зрения безопасности лучшим. В этом случае обеспечивается полная защищенность канала вдоль всего пути следования пакетов сообщений. Однако такой вариант ведет к избыточности ресурсных затрат. Если отсутствует необходимость защиты трафика внутри локальной сети, входящей в виртуальную сеть, то в качестве конечной точки защищенного туннеля целесообразно выбрать брандмауэр или пограничный маршрутизатор этой локальной сети. В случае же, когда внутри локальной сети поток сообщений также должен быть защищен, то в качестве конечной точки туннеля в этой сети должен выступать компьютер, представляющий одну из сторон защищенного взаимодействия. При доступе к локальной сети удаленного пользователя компьютер этого пользователя также должен быть конечной точкой защищенного виртуального канала.

Распространен также *вариант*, характеризующийся более низкой безопасностью, но более высоким удобством применения. Согласно данному варианту, рабочие станции и серверы локальной сети, а также удаленные компьютеры не участвуют в создании защищенного туннеля, который прокладывается только внутри публичной сети с коммутацией пакетов, например, внутри Internet. В качестве конечных точек такого туннеля чаще всего выступают провайдеры Internet и/или пограничные маршрутизаторы (брандмауэры) локальной сети. При удаленном доступе к локальной сети туннель создается между сервером удаленного доступа провайдера Internet, а также пограничным провайдером Internet или маршрутизатором (брандмауэром) локальной сети.

29. Фильтрация трафика МЭ (Малых)

Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов принятой политики безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих *стадий*:

1) анализ информации по заданным в интерпретируемых правилах критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;
2) принятие на основе интерпретируемых правил одного из следующих решений:
   - не пропустить данные;
   - обработать данные от имени получателя и возвратить результат отправителю;
   - передать данные на следующий фильтр для продолжения анализа;
   - пропустить данные, игнорируя следующие фильтры.

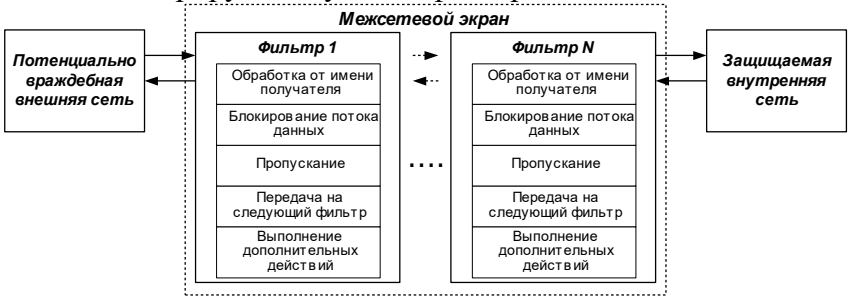


Рис. 2. Структура межсетевого экрана

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

30. Сетевая система обнаружения вторжений (Миннигалин)

Системы для обнаружения и предотвращения вторжений (IPS/IDS intrusion detection and prevention systems) — программно-аппаратные решения, детектирующие и предотвращающие попытки нелегального доступа в корпоративную инфраструктуру.

- системы по обнаружению вторжений (СОВ или в зарубежной терминологии IDS);
- системы по предотвращению вторжений (СПВ или IPS).

Система обнаружения вторжений (IDS) собирает и анализирует полученные данные, хранит события с момента подключения к сетевой инфраструктуре и формирует отчеты и управляется из консоли администратора.

Система IPS, как правило, предотвращает наиболее популярные сетевые атаки, заданные предустановленными политиками безопасности или проанализированные как отклонение от нормального поведения пользователей и систем.

Риск применения IPS в том, что бывают как ложноположительные срабатывания, так и ложноотрицательные. Анализ систем обнаружения вторжений показал, что для оптимальной и своевременной защиты от вторжений важно применять решения, объединяющие в себе функции IDS и все методы подавления атак IPS.

Технология Сетевые системы обнаружения вторжения (NIDS) дает возможность установить систему в стратегически важных местах сети и анализировать входящий/исходящий трафик всех устройств сети. NIDS анализируют трафик на глубоком уровне, «заглядывая» в каждый пакет с канального уровня до уровня приложений.

NIDS *отличается* от межсетевого экрана, или файрволла. Файрволл фиксирует только атаки, поступающие снаружи сети, в то время как NIDS способна обнаружить и внутреннюю угрозу. Сетевые системы обнаружения вторжений контролируют всю сеть, что позволяет не тратиться на дополнительные решения. Но есть недостаток: NIDS отслеживают весь сетевой трафик, потребляя большое количество ресурсов. Чем больше объем трафика, тем выше потребность в ресурсах CPU и RAM. Это приводит к заметным задержкам обмена данными и снижению скорости работы сети. Большой объем информации также может «ошеломить» NIDS, вынудив систему пропускать некоторые пакеты, что делает сеть уязвимой.

31. Хостовая система обнаружения вторжений (Мокрушин)

В повседневной деятельности целесообразно разделить обнаружение атак на уровне сети (network-based) и на уровне хоста (host-based). Первые системы, как правило, используют сигнатуры атак, в то время как вторые - анализ регистрационных журналов.

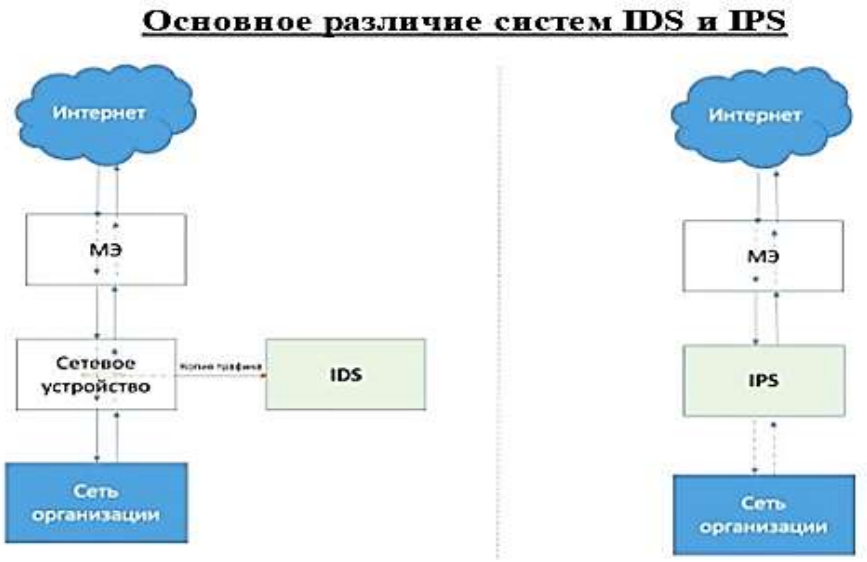
Хостовая система обнаружения вторжений (*Host-based intrusion detection system)* устанавливаются на один хост внутри сети и защищают только его. HIDS также анализируют все входящие и исходящие пакеты, но только для одного устройства. Система HIDS работает *по принципу* создания снапшотов файлов: делает снимок текущей версии и сравнивает его с предыдущей, тем самым выявляя возможные угрозы. HIDS лучше устанавливать на критически важные машины в сети, которые редко меняют конфигурацию.

32. Основные различия IDS и IPS (Морозов)

Система обнаружения вторжений (IDS) представляет собой пассивную систему, которая сканирует трафик и сообщает об угрозах. IDS никоим образом не изменяет сетевые пакеты, тогда как IPS предотвращает доставку пакета в зависимости от содержимого пакета, подобно тому, как межсетевой экран предотвращает трафик по IP-адресу.

Система предотвращения вторжений (IPS) – это средство безопасности для предотвращения сетевых угроз. Система исследует сетевой трафик, потоки для предотвращения эксплойтов,

злонамеренных действий с целевым приложением или службой. Всё для того, чтобы злоумышленники не смогли прервать работу компании и получить контроль над приложением или конечной точкой.



IDS / IPS (Intrusion Detection and Prevention System) – системы обнаружения и предотвращения вторжений используются для защиты от сетевых атак. Основное различие между ними в том, что IDS — это система мониторинга, а IPS – система управления. Они так тесно связаны друг с другом, что их часто объединяют в названии – IDPS.

33. Принцип функционирования SIEM систем (Носов)

Security Information and Event Management - система, которая собирает информацию для дальнейшего анализа и классификации сисадмином или специалистом по ИБ.

Источники данных для SIEM:

- журналы событий, которые регистрируются операционной системой или сторонним приложением
- сетевое оборудование (маршрутизаторы, прокси-серверы, шлюзы и т. д.)
- межсетевые экраны
- сканеры уязвимостей — специальное ПО, которое находит уязвимости внутри инфраструктуры
- CRM-системы
- рабочие станции пользователей
- антивирусное программное обеспечение
- другие ресурсы, которые регистрируют события и способны передавать их через агентов или встроенными средствами

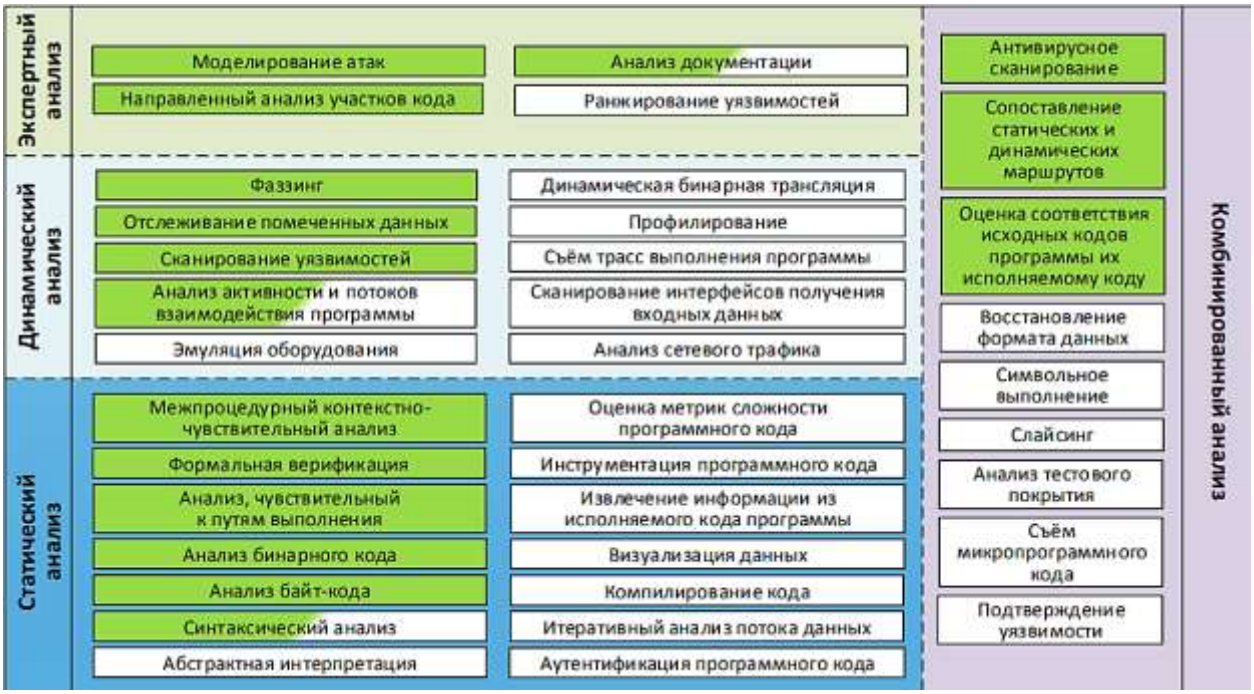
Принцип работы

SIEM используют для мониторинга и анализа поступающей информации, но сама она не защищает инфраструктуру от внешних и внутренних угроз. Собранная аналитика используется для определения инцидентов и оптимизации защиты.

Задаются *критерии*, по которым оценивается состояние инфраструктуры, прописывается оборудование, которое будет мониториться SIEM. Если происходит событие, которое выходит за рамки настроенных шаблонов, то SIEM реагирует на изменение и регистрирует инцидент.

Дополнительная возможность системы: на основе полученных данных анализируются действия злоумышленников. Регистрация инцидентов помогает расследовать такие события. Встроенная *функция оповещения* сообщает администраторам о нарушениях или проблемах. ПО представляет собой инструмент, который конфигурируется по требованиям и желаниям пользователя.

34. Методика выявления уязвимостей и НДВ (Порубай)



35. Общая система оценки уязвимостей CVSS (Шашков)

Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS) – это система, которая позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности.

36. Общие сведения о системах мониторинга информационной инфраструктуры

Мониторинг инфраструктуры – это сбор метрик, описывающих состояние IT-инфраструктуры;
Метрика – это конкретная характеристика, показывающая текущее состояние по определенному параметру;
Сервер мониторинга – ПО, которое выполняет агрегацию, хранение, пересчет данных по метрикам;
Агент мониторинга – ПО, которое выполняет сбор метрик с хоста, который подлежит мониторингу, а также отправку данных на сервер мониторинга.
Назначение:

- Оптимизировать использование информационных ресурсов;
- Повысить качество ИТ-сервисов и скорость устранения сбоев в работе оборудования и программного обеспечения;
- Обеспечить надежность, безопасность и согласованное функционирование всех компонентов ИТ-инфраструктуры;
- Облегчить модернизацию ИТ-инфраструктуры;
- Повысить эффективность работы ИТ-подразделения.
- Оперативно устранять или локализовать сбой в ИТ-системе.
- Предотвращать сбои.

Уровни мониторинга по составляющим:

- физические/виртуальные серверы;

- сервисы и приложения.

Методологии сбора метрик:

- метод выбора и сбора метрик для анализа состояния ИТ инфраструктуры (Utilization, Saturation, Errors – **USE**).
- метод выбора и сбора метрик для анализа состояния ИТ сервисов (Requests rate, Errors Duration – **RED**).
- метод выбора и сбора метрик для анализа состояния бизнес-метрик (Users Conversions Activity – **UCA**).

Модели работы систем мониторинга:

- Push-модель – когда сервер мониторинга ожидает подключений от агентов для получения метрик
- Pull-модель – когда сервер мониторинга сам подключается к агентам мониторинга и забирает данные.

37. Принцип функционирования виртуальной машины и контейнера. Основные отличия

Гипервизор – программа, создающая среду функционирования других программ (в том числе других гипервизоров) за счет имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.
Контейнеризация – это форма виртуализации на уровне операционной системы, которая позволяет запускать приложение и системные библиотеки в изолированной области, «контейнере».
Отличие технологий виртуализации и контейнеризации:

- *Виртуальная машина*. Требуется гипервизор, для каждой ВМ используется собственная гостевая ОС. Позволяет создавать неоднородные вычислительные среды на одном компьютере. Из-за собственной ОС ВМ может занимать несколько ГБ.
- *Контейнер*. Даже несколько контейнеров используют ядро одной хостовой ОС. Позволяет создавать на одном компьютере только однородные вычислительные среды. Намного легче ВМ, размер измеряется в Мб.

38. Тестирование на проникновение подсистем защиты информации

Тестирование на проникновение – метод оценки безопасности компьютерных систем и сетей посредством санкционированного моделирования атак злоумышленников.
Целью тестирования на проникновение является оценка возможности успешного проведения злоумышленником атаки на информационную систему и ее последствий.
Задачи:

- выявление недостатков в применяемых в информационной системе мерах безопасности и оценка возможности использования их нарушителем;
- получение на основе объективных свидетельств оценки текущего уровня защищенности;
- практическая демонстрация возможности использования уязвимостей;
- выработка рекомендаций по устранению выявленных уязвимостей и недостатков для повышения уровня защищенности.

Виды:

- Метод черного ящика (black box);
- Метод белого ящика (white box);
- Метод серого ящика (gray box).

По типу первоначального доступа:

- *Внутренний нарушитель***,** который может действует методу белого или серого ящика.
- *Внешний нарушитель***,** который может действует методу черного или серого ящика.

Этапы:

1. *Сбор информации* (обнаружение сетевых хостов, перечисление прослушивающих служб, обнаружение поверхностей атаки)

2. *Целенаправленное проникновение* (взлом уязвимых хостов: использование отсутствующих патчей, развёртывание полезной нагрузки, интерфейс удалённого доступа)
3. *Постэксплуатация и увеличение прав доступа* (обеспечение повторного входа, сбор учётных данных, движение вбок: обнаружение привилегированных аккаунтов, получение прав администратора домена)
4. *Документирование* (сбор доказательств/скриншотов, пошаговое описание атаки, создание финального документа)

39. Проверка соответствия текущих характеристик информационных объектов эталонным характеристикам (Носов)

Контроль эталонного состояния информационно-программного обеспечения:
1) динамическое формирование и обновление эталонных характеристик информационных объектов компьютерной системы
2) динамическую проверку на соответствие текущих характеристик эталонным. *Объекты* – информационные структуры, хранящиеся в памяти компьютера и передаваемые по каналам связи. Соответственно, к информационным объектам относятся не только данные, но и программы, предназначенные для обработки этих данных.
Контроль эталонного состояния информационного объекта в общем случае предполагает:

1) определение текущей характеристики объекта по тому же способу, по которому формировалась его эталонная характеристика;
2) сравнение текущей и эталонной характеристики;
3) принятие решения о целостности и подлинности проверяемого объекта по результатам сравнения - если текущая и эталонная совпадают, то объект является целостным и подлинным.

Злоумышленник может выполнить следующие несанкционированные действия:

- создать фальшивый информационный объект, соответствующий имеющейся эталонной характеристике; для противодействия атаке необходимо, чтобы вычисляемая характеристика зависела от каждого бита. Достижение такой зависимости реализуется при формировании эталонной характеристики на основе *хэш-функций*.
- подменить эталонную характеристику

Хэш-функция представляет собой криптографическую функцию от информационного объекта, значение которой зависит от каждого бита сообщения. Хэш-функция реализуется в виде итеративной процедуры, которая позволяет вычислить для информационного объекта *M* произвольной длины так называемый хэш-код *H(M)* (это эталонная хар-ка об-ка М) фиксированного размера *m* (128, 160 или 256 бит). Вычисление типовой хэш-функции осуществляется путем последовательного шифрования двоичных блоков M_i.
$H_i=E(H_{i-1},M_i)$
E - базовая функция шифрования, в качестве которой используются стойкие блочные шифры, а также односторонние криптографические функции;
H_0 - специфицированное начальное значение хэш-функции.
Хэш-функция должна удовлетворять следующим *требованиям*:

- вычислительно неосуществимо нахождение информационного объекта *M*, хэш-функция которого была бы равна заданному значению *H*;
- вычислительно неосуществимо нахождение двух разных информационных объектов M_1 и M_2 с равными значениями хэш-функции, т.е. объектов, удовлетворяющих условию $H(M_1) = H(M_2)$.

Если эти требования не выполняются, то потенциальный злоумышленник может подделать сообщение для подписанной хэш-функции.
С целью защиты эталонных характеристик от несанкционированных модификаций их формирование должно осуществляется по секретным ключам.

40. Использование средств анализа защищённости

Процесс анализа защищенности предполагает исследование проверяемых объектов для выявления в них «слабых мест» и обобщение полученных сведений, в том числе в виде отчета.
Средствами анализа защищенности *идентифицируются*:

- ошибки программно-аппаратных средств;
- программные закладки типа RootKit;
- слабые пароли, ключи;
- восприимчивость к проникновению из внешних систем и атакам типа «отказ в обслуживании»;
- отсутствие необходимых обновлений (patch, hotfix) ПО;
- ошибки администрирования, например, выделение незащищенных ресурсов в общее пользование;
- неправильная настройка различных программных систем (межсетевых экранов, Web-серверов, баз данных и др.).

Большинство средств анализа защищенности, охватывающих как сетевой уровень и уровень операционной системы, так уровень приложений построены по архитектуре «менеджер – агенты». *Программа-менеджер* функционирует на управляющей консоли, постоянно взаимодействуя с *модулями-агентами*, которые, как правило, устанавливаются на контролируемых объектах. Данные агенты устанавливаются на компьютеры, выступающие в качестве потребителей этих сетевых ресурсов. На агенты возлагаются функции тестирования объектов контроля и сбора данных об их функционировании. Кроме того, агенты могут вносить изменения в конфигурацию контролируемых объектов по запросу от менеджера.
Сканер уязвимостей (Vulnerability scanner) – программное или аппаратное комплексное решение для сканирования информационной инфраструктуры в реальном времени. Сканер используется для обнаружения брешей (уязвимостей) в сетевом оборудовании, операционной системе, базах данных, приложениях и т. д.
Способы проверки наличия уязвимостей:

- проверка баннеров (пассивное сканирование).
- имитация атак (активное сканирование).