О.В. Сизова

Информационная безопасность

Учебное пособие

Иваново
2015

Министерство образования и науки Российской Федерации

Ивановский государственный химико-технологический университет

О.В. СИЗОВА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Иваново 2015

УДК 004.056(07)
ББК 32.973 я73
С 349

Сизова, О. В.

Информационная безопасность: учеб. пособие / О.В. Сизова; Иван.гос. хим-технол. ун-т. – Иваново, 2015. – 120 с.

Учебное пособие содержит понятие об информационной безопасности, ее роли и значении в системе управления предприятием, краткий обзор основных понятий и категорий информационной безопасности, существующих протоколах и стандартах информационной безопасности, современных тенденциях развития ИТ-угроз и мерах обеспечения информационной безопасности на предприятиях. В пособии приведены тесты для самооценки знаний по изучаемому материалу.

Предназначено для студентов дневной формы обучения по направлению 08.05.00 «Бизнес-информатика».

Ил. 8. Библиогр.: 10 назв.

Печатается по решению редакционно-издательского совета Ивановского государственного химико-технологического университета

Рецензенты:

- доктор экономических наук, профессор кафедры основ экономики функционирования РСЧС С.В. Горинова (ФГБОУ ВО Ивановская пожарно-спасательная академия ГПС МЧС России);
- доктор технических наук, профессор кафедры ОФСЭОН В.Я. Жарницкий (ФГБОУ ВО РГАУ-МСХА им. К.А. Тимирязева)

Оглавление

Введение

Общепризнанным стратегическим фактором роста конкурентоспособности компании является эффективное применение информационных технологий. Многие предприятия в мире переходят к использованию широких возможностей Интернета и электронного бизнеса. *Корпоративные информационные системы* (КИС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании.

Все больше корпоративных систем, приложений и данных становятся доступными из Глобальной сети, вследствие чего компании сталкиваются с возрастающим числом различных угроз для своей информационной инфраструктуры:

- вирусной опасностью;
- несанкционированным доступом;
- атаками типа «отказ в обслуживании»;
- другими видами вторжений, мишенью для которых являются приложения, компьютерные сети и инфраструктура КИС.

Применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности. Поэтому одной из самых актуальных задач, которая стоит сегодня перед разработчиками и поставщиками информационных технологий, является решение проблем информационной безопасности, связанных с широким распространением Интернета, а также сетей intranet и extranet.

Следует заметить, что средства взлома компьютерных сетей и хищения информации развиваются так же быстро, как и все высокотехнологичные компьютерные отрасли. В этих условиях обеспечение информационной безопасности КИС является приоритетной задачей, поскольку от сохранения конфиденциальности, целостности и доступности корпоративных информационных ресурсов во многом зависит эффективность работы КИС.

Задача обеспечения информационной безопасности КИС традиционно решается построением *системы информационной безопасности* (СИБ), определяющим требованием к которой является сохранение вложенных в построение КИС инвестиций.

Создаваемая система информационной безопасности предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к любым элементам корпоративной информационной системы:

- применение открытых стандартов;
- использование интегрированных решений;
- обеспечение масштабирования в широких пределах.

Переход на открытые стандарты составляет одну из главных тенденций развития средств информационной безопасности. Перспективные средства защиты, безусловно, должны поддерживать эти стандарты сегодня.

Под *интегрированными решениями* понимается как интеграция средств защиты с остальными элементами сети (операционными системами, маршрутизаторами, службами каталогов и т.п.), так и интеграция различных технологий безопасности между собой для обеспечения комплексной защиты информационных ресурсов предприятия.

По мере роста и развития КИС система информационной безопасности должна иметь возможность легко масштабироваться без потери целостности и управляемости. Масштабируемость средств защиты позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания системы защиты.

В учебном пособии рассмотрены самые прогрессивные и перспективные технологии информационной защиты, которые способны обеспечить надежную защиту ресурсов корпоративной информационной системы. К ним относятся:

- криптографическая защита данных для обеспечения конфиденциальности, целостности и подлинности информации;
- технологии аутентификации для проверки подлинности пользователей и объектов сети;
- технологии межсетевых экранов для защиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
- технологии виртуальных защищенных каналов и сетей *VPN* для защиты информации, передаваемой по открытым каналам связи;
- гарантированная идентификация пользователей путем применения токенов (смарт-карты, touch-memory, ключи для USB-портов и т.п.) и других средств аутентификации;
- управление доступом на уровне пользователей и защита от несанкционированного доступа к информации;
- поддержка инфраструктуры управления открытыми ключами PKI,
- технологии обнаружения вторжений (Intrusion Detection) для активного исследования защищенности информационных ресурсов;
- технологии защиты от вирусов с использованием специализированных комплексов антивирусной профилактики и защиты;
- централизованное управление средствами информационной безопасности на базе единой политики безопасности предприятия;
- комплексный подход к обеспечению информационной безопасности, обеспечивающий рациональное сочетание технологий и средств информационной защиты.

Пособие состоит из 12 тем. Каждая тема имеет два подраздела. В первом подразделе пособия даются методические указания для студентов, где раскрываются основные понятия и технологии обеспечения информационной безопасности. Во втором подразделе представлен набор тестовых заданий для самостоятельной работы студентов.

Тема 1. Основные понятия и анализ угроз информационной безопасности

Рассмотрим основные понятия защиты информации и информационной безопасности компьютерных систем и сетей с учетом определений стандарта ГОСТ Р 50922-96.

Защита информации - это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты - информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Эффективность защиты информации - степень соответствия результатов защиты информации поставленной цели.

Защита информации от утечки - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации злоумышленниками.

Защита информации от несанкционированного воздействия - деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, природных явлений, а также иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств и систем, деятельностью людей и приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа (НСД) - деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Система защиты информации - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-

распорядительными и нормативными документами по защите информации.

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:

- попытки проникновения злоумышленников,
- ошибки персонала,
- выход из строя аппаратных и программных средств,
- стихийные бедствия (землетрясение, ураган, пожар и т.п.).

Современная *автоматизированная система обработки информации* (АС) представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. *Компоненты АС* можно разбить на следующие группы:

- *аппаратные средства* - компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - дисководы, принтеры, контроллеры, кабели, линии связи и т.д.);
- *программное обеспечение* - приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- *данные* - хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- *персонал* - обслуживающий персонал и пользователи.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы (рис. 1).

Рис. 1. Проявления угроз информации

Перечисленные выше *базовые свойства информации* нуждаются в более полном толковании.

Конфиденциальность данных - это статус, предоставленный данным и определяющий требуемую степень их защиты.

К конфиденциальным данным можно отнести, например, следующие:

- личная информация пользователей;
- учетные записи (имена и пароли);
- данные о кредитных картах;
- данные о разработках и различные внутренние документы;
- бухгалтерские сведения.

Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Установление градаций важности защиты защищаемой информации (объекта защиты) называют *категорированием защищаемой информации.*

Под *целостностью информации* понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения.

Достоверность информации - свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Доступ к информации - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации - это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (НСД) к информации характеризуется нарушением установленных правил разграничения доступа.

Доступность информации подразумевает также *доступность компонента или ресурса* компьютерной системы. Вот примерный перечень ресурсов, которые должны быть доступны:

- принтеры;
- серверы;
- рабочие станции;
- данные пользователей;
- любые критические данные, необходимые для работы.

Целостность ресурса или компонента системы - это свойство ресурса или компонента быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация.

С каждым субъектом системы (сети) связывают некоторую информацию (число, строку символов), идентифицирующую субъект. Эта информация является *идентификатором* субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, является *законным (легальным) субъектом. Идентификация субъекта* - это процедура распознавания субъекта по его идентификатору.

Аутентификация субъекта - это проверка подлинности субъекта с данным идентификатором.

Авторизация субъекта - это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* АС понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности.

Уязвимость компьютерной системы - это присущее системе неудачное свойство, которое может привести к реализации угрозы.

Атака на компьютерную систему - это поиск и/или использование злоумышленником той или иной уязвимости системы.

Защищенная система - это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Способ защиты информации - порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Комплекс средств защиты (КСЗ) представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы .

Техника защиты информации - средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Политика безопасности - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз.

Под *угрозой* (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам.

В настоящее время известен достаточно обширный перечень угроз информационной безопасности АС, содержащий сотни позиций. Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты.

Перечень угроз, оценки вероятностей их реализации, а также модель

нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты АС.

Классификация возможных угроз информационной безопасности АС может быть проведена по ряду базовых признаков:

1. *По природе возникновения* различают:

- естественные угрозы, вызванные воздействиями на АС объективных физических процессов или стихийных природных явлений;
- искусственные угрозы безопасности АС, вызванные деятельностью человека.

2. *По степени преднамеренности проявления* различают:

- угрозы, вызванные ошибками или халатностью персонала, например некомпетентное использование средств защиты; ввод ошибочных данных и т.п.;
- угрозы преднамеренного действия, например действия злоумышленников.

3. *По непосредственному источнику угроз.* Источниками угроз могут быть:

- природная среда, например стихийные бедствия, магнитные бури и пр.;
- человек, например вербовка путем подкупа персонала, разглашение конфиденциальных данных и т.п.;
- санкционированные программно-аппаратные средства, например удаление данных, отказ в работе операционной системы;
- несанкционированные программно-аппаратные средства, например заражение компьютера вирусами с деструктивными функциями.

4. *По положению источника угроз.* Источник угроз может быть расположен:

- вне контролируемой зоны АС, например перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств;
- в пределах контролируемой зоны АС, например применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.;
- непосредственно в АС, например некорректное использование ресурсов АС.

5. *По степени зависимости от активности АС.* Угрозы проявляются*:*

- независимо от активности АС, например вскрытие шифров криптозащиты информации;
- только в процессе обработки данных, например угрозы выполнения и распространения программных вирусов.

6. *По степени воздействия на АС* различают:

- пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС, например угроза копирования секретных данных;

- активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС, например внедрение «троянских коней» и вирусов.

7. *По этапам доступа пользователей или программ к ресурсам АС* различают:

- угрозы, проявляющиеся на этапе доступа к ресурсам АС, например угрозы несанкционированного доступа в АС;
- угрозы, проявляющиеся после разрешения доступа к ресурсам АС, например угрозы несанкционированного или некорректного использования ресурсов АС.

8. *По способу доступа к ресурсам АС* различают:

- угрозы с использованием стандартного пути доступа к ресурсам АС, например незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя;
- угрозы с использованием скрытого нестандартного пути доступа к ресурсам АС, например несанкционированный доступ к ресурсам АС путем использования недокументированных возможностей ОС.

9. *По текущему месту расположения информации, хранимой и обрабатываемой в АС,* различают:

- угрозы доступа к информации на внешних запоминающих устройствах, например несанкционированное копирование секретной информации с жесткого диска;
- угрозы доступа к информации в оперативной памяти, например чтение остаточной информации из оперативной памяти; доступ к системной области оперативной памяти со стороны прикладных программ;
- угрозы доступа к информации, циркулирующей в линиях связи, например незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений; незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;
- угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере, например запись отображаемой информации на скрытую видеокамеру.

Как уже отмечалось, опасные воздействия на АС подразделяют на случайные и преднамеренные.

Причинами *случайных воздействий* при эксплуатации АС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные угрозы связаны с целенаправленными действиями

нарушителя. Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является *несанкционированный доступ* (НСД). Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности.

Перечислим *основные каналы несанкционированного доступа*, через которые нарушитель может получить доступ к компонентам АС и осуществить хищение, модификацию и/или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными средствами АС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

В соответствии с существующими подходами считают, что информационная безопасность АС обеспечена в случае, если для информационных ресурсов в системе поддерживаются определенные *уровни*:

- конфиденциальности (невозможности несанкционированного получения какой-либо информации);
- целостности (невозможности несанкционированной или случайной модификации информации);
- доступности (возможности за разумное время получить требуемую информацию).

Тестовые задания по теме

1. Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию называется …

a) защита информации;
b) защита информации от несанкционированного воздействия;
c) защита информации от утечки;
d) защита информации от непреднамеренного воздействия.

2. Информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации называется …

a) объектом защиты;
b) субъектом защиты;
c) уязвимостью защиты;
d) целью защиты.

3. Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации называется …

a) субъектом защиты информации;
b) системой защиты информации;
c) способом защиты информации;
d) техникой защиты информации.

4. Средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации, называются …

a) объектом защиты информации;
b) системой защиты информации;
c) способом защиты информации;
d) техникой защиты информации.

5. Порядок и правила применения определенных принципов и средств защиты информации называются …

a) объектом защиты информации;
b) системой защиты информации;
c) способом защиты информации;
d) техникой защиты информации.

6. Разглашение, несанкционированный доступ, утечка информации

являются угрозой нарушения ее…

a) конфиденциальности;
b) целостности;
c) доступности;
d) достоверности.

7. Подделка, мошенничество, фальсификация информации являются угрозой нарушения ее…

a) конфиденциальности;
b) целостности;
c) доступности;
d) достоверности.

8. Статус, предоставленный данным и определяющий требуемую степень их защиты, это …

a) конфиденциальность данных;
b) целостность данных;
c) доступность данных;
d) достоверность данных.

9. Свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята называется …

a) конфиденциальностью информации;
b) целостностью информации;
c) доступностью информации;
d) достоверностью информации.

10. Свойство ресурса или компонента быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий называется …

a) конфиденциальностью ресурса или компонента;
b) целостностью ресурса или компонента;
c) доступностью ресурса или компонента;
d) достоверностью ресурса или компонента.

11. Процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы (сети) называется …

a) авторизацией субъекта;
b) идентификацией субъекта;
c) аутентификацией субъекта;
d) легализацией субъекта.

12. Совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы, называется …

a) информационной системой;
b) стандартом безопасности;
c) политикой безопасности;
d) комплексом средств защиты.

13. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы от заданного множества угроз, называется …

a) информационной системой;
b) стандартом безопасности;
c) политикой безопасности;
d) комплексом средств защиты.

14. По природе возникновения различают угрозы информационной безопасности автоматизированных систем …

a) естественные и искусственные;
b) угрозы, вызванные ошибками персонала и угрозы преднамеренного действия;
c) угрозы, вызванные природной средой, человеком или техническим средством;
d) пассивные и активные.

15. По степени преднамеренности проявления различают угрозы информационной безопасности автоматизированных систем …

a) естественные и искусственные;
b) угрозы, вызванные ошибками персонала и угрозы преднамеренного действия;
c) угрозы, вызванные природной средой, человеком или техническим средством;
d) пассивные и активные.

16. По непосредственному источнику угроз различают угрозы информационной безопасности автоматизированных систем …

a) естественные и искусственные;
b) угрозы, вызванные ошибками персонала и угрозы преднамеренного действия;
c) угрозы, вызванные природной средой, человеком или техническим средством;
d) пассивные и активные.

Тема 2. Анализ угроз корпоративных сетей

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов TCP (Transport Control Protocol- протокол управления передачей), обеспечивающий совместимость между компьютерами разных типов. Совместимость - одно из основных преимуществ TCP/IP (Internet Protocol - интернет-протокол межсетевого обмена данными), поэтому большинство компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Интернет.

Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. Создавая свое детище, архитекторы стека TCP/IP не видели причин особенно беспокоиться о защите сетей, строящихся на его основе. Поэтому в спецификациях ранних версий протокола IP отсутствовали требования безопасности, что привело к изначальной уязвимости реализации этого протокола.

Стремительный рост популярности интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д.

С точки зрения безопасности распределенные системы характеризуются прежде всего наличием удаленных атак, поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие). И если активное воздействие на трафик может быть зафиксировано, то пассивное воздействие практически не поддается обнаружению. Но поскольку в ходе функционирования распределенных систем обмен служебной информацией между компонентами системы осуществляется тоже по открытым каналам передачи данных, то служебная информация становится таким же объектом атаки, как и данные пользователя.

Трудность выявления факта проведения удаленной атаки выводит этот вид неправомерных действий на первое место по степени опасности.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий список возможных типов сетевых атак на IP-сети постоянно расширяется.

Существует четыре основных категории сетевых атак:

- атаки доступа;
- атаки модификации;
- атаки типа «отказ в обслуживании»;
- комбинированные атаки.

Атака доступа - это попытка получения злоумышленником информации, на ознакомление с которой у него нет разрешения. Атака доступа направлена на нарушение конфиденциальности информации.

Подслушивание (Sniffing). По большей части данные передаются по компьютерным сетям в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в сети, подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют сниффер. *Сниффер пакетов* представляет собой прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Предотвратить угрозу сниффинга пакетов можно с помощью следующих мер и средств:

- применение для аутентификации однократных паролей;
- установка аппаратных или программных средств, распознающих снифферы;
- применение криптографической защиты каналов связи.

Перехват (Hijacking). В отличие от подслушивания, перехват - это активная атака. Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. Перехват имен и паролей создает большую опасность, так как пользователи часто применяют одни и те же логин и пароль для множества приложений и систем.

В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создаст атрибуты нового пользователя, которые можно в любой момент применить для доступа в сеть и к ее ресурсам.

Перехват сеанса (Session Hijacking). По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например, с почтовым сервером, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

После получения доступа к сети у атакующего злоумышленника появляются большие возможности:

- он может посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию:
- он может также наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в связи с перегрузкой;
- наконец, атакующий может блокировать трафик, что приведет к

потере доступа авторизованных пользователей к сетевым ресурсам.

Атака модификации - это попытка неправомочного изменения информации. Такая атака возможна везде, где существует или передается информация; она направлена на нарушение целостности информации.

Изменение данных. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг - изменить их.

Добавление данных. Другой тип атаки - добавление новых данных, например, в информацию об истории прошлых периодов. Взломщик выполняет операцию в банковской системе, в результате чего средства со счета клиента перемешаются на его собственный счет.

Удаление данных. Атака удаления означает перемещение существующих данных, например аннулирование записи об операции из балансового отчета банка, в результате чего снятые со счета денежные средства остаются на нем.

Атака «отказ в обслуживании» (Denial-of-Service, DoS) отличается от атак других типов. Она не нацелена на получение доступа к вашей сети или на извлечение из этой сети какой-либо информации. DoS-атака делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. По существу, эта атака лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Большинство DoS-атак опирается на общие слабости системной архитектуры. В случае использования некоторых серверных приложений (таких, как веб- или FTP-сервер) DoS-атаки могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей.

DoS-атаки трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть вы это сделать уже не сможете, потому что вся полоса пропускания будет занята.

Отказ в доступе к информации. В результате DoS-атаки, направленной против информации, последняя становится непригодной для использования. Информация уничтожается, искажается или переносится в недоступное место.

Отказ в доступе к приложениям. Другой тип DoS-атак направлен на приложения, обрабатывающие или отображающие информацию, либо на компьютерную систему, в которой эти приложения выполняются. В случае успеха подобной атаки решение задач, выполняемых с помощью такого приложения, становится невозможным.

Отказ в доступе к системе. Общий тип DoS-атак ставит своей целью вывод из строя компьютерной системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становятся недоступными.

Отказ в доступе к средствам связи. Целью атаки является коммуникационная среда. Целостность компьютерной системы и информации не нарушается, однако отсутствие средств связи лишает пользователей доступа к этим ресурсам.

Комбинированная атака заключается в применении злоумышленником нескольких взаимно связанных действий для достижения своей цели.

Подмена доверенного субъекта. Большая часть сетей и операционных систем используют IP-адрес компьютера для того, чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом) - такой способ атаки называют фальсификацией адреса, или *IP-спуфингом* (IP-spoofing).

IP-спуфинг имеет место, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за законного пользователя.

Атаки IP-спуфинга часто являются отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность хакера.

Нужно иметь в виду следующее: IP-спуфинг может быть осуществлен при условии, что аутентификация пользователей производится на базе IP-адресов, поэтому введение дополнительных методов аутентификации пользователей (на основе одноразовых паролей или других методов криптографии) позволяет предотвратить атаки IP-спуфинга.

Посредничество. Атака типа «посредничество» подразумевает активное подслушивание, перехват передаваемых данных невидимым промежуточным узлом и управление ими.

Посредничество в обмене незашифрованными ключами (атака Man-in-the-Middl - «человек-в-середине»). Для проведения атаки «человек-в-середине» злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера ISP в любую другую сеть, может, например, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации.

В более общем случае атаки «человек-в-середине» проводятся с целью

- кражи информации,
- перехвата текущей сессии и получения доступа к частным сетевым ресурсам,
- анализа трафика и получения информации о сети и ее пользователях,
- проведения атак типа DoS,
- искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа «человек-в-середине» можно только с помощью криптографии. Для противодействия атакам этого тина

используется инфраструктура управления открытыми ключами PKI (Public Key Infrastructure).

Атака эксплойта. *Эксплойт* (exploit - эксплуатировать) - это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые для проведения атаки на компьютерную систему. Целью атаки может быть как захват контроля над системой, так и нарушение ее функционирования (DoS-атака).

Парольные атаки. Целью этих атак является завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя такие методы, как:

- подмена IP-адреса (IP-спуфииг);
- подслушивание (сниффинг);
- простой перебор.

Часто хакеры пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название «*атака полного перебора*» (Brute Force Attack). Для этой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате злоумышленнику удается подобрать пароль, он получает доступ к ресурсам на правах обычного пользователя.

Средства перехвата, подбора и взлома паролей в настоящее время считаются практически легальными и официально выпускаются достаточно большим числом компании. Они позиционируются как программы для аудита безопасности и восстановления забытых паролей, и их можно на законных основаниях приобрести у разработчиков.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Использование одноразовых паролей и криптографической аутентификации могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные методы аутентификации.

При использовании обычных паролей необходимо придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее восьми символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, $, &, % и т.д.).

Угадывание ключа. Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа трудно и такие попытки требуют больших затрат ресурсов, тем не менее это возможно. Ключ дает возможность расшифровывать и изменять данные.

Атаки на уровне приложений. Эти атаки могут проводиться несколькими способами. Самый распространенный из них состоит в использовании известных слабостей серверного программного обеспечения (FTP, HTTP, веб-сервера).

Главная проблема с атаками на уровне приложений состоит в том, что злоумышленники часто пользуются портами, которым разрешен проход через межсетевой экран.

Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам устранить проблему с помощью коррекционных модулей (*патчей*). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Невозможно полностью исключить атаки на уровне приложений. Хакеры постоянно открывают и публикуют на своих сайтах в Интернете все новые уязвимые места прикладных программ.

Здесь важно осуществлять хорошее системное администрирование - пользоваться самыми свежими версиями операционных систем и приложений и самыми последними коррекционными модулями (патчами);

Анализ сетевого трафика. Целью атак подобного типа являются прослушивание каналов связи и анализ передаваемых данных и служебной информации с целью изучения топологии и архитектуры построения системы, получения критической пользовательской информации (например, паролей пользователей или номеров кредитных карт, передаваемых в открытом виде). Атакам данного типа подвержены такие протоколы, как FTP и Telnet, особенностью которых является то, что имя и пароль пользователя передаются в рамках этих протоколов в открытом виде.

Сетевая разведка. Сетевая разведка - это сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации.

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (Ping Sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. В результате добывается информация, которую можно использовать для взлома

Злоупотребление доверием. Данный тип действий не является атакой в полном смысле этого слова. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Типичным примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте обычно располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит ко взлому и всех остальных, так как эти серверы доверяют другим системам своей сети.

Псевдоантивирусы. Это мошеннические программы, являющиеся фальшивыми антивирусами. Хотя псевдоантивирусы выводят сообщения об обнаружении вредоносных программ, но на самом деле они ничего не

находят и не лечат. Их задача состоит совсем в другом: убедить пользователя в наличии угрозы (на самом деле несуществующей) для компьютера и спровоцировать его уплатить деньги за активацию «антивирусного продукта».

Для распространения фальшивых антивирусов используются способы, применяемые для распространения большинства вредоносных программ, например скрытая загрузка при помощи Trojan-Downloader, эксплуатация уязвимостей взломанных/зараженных сайтов. Мошенники используют также рекламу в Интернете. В настоящее время множество сайтов размещают баннеры с информацией о новом «волшебном» продукте, который избавляет от всех проблем.

Фишинг (Phishing). Фишинг является относительно новым видом интернет-мошенничества, цель которого - получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов, PIN-кодов и другой конфиденциальной информации, дающей доступ к деньгам пользователя. Фишинг использует не технические недостатки ПО, а легковерность пользователей Интернета. Сам термин phishing, созвучный с fishing (рыбная ловля), расшифровывается как password harvesting fishing - выуживание пароля.

Злоумышленник создает практически точную копию сайта выбранного банка (электронной платежной системы, аукциона и т. п.). Затем при помощи спам-технологии по электронной почте рассылается письмо, составленное таким образом, чтобы быть максимально похожим на настоящее письмо от выбранного банка. При составлении письма используются логотипы банка, имена и фамилии реальных руководителей банка. В таком письме, как правило, сообщается о том, что из-за смены программного обеспечения в системе интернет-банкинга пользователю необходимо подтвердить или изменить свои учетные данные. В качестве причины для изменения данных могут быть названы выход из строя ПО банка или же нападение хакеров. Зайдя на ложный сайт, пользователь вводит в соответствующие строки свои конфиденциальные данные (пароль, номер счета, PIN-код), а далее аферисты получают доступ в лучшем случае к его почтовому ящику, а в худшем - к электронному счету.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. В частности, около 5% пользователей не знают простого факта: банки не рассылают писем с просьбой подтвердить в онлайне номер своей кредитной карты и ее PIN- код. Появилось сопряженное с фишингом понятие - фарминг.

Фарминг (Pharming). Это еще один вид мошенничества, ставящий целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на поддельные, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид

мошенничества еще опаснее, так как заметить подделку практически невозможно.

Для защиты от фишинга и фарминга разрабатываются технические средства безопасности, прежде всего плагины для популярных браузеров. Суть защиты заключается в блокировании сайтов, попавших в черные списки мошеннических ресурсов. Следующим шагом могут стать системы генерации одноразовых паролей для интернет-доступа к банковским счетам и аккаунтам в платежных системах, повсеместное распространение дополнительных уровней защиты за счет комбинации ввода пароля с использованием аппаратного USB-ключа.

Применение ботнетов. Ботнет (зомби-сеть) - это сеть компьютеров, зараженных вредоносной программой поведения Backdoor. Backdoor позволяет киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя. Такие программы называются *ботами*.

Хозяин зараженной машины, как правило, даже не подозревает о том, что она используется злоумышленниками. Именно поэтому зараженные вредоносной программой-ботом компьютеры, находящиеся под тайным контролем киберпреступников, называют еще *зомби-компьютерами*, а сеть, в которую они входят, - зомби-сетью. Чаще всего зомби-машинами становятся персональные компьютеры домашних пользователей.

Ботнеты могут использоваться злоумышленниками для решения криминальных задач разного масштаба: от рассылки спама до атак на государственные сети.

Рассылка спама. Это наиболее распространенный и одни из самых простых вариантов эксплуатации ботнетов. По экспертным оценкам, в настоящее время более 80% спама рассылается с зомби-машин. Спам с ботнетов необязательно рассылается владельцами сети. За определенную плату спамеры могут взять ботнет в аренду. Среднестатистический спамер зарабатывает 50-100 тысяч долларов в год. Многотысячные ботнеты позволяют спамерам осуществлять с зараженных машин миллионные рассылки в течение короткого времени. Еще одно «преимущество» ботнетов - возможность сбора адресов электронной почты на зараженных машинах. Украденные адреса продаются спамерам либо используются при рассылке спама самими хозяевами ботнета. При этом растущий ботнет позволяет получать новые и новые адреса.

Анонимный доступ в Сеть. Злоумышленники могут обращаться к серверам в Сети, используя зомби-машины, и от имени зараженных машин совершать киберпреступления, например взламывать веб-сайты или переводить украденные денежные средства.

Продажа и аренда ботнетов. Один из вариантов незаконного заработка при помощи ботнетов основывается на сдаче ботнета в аренду или

продаже готовой сети. Создание ботнетов для продажи является отдельным направлением киберпреступного бизнеса.

Кража конфиденциальных данных. Этот вид криминальной деятельности постоянно привлекает киберпреступников, а с помощью ботнетов «улов» в виде различных паролей (для доступа к электронной почте, FTP-ресурсам, веб-сервисам) и прочих конфиденциальных данных пользователей увеличивается в тысячи раз. Бот, которым заражены компьютеры в зомби-сети, может скачать другую вредоносную программу, например троянца, ворующего пароли. В таком случае инфицированными троянской программой окажутся все компьютеры, входящие в эту зомби-сеть, и злоумышленники смогут заполучить пароли со всех зараженных машин. Украденные пароли перепродаются или используются, в частности, для массового заражения веб-страниц с целью дальнейшего распространения вредоносной программы-бота и расширения зомби-сети.

При построении ***беспроводных сетей*** одной из наиболее острых проблем является обеспечение их безопасности. Если в обычных сетях информация передается по проводам, то радиоволны, используемые для беспроводных решений, достаточно легко перехватить при наличии соответствующего оборудования. Принцип действия беспроводной сети приводит к возникновению большого количества возможных уязвимостей для атак и проникновений.

Оборудование беспроводных локальных сетей WLAN (Wireless Local Area Network) включает в себя точки беспроводного доступа и рабочие станции для каждого абонента.

Точки доступа AP (Access Point) выполняют роль концентраторов, обеспечивающих связь между абонентами и между собой, а также функцию мостов, осуществляющих связь с кабельной локальной сетью и с Интернетом. Каждая точка доступа может обслуживать несколько абонентов. Несколько близко расположенных точек доступа образуют зону доступа Wi-Fi, в пределах которой все абоненты, снабженные беспроводными адаптерами, получают доступ к сети. Такие зоны доступа создаются в местах массового скопления людей: в аэропортах, студенческих городках, библиотеках, магазинах, бизнес-центрах и т. д.

У точки доступа есть идентификатор набора сервисов SSID (Service Set Identifier). SSID - это 32-битная строка, используемая в качестве имени беспроводной сети, с которой ассоциируются все узлы. Идентификатор SSID необходим для подключения рабочей станции к сети. Чтобы связать рабочую станцию с точкой доступа, обе системы должны иметь один и тот же SSID. Если рабочая станция не имеет нужного SSID, то она не сможет связаться с точкой доступа и соединиться с сетью.

Главное различие между проводными и беспроводными сетями связано с наличием неконтролируемой области между конечными точками беспроводной сети. Это позволяет атакующим, находящимся в

непосредственной близости от беспроводных структур, производить целый ряд нападений, которые невозможны в проводном мире.

При использовании беспроводного доступа к локальной сети угрозы безопасности существенно возрастают. Перечислим основные уязвимости и угрозы беспроводных сетей.

Вещание радиомаяка. Точка доступа включает с определенной частотой широковещательный «радиомаяк», чтобы оповещать окрестные беспроводные узлы о своем присутствии. Эти широковещательные сигналы содержат основную информацию о точке беспроводного доступа, включая, как правило, SSID, и приглашают зарегистрироваться беспроводные узлы в данной области. Любая рабочая станция, находящаяся в режиме ожидания, может получить SSID и добавить себя в соответствующую сеть. Вещание радиомаяка является врожденной патологией беспроводных сетей. Многие модели позволяют отключать содержащую SSID часть этого вещания, чтобы несколько затруднить беспроводное подслушивание, но SSID тем не менее посылается при подключении, поэтому все равно существует небольшое окно уязвимости.

Обнаружение WLAN. Для обнаружения беспроводных сетей WLAN используется, например, утилита NetStumber совместно со спутниковым навигатором глобальной системы позиционирования GPS. Данная утилита идентифицирует SSID сети WLAN, а также определяет, используется ли в ней система шифрования WEP. Применение внешней антенны на портативном компьютере делает возможным обнаружение сетей WLAN во время обхода нужного района или поездки по городу. Надежным методом обнаружения WLAN является обследование офисного здания с переносным компьютером в руках.

Подслушивание. Подслушивание ведут для сбора информации о сети, которую предполагается атаковать впоследствии. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое применяется для обычного доступа к этой сети. Беспроводные сети по своей природе позволяют соединять с физической сетью компьютеры, находящиеся на некотором расстоянии от нее, как если бы эти компьютеры находились непосредственно в сети. Это позволяет подключиться к беспроводной сети, располагающейся в здании, человеку, сидящему в машине на стоянке рядом с ним. Атаку посредством пассивного прослушивания практически невозможно обнаружить.

Ложные точки доступа в сеть. Опытный атакующий может организовать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не подозревая, обращаются к этой ложной точке доступа и сообщают ей свои важные реквизиты, например аутентификационную информацию. Этот тип атак иногда применяют в сочетании с прямым глушением, чтобы заглушить истинную точку доступа в сеть.

Отказ в обслуживании. Полную парализацию сети может вызвать атака типа «отказ в обслуживании» (DoS). Цель любой DoS-атаки состоит в создании помехи при доступе пользователя к сетевым ресурсам. Беспроводные системы особенно восприимчивы к таким атакам. Физический уровень в беспроводной сети - абстрактное пространство вокруг точки доступа. Злоумышленник может включить устройство, заполняющее весь спектр на рабочей частоте помехами и нелегальным трафиком, - такая задача не вызывает особых трудностей. Сам факт проведения DoS-атаки на физическом уровне в беспроводной сети трудно докатить.

Атаки типа «человек-в-середине». Атаки типа «человек-в-середине» выполняются на беспроводных сетях гораздо проще, чем на проводных, так как к проводной сети требуется реализовать определенный вид доступа. Обычно атаки «человек-в-середине» используются для нарушения конфиденциальности и целостности сеанса связи. Атаки «человек-в-середине» более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Злоумышленник использует возможность прослушивания и нелегального захвата потока данных с целью изменения его содержимого, необходимого для удовлетворения некоторых своих целей, например для спуфинга IP-адресов, изменения MAC-адреса для имитирования другого хоста и т. д.

Анонимный доступ в Интернет. Незащищенные беспроводные ЛВС (локальные вычислительные сети) обеспечивают хакерам наилучший анонимный доступ для атак через Интернет. Хакеры могут использовать незащищенную беспроводную ЛВС организации для выхода через нее в Интернет, где они будут осуществлять противоправные действия, не оставляя при этом своих следов.

Атаки, используемые хакерами для взлома беспроводных сетей, не ограничиваются описанными выше.

Тестовые задания по теме

1. Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов …

a) TCP;
b) NCP;
c) IKE;
d) L2TP;
e) LCP.

2. Интернет-протокол межсетевого обмена данными – это протокол …

a) TCP;
b) NCP;
c) IKE;
d) IP;
e) LCP.

3. Подслушивание – это атака, относящаяся к …

a) атакам модификации;
b) атакам доступа;
c) атакам типа «отказ в обслуживании»;
d) комбинированным атакам.

4. Перехват – это атака, относящаяся к …

a) атакам модификации;
b) атакам доступа;
c) атакам типа «отказ в обслуживании»;
d) комбинированным атакам.

5. Добавление данных – это атака, относящаяся к …

a) атакам модификации;
b) атакам доступа;
c) атакам типа «отказ в обслуживании»;
d) комбинированным атакам.

6. Подмена доверенного субъекта – это атака, относящаяся к …

a) атакам модификации;
b) атакам доступа;
c) атакам типа «отказ в обслуживании»;
d) комбинированным атакам.

7. Посредничество – это атака, относящаяся к …

a) атакам модификации;
b) атакам доступа;

c) атакам типа «отказ в обслуживании»;
d) комбинированным атакам.

8. Атака эксплойта – это атака, относящаяся к …
a) атакам модификации;
b) атакам доступа;
c) атакам типа «отказ в обслуживании»;
d) комбинированным атакам.

9. Прикладная программа, которая перехватывает все сетевые пакеты, передаваемые через определенный домен, называется …
a) спуфингом;
b) сниффер пакетов;
c) эксплойтом;
d) патчем.

10. Способ атаки, при котором осуществляется подмена IP-адреса отправителя другим адресом, называют …
a) спуфингом;
b) сниффер пакетов;
c) эксплойтом;
d) патчем.

11. Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые для проведения атаки на компьютерную систему называется …
a) спуфингом;
b) сниффер пакетов;
c) эксплойтом;
d) патчем;

12. Коррекционный модуль, который применяются для устранения проблем на уровне приложений, называется …
a) спуфингом;
b) сниффер пакетов;
c) эксплойтом;
d) патчем;

13. Для диагностики неисправностей и анализа трафика в сетях на законных основаниях используются …
a) спуфинги;
b) снифферы;
c) эксплойты;
d) патчи.

14. Атака, при которой по окончании начальной процедуры аутентификации соединение, установленное законным пользователем, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать соединение, называется…

a) перехват сеанса;
b) подслушивание;
c) посредничество;
d) парольная атака.

15. Большинство атак «отказ в обслуживании» опирается на …

a) ошибки оператора;
b) общие слабости системной архитектуры;
c) природные катаклизмы;
d) технические неполадки;

16. Эффективно бороться с атаками типа «человек-в-середине» можно только с помощью …

a) паролей в не текстовой форме;
b) патчей;
c) криптографии;
d) повышения уровня осведомленности пользователей.

17. Для защиты от фишинга и фарминга применяют такие технические средства безопасности как …

a) эксплойты;
b) плагины;
c) снифферы;
d) патчи.

18. Роль концентраторов, обеспечивающих связь между абонентами и между собой, а также функцию мостов, осуществляющих связь с кабельной локальной сетью и с Интернетом, выполняют …

a) инфраструктуры PKI;
b) протоколы Telnet;
c) точки доступа AP;
d) серверы HTTP.

Тема 3. Тенденции развития ИТ-угроз и меры обеспечения информационной безопасности

По мере развития и усложнения ИТ-инфраструктуры автоматически растет количество потенциальных ИТ-угроз и рисков. Кроме того, угрозы становятся все более изощренными, поскольку злоумышленники активно берут на вооружение возможности, открывающиеся по мере развития информационных технологий.

По данным отчета «Trends in IT Security Threats», подготовленного Computer Economics, в десятку наиболее опасных ИТ-угроз входят:

- угрозы инсайдеров;
- угрозы от вредоносных программ (троянцев, компьютерных вирусов, червей, spyware- и adware-модулей);
- неавторизованный доступ со стороны внешних нарушителей;
- DoS-и DDoS-атаки;
- электронное мошенничество;
- фишинг-атаки;
- фарминг-атаки;
- спам;
- угроза физической потери носителя информации;
- электронный вандализм и саботаж.

Традиционно наиболее опасными считались внешние угрозы (в первую очередь вирусы), защите от которых уделялось особое внимание. Однако постепенно все больше возрастает опасность внутренних ИТ-угроз. Инсайдерские угрозы начинают опережать угрозы от вредоносных программ как по числу инцидентов, так и по объему причиняемого ущерба.

В последние годы растет криминализация атак на информационные системы. Растущий обмен информационными данными в Интернете и электронные платежи более всего привлекают злоумышленников.

Области, наиболее уязвимые для атак:

- интернет-деньги и интернет-банкинг;
- удаленные хранилища данных и приложений. Информацию и приложения все чаще размещают на удаленных внешних серверах, что позволяет преступникам взламывать трафик и получать доступ к финансовой, конфиденциальной и личной информации;
- онлайн-игры. Преступления в этой области - это кража паролей и виртуальной собственности для последующей их продажи и получения хорошей прибыли;
- онлайновые биржевые агентства. Является весьма привлекательной целью для преступников, потому что любая биржевая информация всегда пользуется повышенным спросом;
- Web 2.0. Социальные сети, блоги, форумы, wiki-ресурсы, MySpace, YouTube, Twitter. Эти удобные технологии обмена информацией, позволяющие легко загружать и публиковать данные, делают его участников уязвимыми для заражений вредоносными программами.

Существует два подхода к проблеме обеспечения безопасности компьютерных систем и сетей: фрагментарный и комплексный.

Фрагментарный подход направлен на противодействие четко определенным угрозам в заданных условиях. В качестве примеров реализации такого подхода можно указать

- отдельные средства управления доступом,
- автономные средства шифрования,
- специализированные антивирусные программы и т. п.

Достоинством такого подхода является высокая избирательность к конкретной угрозе. Его существенным недостатком является отсутствие единой защищенной среды обработки информации. Фрагментарные меры защиты информации обеспечивают защиту конкретных объектов компьютерной системы (КС) только от конкретной угрозы. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Комплексный подход ориентирован на создание защищенной среды обработки информации в КС, объединяющей в единый комплекс разнородные меры противодействия угрозам. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень безопасности КС, что является несомненным достоинством комплексного подхода. К недостаткам этого подхода относятся

- ограничения на свободу действий пользователей КС,
- чувствительность к ошибкам установки и настройки средств защиты,
- сложность управления.

Комплексный подход применяют для защиты КС крупных организаций или небольших КС, выполняющих ответственные задачи либо обрабатывающих особо важную информацию. Этот подход нашел свое отражение в различных стандартах.

Комплексный подход к проблеме обеспечения безопасности основан на разработанной для конкретной КС политике безопасности. Политика безопасности регламентирует эффективную работу средств защиты КС. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Надежная система безопасности сети не может быть создана без эффективной политики сетевой безопасности.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (стандарты, законы, норматив акты и т. п.);
- административно-организационного (действия общего характера, предпринимаемые руководством организации, и конкретные меры безопасности, касающиеся людей);
- программно-технического (конкретные технические меры).

Меры законодательного уровня. Они очень важны для обеспечения информационной безопасности. К этому уровню можно отнести весь комплекс мер, направленных на создание и поддержание в обществе

негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности.

Меры административно-организационного уровня. Администрация организации должна сознавать необходимость поддержания режима безопасности и выделения на эти цели соответствующих ресурсов. Основой мер защиты административно-организационного уровня является:

- политика безопасности (совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов организации);
- комплекс организационных мер.

К комплексу организационных мер относятся меры безопасности, реализуемые людьми. Можно выделить следующие *группы организационных мер*:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Для каждой группы в каждой организации должен существовать набор регламентов, определяющих действия персонала.

Для поддержания режима информационной безопасности особенно важны меры *программно-технического уровня*, поскольку основная угроза компьютерным системам исходит от них самих:

- сбои оборудования;
- ошибки программного обеспечения;
- промахи пользователей и администраторов и т. п.

Меры и средства программно-технического уровня. В рамках современных информационных систем должны быть доступны по крайней мере следующие механизмы безопасности:

- идентификация и проверка подлинности пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- экранирование;
- обеспечение высокой доступности.

Необходимость применения стандартов. Информационные системы компаний почти всегда построены на основе программных и аппаратных продуктов различных производителей. Дело в том, что на данный момент нет ни одной компании-разработчика, которая предоставила бы потребителю полный перечень средств (от аппаратных до программных) для построения современной ИС. Чтобы обеспечить в разнородной ИС надежную защиту информации, требуются специалисты высокой квалификации, которые будут отвечать за безопасность каждого компонента ИС:

- правильно их настраивать;
- постоянно отслеживать происходящие изменения;

- контролировать работу пользователей.

Очевидно, что чем разнороднее информационная система, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах устройств защиты, межсетевых экранов, шлюзов и VPN, а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, партнеров и заказчиков приводят к созданию сложной среды защиты, трудной для управления, а иногда и имеющей проблемы совместимости.

Стандарты являются необходимой базой, обеспечивающей совместимость продуктов разных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности, и определяют критерии управления безопасностью.

Комплексный подход к решению проблемы обеспечения безопасности, рациональное сочетание законодательных, административно-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам являются тем фундаментом, на котором строится вся система защиты корпоративных сетей.

Тестовые задания по теме

1. Подход, направленный на противодействие четко определенным угрозам ИБ в заданных условиях, называется …

a) фрагментарным;
b) комплексным;
c) системным;
d) функциональным.

2. Подход, ориентированный на создание защищенной среды обработки информации в корпоративной системе, объединяющей в единый комплекс разнородные меры противодействия угрозам, называется …

a) фрагментарным;
b) комплексным;
c) системным;
d) функциональным.

3. Существенным недостатком фрагментарного подхода к проблеме обеспечения безопасности компьютерных систем и сетей является …

a) ограничение на свободу действий пользователей КС;
b) чувствительность к ошибкам установки и настройки средств защиты;
c) отсутствие единой защищенной среды обработки информации;
d) сложность управления.

4. Недостатком комплексного подхода к проблеме обеспечения безопасности компьютерных систем и сетей *не является* …

a) ограничения на свободу действий пользователей КС;
b) чувствительность к ошибкам установки и настройки средств защиты;
c) отсутствие единой защищенной среды обработки информации;
d) сложность управления.

5. К законодательному уровню защиты интересов субъектов информационных отношений относятся…

a) политика безопасности;
b) реагирование на нарушения режима безопасности;
c) протоколирование и аудит;
d) нормативные акты.

6. К законодательному уровню защиты интересов субъектов информационных отношений относятся…

a) политика безопасности;
b) реагирование на нарушения режима безопасности;
c) стандарты;

d) обеспечение высокой доступности.

7. К административно-организационному уровню защиты интересов субъектов информационных отношений относятся…

a) политика безопасности;
b) управление доступом;
c) стандарты;
d) обеспечение высокой доступности.

8. К административно-организационному уровню защиты интересов субъектов информационных отношений относятся…

a) стандарты;
b) планирование восстановительных работ;
c) управление доступом;
d) обеспечение высокой доступности.

9. К программно-техническому уровню защиты интересов субъектов информационных отношений относятся…

a) стандарты;
b) планирование восстановительных работ;
c) управление доступом;
d) реагирование на нарушения режима безопасности.

10. К программно-техническому уровню защиты интересов субъектов информационных отношений относятся…

a) стандарты;
b) протоколирование и аудит;
c) управление персоналом;
d) реагирование на нарушения режима безопасности.

11. Необходимой базой, обеспечивающей совместимость продуктов разных производителей при создании систем сетевой безопасности в гетерогенных средах, являются …

a) стандарты;
b) протоколирование и аудит;
c) законы;
d) нормативные акты.

Тема 4. Политика информационной безопасности

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

Обычно корпоративная информационная система представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения:

- компьютеров;
- операционных систем;
- сетевых средств;
- СУБД;
- разнообразных приложений.

Все эти компоненты обычно обладают собственными средствами защиты, которые нужно согласовать между собой.

Можно построить такую политику безопасности, которая будет устанавливать:

- кто имеет доступ к конкретным активам и приложениям;
- какие роли и обязанности будут иметь конкретные лица;
- предусмотреть процедуры безопасности, четко предписывающие, как должны выполняться конкретные задачи безопасности.

Индивидуальные особенности работы сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам. Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалисту по отчетности доступны только финансовые данные этих сотрудников. А рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого рядом более конкретных документов специализированных политик и процедур безопасности.

Политика безопасности обычно оформляется в виде документа, включающего такие разделы, как:

- описание проблемы;
- область применения;
- позиция организации;
- распределение ролей и обязанностей;
- санкции и др.

Для того чтобы ознакомиться с основными понятиями политики безопасности, рассмотрим в качестве конкретного примера гипотетическую локальную сеть, принадлежащую некоторой организации, и ассоциированную с ней политику безопасности.

Описание проблемы. Информация, циркулирующая в рамках локальной сети, является критически важной. Локальная сеть позволяет сотрудникам совместно использовать программы и данные, что увеличивает угрозу

безопасности. Эти повышенные меры безопасности и являются темой данного документа.

Область применения. В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия.

Позиция организации. Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. Более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- обеспечение анализа регистрационной информации;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия с имеющимися законами и общей политикой безопасности организации.

Распределение ролей и обязанностей. За реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи сети.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей и за контакты с ними.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности.

Пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Санкции. Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.

Дополнительная информация. Конкретным группам исполнителей могут потребоваться для ознакомления какие-то дополнительные документы, в частности документы специализированных политик и процедур безопасности, а также другие руководящие указания.

Обычно политика безопасности организации включает следующие компоненты (рис. 2):

- базовая политика безопасности;
- процедуры безопасности;
- специализированные политики безопасности.

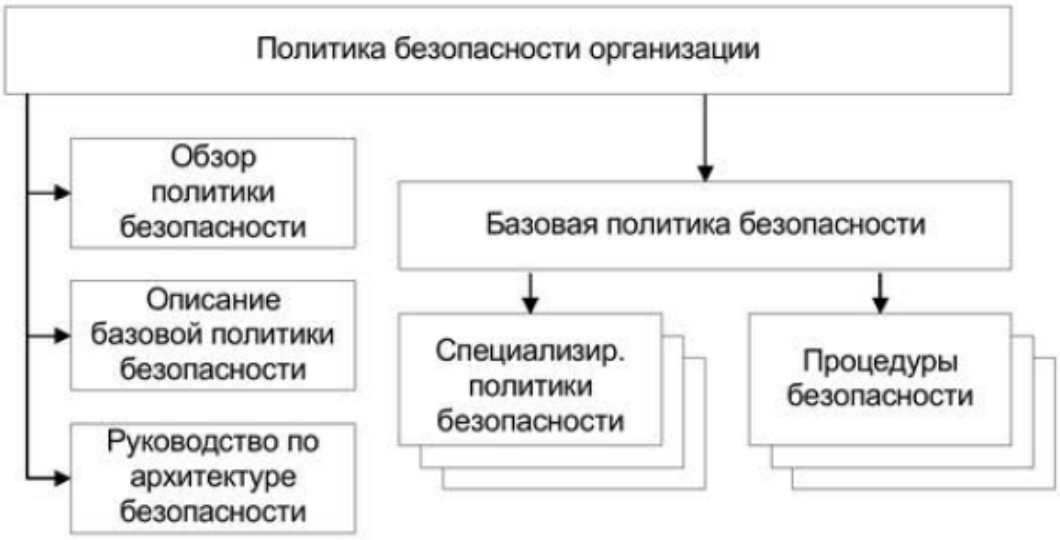

Рис. 2. Структура политики безопасности организации

Основные положения политики безопасности организации описываются в следующих документах:

- обзор политики безопасности;
- описание базовой политики безопасности;
- руководство по архитектуре безопасности.

Главным компонентом политики безопасности организации является базовая политика безопасности.

Базовая политика безопасности устанавливает:

- как организация обрабатывает информацию;
- кто может получить к ней доступ;
- как это можно сделать.

В описании базовой политики безопасности определяются разрешенные и запрещенные действия, а также указываются необходимые средства управления в рамках реализуемой архитектуры безопасности.

Обзор политики безопасности:

- раскрывает цель политики безопасности;
- описывает ее структуру;
- подробно излагает, кто и за что отвечает;
- устанавливает процедуры и предполагаемые временные рамки для внесения изменений.

Руководство по архитектуре безопасности детально определяет контрмеры против угроз, раскрытых при оценке рисков. Это руководство описывает компоненты архитектуры безопасности сети, рекомендует конкретные продукты безопасности и дает инструкции, как их развернуть и управлять ими. В частности, это руководство может содержать рекомендации:

- где следует поставить межсетевые экраны;
- когда использовать шифрование;
- где разместить веб-серверы;
- как организовать управление коммуникациями с бизнес-партнерами и заказчиками.

Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

Специализированные политики безопасности.

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

- политики, затрагивающие значительное число пользователей;
- политики, связанные с конкретными техническими областями.

К специализированным политикам, затрагивающим значительное число пользователей, относятся:

- политика допустимого использования;
- политика удаленного доступа к ресурсам сети;
- политика защиты информации;
- политика защиты паролей и др.

К специализированным политикам, связанным с конкретными техническими областями, относятся:

- политика конфигурации межсетевых экранов;
- политика по шифрованию и управлению криптоключами;
- политика безопасности виртуальных защищенных сетей VPN;
- политика по оборудованию беспроводной сети и др.

Рассмотрим подробнее некоторые из ключевых специализированных политик.

Политика допустимого использования. Базовая политика безопасности обычно связана с рядом политик допустимого использования. Целью политики допустимого использования является установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников с целью защиты корпоративных ресурсов и собственной информации. Конкретный тип и количество политик допустимого использования зависят:

- от результатов анализа требований бизнеса;
- от оценки рисков;

- от корпоративной культуры в организации.

Политика допустимого использования предназначается в основном для конечных пользователей. Эта политика указывает пользователям, какие действия разрешаются, а какие запрещены.

Политика допустимого использования должна установить:

- ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;
- возможность читать и копировать файлы, которые не являются собственными документами пользователей, но доступны им;
- уровень допустимого использования для электронной почты и доступа в Сеть.

Для политики допустимого использования не существует специального формата. В этой политике должно быть указано имя сервиса, системы или подсистемы (например, политика использования компьютера, электронной почты, портативных компьютеров и паролей) и описано в самых четких терминах разрешенное и запрещенное поведение. В этой политике должны быть также подробно описаны последствия нарушения ее правил и санкции, накладываемые на нарушителя.

Политика удаленного доступа. Целью политики удаленного доступа является установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании.

Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими удаленного соединения с сетью компании.

Политика удаленного доступа должна определить:

- какие методы разрешаются для удаленного доступа;
- каковы ограничения на данные, к которым можно получить удаленный доступ;
- кто может иметь удаленный доступ.

Защищенный удаленный доступ должен быть строго контролируемым. Контроль доступа целесообразно выполнять с помощью одноразовой парольной аутентификации или открытых/секретных ключей.

Все хосты, которые подключены к внутренним сетям компании с помощью технологий удаленного доступа, должны использовать самое современное антивирусное обеспечение.

Процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики, т. е. как реализовывать политики безопасности. По существу, процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач.

Многие процедуры, связанные с безопасностью, должны быть стандартными средствами в любом подразделении. В качестве примеров можно указать процедуры для:

- резервного копирования и внесистемного хранения защищенных копий;
- вывода пользователя из активного состояния и/или архивирования его логина и пароля, применяемые сразу, как только данный пользователь увольняется из организации.

Разработка политики безопасности является ключевым этапом построения защищенной информационной системы или сети.

Основные этапы программы обеспечения безопасности:

- определение ценности технологических и информационных активов организации;
- оценка рисков этих активов (сначала путем идентификации тех угроз, для которых каждый актив является целевым объектом, а затем оценкой вероятности того, что эти угрозы будут реализованы на практике);
- установление уровня безопасности, определяющего защиту каждого актива, то есть мер безопасности, которые можно считать рентабельными для применения;
- формирование на базе предыдущих этапов политики безопасности организации;
- привлечение необходимых финансовых ресурсов для реализации политики безопасности, приобретение и установка требуемых средств безопасности;
- проведение разъяснительных мероприятий и обучения персонала для поддержки сотрудниками и руководством требуемых мер безопасности;
- регулярный контроль пошаговой реализации плана безопасности с целью выявления текущих проблем, учета изменения внешнего окружения и внесение необходимых изменений в состав персонала.

Одним из первых шагов является создание команды по разработке политики безопасности организации. В состав команды следует включать квалифицированных специалистов, хорошо разбирающихся в требованиях бизнеса, информационных технологиях и безопасности, юриста и члена руководства, который сможет проводить в жизнь эту политику безопасности.

Как только создана такая команда, ее первым шагом является *анализ требований бизнеса*. Члены команды с различными позициями и точками зрения должны проанализировать требования бизнеса к использованию компьютерных и сетевых сервисов.

После анализа и систематизации требований бизнеса команда по разработке политики безопасности переходит к *анализу и оценке рисков*. Анализ рисков является важнейшим этапом формирования политики безопасности (рис. 3). Иногда этот этап называют также анализом уязвимостей или оценкой угроз.

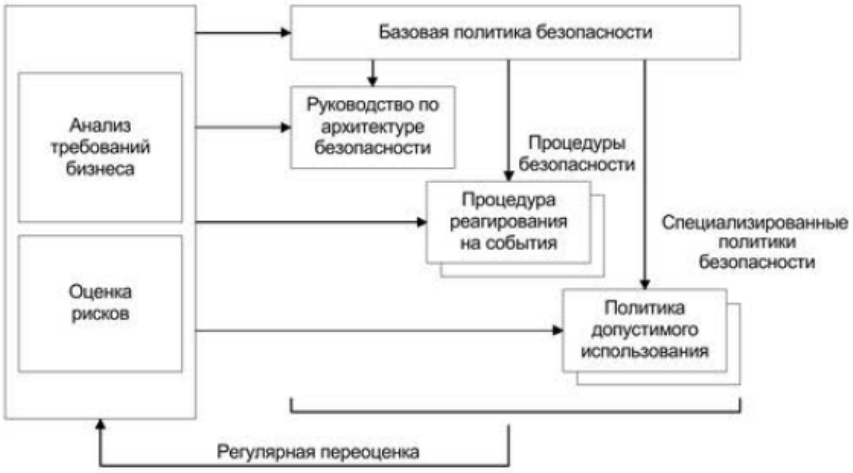

Рис. 3. Схема разработки политики безопасности

На этапе анализа рисков осуществляются следующие действия:

- идентификация и оценка стоимости технологических и информационных активов;
- анализ тех угроз, для которых данный актив является целевым объектом;
- оценка вероятности того, что угроза будет реализована на практике;
- оценка рисков этих активов.

После оценки рисков активов можно переходить к *установлению уровня безопасности*, определяющего защиту каждого актива, то есть мер безопасности, которые можно считать рентабельными для применения.

В принципе, стоимость защиты конкретного актива не должна превышать стоимости самого актива. Необходимо составить подробный перечень всех активов, который включает такие материальные объекты, как серверы и рабочие станции, и такие нематериальные объекты, как данные и программное обеспечение. Должны быть идентифицированы каталоги, которые содержат конфиденциальные файлы или файлы целевого назначения. После идентификации этих активов должно быть проведено определение стоимости замены каждого актива с целью назначения приоритетов в перечне активов.

После проведения описанной выше работы можно переходить к непосредственному составлению политики безопасности. В политике безопасности организации должны быть определены используемые стандарты, правила и процессы безопасности.

Стандарты указывают, каким критериям должно следовать управление безопасностью. *Правила* подробно описывают принципы и способы управления безопасностью. *Процессы* должны осуществлять точную реализацию правил в соответствии с принятыми стандартами.

Кроме того, политика безопасности должна определить значимые для безопасности *роли* и указать *ответственности этих ролей*.

Тестовые задания по теме

1. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов, называется …

a) политикой безопасности;
b) нормативными актами;
c) стандартами ИБ;
d) протоколами ИБ.

2. За обеспечение непрерывного функционирования сети и реализацию технических мер, необходимых для проведения в жизнь политики безопасности отвечают …

a) администраторы сервисов;
b) администраторы локальной сети;
c) операторы;
d) руководители подразделений.

3. За доведение положений политики безопасности до пользователей и за контакты с ними отвечают …

a) администраторы сервисов;
b) администраторы локальной сети;
c) операторы;
d) руководители подразделений.

4. К документам, описывающим основные положения политики безопасности организации *не относятся* …

a) описание базовой политики безопасности;
b) руководство по архитектуре безопасности;
c) процедуры безопасности;
d) обзор политики безопасности.

5. Базовая политика безопасности устанавливает …

a) как организация обрабатывает информацию;
b) цель политики безопасности;
c) структуру безопасности;
d) как организовать управление коммуникациями с бизнес-партнерами и заказчиками.

6. Обзор политики безопасности описывает …

a) кто может получить доступ к информации;
b) цель политики безопасности;
c) как можно получить доступ к информации;
d) как организовать управление коммуникациями с бизнес-партнерами и заказчиками.

7. Руководство по архитектуре безопасности определяет …

a) кто может получить доступ к информации;
b) как можно получить доступ к информации;
c) когда использовать шифрование;
d) структуру безопасности.

8. К специализированным политикам, затрагивающим значительное число пользователей, относятся:

a) политика допустимого использования;
b) политика по шифрованию и управлению криптоключами;
c) политика безопасности виртуальных защищенных сетей VPN;
d) политика по оборудованию беспроводной сети.

9. К специализированным политикам, связанным с конкретными техническими областями, относятся:

a) политика допустимого использования;
b) политика удаленного доступа к ресурсам сети;
c) политика защиты информации;
d) политика по оборудованию беспроводной сети.

10. Каким критериям должно следовать управление безопасностью указывают ...

a) правила ИБ;
b) стандарты ИБ;
c) процессы ИБ;
d) нормативы ИБ.

11. Подробно описывают принципы и способы управления безопасностью …

a) правила ИБ;
b) стандарты ИБ;
c) процессы ИБ;
d) нормативы ИБ.

12. Осуществление точной реализации правил в соответствии с принятыми стандартами обеспечивают …

a) законы ИБ;
b) протоколы ИБ;
c) процессы ИБ;
d) нормативы ИБ.

Тема 5. Стандарты информационной безопасности

Главная задача стандартов информационной безопасности - создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители заинтересованы в методике, которая позволяет обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов и в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора.

Эксперты по квалификации и специалисты по сертификации рассматривают стандарты как инструмент, который позволяет им оценить уровень безопасности, обеспечиваемый продуктами информационных технологий, и предоставить потребителям возможность сделать обоснованный выбор.

Таким образом, перед стандартами информационной безопасности стоит непростая задача - примирить три разных точки зрения и создать эффективный механизм взаимодействия всех сторон.

Необходимость в таких стандартах была осознана достаточно давно, и в этом направлении достигнут существенный прогресс, закрепленный в документах разработки 1990-х годов. Первым и наиболее известным документом была *Оранжевая книга* «Критерии безопасности компьютерных систем» Министерства обороны США. В этом документе определено четыре уровня безопасности – D, C, B и A. По мере перехода от уровня D до A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3). Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее защита должна удовлетворять оговоренным требованиям.

К другим важным стандартам информационной безопасности этого поколения относятся:

- руководящие документы Гостехкомиссии России;
- Европейские критерии безопасности информационных технологий;
- Федеральные критерии безопасности информационных технологий США;
- Канадские критерии безопасности компьютерных систем.

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасностью компании. Это, прежде всего, международные стандарты управления информационной безопасностью ISO 15408, ISO 17799 и некоторые другие.

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации, которые могут быть использованы в отечественных условиях.

Стандарты ISO/IEC 17799:2000 (BS 7799:2000)

В настоящее время международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью - Информационные технологии» является одним из наиболее известных в области защиты информации.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация корпоративных информационных ресурсов и управление ими;
- кадровый менеджмент и информационная безопасность;
- физическая безопасность;
- администрирование безопасности корпоративных информационных систем;
- управление доступом;

- требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
- управление бизнес-процессами компании с точки зрения информационной безопасности;
- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 «Спецификации систем управления информационной безопасностью» определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов (British Standards Institution - BSI), изданные в период 1995- 2003 годов.

В 2002 году международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте этого стандарта большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях.

Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. Важное место в этой системе стандартов занимает стандарт ISO 15408, известный как «*Общие критерии*».

В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК - полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

В концепцию «Общих критериев» входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Требования «Общих критериев» являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Стандарт ISO 15408 поднял стандартизацию информационных технологий на межгосударственный уровень. Возникла реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет

осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем, а это, в свою очередь, откроет новые сферы применения информационных технологий.

Стандарты для беспроводных сетей

Стандарт IEEE 802.11

В 1997 году была ратифицирована первая спецификация беспроводного стандарта IEEE 802.11, обеспечивающего передачу данных с гарантированной скоростью 1 Мбит/с (в некоторых случаях до 2 Мбит/с) в полосе частот 2,4 ГГц. Эта полоса частот доступна для нелицензионного использования в большинстве стран мира.

Стандарт IEEE 802.11 является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей WLAN (Wireless Local Area Network). Основные из них:

- протокол управления доступом к среде MAC (Medium Accsess Control - нижний подуровень канального уровня);
- протокол PHY передачи сигналов в физической среде. В качестве физической среды допускается использование радиоволн и инфракрасного излучения.

В основу стандарта IEEE 802.11 положена сотовая архитектура, причем сеть может состоять как из одной, так и из нескольких ячеек. Каждая сота управляется базовой станцией, называемой *точкой доступа AP* (Access Point), которая вместе с находящимися в пределах радиуса ее действия рабочими станциями пользователей образует базовую зону обслуживания BSS (Basic Service Set). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему DS (Distribution System), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует расширенную зону обслуживания ESS (Extended Service Set).

Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в многосотовых системах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения, однако строгих спецификаций по реализации роуминга стандарт 802.11 не предусматривает.

Для защиты WLAN стандартом IEEE 802.11 предусмотрен алгоритм WEP (Wired Equivalent Privacy). Он включает средства противодействия несанкционированному доступу к сети, а также шифрование для предотвращения перехвата информации.

Однако заложенная в первую спецификацию стандарта IEEE 802.11 скорость передачи данных в беспроводной сети уже не удовлетворяла потребностям пользователей.

Чтобы сделать технологию Wireless LAN недорогой, популярной и удовлетворяющей жестким требованиям бизнес-приложении, разработчики

были вынуждены создать семейство новых спецификаций стандарта IEEE 802.11 a, b,..., i.

Стандарт IEEE 802.11i

Этот стандарт решил существовавшие проблемы в области аутентификации и протокола шифрования, обеспечив значительно более высокий уровень безопасности. Стандарт 802.11i может применяться в сетях Wi-Fi, независимо от используемого стандарта - 802.11a, b или g.

В настоящее время существует два очень похожих стандарта - WPA и 802.11i. Они оба применяют механизм 802.1x для обеспечения надежной аутентификации, оба используют сильные алгоритмы шифрования, оба предназначены для замены протокола WEP. Основное отличие двух стандартов заключается в использовании различных механизмов шифрования.

Стандарт 802.11i предполагает наличие трех участников *процесса аутентификации*:

- сервер аутентификации AS (Authentication Server);
- точка доступа AP (Access Point);
- рабочая станция STA (Station).

В процессе шифрования данных участвуют только AP и STA. Стандарт предусматривает двустороннюю аутентификацию (в отличие от WEP, где аутентифицируется только рабочая станция, но не точка доступа). При этом местами принятия решения о разрешении доступа являются сервер аутентификации AS и рабочая станция STA, а местами исполнения этого решения - точка доступа AP и STA.

Для работы по стандарту 802.11i создается иерархия ключей, включающая:

- мастер-ключ МК (Master Key);
- парный мастер-ключ РМК (Pairwise Master Key);
- парный временный ключ РТК (Pairwise Transient Key);
- групповые временные ключи GTK (Group Transient Key), служащие для защиты широковещательного сетевого трафика.

МК - это симметричный ключ, реализующий решение STA и AS о взаимной аутентификации. Для каждой сессии создается новый МК.

РМК - обновляемый симметричный ключ, владение которым означает разрешение (авторизацию) на доступ к среде передачи данных в течение данной сессии. РМК создается на основе МК. Для каждой пары STA и AP в каждой сессии создается новый РМК.

РТК - это коллекция операционных ключей, которые используются для привязки РМК к данным STA и AP, для распространения GTK и шифрования данных.

Процесс аутентификации и доставки ключей определяется стандартом 802.1x. Он предоставляет возможность использовать в беспроводных сетях такие традиционные серверы аутентификации, как RADIUS. Стандарт 802.

11i не определяет тип сервера аутентификации, но использование RADIUS для этой цели является традиционным решением.

Транспортом для сообщений 802.1x служит протокол EAP (Extensible Authentication Protocol). EAP позволяет легко добавлять новые методы аутентификации. Точке доступа не требуется знать об используемом методе аутентификации, поэтому изменение метода никак не затрагивает точку доступа.

Стандарты информационной безопасности для Интернета

В последнее время в мире бурно развивается электронная коммерция посредством сети Интернет. Развитие электронной коммерции в основном определяется прогрессом в области безопасности информации. При этом базовыми задачами являются обеспечение доступности, конфиденциальности, целостности и юридической значимости информации.

Рассмотрим особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколом передачи данных IP/TCP и с акцентом на защиту телекоммуникаций.

Обеспечение безопасности информационных технологий особенно актуально для открытых систем коммерческого применения, которые обрабатывают информацию ограниченного доступа, не содержащую государственную тайну. Под *открытыми системами* понимают совокупности всевозможного вычислительного и телекоммуникационного оборудования разного производства, совместное функционирование которого обеспечивается соответствием требованиям международных стандартов.

Термин «открытые системы» подразумевает также, что если вычислительная система соответствует стандартам, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, в частности, относится и к механизмам криптографической защиты информации или к защите от несанкционированного доступа к информации.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, SET, IPSec. Перечисленные протоколы появились в Интернете сравнительно недавно в ответ па необходимость защиты ценной информации и сразу стали стандартами де-факто.

Протокол SET

Протокол SET (Security Electronics Transaction) - стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту X.509.

SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карт в Интернете. SET обеспечивает:

- кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты;

- целостность и секретность сообщения;
- шифрование ценных и уязвимых данных.

Поэтому SET более правильно было бы назвать *стандартной технологией* или *системой протоколов выполнения безопасных платежей с использованием пластиковых карт через Интернет*. SET позволяет потребителям и продавцам подтвердить подлинность всех участников сделки, происходящей в Интернете, с помощью криптографии, в том числе применяя цифровые сертификаты.

Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее. SET, в отличие от других протоколов, позволяет решать задачи защиты информации в целом. Он обеспечивает следующие специальные требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной наряду с данными об оплате;
- сохранение целостности данных платежей (обеспечивается с помощью цифровой подписи);
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя по кредитной карте (обеспечивается применением цифровой подписи и сертификатов держателя карт);
- аутентификацию продавца и его возможности принимать платежи по пластиковым картам с применением цифровой подписи и сертификатов продавца;
- аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым картам через связь с процессинговой карточной системой (обеспечивается использованием цифровой подписи и сертификатов банка продавца);
- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению со многими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X509, версия 3), которые ассоциируют держателя карты, продавца и банк продавца с радом банковских учреждений платежных систем Visa и MasterCard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Отечественные стандарты безопасности информационных технологий

В таблице 1 указаны нормативные документы по критериям оценки защищенности средств вычислительной техники и автоматизированных систем и документы, регулирующие информационную безопасность (строки

1-10). Здесь же указаны нормативные документы по криптографической защите систем обработки информации и информационных технологий (строки 11-13).

Таблица 1

Российские стандарты, регулирующие ИБ

Стандарт	Наименование
ГОСТ Р ИСО/МЭК 15408-1-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России
ГОСТ Р ИСО/МЭК 15408-2-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России
ГОСТ Р ИСО/МЭК 15408-3-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России
ГОСТ Р 50922-96	Защита информации. Основные термины и определения. Госстандарт России
ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России
ГОСТ Р 51275-99	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России
ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России
ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
ГОСТ 28147-89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
ГОСТ Р 34.10-2001	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования

Введение в 1999 году международного стандарта ISO 15408 в области обеспечения информационной безопасности имело большое значение как для разработчиков компьютерных информационных систем, так и для их пользователей. Стандарт ISO 15408 стал своего рода гарантией качества и надежности сертифицированных по нему программных продуктов. Этот стандарт позволил потребителям лучше ориентироваться при выборе программного обеспечения и приобретать продукты, соответствующие их требованиям безопасности, и, как следствие этого, повысил

конкурентоспособность IT-компаний, сертифицирующих свою продукцию в соответствии с ISO 15408.

С января 2004 года в России действует стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408, который является аналогом стандарта ISO 15408. Стандарт ГОСТ Р ИСО/МЭК 15408, называемый еще «Общими критериями», является на сегодня самым полным стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

Тестовые задания по теме

1. Первым и наиболее известным стандартом информационной безопасности является …

a) «Критерии безопасности компьютерных систем» Министерства обороны США;

b) Европейские критерии безопасности информационных технологий;

c) Федеральные критерии безопасности информационных технологий США;

d) Канадские критерии безопасности компьютерных систем.

2. В настоящее время одним из наиболее известных в области защиты информации является международный стандарт …

a) X509;

b) IEEE 802.11;

c) WPA;

d) ISO/IEC 17799:2000 (BS 7799-1:2000).

3. Все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности входят в концепцию международного стандарта …

a) ISO 15408;

b) IEEE 802.11;

c) WPA;

d) X509.

4. Базовым стандартом, определяющим протоколы, необходимые для организации беспроводных локальных сетей WLAN, является стандарт …

a) X509;

b) IEEE 802.11;

c) WPA;

d) ISO/IEC 17799:2000 (BS 7799-1:2000).

5. Стандартом безопасных электронных транзакций в сети Интернет, предназначенным для организации электронной торговли через Интернет, является …

a) стандарт ISO 15408;
b) стандарт IEEE 802.11;
c) протокол SET;
d) стандарт WPA.

6. Цифровым сертификатом, который ассоциирует держателя карты, продавца и банк продавца с рядом банковских учреждений, является стандарт …

a) ISO 15408;
b) X509;
c) IEEE 802.11;
d) WPA.

7. Стандарт IEEE 802.11 определяет протоколы …

a) MAC и NCP;
b) IP и TCP;
c) PPTP и PHY;
d) MAC и PHY.

8. В основу стандарта IEEE 802.11 положена архитектура …

a) линейная;
b) сотовая;
c) древовидная;
d) сетевая.

9. Для работы по стандарту 802.11i создается иерархия ключей, которая *не включает* …

a) мастер-ключ МК;
b) парный мастер-ключ РМК;
c) одноразовый ключ ОТК;
d) парный временный ключ РТК.

10. Симметричный ключ, реализующий решение рабочей станции и сервера аутентификации о взаимной, называется …

a) мастер-ключ МК;
b) парный мастер-ключ РМК;
c) одноразовый ключ ОТК;
d) парный временный ключ РТК.

11. Обновляемый симметричный ключ, владение которым означает разрешение (авторизацию) на доступ к среде передачи данных в течение данной сессии, называется …

a) мастер-ключ МК;
b) парный мастер-ключ РМК;
c) групповой временный ключ GTK;
d) парный временный ключ РТК.

12. Коллекция операционных ключей, которые используются для привязки парного мастер-ключа к данным рабочей станции и сервера аутентификации, для распространения групповых временных ключей и шифрования данных, называется …

a) мастер-ключ МК;
b) парный мастер-ключ РМК;
c) групповой временный ключ GTK;
d) парный временный ключ РТК.

13. Процесс аутентификации и доставки ключей в стандартах WPA и 802.11i определяется стандартом …

a) X509;
b) SET;
c) 802.1x;
d) 801.1i.

14. Основное преимущество SET по сравнению со многими существующими системами обеспечения информационной безопасности заключается в использовании …

a) цифровых сертификатов;
b) одноразовых паролей;
c) системы открытых ключей;
d) протоколов EAP.

Тема 6. Криптографическая защита информации

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.

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;
- аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легитимность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Основой большинства криптографических средств защиты информации является шифрование данных.

Под шифром понимают совокупность процедур и правил криптографических преобразований, используемых для шифрования и дешифрования информации по ключу шифрования. Под *шифрованием информации* понимается процесс преобразования открытой информации (исходного текста) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют *дешифрованием*.

Обобщенная схема криптосистемы шифрования показана на рис. 4.

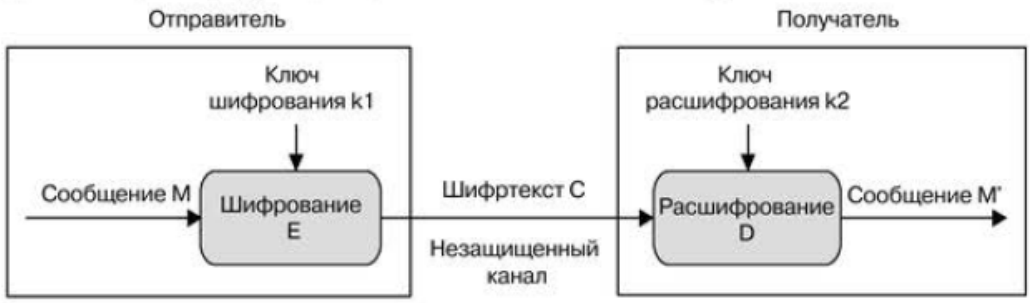

Рис. 4. Обобщенная схема криптосистемы шифрования

Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования $E_{к1}$ с получением в результате шифртекста C.

$$C = E_{к1}(M),$$

где $k1$ - параметр функции E, называемый ключом шифрования.

Шифртекст C, называемый еще *криптограммой*, содержит исходную информацию M в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования $k1$.

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобразования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным.

Обратное преобразование информации выглядит следующим образом:

$$M' = D_{к2}(C).$$

Функция D является обратной к функции E и производит дешифрование шифртекста. Она также имеет дополнительный параметр в виде ключа $к2$. Ключ дешифрования $к2$ должен однозначно соответствовать ключу $к1$, в этом случае полученное в результате дешифрования сообщение M' будет эквивалентно M.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования дешифрования. Соответственно различают два основных *класса криптосистем*:

- симметричные;
- асимметричные.

Известно несколько классификаций *криптографических алгоритмов* (КА). Одна из них подразделяет КА в зависимости от числа ключей, применяемых в конкретном алгоритме:

- бесключевые КА - не используют в вычислениях никаких ключей;
- одноключевые КА - работают с одним ключевым параметром (секретным ключом);
- двухключевые КА - на различных стадиях работы в них применяется два ключевых параметра: секретный и открытый ключи.

Существуют более детальные классификации, например, показанная на рис. 5.

Рис. 5. Классификация криптоалгоритмов защиты информации

Охарактеризуем кратко основные типы КА.

Хэширование - это метод криптозашиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хэш-значение фиксированной длины, однозначно соответствующее исходным данным.

Хэширование может выполняться как с использованием некоторого секретного ключа, так и без него. Такое криптографическое контрольное суммирование широко используется в различных методах защиты информации, в частности, для подтверждения целостности данных, если использование электронной подписи невозможно (например, из-за большой ресурсоемкости) или избыточно. Кроме того, данный метод применяется в схемах электронной подписи («подписывается» обычно хэш-значение данных, а не все данные целиком), а также в схемах аутентификации пользователей (при проверке, действительно ли пользователь является тем, за кого себя выдает).

Симметричное шифрование использует один и тот же ключ как для шифрования, так и для дешифрования информации. Фактически оба ключа (шифрования и дешифрования) могут и различаться, но если в каком-либо КА их легко вычислить один из другого в обе стороны, такой алгоритм однозначно относится к симметричному шифрованию.

Симметричное шифрование подразделяется на два вида: *блочное* и *поточное*, хотя стоит сразу отметить, что в некоторых классификациях они не разделяются и считается, что поточное шифрование - это шифрование блоков единичной длины.

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины (например, 64 или 128 бит). При этом в различных КА или даже в разных режимах работы одного и того же алгоритма блоки могут шифроваться как независимо друг от друга, так и «со сцеплением» - когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

Поточное шифрование применяется прежде всего тогда, когда информацию невозможно разбить на блоки, - скажем, есть некий поток данных, каждый символ которых требуется зашифровать и отправить, не дожидаясь остальных данных, достаточных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

Асимметричное шифрование характеризуется применением двух типов ключей:

- открытого - для шифрования;
- секретного - для ее дешифрования.

Секретный и открытый ключи связаны между собой достаточно сложным соотношением. Главное в этом соотношении - легкость вычисления открытого ключа из секретного и невозможность (за ограниченное время при реальных ресурсах) вычисления секретного ключа из открытого.

Электронная цифровая подпись (ЭЦП) используется для подтверждения целостности и авторства данных. Как и в случае асимметричного шифрования, в данном методе применяются двухключевые алгоритмы с таким же простым вычислением открытого ключа из секретного и практической невозможностью обратного вычисления. Однако назначение ключей ЭЦП совершенно иное. Секретный ключ применяется для вычисления ЭЦП, открытый ключ необходим для ее проверки. При соблюдении правил безопасного хранения секретного ключа никто, кроме его владельца, не в состоянии вычислить верную ЭЦП какого-либо электронного документа.

Симметричные криптосистемы шифрования

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для шифрования и дешифрования информации. Соответственно, с целью предотвращения несанкционированного раскрытия зашифрованной информации все ключи шифрования в симметричных криптосистемах должны держаться в секрете. Именно поэтому симметричные криптосистемы называют *криптосистемами с секретным ключом*. Симметричные криптосистемы называют еще *одноключевыми криптографическими системами* или *криптосистемами с закрытым ключом*. Схема симметричной криптосистемы шифрования показана на рис. 6.

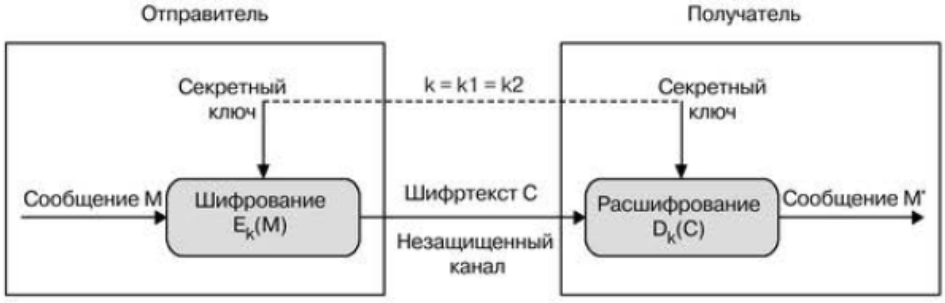

Рис. 6. Схема симметричной криптосистемы шифрования

Данные криптосистемы характеризуются наиболее высокой скоростью шифрования, и с их помощью обеспечивается как конфиденциальность и подлинность, так и целостность передаваемой информации.

Конфиденциальность передачи информации с помощью симметричной криптосистемы зависит от надежности шифра и обеспечения конфиденциальности ключа шифрования. Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например дискете или смарт-карте; обязательно принятие мер, обеспечивающих недоступность персонального ключевого носителя кому-либо, кроме его владельца.

Подлинность обеспечивается за счет того, что без предварительного дешифрования практически невозможно осуществить смысловую модификацию и подлог криптографически закрытого сообщения. Фальшивое сообщение не может быть правильно зашифровано без знания секретного ключа.

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитоприставки), вырабатываемого по секретному ключу. *Имитоприставка* является разновидностью контрольной суммы, то есть некоторой эталонной характеристикой сообщения, по которой осуществляется проверка целостности последнего. Алгоритм формирования имитоприставки должен обеспечивать ее зависимость по некоторому сложному криптографическому закону от каждого бита сообщения. Проверка целостности сообщения выполняется получателем сообщения путем выработки по секретному ключу имитоприставки, соответствующей полученному сообщению, и ее сравнения с полученным значением имитоприставки. При совпадении делается вывод о том, что информация не была модифицирована на пути от отправителя к получателю.

Симметричное шифрование идеально подходит для шифрования информации «для себя», например, с целью предотвратить несанкционированный доступ к ней в отсутствие владельца.

Обладая высокой скоростью шифрования, одноключевые криптосистемы позволяют решать многие важные задачи зашиты информации. Однако автономное использование симметричных криптосистем в компьютерных сетях порождает проблему распределения ключей шифрования между пользователями.

Перед началом обмена зашифрованными данными необходимо обменяться секретными ключами со всеми адресатами. Передача секретного ключа симметричной криптосистемы не может быть осуществлена по общедоступным каналам связи, секретный ключ надо передавать отправителю и получателю по защищенному каналу.

Характерной особенностью симметричных криптоалгоритмов является то, что в ходе своей работы они производят преобразование блока входной информации фиксированной длины и получают результирующий блок того же объема, но недоступный для прочтения сторонним лицам, не владеющим

ключом. Схему работы симметричного блочного шифра можно описать функциями

$$C = E_к (M) \text{ и } M' = D_к (C),$$

где M - исходный (открытый) блок данных; C - зашифрованный блок данных.

Блочные шифры являются той основой, на которой реализованы практически все симметричные криптосистемы. Симметричные криптосистемы позволяют кодировать и декодировать файлы произвольной длины.

Криптоалгоритм считается идеально стойким, если для прочтения зашифрованного блока данных необходим перебор всех возможных ключей до тех пор, пока расшифрованное сообщение не окажется осмысленным. В общем случае стойкость блочного шифра зависит только от длины ключа и возрастает экспоненциально с ее ростом.

К. Шеннон предложил для получения стойких блочных шифров использовать два общих принципа: рассеивание и перемешивание.

Рассеивание представляет собой распространение влияния одного знака открытого текста на много знаков шифртекста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов. Однако шифр должен не только затруднять раскрытие, но и обеспечивать легкость шифрования и дешифрования при известном пользователю секретном ключе.

Распространенным способом достижения эффектов рассеивания и перемешивания является использование *составного шифра*, то есть такого, который может быть реализован в виде некоторой последовательности простых шифров, каждый из которых вносит свой вклад в значительное суммарное рассеивание и перемешивание.

В составных шифрах в качестве простых шифров чаще всего используются простые перестановки и подстановки. При перестановке просто перемешивают символы открытого текста, причем конкретный вид перемешивания определяется секретным ключом. При подстановке каждый символ открытого текста заменяют другим символом из того же алфавита, а конкретный вид подстановки также определяется секретным ключом. Следует заметить, что в современном блочном шифре блоки открытого текста и шифртекста представляют собой двоичные последовательности обычно длиной 64 или 128 бит. При длине 64 бит каждый блок может принимать 2^{64} значений. Поэтому подстановки выполняются в очень большом алфавите, содержащем до $2^{64} = 10^{19}$ «символов».

При многократном чередовании простых перестановок и подстановок, управляемых достаточно длинным секретным ключом, можно получить стойкий шифр с хорошим рассеиванием и перемешиванием.

Характерным признаком блочных алгоритмов является многократное и косвенное использование материала ключа. Это определяется в первую очередь требованием невозможности обратного декодирования в отношении ключа при известных исходном и зашифрованном текстах. Для решения этой задачи в приведенных выше преобразованиях чаще всего используется не само значение ключа или его части, а некоторая, иногда необратимая, функция от материала ключа. Более того, в подобных преобразованиях один и тот же блок или элемент ключа используется многократно.

Алгоритмы симметричного шифрования применяются для абонентского шифрования данных - то есть для шифрования информации, предназначенной для отправки кому-либо, например, через Интернет. Использование только одного секретного ключа для всех абонентов сети, конечно, недопустимо по соображениям безопасности: в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов сети.

Порядок использования систем с симметричными ключами:

1. Симметричный секретный ключ должен создаваться, распространяться и сохраняться безопасным образом.

2. Для получения зашифрованного текста отправитель применяет к исходному сообщению симметричный алгоритм шифрования вместе с секретным симметричным ключом.

3. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается в открытой форме по незащищенным каналам связи.

4. Получатель применяет к зашифрованному тексту тот же самый симметричный алгоритм шифрования/дешифрования вместе с тем же самым симметричным ключом (который уже есть у получателя) для восстановления исходного текста. Его успешное восстановление аутентифицирует того, кто знает секретный ключ.

Для симметричных криптосистем актуальна проблема безопасного распределения симметричных секретных ключей. Всем системам симметричного шифрования присущи следующие *недостатки*:

- принципиальным является требование защищенности и надежности канала передачи секретного ключа для каждой пары участников информационного обмена;
- предъявляются повышенные требования к службе генерации и распределения ключей, обусловленные тем, что для n абонентов при схеме взаимодействия «каждый с каждым» требуется $n\ (n - 1) / 2$ ключей, то есть зависимость числа ключей от числа абонентов является квадратичной; например для $n = 1000$ абонентов требуемое количество ключей будет равно $n\ (n - 1) / 2 = 499\ 500$ ключей.

Поэтому без эффективной организации защищенного распределения ключей широкое использование обычной системы симметричного

шифрования в больших сетях, и в частности в глобальных сетях, практически невозможно.

Асимметричные криптосистемы шифрования

Асимметричные криптографические системы были разработаны в 1970-х годах. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего дешифрования используются различные ключи:

- открытый ключ K – используется для шифрования информации, вычисляется из секретного ключа k;
- секретный ключ k используется для дешифрования информации, зашифрованной с помощью парного ему открытого ключа K.

Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ k из открытого ключа K. Поэтому открытый ключ K может свободно передаваться по каналам связи.

Асимметричные системы называют еще двухключевыми криптографическими системами или *криптосистемами с открытым ключом*.

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом показана на рис. 7.

Рис. 7. Обобщенная схема асимметричной криптосистемы шифрования

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца. Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Особенность асимметричных криптосистем:

1. Открытый ключ K_B и криптограмма C могут быть отправлены по незащищенным каналам.

2. Алгоритмы шифрования и дешифрования – E_K: $M \rightarrow C$, D_k: $C \rightarrow M$ являются открытыми.

У. Диффи и М. Хеллмам сформулировали *требования*, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

1. Вычисление пары ключей (K_B, k_B) получателем В на основе начального условия должно быть простым.

2. Отправитель А, зная открытый ключ K_B и сообщение M, может легко вычислить криптограмму $C = E_K(M)$

3. Получатель В, используя секретный ключ k_B и криптограмму C, может легко восстановить исходное сообщение $M = D_k(C)$

4. Противник, зная открытый ключ K_B, при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему

5. Противник, зная пару (K_B, С), при попытке вычислить исходное сообщение M наталкивается на непреодолимую вычислительную проблему.

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных функций.

Асимметричные криптографические системы обладают следующими важными *преимуществами* перед симметричными криптосистемами:

- в асимметричных криптосистемах решена сложная проблема распределения ключей между пользователями, т. к. каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться по сетевым коммуникациям;
- исчезает квадратическая зависимость числа ключей от числа пользователей; в асимметричной криптосистеме количество используемых ключей связано с количеством абонентов линейной зависимостью (в системе из N пользователей используются $2 \times N$ ключей), а не квадратичной, как в симметричных системах;
- асимметричные криптосистемы позволяют реализовать протоколы взаимодействия сторон, которые не доверяют друг другу, поскольку при использовании асимметричных криптосистем закрытый ключ должен быть известен только его владельцу.

Однако у асимметричных криптосистем существуют и *недостатки*:

- на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;
- по сравнению с симметричным шифрованием асимметричное существенно медленнее, поскольку при шифровании и расшифровке используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;
- необходимо защищать открытые ключи от подмены.

Тестовые задания по теме

1. Целостность и подлинность передаваемых данных обычно достигается с помощью …

a) различных вариантов технологии электронной подписи;

b) взаимной аутентификации абонентов на основе одноразовых паролей;

c) взаимной аутентификации абонентов на основе цифровых сертификатов;

d) взаимной аутентификации абонентов на основе смарт-карт.

2. Процесс восстановления исходного текста по криптограмме называется…

a) шифрованием;

b) дешифрованием;

c) криптоалгоритмом;

d) хэшированием.

3. Исходная информация, в которой последовательность знаков внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования, называется…

a) имитоприставкой;

b) криптоалгоритмом;

c) хэшированием;

d) криптограммой.

4. Различают два основных класса криптосистем …

a) ключевые и бесключевые;

b) активные и пассивные;

c) симметричные и асимметричные;

d) обратимые и необратимые.

5. Криптографические алгоритмы бывают …

a) одноключевые и двухключевые;

b) активные и пассивные;

c) обратимые и необратимые;

d) статические и динамические.

6. Хэширование относится к алгоритмам шифрования …

a) одноключевым;

b) двухключевым;

c) бесключевым;

d) блочным.

7. Симметричное шифрование может быть …

a) бесключевым и двухключевым;
b) активным и пассивным;
c) вероятностным и детерминированным;
d) блочным и поточным.

8. Контрольное преобразование информации, при котором из данных неограниченного размера путем выполнения криптографических преобразований вычисляется значение фиксированной длины, однозначно соответствующее исходным данным, называется…

a) шифрованием;
b) хэшированием;
c) дешифрованием;
d) электронной цифровой подписью.

9. Один и тот же ключ как для шифрования, так и для дешифрования информации использует …

a) ассиметричное шифрование;
b) хэширование;
c) электронная цифровая подпись;
d) симметричное шифрование.

10. Применением двух типов ключей – открытого и секретного – использует …

a) электронная цифровая подпись;
b) хэширование;
c) поточное шифрование;
d) симметричное шифрование.

11. Специальный код, вырабатываемый по секретному ключу, т. е. некоторая эталонная характеристика сообщения, по которой осуществляется проверка целостности последнего, называется…

a) электронной цифровой подписью;
b) хэшированием;
c) имитоприставкой;
d) криптограммой.

12. Для получения стойких блочных шифров используют два общих принципа: …

a) единства и многообразия;
b) рассеивания и перемешивания;
c) легкости и надежности;
d) полноты и достаточности;

13. Распространение влияния одного знака открытого текста на много знаков шифртекста, что позволяет скрыть статистические свойства открытого текста, называется …

a) перемешиванием;
b) покрытием;
c) рассеиванием;
d) пересечением.

14. Зависимость числа ключей от числа абонентов при симметричном шифровании является …

a) линейной;
b) логарифмической;
c) экспоненциальной;
d) квадратичной.

15. Зависимость числа ключей от числа абонентов при асимметричном шифровании является …

a) линейной;
b) логарифмической;
c) экспоненциальной;
d) квадратичной.

16. Преимуществом симметричного шифрования является …

a) отсутствие проблемы распределения ключей между пользователями;
b) высокая скорость;
c) линейная зависимость числа ключей от числа пользователей;
d) возможность реализовать протоколы взаимодействия сторон, которые не доверяют друг другу.

17. Недостатком асимметричного шифрования является …

a) проблема распределения ключей между пользователями;
b) линейная зависимость числа ключей от числа пользователей;
c) низкая скорость шифрования;
d) невозможность реализовать протоколы взаимодействия сторон, которые не доверяют друг другу.

18. Концепция асимметричных криптографических систем с открытым ключом основана на применении …

a) устойчивых функций;
b) обратимых функций;
c) многофакторных функций;
d) однонаправленных функций.

Тема 7. Идентификация, аутентификация и управление доступом

Применение открытых каналов передачи данных создает потенциальные возможности для действий злоумышленников (нарушителей). Поэтому одной из важных задач обеспечения информационной безопасности при взаимодействии пользователей является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны.

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Эту информацию называют *идентификатором* субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

Идентификация - это процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы. Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация - процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация - процедура предоставления пользователю (процессу или устройству) определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации, иными словами, авторизация устанавливает сферу действия пользователя и доступные ему ресурсы.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование - это процесс управления доступом пользователей к ресурсам системы.

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные веб-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации. Примером слабой формы аутентификации может служить использование IP-адреса для определения пользователя.

Для подтверждения своей подлинности субъект может предъявлять системе разные сущности. В зависимости от предъявляемых субъектом сущностей процессы аутентификации могут быть разделены на следующие категории:

- *на основе знания чего-либо*. Примерами могут служить пароль, персональный идентификационный PIN-код (персональный идентификационный номер), а также секретные и открытые ключи, знание которых демонстрируется в протоколах типа запрос-ответ;

на основе обладания чем-либо. Обычно это магнитные карты, смарт-карты, сертификаты, USB-ключи или USB-токены (token - опознавательный признак, маркер);

- *на основе каких-либо неотъемлемых характеристик*. Эта категория включает методы, базирующиеся на проверке *биометрических характеристик пользователя* (голос, радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони и др.). В данной категории не используются криптографические методы и средства. Аутентификация на основе биометрических характеристик применяется для контроля доступа в помещения или к какой-либо технике.

Процессы аутентификации можно также классифицировать *по уровню обеспечиваемой безопасности*. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы:

- простая аутентификация, использующая пароли;
- строгая аутентификация на основе использования многофакторных проверок и криптографических методов;
- биометрическая аутентификация пользователей.

С точки зрения безопасности каждый из перечисленных типов способствует решению своих специфических задач.

Основными атаками на протоколы аутентификации являются:

- *маскарад*. Пользователь пытается выдать себя за другого с целью получения полномочий и возможности действий от лица другого пользователя;
- *подмена стороны аутентификационного обмена*. Злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика;
- *повторная передача*. Заключается в повторной передаче аутентификационных данных каким-либо пользователем;
- *принудительная задержка*. Злоумышленник перехватывает какую-либо информацию и передает ее спустя некоторое время;

- *атака с выборкой текста*. Злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Для предотвращения таких атак при построении протоколов аутентификации применяются следующие *приемы*:

- использование механизмов типа запрос-ответ, меток времени, случайных чисел, идентификаторов, цифровых подписей;
- привязка результата аутентификации к последующим действиям пользователей в рамках системы. Примером подобного подхода может служить осуществление в процессе аутентификации обмена секретными сеансовыми ключами, которые применяются при дальнейшем взаимодействии пользователей;
- периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т. п.

Механизм запроса-ответа состоит в следующем. Если пользователь А хочет быть уверенным, что сообщения, получаемые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент - запрос X (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую функцию $F(X)$). Это невозможно осуществить заранее, так как пользователю В неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий В, пользователь А может быть уверен, что В - подлинный. Недостаток этого метода - возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько устарело пришедшее сообщение, и решить не принимать его, поскольку оно может быть ложным. При использовании отметок времени возникает проблема *допустимого временного интервала задержки* для подтверждения подлинности сеанса. Ведь сообщение с «временным штемпелем» в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При сравнении и выборе протоколов аутентификации необходимо учитывать следующие характеристики:

- *наличие взаимной аутентификации*. Это свойство отражает необходимость обоюдной аутентификации между сторонами аутентификационного обмена;
- *вычислительная эффективность*. Количество операций, необходимых для выполнения протокола;

- *коммуникационная эффективность*. Данное свойство отражает количество сообщений и их длину, необходимую для осуществления аутентификации;
- *наличие третьей стороны*. Примером третьей стороны может служить доверенный сервер распределения симметричных ключей или сервер, реализующий дерево сертификатов для распределения открытых ключей;
- *гарантии безопасности*. Примером может служить применение шифрования и цифровой подписи.

Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене электронными документами существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном электронном документе.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- *активный перехват* - нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- *маскарад* - абонент С посылает документ абоненту В от имени абонента А;
- *ренегатство* - абонент А заявляет, что не посылал сообщения абоненту В, хотя па самом деле послал;
- *подмена* - абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А,
- *повтор* - абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными *достоинствами*:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый.

Система ЭЦП включает две основные процедуры:

- процедуру формирования цифровой подписи;
- процедуру проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки - открытый ключ отправителя.

В новом законе «Об электронной подписи», подписанным Президентом России Д. А. Медведевым 6 апреля 2011 года, определены следующие виды электронных подписей: простая электронная подпись и усиленная электронная подпись. При этом различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Эта подпись предназначена для подписания электронных сообщений, направляемых в государственный орган, орган местного самоуправления или должностному лицу.

Усиленная электронная подпись позволяет не только идентифицировать отправителя, но и подтвердить, что с момента подписания документ не менялся.

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая имеет все признаки неквалифицированной электронной подписи и следующие дополнительные признаки:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с новым законом.

Квалифицированная электронная подпись предназначена для взаимодействия госорганов с использованием государственных информационных систем. Эта подпись дополнительно подтверждается

сертификатом от аккредитованного удостоверяющего центра, а сообщение во всех случаях приравнивается к бумажному документу с собственноручной подписью. Ключ проверки такой подписи указан в квалифицированном сертификате, а для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным согласно новому федеральному закону.

Методы аутентификации, использующие пароли

Одной из распространенных схем аутентификации является *простая аутентификация*, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств их использования и обработки. Пока в некоторых защищенных виртуальных сетях VPN доступ клиента к серверу разрешается по паролю. Однако все чаще применяются более эффективные средства аутентификации, например системы аутентификации на основе:

- смарт-карт;
- USB- токенов;
- цифровых сертификатов;
- программные и аппаратные системы аутентификации на основе одноразовых паролей.

Аутентификация на основе многоразовых паролей

В современных операционных системах предусматривается централизованная служба аутентификации, которая выполняется одним из серверов сети и использует для своей работы базу данных. В этой базе данных хранятся учетные данные о пользователях сети. В эти учетные данные наряду с другой информацией включены идентификатор (login) и пароль (password) пользователя.

Процедуру простой аутентификации пользователя в сети можно представить следующим образом. При попытке логического входа в сеть пользователь набирает на клавиатуре своего компьютера свои идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных учетных записей пользователей, хранящейся на сервере аутентификации, по идентификатору пользователя находится соответствующая запись, из нее извлекается эталонное значение пароля и сравнивается с тем паролем, который ввел пользователь. Если введенная пользователем пара login/password совпала с эталонной, то аутентификация прошла успешно, пользователь получает легальный статус и те права и ресурсы сети, которые определены для его статуса системой авторизации.

Для обеспечения надежной защиты операционной системы пароль каждого пользователя должен быть известен только этому пользователю и никому другому, в том числе и администраторам системы.

С точки зрения безопасности предпочтительным является метод передачи и хранения паролей с использованием односторонних функций. Обычно для шифрования паролей в списке пользователей используют одну из известных криптографически стойких хэш-функций. В списке

пользователей хранится не сам пароль, а *образ пароля*, являющийся результатом применения к паролю хэш-функции.

Системы простой аутентификации на основе многоразовых паролей имеют пониженную стойкость, поскольку в них выбор аутентифицирующей информации происходит из относительно небольшого множества слов. Срок действия многоразового пароля должен быть определен в политике безопасности организации, и такие пароли должны регулярно изменяться. Выбирать пароли нужно так, чтобы они были трудны для угадывания и не присутствовали в словаре.

Схемы аутентификации, основанные на многоразовых паролях, не обладают достаточной безопасностью. Такие пароли можно перехватить, разгадать, подсмотреть или просто украсть.

Аутентификация на основе одноразовых паролей OTP (*One Time Password*).

Суть схемы одноразовых паролей - использование различных паролей при каждом новом запросе на предоставление доступа. Одноразовый динамический пароль действителен только для одного входа в систему, и затем его действие истекает. Даже если кто-то перехватил его, пароль окажется бесполезным. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от угроз извне.

Одноразовые пароли генерируются с помощью OTP-токена. Для этого используется секретный ключ пользователя, размещенный как внутри OTP-токена, так и на сервере аутентификации.

Для того чтобы получить доступ к необходимым ресурсам, пользователь должен ввести пароль, созданный с помощью OTP-токена. Этот пароль сравнивается со значением, сгенерированным на сервере аутентификации, после чего выносится решение о предоставлении доступа. Преимуществом такого подхода является то, что пользователю не требуется соединять токен с компьютером (в отличие от вышеперечисленных типов идентификаторов).

Однако количество приложений ИТ-безопасности, которые поддерживают возможность работы с OTP-токенами, намного меньше, чем для смарт-карт и USB-токенов. Недостатком OTP-токенов является ограниченное время жизни этих устройств (три-четыре года), так как автономность работы предполагает использование батарейки.

Обычно системы аутентификации с одноразовыми паролями используются для проверки удаленных пользователей.

Строгая аутентификация.

Идея строгой аутентификации заключается в следующем. Проверяемая (доказывающая) сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета. Этот секрет может быть предварительно распределен безопасным способом между сторонами аутентификационного обмена.

В соответствии с рекомендациями стандарта X.509 различают процедуры строгой аутентификации следующих типов:

- односторонняя аутентификация;
- двусторонняя аутентификация;
- трехсторонняя аутентификация.

Односторонняя аутентификация предусматривает обмен информацией только в одном направлении. Данный тип аутентификации позволяет:

- подтвердить подлинность только одной стороны информационного обмена;
- обнаружить нарушение целостности передаваемой информации;
- обнаружить проведение атаки типа «повтор передачи»;
- гарантировать, что передаваемыми аутентификационными данными может воспользоваться только проверяющая сторона.

Двусторонняя аутентификация по сравнению с односторонней содержит дополнительный ответ проверяющей стороны доказывающей стороне, который должен убедить ее, что связь устанавливается именно с той стороной, которой были предназначены аутентификационные данные.

Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей.

Процессы строгой аутентификации могут быть реализованы на основе многофакторных проверок и использования криптографических методов.

Строгая аутентификация может быть реализована на основе двух- или трехфакторного процесса проверки, по результатам которого пользователю может быть предоставлен доступ к запрашиваемым ресурсам.

В первом случае пользователь должен доказать, что он знает пароль или PIN-код и имеет определенный персональный идентификатор (смарт-карту или USB- ключ). Во втором случае пользователь предъявляет еще один тип идентификационных данных, например биометрические данные. На практике более широкое применение находит двухфакторная аутентификация.

Применение средств многофакторной аутентификации снижает роль паролей, и в этом проявляется еще одно преимущество строгой аппаратной аутентификации, так как, по некоторым оценкам, пользователям приходится помнить до 15 различных паролей для доступа к учетным записям. Из-за информационной перегруженности сотрудники, чтобы не забыть пароли, записывают их на бумаге, что снижает уровень безопасности из-за риска компрометации пароля. Использование усиленной, или двухфакторной, аутентификации позволяет не только снизить риски ИТ-безопасности, но и оптимизировать внутренние процессы компании вследствие уменьшения прямых финансовых потерь.

Применение смарт-карт и USB-токенов

Применение для двухфакторной аутентификации пользователей внешних носителей информации (смарт-карт и USB-токенов) позволяет

заметно повысить защищенность системы. В отличие от паролей, владелец быстро узнает о краже внешнего носителя информации и может сразу принять необходимые меры для предотвращения ее негативных последствий.

Аутентификацию на основе смарт-карт и USB-токенов сложнее обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. Двухфакторная аутентификация на основе смарт-карт и USB-токенов намного надежнее аутентификации с применением многоразовых паролей.

Духфакторная аутентификация имеет порядок: взамен пароля пользователь должен предъявить физический носитель - смарт-карту или токен, содержащий сертификат и секретный ключ пользователя. При этом пользователь должен предъявить не только данный носитель секретного ключа, но и ввести PIN-код доступа к носителю, причем ни секретный ключ, ни PIN-код ни в каком виде по корпоративной сети не передаются. Отсутствие передачи секретного ключа и PIN-кода через сеть значительно повышает безопасность процесса аутентификации.

Применение смарт-карт

Смарт-карта - это пластиковая карта со встроенным микропроцессором, выполняющим функции контроля доступа к памяти смарт-карты и производящим также ряд специфических функций. Важная особенность смарт-карты состоит в том, что она осуществляет не только хранение, но и обработку содержащейся информации. Содержимое микросхемы смарт-карты надежно защищено от постороннего доступа. Это является одним из главных достоинств смарт-карты.

Смарт-карты можно классифицировать по следующим признакам:

- тип микросхемы;
- способ считывания информации с карты;
- соответствие стандартам;
- область применения.

В зависимости от встроенной микросхемы все смарт-карты делятся на два основных типа: карты с памятью и микропроцессорные карты.

Карты с памятью предназначены для хранения информации. Память на таких типах карт может быть свободной для доступа или содержать логику контроля доступа к памяти карты для ограничения операций чтения и записи данных. Карты памяти могут защищаться PIN-кодом.

Микропроцессорные карты используются в задачах, требующих сложной обработки информации. Микропроцессорная карта содержит микроконтроллер, центральный процессор которого соединен с сопроцессором, оперативным запоминающим устройством ОЗУ, постоянным запоминающим устройством ПЗУ и электрически стираемым программируемым ПЗУ - ЭСППЗУ.

Для использования смарт-карт в компьютерных системах необходимо считывающее устройство (или считыватель) смарт-карт. Устройства чтения

смарт-карт могут подключаться к компьютеру посредством последовательного порта, слота PCMCIA или USB.

Смарт-карты осуществляют хранение сертификатов пользователей и ключевого материала в самом устройстве, поэтому секретный ключ пользователя не попадает во враждебную внешнюю среду. Для проведения успешной аутентификации требуется вставить смарт-карту в считывающее устройство и ввести пароль (PIN-код). Операционная система считывает идентификатор пользователя и соответствующий ему ключ.

Для хранения и применения закрытого ключа используются разные подходы. Наиболее простой из них - использование устройства аутентификации в качестве защищенного носителя аутентификационной информации: при необходимости карта экспортирует закрытый ключ и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, но зато он относительно легко реализуем и предъявляет невысокие требования к устройству аутентификации.

Два других подхода более безопасны, поскольку предполагают выполнение устройством аутентификации криптографических операций. При первом подходе пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства. При втором подходе пользователь генерирует ключи при помощи устройства. В обоих случаях после того, как закрытый ключ сохранен, его нельзя извлечь из устройства и получить любым другим способом.

Следует отметить, что интеллектуальные смарт-карты способны самостоятельно проверять правильность пароля на доступ к ключевой информации и при аутентификации пользователя с использованием интеллектуальной карты проверку пароля на доступ к карте может производить не операционная система, а сама карта. Интеллектуальная карта может быть запрограммирована на стирание хранимой информации после превышения максимально допустимого количества неправильных попыток ввода пароля, что не позволяет подбирать пароль без частого копирования карты, а это весьма дорого.

Смарт-карты оптимальны для использования в инфраструктуре открытых ключей PKI, так как осуществляют безопасное хранение ключевого материала и сертификатов пользователей в самом устройстве. Достоинством смарт-карты является удобство ее хранения (например, ее можно держать в бумажнике вместе с другими карточками).

Недостатком смарт-карт является низкая мобильность, поскольку для работы с ними требуется считывающее устройство.

Тестовые задания по теме

1. Вид злоумышленных действий, при котором абонент С посылает документ абоненту В от имени абонента А, называется …

a) подмена;
b) ренегатство;
c) маскарад;
d) повтор.

2. Вид злоумышленных действий, при котором нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их, называется …

a) подмена;
b) ренегатство;
c) маскарад;
d) активный перехват.

3. Вид злоумышленных действий, при котором абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал, называется …

a) подмена;
b) ренегатство;
c) маскарад;
d) активный перехват.

4. Вид злоумышленных действий, при котором абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А, называется …

a) подмена;
b) ренегатство;
c) маскарад;
d) повтор.

5. Вид злоумышленных действий, при котором абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В, называется …

a) подмена;
b) ренегатство;
c) маскарад;
d) повтор.

6. Электронная цифровая подпись основана на …

a) применении симметричных алгоритмов шифрования;
b) взаимосвязанности содержимого сообщения и самой подписи;
c) взаимосвязанности содержимого сообщения, самой подписи и пары ключей;

d) применении одноключевых алгоритмов шифрования.

7. Электронная цифровая подпись основана на применении … алгоритмов шифрования.

a) симметричных;
b) бесключевых;
c) одноключевых;
d) ассиметричных;

8. Уникальное число, зависящее от подписываемого документа и секретного ключа абонента, представляет собой …

a) ЭЦП;
b) Имитоприставку;
c) хэш-значение;
d) дайджест сообщения.

9. Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом, называется … электронной подписью.

a) усиленной неквалифицированной;
b) усиленной квалифицированной;
c) сложной;
d) простой.

10. Электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания и создается с использованием средств электронной подписи, называется … электронной подписью.

a) усиленной неквалифицированной;
b) усиленной квалифицированной;
c) сложной;
d) простой.

11. Электронная подпись, для создания и проверки которой используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с новым законом, и ключ проверки указан в квалифицированном сертификате, называется … электронной подписью

a) усиленной неквалифицированной;
b) усиленной квалифицированной;
c) сложной;
d) простой.

12. По уровню обеспечиваемой безопасности аутентификация бывает …

a) на основе знания чего-либо, обладания чем-либо, каких-либо неотъемлемых характеристик;
b) статическая, динамическая;
c) простая, сложная, биометрическая;
d) простая, сложная, комбинированная.

13. В зависимости от предъявляемых субъектом сущностей аутентификация бывает …

a) на основе знания чего-либо, обладания чем-либо, каких-либо неотъемлемых характеристик;
b) статическая, динамическая;
c) простая, сложная, биометрическая;
d) простая, сложная, комбинированная.

14. Атаками на протоколы аутентификации, при которой злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах, называется …

a) маскарад;
b) атака с выборкой текста;
c) принудительная задержка;
d) повторная передача.

15. Аутентификация, которая основана на применении традиционных многоразовых паролей с одновременным согласованием средств их использования и обработки, называется …

a) строгой;
b) сложной;
c) двухсторонней;
d) простой.

16. Аутентификация, при которой проверяемая сторона доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета, называется …

a) строгой;
b) сложной;
c) секретной;
d) простой.

Тема 8. Обеспечение безопасности операционных систем

Проблема зашиты от несанкционированных действий при взаимодействии с внешними сетями может быть успешно решена только на основе комплексной защиты корпоративных информационных систем. Защищенные операционные системы относятся к базовым средствам многоуровневой комплексной зашиты КИС.

Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка операционной системы (ОС). Окружение, в котором функционирует ОС, называется *доверенной вычислительной базой* (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность:

- операционную систему;
- программы;
- сетевое оборудование;
- средства физической защиты;
- организационные процедуры.

Краеугольным камнем этой пирамиды является защищенная ОС. Без нее доверенная вычислительная база оказывается построенной на песке.

ОС называют *защищенной*, если она предусматривает средства защиты от основных классов угроз. Защищенная ОС обязательно должна содержать:

- средства разграничения доступа пользователей к своим ресурсам;
- средства проверки подлинности пользователя, начинающего работу с операционной системой;
- средства противодействия случайному или преднамеренному выводу операционной системы из строя.

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

Организация эффективной и надежной защиты ОС невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности ОС можно классифицировать по различным аспектам их реализации.

Классификация угроз *по цели атаки*:

- несанкционированное чтение информации;
- несанкционированное изменение информации;
- несанкционированное уничтожение информации;
- полное или частичное разрушение операционной системы.

Классификация угроз *по принципу воздействия на операционную систему*:

- использование известных (легальных) каналов получения информации, например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно - разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;

- использование скрытых каналов получения информации, например угроза использования злоумышленником недокументированных возможностей операционной системы;
- создание новых каналов получения информации с помощью программных закладок.

Классификация угроз *по типу используемой злоумышленником уязвимости защиты*:

- неадекватная политика безопасности, в том числе и ошибки администратора системы;
- 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;
- ранее внедренная программная закладка.

Классификация угроз *по характеру воздействия на ОС*:

- активное воздействие - несанкционированные действия злоумышленника в системе;
- пассивное воздействие - несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

ОС может подвергнуться следующим *типичным атакам*:

- *сканирование 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;
- *подбор пароля*. Существует 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.);
- *кража 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;
- *сборка 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;
- *превышение 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;

- *программные закладки*. Программные закладки, внедряемые в ОС, не имеют существенных отличий от других классов программных закладок;
- *жадные программы* - 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.

Существует два основных подхода к созданию защищенных операционных систем:

- фрагментарный;
- 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 (например, Windows 98), на нее устанавливают:

- антивирусный пакет;
- систему шифрования;
- систему 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.

Подсистема защиты ОС выполняет следующие основные функции:

1. *Идентификация и аутентификация*. Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

2. *Разграничение доступа*. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

3. *Аудит*. Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

4. *Управление политикой безопасности*. Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в операционную систему.

5. *Криптографические функции*. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

6. *Сетевые функции*. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе имеющих прямое отношение к защите информации.

Подсистема защиты обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями подсистемы зашиты должен существовать четко определенный интерфейс, используемый при взаимодействии модулей для решения общих задач.

Тестовые задания по теме

1. По цели атаки на операционную систему угрозы классифицируются …

a) легальные и скрытые;

b) неадекватная политика безопасности, ошибки в ПО, внедренные закладки;

c) несанкционированное чтение, изменение или уничтожение информации;

d) активные и пассивные.

2. По принципу воздействия на операционную систему угрозы классифицируются …

a) с использованием легальных, скрытых и новых каналов получения информации;

b) несанкционированное чтение, изменение или уничтожение информации;

c) неадекватная политика безопасности, ошибки в ПО, внедренные;

d) простые, сложные, комбинированные.

3. По типу используемой злоумышленником уязвимости защиты ОС угрозы классифицируются…

a) с использованием легальных, скрытых и новых каналов получения информации;

b) несанкционированное чтение, изменение или уничтожение информации;

c) статические и динамические;

d) неадекватная политика безопасности, ошибки в ПО, внедренные закладки.

4. По характеру воздействия на операционную систему угрозы классифицируются …

a) с использованием легальных, скрытых и новых каналов получения информации;

b) несанкционированное чтение, изменение или уничтожение информации;

c) неадекватная политика безопасности, ошибки в ПО, внедренные;

d) активные и пассивные.

5. Типичными атаками на операционную систему являются …

a) маскарад;

b) сборка мусора;

c) ренегатство;

d) активный перехват.

6. Типичными атаками на операционную систему являются …

a) жадные программы;
b) ренегатство;
c) повтор;
d) перебор.

7. Основными подходами к созданию защищенных операционных систем являются …

a) функциональный и стоимостной;
b) системный и стоимостной;
c) структурный и фрагментарный;
d) фрагментарный и комплексный.

8. Подсистема защиты ОС представляет собой набор разрозненных программных продуктов, как правило, от разных производителей при применении … подхода.

a) фрагментарного;
b) стоимостного;
c) структурного;
d) комплексного.

9. Внесение защитных функции в ОС на этапе проектирования ее архитектуры, когда отдельные элементы подсистемы защиты тесно взаимодействуют друг с другом при решении различных задач, характерно при применении … подхода.

a) фрагментарного;
b) стоимостного;
c) структурного;
d) комплексного.

10. К функциям подсистемы защиты ОС *не относятся* …

a) определение ролей;
b) идентификация и аутентификация;
c) аудит;
d) криптографические функции.

11. Любой элемент ОС, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен, называется … доступа.

a) субъект;
b) метод;
c) способ;
d) объект.

Тема 9. Протоколы защищенных каналов

Основная задача, решаемая при создании компьютерных сетей, - обеспечение совместимости оборудования по электрическим и механическим характеристикам и совместимости информационного обеспечения (программ и данных) по системам кодирования и формату данных. Решение этой задачи относится к области стандартизации. Методологической основой стандартизации в компьютерных сетях является многоуровневый подход к разработке средств сетевого взаимодействия. На основе этого подхода и технических предложений Международного института стандартов ISO (International Standards Organization) в начале 1980-х годов была разработана стандартная модель взаимодействия открытых систем OSI (Open Systems Interconnection).

Модель ISO/OSI определяет различные уровни взаимодействия систем и указывает, какие функции должен выполнять каждый уровень.

В модели OSI средства взаимодействия делятся на семь уровней:

- прикладной;
- представительный;
- сеансовый;
- транспортный;
- сетевой;
- канальный;
- физический.

Самый верхний уровень - прикладной. На этом уровне пользователь взаимодействует с приложениями. Самый нижний уровень - физический. Этот уровень обеспечивает обмен сигналами между устройствами.

Обмен данными через каналы связи происходит путем перемещения данных с верхнего уровня на нижний, затем транспортировки по линиям связи и наконец, обратным воспроизведением данных на компьютере клиента в результате их перемещения с нижнего уровня на верхний.

Для обеспечения необходимой совместимости на каждом из уровней архитектуры компьютерной сети действуют специальные стандартные протоколы. Они представляют собой формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах сети.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком коммуникационных протоколов*. Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней - как правило, чисто программными средствами.

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol) является промышленным стандартом стека коммуникационных протоколов, разработанным для глобальных сетей. Стек TCP/IP объединяет в

себе целый набор взаимодействующих между собой протоколов. Самыми важными из них являются протокол IP отвечающий за поиск маршрута (или маршрутов) в Интернете от одного компьютера к другому через множество промежуточных сетей, шлюзов и маршрутизаторов и передачу блоков данных по этим маршрутам, и протокол TCP, обеспечивающий надежную доставку, безошибочность и правильный порядок приема передаваемых данных.

Сегодня стек TCP/IP используется для связи компьютеров по всемирной информационной сети Интернет, а также в огромном числе корпоративных сетей. Стек TCP/IP является самым распространенным средством организации составных компьютерных сетей.

Стек протоколов TCP/IP имеет четыре уровня:

- прикладной;
- транспортный;
- уровень межсетевого взаимодействия;
- уровень сетевых интерфейсов.

Прикладной уровень включает большое число прикладных протоколов и сервисов. К ним относятся такие популярные протоколы, как:

- протокол копирования файлов FTP;
- протокол эмуляции терминала Telnet;
- почтовый протокол SMPT, используемый в электронной почте сети Интернет;
- гипертекстовые сервисы доступа к удаленной информации, например WWW, и многие другие.

На транспортном уровне стека TCP/IP, называемом также основным уровнем, функционируют протоколы TCP и UDP.

Протокол управления передачей TCP (Transmission Control Protocol) решает задачу обеспечения надежной информационной связи между двумя конечными узлами.

Протокол дейтаграмм пользователя UDP (User Datagram Protocol) обеспечивает передачу прикладных пакетов дейтаграммным способом, т. е. каждый блок передаваемой информации (пакет) обрабатывается и распространяется от узла к узлу как независимая единица информации - *дейтаграмма*. Необходимость в протоколе UDP обусловлена тем, что он «умеет» различать приложения и доставляет информацию от приложения к приложению.

Уровень межсетевого взаимодействия реализует концепцию коммутации пакетов без установления соединений. Основным протоколом этого уровня является адресный протокол IP.

К уровню межсетевого взаимодействия относятся и протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol). Последний протокол

предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета.

Уровень сетевого интерфейса соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня:

- для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet;
- для глобальных сетей - протоколы соединений точка-точка SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, Frame Relay.

Что касается безопасности протоколов TCP/IP, т. е. безопасности передачи данных в Интернете в целом, пользователям необходимо иметь в виду, что, если не принято специальных мер, все данные передаются протоколами TCP/IP в открытом виде. Это значит, что любой узел (и, соответственно, его оператор), находящийся на пути следования данных от отправителя к получателю, может скопировать себе все передаваемые данные и использовать их в дальнейшем в своих целях. В равной мере данные могут быть искажены или уничтожены.

Виртуальный защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели взаимодействия открытых систем OSI.

Для независимости от прикладных протоколов и приложений виртуальные защищенные каналы формируются на одном из более низких уровней модели OSI - канальном, сетевом или сеансовом.

Защита на *канальном* уровне.

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 через Интернет.

Оба протокола - PPTP и L2TP - 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, поскольку поддерживают только функции туннелирования. Функции защиты данных (шифрование, целостность, аутентификация) в этом протоколе не поддерживаются. Для защиты туннелируемых данных в протоколе L2TP необходимо использовать дополнительный протокол, в частности IPSec.

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. Преимущество такого выбора заключается в том очевидном факте, что в IP-сетях именно сетевой уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня транспортировка данных по сети не может быть произведена в обход протокола IP. Поэтому реализация защиты сети на третьем уровне автоматически гарантирует как минимум такую же степень защиты всех сетевых приложений, причем без какой-либо модификации последних.

Стек протоколов IPSec (Internet Protocol Security) используется для:

- аутентификации участников обмена;
- туннелирования трафика;
- шифрования IP-пакетов.

Основное назначение протокола IPSec - обеспечение безопасной передачи данных по сетям IP. Протокол IPSec может защищать трафик как текущей версии протокола IPv4, применяемой сегодня в Интернете, так и версии IPv6, которая постепенно внедряется в Интернет.

Защита на *сеансовом* уровне.

При построении защищенных виртуальных сетей на сеансовом уровне появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализацию ряда функций посредничества между взаимодействующими сторонами.

Для защиты информационного обмена на сеансовом уровне широкое распространение получили протоколы SSL и SOCKS.

Протокол SSL (Secure Socket Layer) был разработан для реализации защищенного обмена информацией в клиент/серверных приложениях. В настоящее время протокол SSL применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI.

Протокол SSL использует криптографические методы защиты информации для обеспечения безопасности информационного обмена. Этот протокол выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Ядром протокола SSL является технология комплексного использования асимметричных и симметричных криптосистем.

Протокол SOCKS организует процедуру взаимодействия клиент/серверных приложений на сеансовом уровне модели OSI через сервер-посредник, или прокси-сервер.

Защита *беспроводных сетей.*

Беспроводные сети начинают использоваться практически во всем мире. Это обусловлено их удобством, гибкостью и сравнительно невысокой стоимостью.

Сложность обеспечения безопасности беспроводной сети очевидна. Если в проводных сетях злоумышленник должен сначала получить

физический доступ к кабельной системе или оконечным устройствам, то в беспроводных сетях это условие отпадает само собой: поскольку данные передаются «по воздуху», для получения доступа достаточно обычного приемника, установленного в радиусе действия сети.

Система защиты беспроводных сетей WLAN, основанная на протоколе WEP (Wired Equivalent Privacy) первоначального стандарта 802.11, страдает существенными недостатками. К счастью, появились более эффективные технологии обеспечения информационной безопасности WLAN, которые описаны в стандарте WPA (Wi-Fi Protected Access) и стандарте 802.11i и призваны устранить недостатки стандарта 802.11.

Между технологиями 802.11i и WPA много общего. Так, в них определена идентичная архитектура системы безопасности с улучшенными механизмами аутентификации пользователей и протоколами распространения и обновления ключей. Но есть и существенные различия. Например, технология WPA базируется на протоколе динамических ключей TKIP (Temporal Key Integrity Protocol), поддержку которого в большинстве устройств WLAN можно реализовать путем обновления их программного обеспечения, а в более функциональной концепции 802.11i предусмотрено использование нового стандарта шифрования AES (Advanced Encryption Standard), с которым совместимо лишь новейшее оборудование для WLAN. До тех пор пока средства стандарта 802.11i не станут доступными на рынке, WPA будет оставаться самым подходящим стандартом для защиты WLAN.

Тестовые задания по теме

1. В модели OSI средства взаимодействия делятся на … уровней.
a) 4;
b) 5;
c) 6;
d) 7.

2. В модели OSI самый верхний уровень называется …
a) прикладной;
b) представительный;
c) физический;
d) транспортный.

3. В модели OSI самый нижний уровень называется …
a) прикладной;
b) представительный;
c) физический;
d) транспортный.

4. В модели OSI прикладной уровень обеспечивает …
a) транспортировку данных по линиям связи;

b) обмен сигналами между устройствами;
c) совместимость узлов в сети;
d) взаимодействие пользователя с приложениями.

5. В модели OSI физический уровень обеспечивает …
a) транспортировку данных по линиям связи;
b) обмен сигналами между устройствами;
c) совместимость узлов в сети;
d) взаимодействие пользователя с приложениями.

6. Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах сети, называются …
a) специальные стандартные протоколы;
b) нормативы сетевых компонентов;
c) процедуры совместимости узлов в сети;
d) методы сетевого обмена.

7. Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется … коммуникационных протоколов.
a) иерархией;
b) нормативом;
c) процедурой;
d) стеком.

8. Коммуникационные протоколы могут быть реализованы …
a) как программно, так и аппаратно;
b) только программно;
c) только аппаратно.

9. Правилам, которые определяют взаимодействия модулей соседних уровней в одном узле сети, называются …
a) методом взаимодействия;
b) межуровневым интерфейсом;
c) процедурами протоколов;
d) стеком протоколов.

10. Правилам, которые определяют взаимодействия модулей одного уровня в разных узлах сети, называются …
a) методом взаимодействия;
b) межуровневым интерфейсом;
c) процедурами протоколов;
d) стеком протоколов.

11. Промышленным стандартом стека коммуникационных протоколов, разработанным для глобальных сетей, является стек протоколов …

a) DHCP;
b) ICMP;
c) TCP/IP;
d) LDAP.

12. Протокол, отвечающий за поиск маршрута в Интернете от одного компьютера к другому через множество промежуточных сетей, шлюзов и маршрутизаторов и передачу блоков данных по этим маршрутам, называется протоколом …

a) IP;
b) ICMP;
c) TCP;
d) LDAP.

13. Протокол, обеспечивающий надежную доставку, безошибочность и правильный порядок приема передаваемых данных, называется протоколом …

a) IP;
b) ICMP;
c) TCP;
d) LDAP.

14. Стек протоколов TCP/IP имеет …

a) 3 уровня;
b) 4 уровня;
c) 5 уровней;
d) 7 уровней.

15. Прикладной уровень стека протоколов TCP/IP включает такие протоколы как …

a) TCP и UDP;
b) IP;
c) не регламентируется, поддерживает все стандарты физического и канального уровня;
d) FTP, Telnet, SMPT.

16. Уровень сетевого интерфейса стека протоколов TCP/IP включает такие протоколы как …

a) TCP и UDP;
b) IP;
c) не регламентируется, поддерживает все стандарты физического и канального уровня;

d) FTP, Telnet, SMPT.

17. Транспортный уровень стека протоколов TCP/IP включает такие протоколы как …

a) TCP и UDP;
b) IP;
c) не регламентируется, поддерживает все стандарты физического и канального уровня;
d) FTP, Telnet, SMPT.

18. Решением вопросов, что какой компьютер считать «ближе», а какой «дальше» при пересылке пакетов по сети, занимаются …

a) маршрутизаторы;
b) шлюзы;
c) точки доступа;
d) брандмауэры.

19. Протоколами туннелирования канального уровня модели OSI являются протоколы …

a) 802.11i и WPA;
b) PPTP и L2TP;
c) IPSec и IP;
d) SSL, SOCKS.

20. Протоколами защиты на сетевом уровне модели OSI являются протоколы …

a) 802.11i и WPA;
b) PPTP и L2TP;
c) IPSec;
d) SSL, SOCKS.

21. Протоколами защиты на сеансовом уровне модели OSI являются протоколы …

a) 802.11i и WPA;
b) PPTP и L2TP;
c) IPSec и IP;
d) SSL, SOCKS.

22. Стандартами защиты беспроводных сетей являются технологии …

a) 802.11i и WPA;
b) PPTP и L2TP;
c) IPSec и IP;
d) SSL и SOCKS.

Тема 10. Технология межсетевого экранирования

Межсетевое экранирование является одним из основных элементов обороны корпоративной сети.

Межсетевой экран (МЭ) - это специализированный комплекс межсетевой зашиты, называемый также *системой firewall* или *брандмауэром*. Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет.

Для противодействия несанкционированному межсетевому доступу межсетевой экран МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 8).

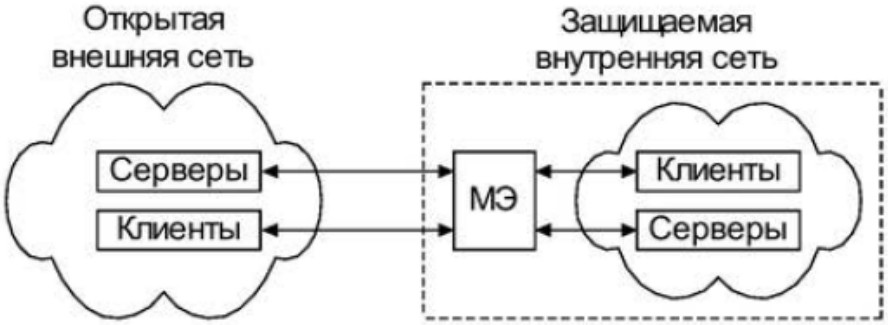

Рис. 8. Схема подключения межсетевого экрана

Все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно межсетевой экран входит в состав защищаемой сети.

Межсетевой экран, защищающий сразу множество узлов внутренней сети, призван решить две основные *задачи*:

- ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающие получить доступ к серверам баз данных, защищаемых межсетевым экраном;
- разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей.

МЭ можно классифицировать по следующим основным признакам.

По функционированию на уровнях модели OSI:

- пакетный фильтр (экранирующий маршрутизатор - Screening Router);
- шлюз сеансового уровня (экранирующий транспорт);
- прикладной шлюз (Application Gateway);
- шлюз экспертного уровня (Stateful Inspection Firewall).

По используемой технологии:

- контроль состояния протокола (Stateful Inspection);
- на основе модулей посредников (прокси).

По исполнению:

- аппаратно-программный;
- программный.

По схеме подключения:

- схема единой защиты сети;
- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
- схема с раздельной защитой закрытого и открытого сегментов сети.

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразовании. Фильтрация осуществляется на основе набора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток.

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих действий:

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.

В качестве *критериев* анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

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

Функции посредничества МЭ выполняет с помощью специальных программ, называемых *программами-посредниками* или *экранирующими*

агентами. Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетями.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере МЭ. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сетей осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

В общем случае программы-посредники, блокируя прозрачную передачу потока сообщений, могут выполнять следующие *функции*:

- проверку подлинности передаваемых данных;
- фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- кэширование данных, запрашиваемых из внешней сети.
- идентификацию и аутентификацию пользователей;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ-посредников:

- экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet;
- универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Помимо выполнения фильтрации трафика и функций посредничества, современные межсетевые экраны позволяют реализовать ряд других, не менее важных функций, без которых обеспечение защиты периметра внутренней сети было бы неполным. Рассмотрим дополнительные возможности современных межсетевых экранов.

Идентификация и аутентификация пользователей. Кроме разрешения или запрещения допуска различных приложений в сеть, межсетевые экраны могут также выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым межсетевым экраном.

Трансляция сетевых адресов. Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, межсетевые экраны выполняют очень важную функцию - трансляцию внутренних сетевых адресов.

Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP- адрес.

IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью.

Администрирование, регистрация событий и генерация отчетов. Простота и удобство администрирования являются одним из ключевых аспектов в создании эффективной и надежной системы защиты. Ошибки при определении правил доступа могут образовать дыру, через которую может быть взломана система. Поэтому в большинстве межсетевых экранов реализованы сервисные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактирования правил. Обычно эти утилиты позволяют просматривать информацию, сгруппированную по каким либо критериям, - например, все, что относится к конкретному пользователю или сервису.

Важными функциями межсетевых экранов являются:

- регистрация событий;
- реагирование на задаваемые события;
- анализ зарегистрированной информации;
- составление отчетов.

Многие МЭ содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись:

- по адресам клиента и сервера;
- по идентификаторам пользователей;
- по времени сеансов;
- по времени соединений;
- по количеству переданных/принятых данных;
- по действиям администратора и пользователей.

Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов МЭ могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга.

Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые МЭ, как:

- экранирующий маршрутизатор;
- шлюз сеансового уровня;
- шлюз прикладного уровня (экранирующий шлюз).

Экранирующий маршрутизатор, называемый также пакетным *фильтром*, предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне эталонной модели OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели.

Шлюз сеансового уровня, называемый еще *экранирующим транспортом*, предназначен для контроля виртуальных соединений и трансляции IP-адресов при взаимодействии с внешней сетью. Он функционирует на сеансовом уровне модели OSI, охватывая в процессе своей работы также транспортный и сетевой уровни эталонной модели. Защитные функции шлюза сеансового уровня относятся к функциям посредничества.

Прикладной шлюз, называемый также *экранирующим шлюзом*, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

- идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
- проверка подлинности информации, передаваемой через шлюз;
- разграничение доступа к ресурсам внутренней и внешней сетей;
- фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
- кэширование данных, запрашиваемых из внешней сети.

Существует два основных варианта исполнения межсетевых экранов - программный и программно-аппаратный. В свою очередь, программно-аппаратный вариант исполнения межсетевых экранов имеет две разновидности - в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

Тестовые задания по теме

1. Межсетевой экран называется также …

a) коммутатором;
b) туннелем;
c) firewall;
d) дейтаграммой.

2. Межсетевой экран называется также …

a) брандмауэром;
b) туннелем;
c) коммутатором;
d) дейтаграммой.

3. Устройство, позволяющее разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую, называется …

a) туннелем;
b) межсетевым экраном;
c) коммутатором;
d) дейтаграммой.

4. По функционированию на уровнях модели OSI различают межсетевые экраны …

a) контроля состояния протокола и на основе модулей посредников;
b) аппаратно-программный и программный;
c) пакетный фильтр и прикладной шлюз;
d) единой защиты сети и с раздельной защитой закрытого и открытого сегментов сети.

5. По используемой технологии различают межсетевые экраны …

a) контроля состояния протокола и на основе модулей посредников;
b) аппаратно-программный и программный;
c) пакетный фильтр и прикладной шлюз;
d) единой защиты сети и с раздельной защитой закрытого и открытого сегментов сети.

6. По исполнению различают межсетевые экраны …

a) контроля состояния протокола и на основе модулей посредников;
b) аппаратно-программный и программный;
c) пакетный фильтр и прикладной шлюз;
d) единой защиты сети и с раздельной защитой закрытого и открытого сегментов сети.

7. По схеме подключения различают межсетевые экраны …

a) контроля состояния протокола и на основе модулей посредников;
b) аппаратно-программный и программный;
c) пакетный фильтр и прикладной шлюз;
d) единой защиты сети и с раздельной защитой закрытого и открытого сегментов сети.

8. Межсетевой экран удобно представлять как последовательность …

a) фильтров;
b) резидентов;
c) дейтаграмм;
d) туннелей.

9. Функции посредничества МЭ выполняет с помощью специальных программ, называемых …

a) фильтрами;
b) резидентами;
c) дейтаграммами;
d) экранирующими агентами.

10. К возможностям МЭ *не относятся* …

a) фильтрация трафика;
b) выполнение функций посредничества;
c) трансляция сетевых адресов;
d) идентификация и аутентификация пользователей;
e) внутренний аудит.

11. Межсетевой экран, предназначенный для фильтрации пакетов сообщений и обеспечения прозрачного взаимодействия между внутренней и внешней сетями, называется …

a) экранирующим маршрутизатором;
b) шлюзом сеансового уровня;
c) экранирующим шлюзом;
d) шлюзом физического уровня.

12. Экранирующий маршрутизатор функционирует на … уровне эталонной модели OSI.

a) сеансовом;
b) прикладном;
c) физическом;
d) сетевом.

13. Межсетевой экран, предназначенный для контроля виртуальных соединений и трансляции IP-адресов при взаимодействии с внешней сетью,

называется …

a) экранирующим маршрутизатором;
b) шлюзом сеансового уровня;
c) экранирующим шлюзом;
d) шлюзом физического уровня.

14. Экранирующий транспорт функционирует на … уровне эталонной модели OSI.

a) сеансовом;
b) прикладном;
c) физическом;
d) сетевом.

15. Экранирующий шлюз функционирует на … уровне эталонной модели OSI.

a) сеансовом;
b) прикладном;
c) физическом;
d) сетевом.

Тема 11. Технологии виртуальных защищенных сетей VPN

В последнее десятилетие в связи с бурным развитием Интернета и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные каналы связи. Стремясь к экономии средств, предприятия хотят использовать такие каналы для передачи критичной коммерческой и управленческой информации.

Для эффективного противодействия сетевым атакам и обеспечения возможности активного и безопасного использования в бизнесе открытых сетей в начале 1990-х годов родилась и активно развивается концепция построения виртуальных частных сетей - VPN (Virtual Private Network).

В основе концепции построения виртуальных сетей VPN лежит достаточно простая идея: если в глобальной сети имеются два узла, которым нужно обменяться информацией, тогда между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети. Доступ к этому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям.

Преимущества, получаемые компанией от создания таких виртуальных туннелей, заключаются прежде всего в значительной экономии финансовых средств, поскольку в этом случае компания может отказаться от построения или аренды дорогих выделенных каналов связи для создания собственных интранет/экстранет-сетей и использовать для этого дешевые интернет-каналы, надежность и скорость передачи которых сегодня не уступает выделенным линиям. Очевидная экономическая эффективность от внедрения VPN-технологий стимулирует предприятия к активному их внедрению.

Виртуальной защищенной сетью VPN называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

Существуют разные варианты классификации VPN. Наиболее часто используют следующие три признака классификации:

- рабочий уровень модели OSI;
- архитектура технического решения VPN;
- способ технической реализации VPN.

По признаку рабочего уровня модели OSI различают следующие группы VPN:

- VPN канального уровня;
- VPN сетевого уровня;
- VPN сеансового уровня.

По архитектуре технического решения принято выделять три основных вида виртуальных частных сетей:

- внутрикорпоративные VPN;

- VPN с удаленным доступом;
- межкорпоративные VPN.

По способу технической реализации различают следующие группы VPN:

- VPN на основе маршрутизаторов;
- VPN на основе межсетевых экранов;
- VPN на основе программных решений;
- VPN на основе специализированных аппаратных средств со встроенными шифропроцессорами.

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*.

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 выполнении следующих *функций*:

- аутентификация взаимодействующих сторон;
- криптографическое закрытие (шифрование) передаваемых данных;
- проверка подлинности и целостности доставляемой информации.

Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, причем эта защищенная выделенная линия развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль:

- VPN-клиента;
- VPN-сервера;
- шлюза безопасности VPN.

VPN-клиент представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера. Его сетевое программное обеспечение модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную операционную систему.

VPN-сервер представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера. VPN-сервер является функциональным аналогом продукта VPN-клиент для серверных платформ. Он отличается прежде всего расширенными ресурсами для поддержания множественных соединений с VPN-клиентами. VPN-сервер может поддерживать защищенные соединения с мобильными пользователями.

Шлюз безопасности VPN - это сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для

многочисленных хостов, расположенных за ним. Шлюз безопасности VPN может быть реализован в виде отдельного программного решения, отдельного аппаратного устройства, а также в виде маршрутизатора или межсетевого экрана, дополненного функциями VPN.

При проектировании VPN обычно рассматриваются две основные схемы:

- виртуальный защищенный канал между локальными сетями;
- виртуальный защищенный канал между узлом и локальной сетью.

Первая схема соединения позволяет заменить дорогостоящие выделенные линии между отдельными офисами и создать постоянно доступные защищенные каналы между ними. Вторая схема защищенного канала VPN предназначена для установления соединений с удаленными или мобильными пользователями. Для связи со шлюзом, защищающим удаленную сеть, он запускает на своем компьютере специальное клиентское программное обеспечение.

Для обеспечения безопасности передаваемых данных в виртуальных защищенных сетях должны быть решены следующие основные задачи сетевой безопасности:

- взаимная аутентификация абонентов при установлении соединения;
- обеспечение конфиденциальности, целостности и аутентичности передаваемой информации;
- авторизация и управление доступом;
- безопасность периметра сети и обнаружение вторжений;
- управление безопасностью сети.

Современные средства идентификации и аутентификации должны удовлетворять двум условиям:

- поддерживать принцип единого входа в сеть;
- быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети).

Суть *принципа единого входа в сеть* состоит в том, что пользователь осуществляет один логический вход в сеть и после успешного прохождения аутентификации получает некоторый набор разрешений по доступу к сетевым ресурсам на все время работы в сети. Единый вход в сеть - это в первую очередь требование удобства для пользователей.

Второе требование можно реализовать, используя криптографические методы. В настоящее время общепринятыми являются подходы, основанные на службе каталогов с сертификатами в стандарте X.509 или системе Kerberos.

Задача обеспечения конфиденциальности информации обеспечивается шифрованием.

Задача обеспечения *целостности* передаваемых данных заключается в проверке того, что данные в процессе передачи не были искажены злоумышленником или из-за ошибок передачи в сети. Для осуществления

аутентификации данных обычно используется криптографический механизм электронной цифровой подписи.

Ключевым компонентом безопасности VPN является гарантия того, что доступ к компьютерным ресурсам получают *авторизованные пользователи*. Система авторизации предоставляет легальным пользователям не только определенные права доступа к каталогам, файлам и принтерам, но и регулирует доступ пользователя к средствам шифрования пакетов, формирования цифровой подписи и определенным VPN-устройствам.

Процедуры авторизации реализуются программными средствами, встроенными в операционную систему или в приложение. При построении программных средств авторизации применяется два подхода:

- централизованная схема авторизации;
- децентрализованная схема авторизации.

Основное назначение централизованной системы авторизации - реализовать принцип единого входа. Управление процессом предоставления ресурсов пользователю осуществляется сервером.

При децентрализованном подходе к процессу авторизации каждая рабочая станция оснащается средствами защиты. В этом случае доступ к каждому приложению должен контролироваться средствами защиты той операционной среды, в которой работает данное приложение. Администратор сети должен контролировать работу средств безопасности, используемых всеми типами приложений.

Для безопасности периметра сети и обнаружения вторжений используют такие средства безопасности, как:

- межсетевые экраны;
- системы обнаружения вторжений;
- системы аудита безопасности;
- антивирусные комплексы.

Система предотвращения вторжений IPS (Intrusion Prevention System) работает в реальном времени и предназначена для обнаружения, фиксации и прекращения неавторизованной сетевой активности как от внешних, так и от внутренних источников.

Тестовые задания по теме

1. Идея – если в глобальной сети имеются два узла, которым нужно обменяться информацией, тогда между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети – является концепцией …

a) NCP;
b) RADIUS;
c) VPN;
d) LAN.

2. Преимущества, получаемые компанией от создания виртуальных защищенных сетей, заключаются прежде всего в …

a) экономии финансовых средств;
b) повышении надежности передачи данных;
c) повышении скорости передачи данных;
d) снижении трудностей администрирования.

3. Программный или программно-аппаратный комплекс в VPN, выполняемый обычно на базе персонального компьютера, называется …

a) шлюзом безопасности VPN;
b) VPN-клиентом;
c) VPN-севером;
d) VPN-идентификатором.

4. Программный или программно-аппаратный комплекс в VPN, устанавливаемый на компьютере, выполняющем функции сервера, называется …

a) шлюзом безопасности VPN;
b) VPN-клиентом;
c) VPN-севером;
d) VPN-идентификатором.

5. Сетевое устройство в VPN, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним, называется…

a) шлюзом безопасности VPN;
b) VPN-клиентом;
c) VPN-севером;
d) VPN-идентификатором.

6. По признаку рабочего уровня модели OSI различают следующие виды VPN …

a) VPN канального, сетевого и сеансового уровней;

b) внутрикорпоративные, межкорпоративные VPN и VPN с удаленным доступом;

c) VPN на основе маршрутизаторов, МЭ и программных решений;

d) VPN канального, прикладного и физического уровней.

7. По архитектуре технического решения различают следующие виды VPN …

a) VPN канального, сетевого и сеансового уровней;

b) внутрикорпоративные, межкорпоративные VPN и VPN с удаленным доступом;

c) VPN на основе маршрутизаторов, МЭ и программных решений;

d) VPN канального, прикладного и физического уровней.

8. По способу технической реализации различают следующие виды VPN …

a) VPN канального, сетевого и сеансового уровней;

b) внутрикорпоративные, межкорпоративные VPN и VPN с удаленным доступом;

c) VPN на основе маршрутизаторов, МЭ и программных решений;

d) VPN канального, прикладного и физического уровней.

9. Для обеспечения защищенного обмена информацией со стратегическими партнерами по бизнесу, поставщиками, крупными заказчиками, пользователями, клиентами, предназначены …

a) виртуальные частные сети VPN с удаленным доступом;

b) внутрикорпоративные сети VPN;

c) локальные сети VPN;

d) межкорпоративные сети VPN.

10. Для обеспечения защищенного взаимодействия между подразделениями внутри предприятия или между группой предприятий, объединенных корпоративными сетями связи, включая выделенные линии, предназначены …

a) виртуальные частные сети VPN с удаленным доступом;

b) внутрикорпоративные сети VPN;

c) локальные сети VPN;

d) межкорпоративные сети VPN.

Тема 12. Технологии защиты от вредоносных программ и спама

Существуют программы, намеренно написанные с целью:

- уничтожения данных на чужом компьютере;
- похищения чужой информации;
- несанкционированного использования чужих ресурсов.

Такие программы несут вредоносную нагрузку и, соответственно, называются *вредоносными*.

Вредоносные программы классифицируют:

- по способу проникновения;
- по способу размножения;
- по типу вредоносной нагрузки.

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

- компьютерные вирусы;
- черви;
- трояны;
- другие программы.

Компьютерный вирус - это программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Основная цель любого компьютерного вируса - это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 21 числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения - фактически все каналы, по которым можно скопировать файл. Однако, в отличие от червей, вирусы не используют сетевые ресурсы - заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал, например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить разными путями, и в зависимости от выбранного метода вирусы делятся на такие виды:

- *загрузочные вирусы* заражают загрузочные сектора жестких дисков и мобильных носителей;
- *файловые вирусы* заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Так, вирус для Microsoft Windows не будет работать и заражать файлы на

компьютере с другой установленной операционной системой, например UNIX.

При подготовке своих копий вирусы могут применять для маскировки разные технологии:

- *шифроваиие* - в этом случае вирус состоит из двух частей: сам вирус и шифратор;
- *метаморфизм* - при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Соответственно, в зависимости от используемых методов маскировки вирусы можно делить:

- на шифрованные;
- на метаморфные;
- на полиморфные, использующие комбинацию двух типов маскировки.

В отличие от вирусов, сетевые черви - это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения в систему черви делятся на следующие типы:

- *сетевые черви* используют для распространения локальные сети и Интернет;
- *почтовые черви* распространяются с помощью почтовых программ;
- *IM-черви* используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;
- *IRC-черви* распространяются через чаты IRC (Internet Relay Chat);
- *P2P-черви* распространяются при помощи пиринговых файлообменных сетей P2P (Peer-to-Peer).

После проникновения на компьютер червь должен активироваться - иными словами, запуститься. По методу активации все черви можно разделить на две большие группы:

- тех, которые требуют активного участия пользователя;
- тех, кто его не требует.

Отличительная особенность червей из первой группы - это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. Черви из второй группы используют ошибки в настройке или бреши в системе безопасности ОС. В последнее время наметилась тенденция к совмещению этих двух технологий - такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Троянская программа (программа класса «троянский конь», или просто *троян*) имеет только одно назначение - нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий:

- кражи;
- порчи или удаления конфиденциальных данных;
- нарушения работоспособности компьютера;
- использования ресурсов компьютера в неблаговидных целях.

В отличие от вирусов и червей, трояны сами не размножаются. Некоторые трояны способны к самостоятельному преодолению систем зашиты компьютерной системы с целью проникновения в нее. Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем – т. е. такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя - либо требует активных действий от пользователя, либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель троянов - это выполнение несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

- *похитители паролей* предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;
- *утилиты скрытого удаленного управления* - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы;
- *логические бомбы* характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, в ответ на определенное действие пользователя или команды извне) выполнять какое-либо действие, например удаление файлов;
- *клавиатурные шпионы*, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры, с целью последующей их передачи своему автору;
- *анонимные SMTP- и прокси-серверы* - такие трояны на зараженном компьютере организуют несанкционированную отправку электронной почты, что часто используется для рассылки спама;
- *утилиты дозвона* в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернета;
- *модификаторы настроек браузера* меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.

Кроме вирусов, червей и троянов существует еще много других вредоносных программ и нежелательной корреспонденции. Среди них можно выделить следующие группы:

- *шпионское ПО* (Spyware) - опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне - создателю или заказчику такой программы. Шпионские программы интересуются:
  - ✓ системными данными;
  - ✓ типом браузера;
  - ✓ посещаемыми веб-узлами;
  - ✓ иногда и содержимым файлов на жестком диске компьютера-жертвы.
- *условно опасные программы*, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:
  - ✓ *апплеты* - прикладные программы, небольшие Java-приложения, встраиваемые в HTML-страницы. По своей сути эти программы не вредоносные, но могут использоваться в злонамеренных целях;
  - ✓ *рекламные утилиты* - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается, и программы начинают работать в обычном режиме;
  - ✓ *riskware* - вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернета, утилиты восстановления забытых паролей и др.;
- *хакерские утилиты* - к этому виду программ относятся программы:

✓ сокрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);

✓ автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов);

✓ наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit);

✓ и другие подобные утилиты.

Такие специфические программы обычно используют только хакеры;

- *мистификации* - программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений зависит от фантазии автора программы;

- *спам* - нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.

Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются *антивирусами*, и для того, чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно.

В современных антивирусных продуктах используется два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический.

Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

Проактивные/эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами.

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют *антивирусную базу*.

Эта технология предполагает непрерывное отслеживание новых экземпляров вредоносных программ, их описание и включение в базу сигнатур. Задачу выделения сигнатур, как правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска.

Главный *недостаток сигнатурного метода* - задержка при реакции на новые угрозы. Для получения сигнатуры необходимо иметь образец вируса. Создать его сигнатуру невозможно, пока вирус не попал на анализ к экспертам. Поэтому сигнатуры всегда появляются только через некоторое время после появления нового вируса. С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно. Именно поэтому традиционный сигнатурный метод непригоден для оперативной защиты от вновь появляющихся вирусов.

Этот недостаток традиционного сигнатурного анализа позволяет преодолеть «облачная» антивирусная зашита.

В отличие от традиционного сигнатурного анализа при использовании облачной антивирусной зашиты процесс обмена информацией между ПК и сервером производителя антивирусной программы происходит постоянно. Все ПК подключены к удаленному серверу производителя антивирусной программы и образуют так называемое антивирусное облако. *Антивирусное*

облако представляет собой инфраструктуру, которая используется для обработки сервером поступающей от пользователей ПК информации о подозрительных вредоносных программах с целью своевременно распознать новые, ранее неизвестные угрозы. Чем больше ПК подключено к системе, тем лучше работает облако: об одном и том же подозрительном объекте на сервер приходит информация от многих пользователей, и это стимулирует производителя антивирусной программы к разработке обновления антивирусных баз.

Собирая и обрабатывая поступающую информацию, антивирусная облачная защита работает как мощная экспертная система. Данные, необходимые для блокирования атак, мгновенно передаются всем участникам облака, предотвращая масштабные вирусные эпидемии.

Единственным недостатком облачной антивирусной защиты (как и всех облачных сервисов в целом) является зависимость от стабильности канала связи.

В защите от новых вирусов помогают используемые в антивирусных программах проактивные/эвристические методы обнаружения вирусов.

Существует несколько подходов к проактивной защите. Рассмотрим два наиболее популярных подхода: эвристические анализаторы и поведенческие блокираторы.

Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок.

Эвристический анализатор (*эвристик*) - это программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным. Работа эвристического анализатора, как правило, начинается с поиска в программном коде подозрительных признаков (команд), характерных для вредоносных программ.

Недостатки эвристических анализаторов:

- невозможность лечения - в силу потенциальных ложных срабатываний и возможного неточного определения типа вируса попытка лечения может привести к большим потерям информации, чем из-за самого вируса, а это недопустимо;
- низкая эффективность против принципиально новых типов вирусов.

Поведенческий блокиратор - это программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия.

К основным вредоносным действиям относят:

- ✓ удаление файла;
- ✓ запись в файл;
- ✓ запись в определенные области системного реестра;
- ✓ открытие порта на прослушивание;
- ✓ перехват данных, вводимых с клавиатуры;
- ✓ рассылка писем и др.

Выполнение каждого такого действия по отдельности не даст повода считать программу вредоносной, но если программа последовательно выполняет несколько таких действий, например перехватывает данные, вводимые с клавиатуры, и с определенной частотой пересылает их на какой-то адрес в Интернете, значит, эта программа по меньшей мере подозрительна.

В отличие от эвристических анализаторов поведенческие блокираторы работают в реальных условиях. Принцип действия поведенческих блокираторов прост. При обнаружении потенциально опасного действия задавался вопрос пользователю: разрешить или запретить это действие.

Недостатком поведенческих блокираторов остается срабатывание на действия ряда легитимных программ. Для принятия окончательного решения о вредоносности приложения требуется вмешательство пользователя, что предполагает наличие у него достаточной квалификации.

Для оптимальной антивирусной защиты необходимо сочетание проактивных и сигнатурных подходов. Максимального уровня обнаружения угроз можно достигнуть, только комбинируя эти методы.

Тестовые задания по теме

1. Программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты, называется …

a) червь;
b) компьютерный вирус;
c) троян;
d) апплет.

2. Вредоносная программа, способная к саморазмножению и самостоятельному распространению с использованием сетевых каналов, называется …

a) червь;
b) компьютерный вирус;
c) троян;
d) Spyware.

3. Вредоносная программа, предназначенная для слежения за системой и отсылки собранной информации третьей стороне, называется …

a) червь;
b) компьютерный вирус;
c) троян;
d) Spyware.

4. Отличительным признаком компьютерных вирусов от других вредоносных программ служит их …

a) способность к саморазмножению;
b) привязанность к операционной системе или программной оболочке;
c) способность к распространению по сетям;
d) способность к краже информации.

5. Метод маскировки, при котором вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд, называется …
a) метаморфизм;
b) полиморфизм;
c) шифрование;
d) изоморфизм.

6. Отличительным признаком троянских программ служит их …
a) неспособность к саморазмножению;
b) привязанность к программной оболочке;
c) способность к распространению по сетям;
d) привязанность к операционной системе.

7. Нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей, называется …
a) мистификация;
b) спам;
c) riskware;
d) апплет.

8. Программа, которая намеренно вводит пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит, называется …
a) мистификация;
b) спам;
c) riskware;
d) апплет.

9. Вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями, называются …
a) мистификации;
b) спам;
c) riskware;
d) апплеты.

10. Прикладные программы, небольшие Java-приложения, встраиваемые в HTML-страницы, называются …

a) мистификации;
b) спам;
c) riskware;
d) апплеты.

11. Точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов, называются …

a) сигнатурными;
b) проактивными;
c) эвристическими;
d) логистическими.

12. Приблизительные методы обнаружения вирусов, которые позволяют с определенной вероятностью предположить, что файл заражен, называются …

a) сигнатурными;
b) проактивными;
c) статистическими;
d) логистическими.

13. Совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле, называется … вируса.

a) идентификатором;
b) кодом;
c) сигнатурой;
d) дайджестом.

14. Главный недостаток сигнатурного метода обнаружения вирусов …

a) зависимость от стабильности канала связи;
b) срабатывание на действия ряда легитимных программ;
c) невозможность лечения зараженных ресурсов системы;
d) задержка при реакции на новые угрозы заражения.

15. Главный недостаток эвристических анализаторов …

a) зависимость от стабильности канала связи;
b) срабатывание на действия ряда легитимных программ;
c) невозможность лечения зараженных ресурсов системы;
d) задержка при реакции на новые угрозы заражения.

16. Главный недостаток поведенческих блокираторов …

a) зависимость от стабильности канала связи;
b) срабатывание на действия ряда легитимных программ;
c) невозможность лечения зараженных ресурсов системы;

d) задержка при реакции на новые угрозы заражения.

17. Главный недостаток облачной антивирусной защиты …
a) зависимость от стабильности канала связи;
b) срабатывание на действия ряда легитимных программ;
c) невозможность лечения зараженных ресурсов системы;
d) задержка при реакции на новые угрозы заражения.

18. Отличие «облачной» антивирусной зашиты от традиционного сигнатурного анализа заключается в …
a) точном распознавании новых, ранее неизвестных угроз заражения;
b) срабатывании на действия ряда легитимных программ;
c) невозможности лечения зараженных ресурсов системы;
d) постоянном процессе обмена информацией между ПК и сервером производителя антивирусной программы.

19. Инфраструктура, которая используется для обработки сервером поступающей от пользователей ПК информации о подозрительных вредоносных программах с целью своевременно распознавания новых, ранее неизвестных угроз, называется…
a) сигнатурой вируса;
b) антивирусное облако;
c) сетевой защитой;
d) идентификатором вируса.

20. Программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным, называется…
a) поведенческий блокиратор;
b) антивирусное облако;
c) эвристический анализатор;
d) идентификатором вируса.

21. Программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия, называется…
a) поведенческий блокиратор;
b) антивирусное облако;
c) эвристический анализатор;
d) идентификатором вируса.

Библиографический список

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М.: ДМК Пресс, 2010. – 544 с.
2. Горбатов, В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская. – М.: Горячая Линия – Телеком, 2011. – 248 с.
3. Петренко, С.А. Политики безопасности компании при работе в интернет / С.А. Петренко, В.А. Курбатов. – М.: ДМК Пресс, 2011. – 396 с.
4. Блинов, А.М. Информационная безопасность ч. 1: учеб. пособие / А.М. Блинов. – СПб.: СПбГУЭФ, 2010. – 96 с.
5. Милославская, Н. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учеб. пособие / Н. Милославская, М. Сенаторов, А. Толстой. - 2-е изд. – М.: Горячая Линия – Телеком, 2014
6. Милославская, Н. Управление рисками информационной безопасности: учеб. пособие / Н. Милославская, М. Сенаторов, А. Толстой. - 2-е изд. – М.: Горячая Линия – Телеком, 2014
7. Бирюков, А. Информационная безопасность: защита и нападение / А. Бирюков. – М.: ДМК Пресс, 2013
8. Платонов, В. В. Программно-аппаратные средства защиты информации: учебник / В. В. Платонов. – М.: Академия, 2013. – 336 с.
9. Щербаков, В. Безопасность беспроводных сетей: Стандарт IEEE 802.11/ В. Щербаков, С. Ермаков. – М.: РадиоСофт, 2010
10. Гладкий, А. Безопасность и анонимность работы в Интернете. Как защитить компьютер от любых посягательств извне / А. Гладкий . – М.: Литрес, 2012. – 157 с.

Учебное издание

Сизова Ольга Владимировна

Информационная безопасность
Учебное пособие

Редактор В.Л. Родичева

Подписано в печать 3.11.2015. Формат 60х84 $^{1}/_{16}$. Бумага писчая.
Усл.печ.л. 6,98. Уч.-изд.л. 7,74. Тираж 50 экз. Заказ.

ФГБОУ ВПО «Ивановский государственный
химико-технологический университет»

Отпечатано на полиграфическом оборудовании
кафедры экономики и финансов ФГБОУ ВПО «ИГХТУ»

153000, г. Иваново, Шереметевский пр., 7