Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий
Кафедра информационной безопасности и теории управления

А.М. Иванцов, В.Г Козловский

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. КУРС ЛЕКЦИЙ

Учебное пособие
Часть 2

Ульяновск
2020

Печатается по решению Ученого совета
факультета математики, информационных и авиационных
технологий Ульяновского государственного университета
(протокол № 4/19 от 21.05.2019г)

Рецензенты:

М.А. Волков – кандидат физико-математических наук,
ФГБОУ ВО «Ульяновский государственный университет»,
С.М. Бородин – кандидат технических наук,
ФГБОУ ВО «Ульяновский государственный технический университет».

Иванцов А.М., Козловский В.Г.

И 23 Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 4 с.

Рассматриваются лекции по курсу «Основы информационной безопасности» для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем».
Предназначено для студентов в качестве основного лекционного материала при изучении курса «Основы информационной безопасности».

УДК 004.056 (075.8)
ББК 32.972.53 я 73
И 23

Оглавление

Часть 2

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

ИБ – информационная безопасность;
НСД - несанкционированный доступ;
ЗИ - защита информации;
СМИ - средства массовой информации;
ПО - программное обеспечение;
АС - автоматизированная система;
ИС – информационная система;
СУБД – система управления базами данных;
ОС - операционная система;
ОТКС - открытые информационно-телекоммуникационные сети;
РЭП - радиоэлектронное подавление;
ИВ - информационное воздействие;
ИОБ системы - информационные обучающиеся системы;
НТВ – российский телевизионный канал;
СВТ - средства вычислительной техники;
ГТК - Гостехкомиссия при Президенте Российской Федерации;
ФСТЭК - Федеральная служба по техническому и экспортному контролю;
ФСБ - Федеральная служба безопасности;
СРД - система разграничения доступа;
ДЛ - должностное лицо;
СРУ - система регистрации и учета;
СКУД - система контроля и управления доступом;
ПЭМИН - побочные электромагнитные излучения и наводки;
МЭ - межсетевой экран;
СОВ - система обнаружения вторжений;
СПВ - система предотвращения вторжений;
СЗИ – система защиты информации;
ЭП – электронная подпись;
БД – база данных;
КСА - комплекс средств автоматизации
МЭ - межсетевой экран;
OSI - Open System Interconnection (Сетевая модель взаимодействия открытых систем (эталонная модель);
VPN - Virtual Private Network (виртуальная частная сеть).

ВВЕДЕНИЕ

В учебное пособие включены лекционные материалы по курсу «Основы информационной безопасности для специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем».

Учебное пособие может быть полезно студентам, преподавателям и аспирантам, осваивающим вопросы защиты информации.

В учебное пособие включено 4 раздела (18 тем), направленных на освоение студентами специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем» основ информационной безопасности в соответствии с учебными планами.

Темы № 1-4,11,14-16 могут рекомендованы в ходе изучения дисциплины «Информационная безопасность и защита информации» для студентов по направлению 46.03.02 «Документоведение и архивоведение» (бакалавриат).

Темы № 3-4,16-18 могут рекомендованы в ходе изучения дисциплины «Обнаружение вторжений и защита информации» для студентов по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем» (бакалавриат).

Темы № 1-4, 9, 11, 14, 16-18 могут рекомендованы в ходе изучения дисциплины «Информационная безопасность» для студентов по направлению 09.03.03 «Прикладная информатика» (бакалавриат).

Темы № 1-10 могут рекомендованы в ходе изучения дисциплины «Компьютерная безопасность» для магистров по направлению 11.04.02 "Инфокоммуникационные технологии и системы связи".

Темы № 1-10 могут рекомендованы в ходе изучения дисциплины «Защита информации и информационная безопасность» для студентов направления 11.03.02 "Инфокоммуникационные технологии и системы связи" (бакалавриат).

РАЗДЕЛ 3. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

ТЕМА 8. КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. Концепция защиты автоматизированных систем и средств вычислительной техники

2. Классификация автоматизированных систем по уровню их защищённости

3. Требования к автоматизированным системам по обеспечению безопасности информации

Литература:

1. Руководящие документы Гостехкомиссии при Президенте Российской Федерации от 30 марта 1992 г.: Защита от несанкционированного доступа к информации. Термины и определения; Концепция защиты СВТ и АС от НСД к информации; Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации; Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации; Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники.

2. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.

3. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.:РИОР: ИНФРА-М, 2015. -392с.

1. Концепция защиты автоматизированных систем и средств вычислительной техники

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации разработала и опубликовала пять руководящих документов, посвященных вопросам защиты информации в АС в процессе ее обработки. Основой этих документов является **концепция защиты средств СВТ и АС от НСД к информации**, содержащая систему взглядов ГТК на проблему ИБ и основные принципы защиты компьютерных систем. С точки зрения разработчиков документов, основная задача средств безопасности - это обеспечение защиты от НСД.

Определенный уклон в сторону поддержания секретности информации объясняется тем, что данные документы были разработаны в расчете на применение в ИС системах силовых структур РФ.

Структура требований безопасности:

Руководящие документы ГТК состоят из пяти частей (См. п.1 литературы).

Наибольший интерес представляют 2-4 части. Во второй части излагается система взглядов и основные принципы, которые закладываются в основу проблемы ЗИ от НСД. Руководящие документы ГТК предлагают две группы требований к безопасности - показатели защищенности СВТ от НСД и критерии защищенности АС обработки данных. Первая группа позволяет оценить степень защищенности отдельно поставляемых потребителю компонентов АС и рассматривается в четвертой части, а вторая рассчитана на более сложные комплексы, включающие несколько единиц СВТ, и представлена в третьей части руководящих документов.

2. Классификация АС по уровню их защищённости

Классификация необходима для более детальной, дифференцированной разработки требований по защите от НСД с учетом специфических особенностей этих систем. В основу классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способы их взаимодействия:

информационные – определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования ИС из-за искажения (потери) информации;

организационные – определяющие полномочия пользователей;

технологические – определяющие условия обработки информации, например, способов обработки (автономный, мультипрограммный и т.д.), время циркуляции (транзит, хранение и т.д.), вид АС (автономная, сеть, стационарная, подвижная и т.д.).

Основными этапами классификации являются: - разработка и анализ исходных данных; - выявление признаков АС, необходимых для классификации; - сравнение выявленных признаков АС с классифицируемыми; - присвоение АС соответствующего класса ЗИ от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС является: - перечень защищаемых информационных ресурсов и их уровень конфиденциальности; - перечень лиц, имеющих доступ к штатным средствам АС с указанием их уровня полномочий; - матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам ИС; - режим обработки данных в АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

1. Наличие в АС информации различного уровня конфиденциальности.

2. Уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации.

3. Режим обработки данных в АС – коллективный или индивидуальный.

Устанавливается **девять классов защищенности АС от НСД** к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Самый низкий класс – третий, самый высокий – первый.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации ИС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – **2Б и 2А**.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации ИС. Группа содержит пять классов – 1Д, 1Г, 1В. 1Б, 1А. (Рис. 8.1). (А строже Б,..Г).

Кроме классификации АС по степени защищенности руководящие документы ГТК России предусматривают классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Данные документы устанавливают **семь классов защищенности СВТ от НСД** к информации. Самый низкий класс – седьмой, самый высокий – пер-

вый.

Рис. 8.1. Классификация АС по степени их защищенности

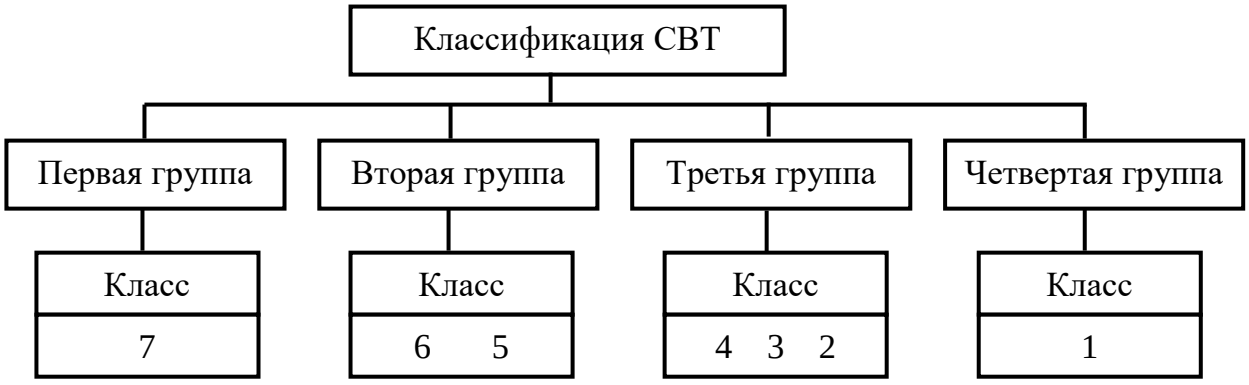

Рис.8.2. Классификация СВТ по уровню защищенности.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты: первая группа содержит только один седьмой класс; вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы; третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы; четвертая группа характеризуется верифицированной защитой и содержит только первый класс (Рис.8.2).

Выбор класса защищенности СВТ для АС, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Применение в комплекте СВТ средств криптографической ЗИ может быть использовано для повышения гарантий качества защиты.

Таким образом, класс защиты АС и СВТ определяет требования по использованию определенных средств и методов защиты.

3. Требования к АС по обеспечению безопасности информации

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по ЗИ от НСД должны осуществляться взаимосвязано с мероприятиями по специальной за-

щите основных и вспомогательных СВТ, средств и систем связи от технических средств разведки и промышленного шпионажа. В общем случае комплекс программно-аппаратных средств и организационных (процедурных) решений по ЗИ от НСД реализуется в рамках СЗИ от НСД.

Рассмотрим требования к АС первой группы класса 1А, так как они содержат наиболее полный набор средств защиты:

1. Подсистема управления доступом

1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему; к терминалам; ЭВМ; узлам сети ЭВМ; каналам связи; внешним устройствам ЭВМ; к программам; к томам, каталогам, файлам, записям, полям записей.

1.2. Управление потоками информации.

2. Подсистема регистрации и учета

2.1. Регистрация и учет: входа (выхода) субъектов доступа в (из) системы (узла сети); выдачи печатных (графических) выходных документов; запуска (завершения) программ и процессов (заданий, задач); доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; изменение полномочий субъектов доступа; создаваемых защищаемых объектов доступа.

2.2. Учет носителей информации.

2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.

2.4. Сигнализация попыток нарушения защиты.

3. Криптографическая подсистема

3.1. Шифрование конфиденциальной информации.

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.

3.3. Использование аттестационных (сертифицированных) криптографических средств.

4. Подсистема обеспечения целостности

4.1. Обеспечение целостности программных средств и обрабатываемой информации.

4.2. Физическая охрана СВТ и носителей информации.

4.3. Наличие администратора (службы) защиты информации в АС.

4.4. Периодическое тестирование СЗИ от НСД.

4.5. Наличие средств восстановления СЗИ от НСД.

4.6. Использование сертифицированных средств защиты.

При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

не ниже 4-го класса – для класса защищенности АС 1В;

не ниже 3-го класса – для класса защищенности АС 1Б;

не ниже 2-го класса – для класса защищенности АС 1А.

Организационные мероприятия в рамках СЗИ от НСД в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

Контрольные вопросы

1. Назвать и охарактеризовать пять руководящих документов ГТК России, посвященных вопросам защиты информации в АС в процессе ее обработки.
2. В чём суть Концепции защиты автоматизированных систем и средств вычислительной техники.
3. Классификация АС по уровню их защищённости.
4. Дать характеристику основных этапов классификации АС.
5. Классификация СВТ по уровню защищенности.
6. Привести основные требования к АС по обеспечению безопасности информации.

ТЕМА 9. СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. НАЗНАЧЕНИЕ И ФУНКЦИИ ЭЛЕМЕНТОВ

1. Принципы защиты информации от НСД.

2. Структура системы защиты информации, назначение и функции элементов.

3. Типовая структура комплексной системы защиты информации от НСД.

Литература:

1. Руководящие документы ГТК при Президенте Российской Федерации от 30.03.1992:

1.1 «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

1.2 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

2. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.

1. Принципы защиты информации от НСД

Под несанкционированным доступом (НСД) понимается доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Выделяют два направления защиты от НСД: - связанные с СВТ; - связанные с АС.

СВТ представляют собой элементы, из которых строятся АС. Для СВТ, в отличии от АС, контролируется реализация исключительно тех функций защиты, для реализации которых они предназначены.

Выделяют следующие **основные способы НСД:**

- непосредственное обращение к объектам доступа;
- создание программных и аппаратных средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД (например, путём внедрения программных закладок);
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД (например, выполнить загрузку компьютера в обход штатной операционной системы).

Основные принципы защиты от НСД:

1. Защита СВТ и АС основывается на положениях и требованиях соответствующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

2. Защита СВТ обеспечивается комплексом технических средств.

3. Защита АС обеспечивается комплексом технических средств и поддерживающих их организационных мер.

4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе, при проведении ремонтных и регламентных работ.

5. Технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надёжность, быстродействие, возможность изменения конфигурации АС и др.).

6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД, который либо может быть периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

2. Структура системы защиты информации, назначение и функции элементов

На основе анализа требований Гостехкомиссии РФ по обеспечению безопасности информации (ныне это Федеральная служба по техническому и экспортному контролю – ФСТЭК России), вашему вниманию предлагается вариант структуры СЗИ, в составе которой целесообразно иметь следующие подсистемы:

1. Разграничения доступа.
2. Регистрации и учета.
3. Обеспечения целостности.
4. Криптографической защиты.
5. Управления СЗИ (в документе ГТК она только подразумевается).

Появление подсистемы управления СЗИ обусловлено необходимостью организации процесса защиты информации в АС, то есть проведения комплекса мероприятий по созданию, обеспечению эффективного функционирования и совершенствованию системы, реализующей процесс защиты.

Подсистема разграничения доступа выполняет следующие задачи:

- аутентификацию всех субъектов доступа, обращающихся к защищаемой информации;

- аутентификацию всех объектов доступа, обрабатывающих защищаемую информацию;
- разграничение доступа объектов и субъектов к информации.

Подсистема регистрации и учета обеспечивает:

- регистрацию и учет входа (выхода) субъектов в/из АС (элемент АС);
- регистрацию и учет бумажных выходных документов;
- регистрацию и учет запуска (завершение) программ и процессов;
- регистрацию и учет доступа программ субъектов, доступа к защищаемой информации, включая ее создание и удаление, передачу по линиям и каналам связи;
- регистрацию и учет изменение полномочий субъектов и объектов доступа;
- регистрацию и учет защищаемых объектов доступа;
- очистку освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;
- сигнализацию попыток нарушения защиты;
- регистрацию, учет и сигнализацию некорректного завершения сеанса работы пользователей РИС.

Криптографическая подсистема реализует:

- криптографическое преобразование информации, хранящейся или передаваемой в АС;
- контрольное суммирование информации.

Подсистема обеспечения целостности должна выполнять следующие функции:

- обеспечение целостности программных средств и информации, хранимой, передаваемой и обрабатываемой в АС;
- физическая охрана СВТ и носителей информации;
- периодическое тестирование и самотестирование СЗИ;
- резервирование информации;
- восстановление и самовосстановление информационно-программного обеспечения АС.

Подсистема управления СЗИ должна обеспечить:

- сбор и анализ данных о состоянии СЗИ;
- сбор и анализ данных о состоянии защищенности АС;
- оценку эффективности СЗИ;
- выработку и передачу на исполнение управляющих воздействий;

- анализ данных и разработку мероприятий по модификации и совершенствованию СЗИ;
- оперативное управление функционированием подсистем СЗИ от НСД.

Иными словами, система управления СЗИ должна осуществлять функции прогнозирования, планирования, контроля, оперативного регулирования на различных этапах существования системы защиты (построения, функционирования, совершенствования).

Предложенный состав СЗИ является функционально достаточным, т.к. реализует все функций СЗИ, необходимые для достижения сформулированных целей защиты от НСД.

На этапе настройки СЗИ от НСД должны быть эталонные копии всех компонентов ПО и создана эталонная конфигурация технических средств.

При начальной загрузке ПО АС системой разграничения доступа (СРД) разрешается загрузка только эталонных копий. Вход пользователя в систему разрешается, только если он является должностным лицом (ДЛ), участвующим в информационном процессе и только со своего автоматизированного рабочего места.

Должностное лицо должно взаимодействовать со средствами АС только через пользовательский интерфейс. Через систему управления СЗИ для каждого ДЛ целесообразно задавать перечень ресурсов, которые могут ему предоставляться в соответствии с его полномочиями, а также порядок их предоставления. Контроль за предоставлением ресурсов ДЛ должен осуществляться системой регистрации и учета (СРУ) в тесном взаимодействии с СРД.

Потоки информации различного грифа конфиденциальности должны контролироваться системой регистрации и учета (СРУ).

Криптографическая система должна осуществлять криптографическое преобразование информации ограниченного доступа, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах и использовать аттестованные (сертифицированные) криптографические средства. Таким образом, криптографическая система осуществляет создание безопасных каналов между узлами сети, а также обеспечивает шифрование информации ограниченного доступа, хранящейся на носителях.

Все действия субъектов и объектов должны регистрироваться СРУ. Она, на основании имеющихся у нее сведений о процессе нормального функционирования и каналах НСД, может прекращать процессы АС, информировать администратора защиты. Целесообразно осуществление взаимодействия СРУ с систе-

мой обеспечения целостности, которая должна выполнять восстановление информации после ее несанкционированного изменения.

Работа СЗИ начинается проверкой очередей запросов на открытие сеанса работы в АС. В случае пустой очереди подсистемой обеспечения целостности инициализируется в соответствии с принятыми допущениями самоконтроль СЗИ, выполняемый встроенными тестовыми средствами. Выполнение операций самоконтроля осуществляется в течение некоторого времени, после которого в случае нормального результата тестирования вновь проверяется наличие запроса на решение задач.

Подобный механизм синхронизации действий СЗИ по самотестированию и отслеживанию состояния входной очереди запросов функционирует по так называемому расписанию. Альтернативой такому решению может служить синхронизация, выполняемая средствами штатной системы прерывания ПЭВМ, составляющей основу узла обработки. Условием успешного функционирования альтернативного способа является, безусловно, меньший приоритет тестовых программ по отношению к любым прикладным.

В случае поступления запроса тестовый контроль прекращается, и СРУ осуществляется фиксация запроса субъекта доступа на открытие сеанса работы в АС, а системой обеспечения целостности - проверка на наличие компьютерных вирусов. После успешного завершения антивирусного контроля выполняется первичная идентификация субъекта доступа, сущность которой сводится к проверке факта регистрации. Независимо от успеха этой проверки подсистемой регистрации и учета осуществляется фиксация обращения в специальном журнале.

В случае, когда результат проверки положителен, то есть к АС обращается законный пользователь, выполняется аутентификация запроса и выясняется степень конфиденциальности запрашиваемой информации.

В полной мере защитные свойства рассматриваемой системы проявляются по отношению к информации, имеющей соответствующие грифы конфиденциальности.

В соответствии с грифом конфиденциальности выбирается метод вторичной идентификации, реализующий проверку подлинности субъектов. Эта проверка может осуществляться по биометрическим параметрам или другими надежными методами аутентификации. Успешный исход вторичной идентификации субъекта приводит к выяснению его полномочий, чем и завершается определение законности обращения.

Поскольку всякий запрос субъекта доступа связан с обработкой данных, хранимых в общей информационной базе, то система защиты по соответствую-

щему грифу конфиденциальности выбирает метод криптозащиты и ключевую информацию. Только после этого запрос получает собственно доступ к данным.

Таким образом, в предложенном варианте структуры СЗИ решение задач защиты достигается выполнением соответствующих работ, которые могут быть реализованы выбранными элементами предложенных подсистем СЗИ.

3. Типовая структура комплексной системы защиты информации от НСД

За последние 3-4 десятилетия обеспечение ИБ корпоративных ИС выросла из частной проблемы отдельных компаний в большое самостоятельное направление развития современных информационных технологий. Наглядным подтверждением этому стало появление специализированных международных институтов, занимающихся проблемами защиты информации; открытых стандартов на технологии обеспечения ИБ; законодательной базы, регулирующей вопросы построения систем защиты информации (СЗИ); специализированных продуктов и решений по ЗИ и т.д. Но главное – за это время появился реальный растущий рынок разнообразных продуктов и услуг в области обеспечения ИБ корпоративных АС.

Можно выделить четыре основных типа (этапа) развития СЗИ:

• однокомпонентные СЗИ, которые строятся на базе одного, как правило, узкоспециализированного продукта по ЗИ (обычно таким продуктом становился антивирусный пакет);

• многокомпонентные СЗИ, строящиеся уже на базе нескольких продуктов, каждый из которых решает свою конкретную задачу. При этом используемые в многокомпонентной СЗИ продукты и технологии по ЗИ никак не связанны между собой ни на техническом, ни на организационном уровнях;

• комплексные СЗИ – дальнейшее развитие многокомпонентных СЗИ, в которых используемые продукты, технологии и решения объединяются в единую систему на организационном уровне с тем, чтобы обеспечить максимальную степень защищенности всей АС в целом. Очевидно, что при этом стойкость всей СЗИ эквивалентна стойкости самого «слабого» ее звена;

• интегрированные СЗИ, в которых все элементы комплексных СЗИ объединяются (вернее интегрируются) не только на организационном, но и на техническом, и даже технологическом уровнях. В такой интегрированной системе компрометация одного из элементов защиты должна надежно компенсироваться противодействием других ее элементов.

К сожалению, на современном этапе развития технологий обеспечения ИБ использование явления синергизма в масштабах всей корпоративной СЗИ

пока еще невозможно в силу отсутствия на рынке реальных решений, позволяющих строить именно интегрированные СЗИ. По-видимому, это объясняется недостаточной зрелостью международных стандартов в области защиты информации, хотя движение в этом направлении прослеживается уже достаточно явно. С другой стороны построение многокомпонентных, а тем более однокомпонентных СЗИ в большинстве случаев уже не является современным решением проблемы ИБ, особенно для крупных компаний. Поэтому в настоящее время оптимальным решением является построение именно комплексных СЗИ. В состав типовой комплексной СЗИ на предприятии могут входить следующие составляющие (подсистемы):

- система контроля и управления доступом (СКУД);
- система видеонаблюдения или охранного телевидения;
- охранно-пожарные системы (например, «Орион»);
- система противодействия экономическому шпионажу (подсистемы защиты: от утечек по акустическому каналу, за счёт побочных электромагнитных излучений и наводок (ПЭМИН) СВТ, по цепям питания и заземления, по каналу визуального наблюдения и др.);
- комплекс защиты корпоративных сетей (контроль трафика, разграничение доступа, защита компьютеров от НСД, межсетевые экраны (МЭ), системы обнаружения (предотвращения вторжений) (СОВ, СПВ) и др.).

Контрольные вопросы

1. Дать определение несанкционированного доступа и перечислить основные способы НСД.
2. Основные принципы защиты от НСД.
3. Характеристика основным подсистем СЗИ.
4. Раскрыть функционал подсистемы управления СЗИ.
5. Обобщённый алгоритм функционирования СЗИ.
6. Основные этапы развития СЗИ.
7. Состав типовой комплексной СЗИ предприятия.

ТЕМА 10. МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ

1. **Дискреционная политика**
2. **Мандатная политика (MLS)**

Литература:

1. Руководящие документы Гостехкомиссии при Президенте Российской Федерации от 30 марта 1992 г.: Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных сис-

тем и требования по защите информации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации.

2. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по спец. группы 090100 "Информационная безопасность"/ Грушо А.А., Применко Э. А., Тимонина Е.Е.. - М.: Академия, 2009. 272 с.

3. Информационная безопасность и защита информации: учебное пособие для вузов по спец. 230201 "Информационные системы и технологии"/ Мельников Владимир Павлович, Клейменов С. А., Петраков А. М.; под ред. С. А. Клейменова. - М.: Академия, 2008. - 336 с.

Управление доступом (Разграничение доступа) — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы. Также данные правила называют правами доступа или политиками безопасности.

Одной из обязательных подсистем СЗИ от НСД является подсистема управления доступом. В руководящих документах Гостехкомиссии России определены два принципа управления доступом: **дискреционный и мандатный.**

В ГОСТ ИСО/МЭК 15408, кроме указанных, описан еще **ролевой принцип управления доступом,** однако допускаются любые другие недискреционные принципы управления доступом.

Формальные модели управления доступом используются в тех случаях, когда те или иные утверждения о стойкости систем защиты информации требуют строгого доказательства, например, в случае, если оценочный стандарт требует использования формальных методов проектирования средств ЗИ. На практике применение таких методов является чрезвычайно трудоемкой и дорогостоящей задачей, поэтому их практическое использование весьма и весьма ограничено.

На сегодняшний день используются **четыре основных класса моделей управления доступом:**

1. **Дискреционные модели управления доступом** — модели, в которых владелец ресурса сам задает права доступа к нему. Метрики и модели испытаний случаев права доступа субъектов к объектам представляются в виде матрицы доступа.

2. **Мандатные модели управления доступом,** в которых режим доступа субъектов к объектам определяется установленным режимом конфиденциальности.

3. **Ролевая модель управления доступом**, копирующая иерархическую структуру организации и позволяющая упростить администрирование.

4. **Атрибутная модель,** являющаяся наиболее универсальной и позволяющая

контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа.

1. Дискреционная политика

Дискреционное управление доступом - разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Дискреционное (избирательное, контролируемое) разграничение доступа — управление доступом субъектов к объектам базируется на том, что пользователи в том или ином объеме могут управлять настройками политик безопасности. Наиболее популярной реализацией дискреционной модели является модель, которая реализует ограничение доступа к файлам и объектам межпроцессной коммуникации в обычных пользовательских представителях семейств операционных систем Unix и Windows. В этих реализациях пользователь может произвольно изменить права доступа к файлу, который он создал, например, сделать его общедоступным.

Владелец. Одним из понятий, появляющихся в стандартной реализации дискреционной модели доступа в рамках файловой системы, является владелец объекта — субъект, который несет ответственность за конфиденциальность, целостность и доступность объекта. На владельца возлагается ответственность за корректное ограничение доступа к данному объекту других субъектов, другими словами, имеет возможность предоставить те или иные права доступа к объекту любому другому субъекту. Обычно владельцем объекта автоматически назначается субъект, создавший данный объект. В дальнейшем владелец с помощью соответствующего метода доступа к объекту может быть изменен.

Избирательное управление доступом является базовой реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений, согласно требованиям к системе защиты информации.

Привилегии. Другим понятием, возникающим в реализациях дискреционной модели доступа, является понятие привилегии на определенный метод доступа. Говорят, что субъект имеет некоторую привилегию, если он имеет право на доступ по некоторому методу ко всем объектам, поддерживающим данный метод доступа.

Как правило, небольшая группа привилегированных пользователей — контролирует все процессы и настройки системного уровня. Подобных пользователей называют суперпользователями.

Дискреционное управление доступом определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;

- права доступа субъекта к объекту системы определяются на основании некоторого, внешнего, по отношению к системе, правила.

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство распространенных в настоящее время ИС обеспечивают выполнение положений именно данной политики безопасности.

В качестве примера реализаций дискреционной политики безопасности в ИС можно привести матрицу доступов, строки которой соответствуют субъектам системы, а столбцы - объектам; элементы матрицы характеризуют права доступа. К недостаткам относится статичность модели. Это означает, что данная политика безопасности не учитывает динамику изменений состояния ИС, не накладывает ограничений на состояния системы. Кроме этого, при использовании дискреционной политики безопасности, возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность ИС.

В то же время имеются модели ИС, реализующие дискреционную политику безопасности, которые предоставляют алгоритмы проверки безопасности. Так или иначе, матрица доступов не является тем механизмом, который бы позволил реализовать ясную и четкую систему защиты информации в ИС. Этим обуславливается поиск других более совершенных политик безопасности.

Пусть O - множество объектов, S - множество субъектов, $S \subseteq O$. Пусть $U=\{U_1,...,U_m\}$- множество пользователей. Определим отображение: own: $0 \rightarrow U$.

В соответствии с этим отображением каждый объект объявляется собственностью соответствующего пользователя. Пользователь, являющийся собственником объекта, имеет все права доступа к нему, а иногда и право передавать часть или все права другим пользователям. Кроме того, собственник объекта определяет права доступа других субъектов к этому объекту, то есть политику безопасности в отношении этого объекта. Указанные права доступа записываются в виде матрицы доступа (рис10.1), элементы которой - суть подмножества множества R, определяющие доступы субъекта S, к объекту $0_i (i = 1, 2,...,; j = 1, 2,...)$.

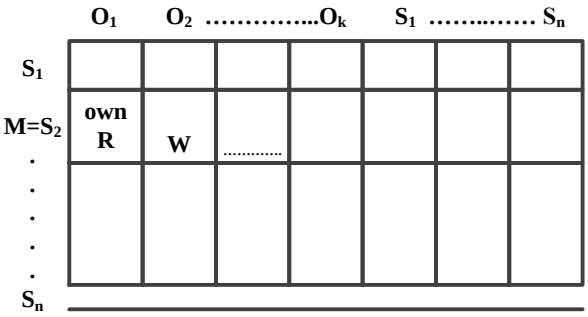

Рис.10.1 Матрица доступа

Существует несколько вариантов задания матрицы доступа.

1. Листы возможностей: для каждого субъекта S_i создается лист (файл) всех объектов, к которому имеет доступ данный объект.

2. Листы контроля доступа: для каждого объекта создается список всех субъектов, имеющих право доступа к этому объекту.

Дискреционная политика связана с исходной моделью таким образом, что траектории процессов в вычислительной системе ограничиваются в каждом доступе. Причем вершины каждого графа разбиваются на классы и доступ в каждом классе определяется своими правилами каждым собственником. Множество неблагоприятных траекторий *N* для рассматриваемого класса политик определяется наличием неблагоприятных состояний, которые в свою очередь определяются запретами на некоторые дуги. Дискреционная политика, как самая распространенная, чаще всего подвергалась исследованиям. Существует множество разновидностей этой политики. Однако многих проблем защиты эта политика решить не может. Одна из самых существенных слабостей этого j класса политик - то, что они не выдерживают атак при помощи "Троянского коня". Это означает, в частности, что **система защиты, реализующая дискреционную политику, плохо защищает от проникновения вирусов в систему и других средств скрытого разрушающего воздействия.** Покажем на примере принцип атаки "Троянским конем" в случае дискреционной политики.

Пример 1. Пусть U_1 - некоторый пользователь, а U_2 - пользователь-злоумышленник, O_1 - объект, содержащий ценную информацию, O_2 - программа с "Троянским конем" T, и M - матрица доступа, которая имеет вид (Рис.10.2):

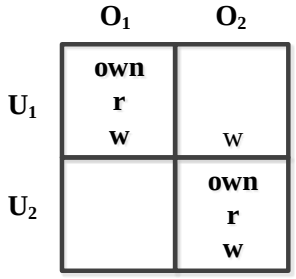

Рис.10.2 Матрица доступа

Проникновение программы происходит следующим образом. Злоумышленник U_2 создает программу O_2 и, являясь ее собственником, дает U_1 запускать ее и писать в объект O_2 информацию. После этого он инициирует каким-то образом, чтобы U_1 запустил эту программу (например, O_2 - представляет интересную компьютерную игру, которую он предлагает U_1 для развлечения). U_1 запускает O_2 и тем самым запускает скрытую программу T, которая обладая правами U_1 (т.к. была запущена U_1), списывает в себя информацию, содержащуюся в O_1. После этого хозяин U_2 объекта O_2, пользуясь всеми правами, имеет возможность считать из O_2 ценную информацию объекта O_1.

Следующая проблема дискреционной политики - это автоматическое определение прав. Так как объектов много, то задать заранее вручную перечень прав каждого субъекта на доступ к объекту невозможно. Поэтому матрица доступа различными способами агрегируется, например, оставляются в качестве субъектов только пользователи, а в соответствующую ячейку матрицы вставляются формулы функций, вычисление которых определяет права доступа субъекта, порожденного пользователем, к объекту O. Разумеется, эти функции могут изменяться во времени. В частности, возможно изъятие прав после выполнения некоторого события. Возможны модификации, зависящие от других параметров.

Одна из важнейших проблем при использовании дискреционной политики - это проблема контроля распространения прав доступа. Чаще всего бывает, что владелец файла передает содержание файла другому пользователю и тот, тем самым, приобретает права собственника на информацию. Таким образом, права могут распространяться, и даже, если исходный владелец не хотел передавать доступ некоторому субъекту S к своей информации в O, то после нескольких шагов передача прав может состояться независимо от его воли. Возникает задача об условиях, при которых в такой системе некоторый субъект рано или поздно получит требуемый ему доступ. Эта задача

исследовалась в модели "take-grant", когда форма передачи или взятия прав определяются в виде специального права доступа (вместо own).

Классической дискреционной моделью управления доступом является модель Харрисона-Руззо-Ульмана (Harrison-Ruzzo-Ullmanmodel), которая формализует понятие матрицы доступа — таблицы, описывающей права доступа субъектов к объектам.

2. Мандатная политика (MLS)

Мандатное управление доступом - разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Основу мандатной (полномочной) политики безопасности составляет мандатное управление доступом, которое подразумевает, что: - все субъекты и объекты системы должны быть однозначно идентифицированы; - задан линейно упорядоченный набор меток секретности; - каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности в ИС; - каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в ИС - максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

Основная цель мандатной политики безопасности – предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т.е. противодействие возникновению в ИС информационных каналов сверху вниз.

Чаще всего мандатную политику безопасности описывают в терминах, понятиях и определениях свойств **модели Белла-Лападула,** в рамках которой доказывается важное утверждение, указывающее на принципиальное отличие систем, реализующих мандатную защиту, от систем с дискреционной защитой: если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.

Кроме того, по сравнению с ИС, построенными на основе дискреционной политики безопасности, для систем, реализующих мандатную политику, характерна более высокая степень надежности. Это связано с тем, что отслеживаются не только правила доступа субъектов системы к объектам, но и состояния самой ИС.

Таким образом, каналы утечки в системах данного типа не заложены в нее непосредственно (что мы наблюдаем в положениях предыдущей политики безопасности), а могут появиться только при практической реализации системы вследствие ошибок разработчика. В дополнении к этому правила мандатной политики безопасности более ясны и просты для понимания разработчиками и пользователями ИС, что также является фактором, положительно влияющим на уровень безопасности системы. С другой стороны, реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов вычислительной системы.

В мандатной модели обычные пользователи лишены возможности управлять настройками политик безопасности. Например, возможность доступа к тому или иному объекту определяется уровнем секретности объекта и уровнем доступа пользователя, которые жестко заданы для каждого пользователя и объекта. Данная модель обладает невысокой гибкостью и высокой трудоемкостью настройки политик безопасности, но при этом позволяет достичь высокого уровня управляемости безопасностью.

Улучшенные с точки зрения безопасности версии операционных систем ограничивают доступ к файлам и другим объектам с помощью мандатного ограничения доступа. В результате пользователь, даже являясь создателем объекта, не может произвольно менять права доступа к этому файлу. Не гарантируется и то, что после создания пользователь сохранит доступ к созданному объекту, если специально это не оговорено в соответствующей политике безопасности.

Многоуровневая политика безопасности (политика MLS) принята всеми развитыми государствами мира. В повседневном секретном делопроизводстве госсектор России также придерживается этой политики.

Решетка ценностей SC является основой политики MLS. Другой основой этой политики является понятие информационного потока. Для произвольных объектов X и Y пусть имеется информационный поток $X \to_{\alpha} Y$, где X -источник, Y - получатель информации. Отображение: O->SC считается заданным. Если c(Y)>c(X), то Y -более ценный объект, чем X.

Определение. Политика MLS считает информационный поток X->Y разрешенным тогда и только тогда, когда c(Y)>c(X) в решетке SC.

Таким образом, политика MLS имеет дело с множеством информационных потоков в системе и делит их на разрешенные и неразрешенные очень простым условием. Однако эта простота касается информационных потоков, которых в системе огромное количество. Поэтому приведенное выше опре-

деление неконструктивно. Хотелось бы иметь конструктивное определение на языке доступов.

Рассмотрим класс систем с двумя видами доступов r и w (хотя могут быть и другие доступы, но они либо не определяют информационных потоков, либо выражаются через w и r). Пусть процесс S в ходе решения своей задачи последовательно обращается к объектам $O_1,O_2,...,O_n$ (некоторые из них могут возникнуть в ходе решения задачи). Пусть

$$S \xrightarrow{r} O_{i1}, S \xrightarrow{r} O_{i2}, S \xrightarrow{r} O_{ik}, S \xrightarrow{w} O_{i1}, S \xrightarrow{w} O_{jn-k}$$

Тогда при выполнении условий $c(S)>c(Oi_t)$, t=l,....k, соответствующие потоки информации будут идти в разрешенном политикой MLS направлении, а при $c(S)<c(Oj_t)$, t=l,.., n-k, потоки, определяемые доступом w, будут идти в разрешенном направлении.

Таким образом, в результате выполнения задачи процессом S, информационные потоки, с ним связанные, удовлетворяют политике MLS. Такого качественного анализа оказывается достаточно, чтобы классифицировать почти все процессы и принять решение о соблюдении или нет политики MLS. Если где-то политика MLS нарушается, то соответствующий доступ не разрешается. Причем, разрешенность цепочки (1) вовсе не означает, что субъект S не может создать объект O такой, что $c(S)>c(0)$. Однако он не может писать туда информацию. При передаче управления поток информации от процесса S или к нему прерывается (хотя в него другие процессы могут записывать или считывать информацию как в объект). При этом, если правила направления потока при r и w выполняются, то MLS соблюдается, если нет, то соответствующий процесс не получает доступ. Таким образом, мы приходим к управлению потоками через контроль доступов. В результате для определенного класса систем получим конструктивное описание политики MLS.

Определение. В системе с двумя доступами r и w политика MLS определяется следующими правилами доступа

$$X \xrightarrow{r} Y \Leftrightarrow c(X) \geq c(Y),$$

$$X \xrightarrow{w} Y \Leftrightarrow c(X) \leq c(Y).$$

Структура решетки очень помогает организации поддержки политики MLS. В самом деле, пусть имеется последовательная цепочка информационных потоков

$$O_1 \xrightarrow{\alpha} O_2 \xrightarrow{\beta} O_3 \xrightarrow{\gamma} \dots \xrightarrow{\delta} O_k$$

Если каждый из потоков разрешен, то свойства решетки позволяют утверждать, что разрешен сквозной поток $O_1 \xrightarrow{\alpha} \ldots \xrightarrow{\delta} O_k$. Действительно, если информационный поток на каждом шаге разрешен, то $c(O_{i+1}) \geq c(O_i)$, тогда по свойству транзитивности решетки $c(O_1) \leq c(O_k)$, то есть сквозной поток разрешен.

MLS политика в современных системах защиты реализуется через мандатный контроль (или, также говорят, через мандатную политику). Мандатный контроль реализуется подсистемой защиты на самом низком аппаратно-программном уровне, что позволяет эффективно строить защищенную среду для механизма мандатного контроля. Устройство мандатного контроля, удовлетворяющее некоторым дополнительным, кроме перечисленных, требованиям, называется монитором обращений. **Мандатный контроль еще называют обязательным, так как проходит каждое обращение субъекта к объекту**, если субъект и объект находятся под защитой системы безопасности. Организуется мандатный контроль следующим образом. Каждый объект O имеет метку с информацией о классе c(O). Каждый субъект также имеет метку, содержащую информацию о том, какой класс доступа c(S) он имеет. Мандатный контроль сравнивает метки и удовлетворяет запрос субъекта S к объекту O на чтение, если c(S)>c(0) и удовлетворяет запрос на запись, если c(S)<c(0). Тогда согласно изложенному выше мандатный контроль реализует политику MLS.

Политика MLS устойчива к атакам "Троянским конем". На чем строится защита от таких атак поясним на примере.

Пример 1. Пусть пользователи U_1 и U_2 находятся на разных уровнях, то есть $c(U_1)>c(U_2)$. Тогда, если U_1 может поместить в объект O_1 ценную информацию, то он может писать туда и $c(U_2)<c(U_1)<c(0_1)$, то есть $c(U_2)<c(0_1)$. Тогда любой "Троянский конь" T, содержащийся в объекте O_2, который может считать информацию в O_1, должен отражать соотношение $c(O_2) \geq c(O_1)$.

Тогда $c(O_2)>c(U_2)$ и пользователь U_2 не имеет право прочитать в O_2, что делает съем в O_1 и запись в O_2 бессмысленным.

Несколько слов о реализации политики безопасности MLS в рамках других структур, внесенных в информацию. Обратимся к примеру реляционной базы данных. Пусть структура РМ и структура решетки ценностей MLS согласованы. Пусть в системе реализован мандатный контроль, который при обращении пользователя U к базе данных на чтение позволяет извлекать и формировать "обзор" только такой информации, класс которой <c(U). Ана-

логично, мандатный контроль и правила декомпозиции позволяют поддерживать в нужном направлении информационные потоки в процессе функционирования базы данных. В результате получаем, что при наличии мандатного контроля реляционная многоуровневая база данных поддерживает политику MLS.

Политика MLS создана, в основном, для сохранения секретности информации. Вопросы целостности при помощи этой политики не решаются или решаются как побочный результат защиты секретности.

Пример 2. (Политика целостности Biba). Предположим, что опасности для нарушения секретности не существует, а единственная цель политики безопасности - защита от нарушений целостности информации. Пусть, попрежнему, в информацию внесена решетка ценностей SC. В этой связи любой информационный поток X -> Y может воздействовать на целостность объекта Y и совершенно не воздействовать на целостность источника X. Если в Y более ценная информация, чем в X, то такой поток при нарушении целостности Y принесет более ощутимый ущерб, чем поток в обратном направлении от более ценного объекта Y к менее ценному X. Biba предложил в качестве политики безопасности для защиты целостности следующее.

Определение. В политике Biba информационный поток X -->$_{\alpha}$Y разрешен тогда и только тогда, когда $c(Y) \le c(X)$

Можно показать, что в широком классе систем эта политика эквивалентна следующей.

Определение. Для систем с доступами w и r политика Biba разрешает доступ в следующих случаях:

$$S \xrightarrow{r} O \Leftrightarrow c(S) \le c(O),$$
$$S \xrightarrow{w} O \Leftrightarrow c(S) \ge c(O).$$

Очевидно, что для реализации этой политики также подходит мандатный контроль.

Одной из самых известных моделей мандатного управления доступа является модель Белла-ЛаПадулы. Мандатный принцип разграничения доступа, изначально, ставил своей целью перенести на автоматизированные системы практику секретного документооборота, принятую в правительственных и военных структурах, когда все документы и допущенные к ним лица ассоциируются с иерархическими уровнями секретности.

Основным положением политики Белла - ЛаПадулы, взятым ими из реальном жизни, является назначение всем участникам процесса обработки защищаемой информации, и документам, в которых она содержится, специальной

метки, например, секретно, сов. секретно и т. д, получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень сов. секретно считается более высоким чем уровень секретно, или доминирует над ним. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух простых правил:

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный.

2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых).

Второе правило (далее мы увидим, что оно более важное) предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом — с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними.

Система в модели безопасности Белла–Ла Падулы, как и другие модели, представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, ScO) и прав доступа read и write. В мандатной модели рассматриваются только эти два вида доступа, и, хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и т.д.), все они будут отображаться в базовые (чтение и запись).

Контрольные вопросы

1. Что такое «Управление доступом (Разграничение доступа)»?
2. Основные классы моделей управления доступом.
3. Дать характеристику дискреционного управления доступом.
4. Свойства дискреционного управления доступом и варианты задания матрицы доступа.
5. Основные проблемы дискреционной политики.
6. Мандатное управление доступом.

7. Основные свойства и правила модели Белла-Лападулы.

8. Сравнительный анализ мандатного и дискреционного управления доступом.

РАЗДЕЛ 4. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 11. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1. Основные понятия криптографии

2. История криптографии

3. Пример простейшего шифра

Литература:

1. Дэвид Кан. Взломщики кодов.

1. Основные понятия криптографии

Проблемой ЗИ при ее передаче между абонентами люди занимаются на протяжении всей истории. Человечеством изобретено множество способов, позволяющих в той или иной мере скрыть смысл передаваемых сообщений от противника. На практике выработалось несколько групп способов защиты секретных посланий. Назовем некоторые из них, применяющиеся так же давно, как и криптографические.

Первым способом является физическая защита материального носителя информации от противника. В качестве носителя данных может выступать бумага, компьютерный носитель (DVD-диск, флэш-карта, магнитный диск, жесткий диск компьютера и т.д.). Для реализации этого способа необходим надежный канал связи, недоступный для перехвата. В различное время для этого использовались почтовые голуби, специальные курьеры и др. Методы физической ЗИ используются и в современных ИС. Так, например, системы защиты информации (СЗИ) невозможны без систем ограждения и без охранных систем.

Второй способ ЗИ, известный с давних времен – стеганографическая ЗИ. Этот способ основан на попытке скрыть от противника сам факт наличия интересующей его информации. При стеганографической защите прячут физический носитель данных или маскируют искомое сообщение среди открытой информации.

К таким способам относят, например, «сокрытие» микрофотографии с тайной информацией в открытом месте: под маркой на почтовом конверте, под обложкой книги и т.д. К стеганографии относятся также такие известные приемы, как «запрятывание» конфиденциального послания в корешках книг, в пуговицах, в каблуках, в пломбе зуба и т.д. Некоторые из способов были разработаны

еще в древние времена. Так, например, греки нашли необычное решение: они брили наголо голову раба и писали на ней свое послание. Когда волосы на голове раба отрастали вновь, его посылали доставить сообщение. Получатель брил голову раба и прочитывал текст. К сожалению, на отправку сообщения и получение ответа таким способом уходило несколько недель. В более поздние времена в этом направлении наибольшее распространение получили химические (симпатические) чернила. Текст, написанный этими чернилами между строк открытого сообщения, невидим. Он появлялся только в результате применения определенной технологии проявления. В условиях повсеместного использования информационных технологий возникают новые стеганографические приемы. Например, известен способ, при котором секретное сообщение прячется в файле графического изображения. При использовании этого способа младший значащий бит в описании каждого пикселя изображения заменяется битом сообщения. Разделив все исходное сообщение на биты и разместив эти биты по всему графическому файлу, мы пересылаем изображение с замаскированным сообщением получателю. Графическое изображение при этом меняется не слишком сильно, особенно если использовался режим с большим количеством цветов, например, с глубиной цвета 24 бита на пиксель. Это связано с тем, что человеческий глаз не может различать такое большое количество цветов. В результате в картинке размером всего 32 на 32 точки можно вместить тайное сообщение длиной 1024 бита или 128 байт.

Третий способ ЗИ – наиболее надежный и распространенный в наши дни – криптографический. Этот способ предполагает преобразование информации для сокрытия ее смысла от противника. Криптография в переводе с греческого означает "тайнопись". В настоящее время криптография занимается поиском и исследованием математических методов преобразования информации.

В настоящее время криптография прочно вошла в нашу жизнь. Перечислим лишь некоторые сферы применения криптографии в современном обществе:

- шифрование данных при передаче по открытым каналам связи (например, при совершении покупки в Интернете). Сведения о сделке, такие как адрес, телефон, номер кредитной карты, обычно зашифровываются в целях безопасности;
- обслуживание банковских пластиковых карт;
- хранение и обработка паролей пользователей в сети;
- сдача бухгалтерских и иных отчетов через удаленные каналы связи;
- банковское обслуживание предприятий через локальную или глобальную сеть;

• безопасное от НСД хранение данных на жестком диске компьютера (в операционной системе Windows даже имеется специальный термин – шифрованная файловая система (EFS)).

До начала XX века криптографические методы применялись лишь для шифрования данных с целью защиты от НСД. В настоящее время, в связи с развитием техники передачи информации на дальние расстояния, интерес к криптографии значительно возрос. Благодаря созданию новых криптографических методов расширился и спектр задач криптографии.

Криптография предназначена решать следующие задачи:

• собственно шифрование данных с целью защиты от НСД;

• проверка подлинности сообщений;

• проверка целостности передаваемых данных: получатель может проверить, не было ли сообщение изменено или подменено в процессе пересылки;

• обеспечение невозможности отказа, то есть невозможности как для получателя, так и для отправителя отказаться от факта передачи.

Криптография и криптоанализ это 2 направления науки (Криптологии). Цели этих направлений прямо противоположны. Криптография занимается поиском и исследованием математических методов преобразования информации. Сфера интересов криптоанализа — исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- системы электронной подписи;
- управление ключами.

Рассмотрим **основные понятия криптографии**.

Алфавит — конечное множество используемых знаков.

В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие (алфавит Z33 — 32 буквы русского алфавита и пробел; алфавит Z256 — символы, входящие в стандартные коды ASCII и КОИ-8; бинарный алфавит — Z2 = {0,1}; восьмеричный или шестнадцатеричный алфавит др.

Текст — упорядоченный набор из элементов алфавита.

Сообщение, полученное после преобразования любым шифром, называется шифрованным сообщением (**закрытым текстом**, **криптограммой**).

Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (Рис.11.1).

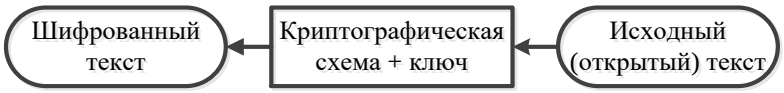

Рис.11.1 Шифрование

Расшифрование — процесс, обратный шифрованию. На основе ключа шифрованный текст преобразуется в исходный.

Ключ — информация, необходимая для беспрепятственного шифрования и расшифрования текстов.

Дешифрование – процесс расшифрования без знания ключа.

Криптографическая система представляет собой семейство преобразований открытого текста. Члены этого семейства индексируются или обозначаются k символом, параметр k является ключом.

Пространство ключей К — это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы подразделяют на симметричные и с открытым ключом.

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используют два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Электронной подписью (ЭП) называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Для современных криптографических систем защиты процессов переработки информации сформулированы следующие **общепринятые требования:**

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Методы шифрования и расшифрования подразделяют на два класса: с симметричным ключом и системы с открытыми ключами. Все известные методы шифрования с симметричными ключами можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование (расшифрование).

Каждый из этих методов может иметь несколько разновидностей.

В методах шифрования с симметричными ключами способом замены применяются алгоритмы прямой замены, многоалфавитной подстановки или полиалфавитной замены. Это наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу.

Для обеспечения высокой криптостойкости требуется использование больших ключей, кроме того, применяется модифицированная матрица шифрования.

Метод перестановки — несложный метод криптографического преобразования. Он используется, как правило, в сочетании с другими методами.

Аддитивные методы (гаммирование) заключаются в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры относятся к комбинированным методам и представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста.

Блочные шифры на практике встречаются чаще, чем «чистые» преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

2. История криптографии

Исторически криптография развивалась как практическая дисциплина, изучающая и разрабатывающая способы шифрования письменных сообщений. В распоряжении историков имеются данные, что криптографические методы применялись в Древнем Египте, Индии, Месопотамии. Так, например, в записях египетских жрецов есть сведения о системах и способах составления шифрованных посланий.

Древние греки оставили документальные подтверждения о различных применяемых ими шифровальных системах. Греками, а вернее спартанцами, во время многочисленных войн применялось одно из первых шифровальных устройств – **Сцитала**. Сцитала представляла собой цилиндрический жезл определенного диаметра. На Сциталу виток к витку наматывалась узкая полоска папируса (или кожаного ремня). На намотанной ленте вдоль оси жезла писали открытое сообщение. Затем ленту разматывали и переправляли адресату. После снятия папируса с жезла выходило как будто буквы сообщения написаны в беспорядке поперек ленты. Если папирус попадал в руки противника, то секретное сообщение прочитать было невозможно. Для получения исходного текста была необходима Сцитала точно такого же диаметра – на нее наматывалась полученная полоска папируса, строки сообщения совмещались, и в результате можно было прочитать секретное послание. Ключом в данном методе шифрования являлся диаметр Сциталы. Интересно, что изобретение дешифровального "устройства" приписывается Аристотелю. Предполагается, что именно он предложил использовать конусообразное "копье", на которое наматывалась перехваченная лента с зашифрованным сообщением. Лента с буквами передвигалась вдоль оси конуса до тех пор, пока не появлялся осмысленный текст.

В арабских странах шифрование сообщений довольно широко использовалось как в военных, так и в политических целях и даже в переписке между торговыми партнерами. Кстати, слово "шифр" арабского происхождения, как и слово "цифра". В VIII – XV веках на свет появляются научные труды, содержащие сведения по криптографии: описания различных шифров и даже некоторых методов криптоанализа. Так, в многотомной энциклопедии "Шауба аль-Аша" упоминается о частотном криптоанализе (то есть анализе, основанном на частоте встречаемости букв открытого и зашифрованного сообщений). В этой же энциклопедии приводится таблица частотных характеристик букв арабского языка.

В XVII-XVIII веках во многих государствах Европы появились специальные шифровальные службы. В России датой появления криптографической службы специалисты называют 1549 год, когда был создан "посольский приказ", в котором имелось "цифирное" отделение. В эпоху Петра I криптографическая служба была реорганизована в "Посольскую канцелярию".

В различные времена криптографией занимались многие политики и ученые. Среди них Пифагор, Аристотель, Платон, Галилей, Л. да Винчи, Б. Паскаль, И. Ньютон, Л. Эйлер, и другие.

Огромное влияние на развитие криптографии оказывают достижения научно-технического прогресса. Так, например, в середине XIX века после изобретения телеграфа появилось несколько дипломатических и коммерческих шифров, ориентированных на применение телеграфа. Возрастание скорости передачи данных требовало увеличения скорости шифрования. В конце XIX века появились механические шифраторы Т. Джефферсона и Ч. Уитстона. С конца XIX века криптография стала серьезной отраслью научных знаний и стала изучаться как отдельная наука в военных академиях.

В 20-х годах XX века для автоматизации процесса шифрования появились многочисленные механические устройства. В частности, широко использовались роторные шифровальные машины, в которых для выполнения операций замены символов применялись механические колеса – роторы. Шифровальные машины преобразовывали открытый текст в зашифрованный, состоящий из символов того же алфавита. После преобразования зашифрованная информация могла передаваться различными способами, например, по радиоканалу. Во всех развитых странах, в том числе и в СССР, создавались высокоскоростные шифрмашины, которые широко применялись во время второй мировой войны и позже.

В середине XX века разработкой криптографических алгоритмов стали заниматься профессиональные математики и специалисты в области информатики. Существенное влияние на развитие криптографии оказала работа американского инженера-математика К. Шеннона "Теория связи в секретных системах", в которой были сформулированы и математически доказаны условия "невскрываемости" шифров.

С 50-х годов XX века в криптографии используется электронная вычислительная техника. Начинается создание так называемых блочных шифров, которые позволяют обрабатывать информацию целыми фрагментами или блоками. Первоначально для операций блочного шифрования разрабатывали аппаратные устройства с жесткой логикой, однако стремительное развитие возможностей вычислительной техники позволило создать программные аналоги блочных сис-

тем шифрования. Криптографические программные и аппаратные средства стали использоваться в гражданских целях, например, в коммерческих системах передачи информации.

3. Пример простейшего шифра

Теперь, когда даны основные определения, рассмотрим одну из простейших систем шифрования, которая носит имя "шифр Юлия Цезаря". Предполагается, что знаменитый римский император и полководец, живший в 1 веке до нашей эры, использовал этот шифр в своей переписке.

Шифр Цезаря применительно к русскому языку состоит в следующем. Каждая буква сообщения заменяется на другую, которая в русском алфавите отстоит от исходной на три позиции дальше. Таким образом, буква А заменяется на Г, Б на Д и так далее вплоть до буквы Ь, которая заменялась на Я, затем Э на А, Ю на Б и, наконец, Я на В.

Например, слово ЗАМЕНА после шифрования методом Цезаря превратится в КГПЗРГ

Это не очень сложный метод, тем более что при шифровании сообщений из нескольких слов сразу становится понятным, сколько слов содержал исходный текст. Кроме того, можно получить некоторую информацию по анализу повторов букв в зашифрованном сообщении. Например, в зашифрованном КГПЗРГ одна из букв повторяется дважды. Тем не менее, Цезарь вошел в историю криптографии, а "шифр Юлия Цезаря", как его до сих пор называют, служит примером одной из первых систем шифрования.

Для расшифрования сообщения КГПЗРГ необходимо знать только сам алгоритм шифрования. Любой человек, знающий способ шифрования, легко может расшифровать секретное сообщение. Таким образом, ключом в данном методе является сам алгоритм. Каким образом можно усовершенствовать шифр Цезаря? Можно было бы попытаться расширить алфавит с 33 до 36 символов и более за счет включения знаков препинания и пробелов. Это увеличение алфавита замаскировало бы длину каждого отдельного слова.

Приведенные простые примеры показывают, что вероятность успешного криптоанализа зависит от многих факторов: от системы шифрования, от длины перехваченного сообщения, от языка и алфавита исходного сообщения.

Контрольные вопросы

1. Основные способы защиты информации.
2. Сферы применения криптографии в современном обществе.
3. Назвать основные понятия криптографии.
4. Криптосистемы: симметричные и с открытым ключом.

5. Что такое электронная подпись?
6. Основные требования к криптографическим системам.
7. Методы шифрования с симметричными ключами.
8. История развития криптографии.
9. Шифр Юлия Цезаря.
10. Способы усовершенствования Шифра Юлия Цезаря.

ТЕМА 12. СИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

1. Обобщенная схема симметричной криптосистемы

2. Алгоритм шифрования DES

3. ГОСТ Р 34.12-2015 «Магма»

4. Особенности применения алгоритмов симметричного шифрования

Литература:

1. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.

1. Обобщенная схема симметричной криптосистемы

Исторически первыми появились симметричные криптографические системы. В симметричной криптосистеме шифрования используется один и тот же ключ для шифрования и расшифрования информации. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. 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** — ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Симметричные криптосистемы называют еще одноключевыми системами или криптосистемами с закрытым ключом. Схема такой системы показана на Рис. 12.1.

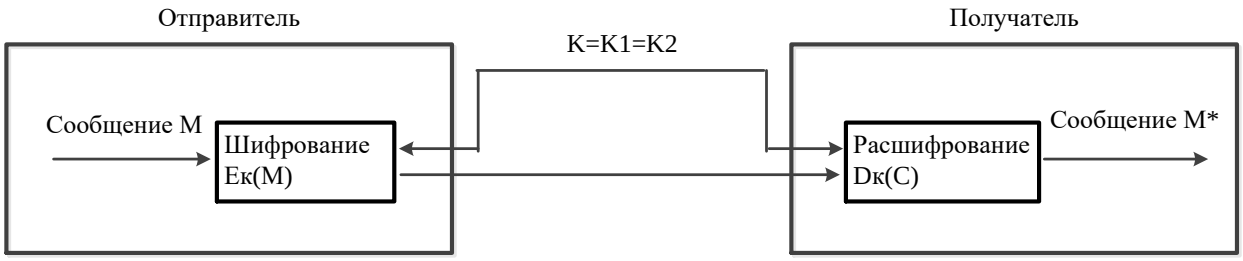

Рис. 12.1 Схема симметричной криптосистемы шифрования

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 расшифровывания 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, имитовставки), вырабатываемого по секретному ключу. Имитоприставка является разновидностью контрольной суммы, т. е. 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 НСД в отсутствие владельца! Это может быть как архивное шифрование выбранных файлов, так и прозрачное шифрование целых логических или физических дисков.

Обладая высокой скоростью шифрования, одноключевые криптосистемы позволяют решать многие важные задачи защиты, 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.

Существуют реализации алгоритмов симметричного шифрования для абонентского шифрования данных — т. е. для отправки шифрованной информации абоненту, например, через Интернет. Использование одного ключа для всех абонентов подобной криптографической сети недопустимо по соображениям безопасности.

Действительно, в случае компрометации (утери, хищения) ключа под угрозой будет находиться документооборот всех абонентов. В этом случае может быть использована матрица ключей (рис. 12.2).

1	2	3	….	n	
K11	**K12**	**K13**	**….**	**K1n**	**Набор ключей для абонента 1**
K21	**K22**	**K23**	**….**	**K2n**	**Набор ключей для абонента 2**
K31	**K32**	**K33**	**….**	**K3n**	**Набор ключей для абонента 3**
…..	**……**	**…..**	**…..**	**……**	
Kn1	**Kn2**	**Kn3**	**….**	**Knn**	**Набор ключей для абонента n**

Рис. 12.2 Матрица ключей

Матрица, ключей представляет собой таблицу, содержащую ключи парной связи абонентов. Каждый элемент таблицы *Kij* предназначен для связи абонентов i и *j* и доступен только двум данным абонентам. Соответственно, для всех элементов матрицы ключей соблюдается равенство *Kij = Kji*. Каждая i-я строка матрицы представляет собой набор ключей конкретного абонента для связи с остальными *N* - 1 абонентами.

Набор ключей (сетевые наборы) распределяются между всеми абонентами криптографической сети.

Аналогично сказанному выше, сетевые наборы должны распределяться *по защищенным каналам* связи или из рук в руки.

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=Ек(M) и M=Dk(C)

где *M* — исходный (открытый) блок данных; *C* - зашифрованный блок данных. Ключ *K* является параметром симметричного блочного криптоалго-

ритма и представляет собой блок двоичной информации фиксированного размера. Исходный «*M*» и зашифрованный «*C*» блоки данных также имеют фиксированную разрядность, равную между собой, но необязательно равную длине ключа *K*.

Блочные шифры являются той основой, на которой реализованы практически все симметричные криптосистемы.

Симметричные криптосистемы позволяют зашифровывать и расшифровывать файлы произвольной длины. Практически все алгоритмы используют для преобразований определенный набор обратимых математических преобразований.

Методика создания цепочек из зашифрованных блочными алгоритмами байтов позволяет шифровать ими пакеты информации неограниченной длины. Отсутствие статистической корреляции между битами выходного потока блочного шифра используется для вычисления контрольных сумм пакетов данных и в хэшировании паролей. На сегодняшний день разработано достаточно много стойких блочных шифров.

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 его 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 зашифрования и расшифрования при известном пользователю секретном ключе.

Распространенным способом достижения эффектов рассеивания и перемешивания является использование составного шифра, т. е. 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, причём 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.

Все действия, производимые блочным криптоалгоритмом над данными, основаны на том факте, что преобразуемый блок может быть представлена, в виде целого неотрицательного числа из диапазона, соответствующего его разрядности.

Например, 32-битный блок данных можно интерпретировать как число из диапазона 0...4 294 967 295. Кроме того, блок, разрядность которого представляет собой «степень двойки», можно трактовать как сцепление нескольких независимых неотрицательных чисел из меньшего диапазона (указанный выше 32-битный блок можно также представить в виде сцепления двух независимых 16-битных чисел, из диапазона. 0...65535 или в виде сцепления четырех независимых 8-битных чисел из диапазона 0..55). Над этими числами блочный криптоалгоритм производит по определенной схеме действия.

Последовательность выполняемых над блоком операций составляет отличительные особенности конкретного симметричного блочного криптоалгоритма. Характерным признаком блочных алгоритмов является многократное и косвенное использование материала ключа. Это определяется в первую очередь требованием невозможности обратного дешифрования 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 шли элемент ключа используется многократно. Это позволяет при выполнении условия обратимости функции относительно величины X сделать функцию необратимой относительно ключа К.

2. Алгоритм шифрования DES

Алгоритм шифрования данных DES (Data Encryption Standard) был опубликован в 1977 г. DES представляет собой блочный шифр, он шифрует

данные 64-битовыми блоками. На вход алгоритма подается 64-битовый блок открытого текста, а выходит 64-битовый блок шифртекста. DES является симметричным алгоритмом: для шифрования и расшифрования используются одинаковые алгоритм и ключ (за исключением небольших различий в использовании ключа). Блочный симметричный алгоритм DES остается пока распространенным алгоритмом, используемым в системах защиты коммерческой информации. Алгоритм DES построен в соответствии с методологией сети Фейстеля и состоит из чередующейся последовательности перестановок и подстановок. Алгоритм DES осуществляет шифрование 64-битных блоков данных с помощью 64-битного ключа, в котором значащими являются 56 бит (остальные 8 бит — проверочные биты для контроля на четность).

Процесс шифрования заключается в начальной перестановке битов 64-битного блока, шестнадцати циклах (раундах) шифрования и, наконец, в конечной перестановке битов. Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности.

Основные достоинства алгоритма DES:

• используется только один ключ длиной 56 бит;

• относительная простота алгоритма обеспечивает высокую скорость обработки;

• зашифровав сообщение с помощью одного пакета программ, для расшифровки можно использовать любой другой пакет программ, соответствующий алгоритму DES;

• криптостойкость алгоритма вполне достаточна для обеспечения ИБ большинства коммерческих приложений.

Современная микропроцессорная техника позволяет уже сегодня за достаточно приемлемое время взламывать симметричные блочные шифры с длиной ключа 40 бит. Для такого взламывания используется метод полного перебора — тотального опробования всех возможных значений ключа (метод «грубой силы»). До недавнего времени блочный алгоритм DES, имеющий ключ с эффективной длиной 56 бит, считался относительно безопасным алгоритмом шифрования. Он многократно подвергался тщательному криптоанализу в течение 20 лет, и самым практичным способом его взламывания является метод перебора всех возможных значений ключа. Ключ шифра DES имеет 2^{56} возможных значений. Возникает естественный вопрос: нельзя ли использовать DES в качестве строительного блока для создания другого алгоритма с более длинным ключом?

В принципе, существует много способов комбинирования блочных алгоритмов для получения новых алгоритмов. Одним из таких способов комбинирования является многократное шифрование, т. е. использование блочного алгоритма несколько раз с разными ключами для шифрования одного и того же блока открытого текста.

3. ГОСТ Р 34.12-2015 («Магма»)

ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры" и ГОСТ Р 34.13-2015 "Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров", которые вступили в действие с 1 января 2016 года.

ГОСТ Р 34.12-2015 содержит описание двух блочных шифров с длинами блока 128 и 64 бит. Шифр ГОСТ 28147-89 с зафиксированными блоками нелинейной подстановки включен в новый ГОСТ Р 34.12-2015 в качестве 64-битового шифра под названием "Магма" ("Magma").

Новый стандарт ГОСТ Р 34.12-2015 терминологически и концептуально связан с международными стандартами ИСО/МЭК 10116 "Информационные технологии. Методы обеспечения безопасности. Режимы работы для n-битовых блочных шифров" (ISO/IEC 10116:2006 Information technology -- Security techniques - Modes of operation for an n-bit block cipher) и серии ИСО/МЭК 18033 "Информационные технологии. Методы и средства обеспечения безопасности. Алгоритмы шифрования": ИСО/МЭК 18033-1:2005 "Часть 1. Общие положения" (ISO/IEC 18033-1:2005 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General) и ИСО/МЭК 18033-3:2010 "Часть 3. Блочные шифры" (ISO/IEC 18033-3:2010 (Information technology -- Security techniques -- Encryption algorithms – Part 3: Block ciphers).

В стандарт ГОСТ Р 34.12-2015 включен также новый блочный шифр ("Кузнечик") с размером блока 128 бит. Ожидается, что этот шифр будет устойчив ко всем известным на сегодняшний день атакам на блочные шифры.

Рассмотрим, в качестве примера, старый **ГОСТ 28147— 89 .**

Алгоритм шифрования данных представляет собой 64-битный блочный алгоритм с 256-битным ключом. Данные, подлежащие зашифрованию, разбивают на 64-разрядные блоки. Эти блоки разбиваются на два субблока N1 и N2 по 32 бита. Субблок N1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N2 (сложение выполняется по модулю 2, т. е. применяется логическая операция XOR — исключающее ИЛИ), а затем субблоки меняются местами. Данное преобразование

выполняется определенное число раз (раундов): 16 или 32 в зависимости от режима работы алгоритма. В каждом раунде выполняются две операции.

Первая операция — наложение ключа. Содержимое субблока N1, складывается, по модулю, 2^{32} с 32-битной частью ключа, Кх. Полный ключ шифрования представляется в виде конкатенации 32-битных подключей: $К_0$, $К_1$, $К_2$, $К_3$, $К_4$, $К_5$, $К_6$, $К_7$. В процессе шифрования, используется один из этих подключей — в зависимости от номера раунда и режима работы алгоритма.

Вторая операция табличная замена. После наложения ключа субблок N1 разбивается на 8 частей по 4 бит, значение каждой из которых заменяется, в соответствии с таблицей замены для данной части субблока. Затем выполняется побитный циклический сдвиг субблока влево на 11 бит. И т.д., в соответствии с алгоритмом. Кроме того, имеется несколько режимов шифрования, с которыми вы познакомитесь на 4 курсе.

Данный алгоритм считается очень стойким — в настоящее время для его раскрытия не предложено более эффективных методов, чем упомянутый выше метод «грубой силы». Его высокая стойкость достигается в; первую очередь за счет большой длины ключа —256 бит. При использовании секретной синхропосылки эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты. Кроме того, криптостойкость зависит от количества раундов преобразований, которых по ГОСТ 28147—89 должно быть 32 (полный эффект рассеивания входных данных достигается уже после 8 раундов).

4. Особенности применения алгоритмов симметричного шифрования

Алгоритмы симметричного шифрования используют ключи относительно небольшой длины и могут быстро шифровать большие объемы данных. Алгоритмы симметричного шифрования строятся исходя из предположения, что зашифрованные данные не сможет прочитать никто из тех, кто не обладает ключом для их расшифрования. Если, ключ не был скомпрометирован, то при расшифровании автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, позволяющий расшифровать информацию. Алгоритмы симметричного шифрования применяются для абонентского шифрования данных — т. е. для, шифрования информации, предназначенной для отправки кому-либо, например, через Интернет.

Использование только одного секретного ключа для всех абонентов Сети, конечно, увеличивает риски: 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. Таким образом, неявно подготавливается аутентификация отправителя и получателя, так как только отравитель знает симметричный секретный ключ и может зашифровать этот текст. Только получатель знает симметричный секретный ключ и может расшифровать этот текст.

3. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается в открытой форме по незащищенным каналам связи. Получатель применяет к зашифрованному тексту тот же самый симметричный алгоритм, шифрования/расшифрования 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, т.е. 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, в частности в глобальных сетях, практически невозможно.

Контрольные вопросы

1. Обобщенная схема симметричной криптосистемы.
2. От чего зависит конфиденциальность передачи информации с помощью симметричной криптосистемы?
3. Каким образом обеспечивается целостность данных?
4. Как осуществляется распределения ключей между пользователями.
5. Общая характеристика алгоритма шифрования DES.
6. Общая характеристика ГОСТ Р 34.12-2015 («Магма»).
7. Особенности применения алгоритмов симметричного шифрования.

ТЕМА 13. АСИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

1. **Обобщенная схема асимметричной криптосистемы шифрования**
2. **Функция хэширования**
3. **Электронная подпись**

Литература:

1. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.

1. Обобщенная схема асимметричной криптосистемы шифрования

Асимметричные криптографические системы были разработаны в семидесятых годах 20 века. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифрования используются различные ключи:

• открытый ключ **К**: используется для шифрования информации, вычисляется из секретного ключа **к**;

• секретный ключ **к**, используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа К.

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

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

Обобщенная схема асимметричной криптосистемы оказана на рис. 13.1.

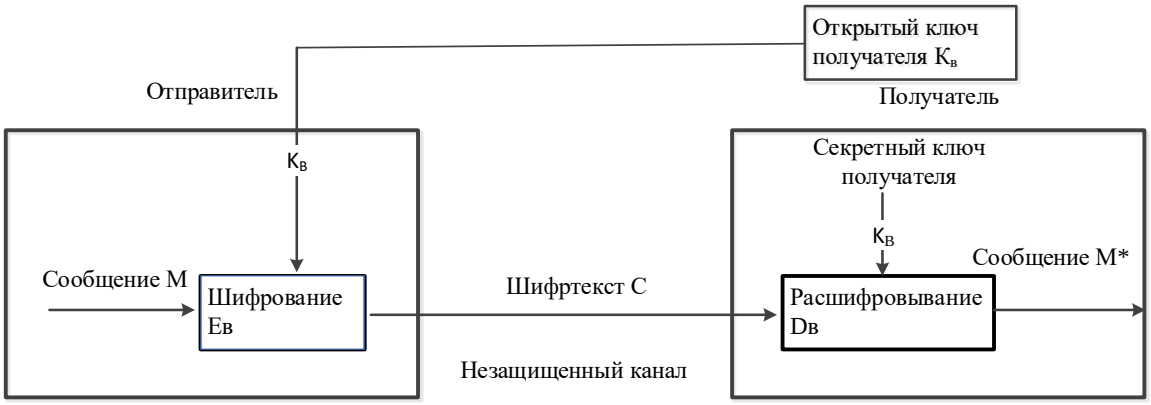

Рис. 13.1 Обобщенная схема асимметричной криптосистемы шифрования

Для шифрования и последующего, расшифровывания передаваемой информации используются, открытый и секретный ключи получателя В.

В качестве ключа зашифровывания используется открытый ключ получателя, а в качестве ключа расшифровывания — его секретный ключ.

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца, он должен быть надежно защищен от несанкционированного доступа, (аналогично ключу шифрования в симметричных алгоритмах). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом:

1. Подготовительный этап:

• абонент **В** генерирует пару ключей: секретный ключ $\boldsymbol{к_b}$ и открытый ключ $\boldsymbol{К_b}$;

• открытый ключ $\boldsymbol{К_b}$ посылается абоненту **А** и остальным, абонентам (или делается доступным, например, на каком-то ресурсе);

2. **Использование** — обмен информацией между абонентами А и В:

• абонент **А** зашифровывает сообщение с помощью открытого ключа $\boldsymbol{К_b}$ абонента **В** и отправляет шифртекст абоненту В;

• абонент **В** расшифровывает сообщение с помощью своего секретного ключа $\boldsymbol{к_b}$. Никто другой (в том числе абонент **А**) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента В. Защита информации в асимметричной криптосистеме основана на секретности ключа $\boldsymbol{к_b}$ получателя сообщения.

Отметим **характерные особенности асимметричных криптосистем:**

- открытый ключ $\mathbf{К_b}$ и криптограмма **С** могут быть отправлены по незащищенным каналам, т. е. противнику известны $\mathbf{К_b}$ и **С**.

- алгоритмы шифрования и расшифрования: $E_в$:M->C; $D_в$:C->M являются открытыми.

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

1. Вычисление пары ключей ($\mathbf{К_b}$ и $\mathbf{к_{b)}}$ получателем **В** (на основе начального условия) должно быть простым.

2. Отправитель А, зная открытый ключ $\mathbf{К_b}$ и сообщение **М**, может легко вычислить криптограмму $C=\mathbf{E_{Кb}}(M)$.

3. Получатель **В**, используя секретный ключ $\mathbf{к_b}$ и криптограмму **С**, может легко восстановить исходное сообщение $\mathbf{M}=D\mathbf{к_b}(\mathbf{C})$.

4. Противник, зная открытый ключ $\mathbf{К_b}$, при попытке вычислить секретный, ключ $\mathbf{к_b}$, (наталкивается на непреодолимую вычислительную проблему.

5. Противник, зная пару ($\mathbf{К_b}$, **С**), при попытке вычислить исходное сообщение М наталкивается на непреодолимую вычислительную проблему.

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

Неформально однонаправленную функцию можно определить следующим образом. Пусть X и Y — некоторые произвольные множества. Функция f: X->Y является однонаправленной, если для всех **xϵX** можно легко вычислить функцию **y =f(x),** где **yϵY.** И в то же время для, большинства **yϵY** достаточно сложно получить значение **xϵX**, такое, что **f(x) = y** (при этом полагает, что существует по крайней мере одно такое значение x).

Основным критерием отнесения функции **f** к классу однонаправленных функций является отсутствие эффективных алгоритмов обратного преобразования Y->X.

В качестве примера однонаправленной функции можно указать целочисленное умножение. Прямая задача - вычисление произведения двух очень больших целых, чисел P и Q т.е. нахождение значения N= P*Q является относительно несложной задачей для компьютера. Обратная задача - факторизация, или разложение на множители большого целого числа, т. е; нахождение делителей P и Q большого целого числа N= P*Q — является практически неразрешимой при достаточно больших значениях N.

По современным оценкам теории чисел, при целом $N=2^{664}$ и P приблизительно равном Q для разложения числа N потребуется около 10^{23} операций, т.е. задача практически неразрешима для современных компьютеров.

Все предлагаемые в настоящее время криптосистемы с открытым ключом основаны на одном из следующих типов необратимых преобразований:

- разложение больших чисел на простые множители;
- вычисление логарифма в конечном поле;
- вычисление корней алгебраических уравнений.

Следует отметить, что пока не удалось доказать невозможность существования эффективного алгоритма вычисления дискретного логарифма за приемлемое время. Исходя из этого модульная экспонента отнесена к однонаправленным функциям условно, что, однако не мешает с успехом применять её на практике.

Вторым важным классом функций, используемых при построении криптосистем с открытым ключом, являются так называемые **однонаправленные функции с секретом.**

Дадим неформальное определение такой функции. Функция f: X->Y относится к классу однонаправленных функций с секретом в том случае, если она является однонаправленной и, кроме того, возможно эффективное вычисление обратной функции, если известен секрет (секретное число, строка или другая информация, ассоциирующаяся с данной функцией).

В качестве примера однонаправленной функции с секретом можно указать используемую в криптосистеме RSA модульную экспоненту с фиксированными модулем и показателем степени. Переменное основание модульной экспоненты используется для представления числового значения сообщения M либо криптограммы C.

Как и в случае симметричных криптографических систем, с помощью асимметричных криптосистем обеспечивайся не только конфиденциальность, но также подлинность и целостность передаваемой информации. Подлинность и целостность любого сообщения обеспечивается формированием электронной подписи (ЭП) этого сообщения и отправкой в зашифрованном виде сообщения вместе с ЭП.

Преимущества асимметричных криптосистем:

- решена сложная проблема распределения ключей между пользователями, так как каждый пользователь может сгенерировать свою пару ключей сам, а открытые ключи пользователей могут свободно публиковаться и распространяться посредством сетевых коммуникаций;

- 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 x 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 расшифровании используются весьма ресурсоемкие операции. По этой же причине реализовать аппаратный шифратор с асимметричном алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;

• необходимо защищать открытые ключи от подмены (от подмены открытых ключей может спасти процедура сертификации открытых ключей).

Алгоритм шифрования RSA

Криптоалгоритм RSA предложили в 1978 г. три автора: Р. Райвест (Bivest), А. Шамир (Shamir), Л. Эйдельман (Adlenian). Алгоритм получил свое название по, первым буквам фамилий его авторов. Алгоритм RSA стал первым алгоритмом с, открытым ключом, который может работать как в режиме шифрования данных, так и в режиме ЭП.

Надежность алгоритма RSA основывается на трудности факторизации больших чисел и вычисления дискретных логарифмов в конечном поле.

В алгоритме RSA открытый ключ Кв, секретный ключ $\mathbf{к_b}$, сообщение М и криптограмма С принадлежат, множеству целых чисел Zn = {0,1,2, ..., N-1},

где N — модуль: N= P x Q.

Здесь Р и Q — случайные большие простые числа. Для обеспечения максимальной безопасности выбирают Р и Q равной длины и хранят в секрете.

Множество Z_N с операциями сложения и умножения по модулю N образует арифметику по модулю N.

Открытый ключ Кв выбирают случайным образом так, чтобы выполнялись условия: $1<K_b<\varphi(N)$), НОД (K_b, $\varphi(N)$) = 1;

$\varphi(N)$ = (P - l) (Q - 1), ... где $\varphi(N)$ — функция Эйлера.

Функция Эйлера <p(N) указывает количество положительных целых чисел в интервале от 1 до N, которые взаимно просты с N.

Второе из указанных выше условий означает, что открытый ключ Кв и функция Эйлера $\varphi(N)$ должны быть взаимно простыми.

Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ $\mathbf{к_b}$.

Открытый, ключ Кв используют для шифрования данных, а секретный ключ $\mathbf{к_b}$ для расшифрования.

Криптоалгоритм RSA всесторонне исследован и признан стойким при достаточной длине ключей. В настоящее время длина ключа 1024 бит считается приемлемым вариантом. Некоторые авторы утверждают, что с ростом мощности процессоров криптоалгоритм RSA потеряет стойкость к атаке полного перебора. Однако увеличение мощности процессоров позволит применить более длинные ключи, что повышает стойкость RSA. Следует отметить, что алгоритм RSA можно применять как для шифрования сообщений, так и для электронной подписи.

2. Функция хэширования

Хэширование применяется для построения ассоциативных массивов, поиска дубликатов в сериях наборов данных, построения достаточно уникальных идентификаторов для наборов данных, контрольного суммирования с целью обнаружения случайных или намеренных ошибок при хранении или передаче, для хранения паролей в системах защиты (в этом случае доступ к области памяти, где находятся пароли, не позволяет восстановить сам пароль), при выработке ЭП (на практике часто подписывается не само сообщение, а его хэш-образ).

Функция хэширования (хэш-функция) представляет собой преобразование, на вход которого подается сообщение переменной длины M, а выходом является строка фиксированной длины h(M). Иначе говоря, хэш-функция h(•) принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение (хэш) H = h(M) фиксированной длины.

Хэш-значение h(M) - это дайджест сообщения M, то есть сжатое двоичное представление основного сообщения M произвольной длины. Хэш-значение h(M) формируется функцией хэширования.

Функция хэширования позволяет сжать подписываемый документ M до 128 бит и более (в частности, 128 или 256 бит), тогда как M может быть размером в мегабайт или более. Следует отметить, что значение хэш-функции

h(M) зависит сложным образом от документа M и не позволяет восстановить сам документ M.

Функция хэширования должна обладать следующими свойствами:

1. Хэш-функция может быть применена к аргументу любого размера.
2. Выходное значение хэш-функции имеет фиксированный размер.
3. Хэш-функцию h(x) достаточно просто вычислить для любого x.

Скорость вычисления хэш-функции должна быть такой, чтобы скорость выработки и проверки ЭП при использовании хэш-функции была значительно больше, чем при использовании самого сообщения.

4. Хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки и т.п.
5. Хэш-функция должна быть однонаправленной, то есть обладать свойством необратимости. Иными словами, задача подбора документа M, который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима.
6. Вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала.

Теоретически возможно, что два различных сообщения могут быть сжаты в одну и ту же свертку (так называемая коллизия, или столкновение). Поэтому для обеспечения стойкости функции хэширования необходимо предусмотреть способ избегать столкновений. Полностью столкновений избежать нельзя, поскольку в общем случае количество возможных сообщений превышает количество возможных выходных значений функции хэширования. Однако вероятность столкновения должна быть низкой.

Свойство 5 эквивалентно тому, что h( ) является односторонней функцией. Свойство 6 гарантирует, что не может быть найдено другое сообщение, дающее ту же свертку. Это предотвращает фальсификацию сообщения.

Таким образом, функция хэширования может использоваться для обнаружения изменений сообщения, то есть она может служить для формирования криптографической контрольной суммы (также называемой кодом обнаружения изменений или кодом аутентификации сообщения). В этом качестве хэш-функция используется для контроля целостности сообщения, при формировании и проверке ЭП.

Хэш-функции широко используются также в целях аутентификации пользователей. В ряде технологий информационной безопасности применяется своеобразный прием шифрования - шифрование с помощью односторонней хэш-функции.

Своеобразие этого шифрования заключается в том, что оно, по существу, является односторонним, то есть не сопровождается обратной процедурой - расшифрованием на приемной стороне. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования на основе хэш-функции.

Известные функции хэширования: Отечественный стандарт ГОСТ Р 34.11-2012; MD (Message Digest) - ряд алгоритмов хэширования, наиболее распространенных в мире. Каждый из них вырабатывает 128-битовый хэш-код. Алгоритм MD2 - самый медленный из них, MD4 - самый быстрый. Алгоритм MD5 является модификацией MD4, при которой пожертвовали скоростью ради увеличения безопасности. Алгоритм MD5 применяется в последних версиях Microsoft Windows для преобразования пароля пользователя в 16-байтовое число и др.

3. Электронная подпись

Электронная подпись (англ. signature) – цифровой код (последовательность символов), присоединяемый к электронному сообщению для идентификации отправителя.

По назначению ЭП соответствует обычной подписи на документе, подтверждающей юридические полномочия документа. ЭП получается методами асимметричной криптографии, основанными на математической функции, комбинирующей открытый текст с последовательностью чисел (ключом). Алгоритм устроен таким образом, что пара «открытый ключ участника А – закрытый ключ участника Б» позволяет зашифровать сообщение, а пара «закрытый ключ А – открытый ключ Б» его дешифровать.

Технология ЭП пересылаемого документа начинается с формирования его дайджеста (digest) – короткой последовательности чисел, восстановить исходный текст по которой нельзя. Любое изменение исходного документа вызовет его несоответствие дайджесту.

К дайджесту добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой электронную подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

ЭП 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, то есть 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 на 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.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

Проблему проверки целостности сообщения и подлинности автора сообщения позволяет эффективно решить методология электронной подписи.

Система ЭП включает две основные процедуры:

- процедуру формирования ЭП;
- процедуру проверки ЭП.

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

Для формирования ЭП отправитель А прежде всего вычисляет значение хэш-функции h(M) подписываемого текста М.

Хэш-функция служит для сжатия исходного подписываемого текста М в дайджест м - относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст М в целом. Далее отправитель А шифрует дайджест м своим секретным ключом. Получаемая при этом пара чисел представляет собой ЭП для данного текста М. Сообщение М вместе с цифровой подписью отправляется в адрес получателя.

Процедура проверки ЭП. Абоненты сети могут проверить ЭП полученного сообщения M с помощью открытого ключа отправителя этого сообщения.

При проверке ЭП абонент B - получатель сообщения M - расшифровывает принятый дайджест открытым ключом отправителя A. Кроме того, получатель сам вычисляет с помощью хэш-функции h(M) дайджест м принятого сообщения M и сравнивает его с расшифрованным. Если эти два дайджеста совпадают, то ЭП является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

Принципиальным моментом в системе ЭП является невозможность подделки ЭП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защитить секретный ключ подписывания от несанкционированного доступа. Секретный ключ ЭП, аналогично ключу симметричного шифрования, рекомендуется хранить на персональном ключевом носителе в защищенном виде.

ЭП представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более ЭП.

Важно отметить, что, с точки зрения конечного пользователя, процесс формирования и проверки ЭП отличается от процесса криптографического закрытия передаваемых данных следующими особенностями.

При формировании ЭП используется закрытый ключ отправителя, тогда как при зашифровании применяется открытый ключ получателя.

При проверке ЭП используется открытый ключ отправителя, а при расшифровывании - закрытый ключ получателя.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, то есть о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети.

Контрольные вопросы

1. Обобщенная схема асимметричной криптосистемы шифрования.
2. Процесс передачи зашифрованной информации в асимметричной криптосистеме.
3. Назвать характерные особенности асимметричных криптосистем.

4. Требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы.
5. Привести пример однонаправленной функции.
6. Преимущества и недостатки асимметричных криптосистем.
7. Функция хэширования и её свойства.
8. Что такое дайджест сообщения?
9. Электронная подпись.
10. От каких видов злоумышленных действий позволяет защитить использование ЭП?
11. Процедуры формирования и проверки ЭП.

ТЕМА 14. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

1. Основы идентификации и аутентификации

2. Классификация протоколов аутентификации

Литература:

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. -392с.

1. Основы идентификации и аутентификации

Одной из важных задач обеспечения защиты от НСД является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны.

С каждым зарегистрированным в ИС субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов. 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 ИС, пользователь должен пройти процесс первичного взаимодействия с ИС, который включает идентификацию и аутентификацию.

Идентификация - процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает ИС по ее запросу свой идентификатор, и система проверяет в своей БД его наличие.

Аутентификация - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем,

кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль).

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. Процесс идентификации и аутентификации показан на рис. 14.1.

Авторизация - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы.

Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены.

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

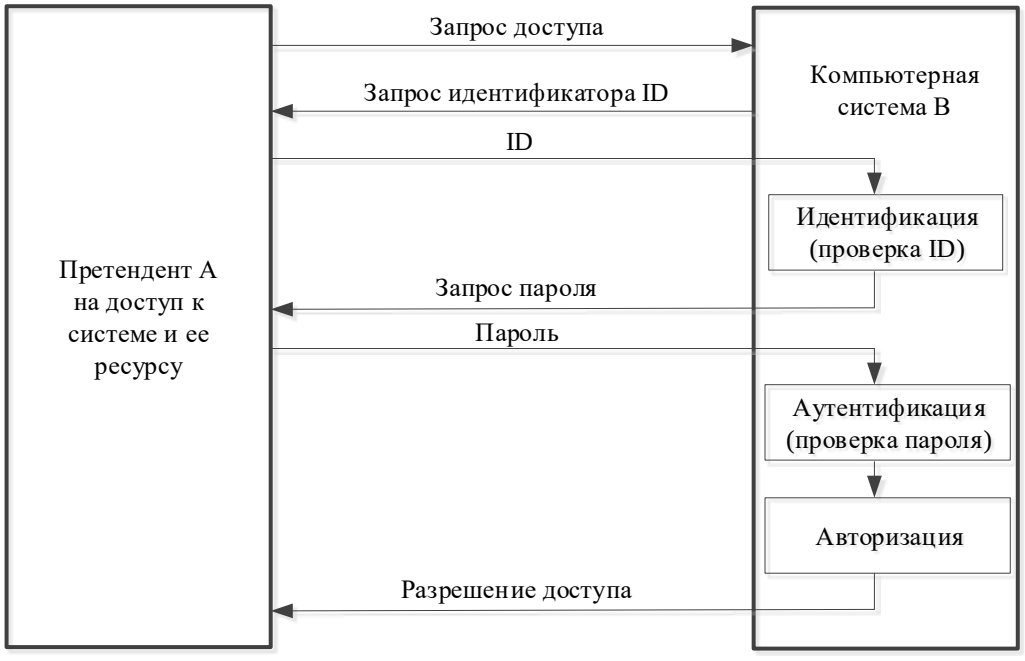

Рис. 14.1 Процесс идентификации и аутентификации

Администрирование — это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Записи в системном журнале, аудиторские проверки и администрирование ПО - все это может быть ис-

пользовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

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

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

2. На основе обладания чем-либо. Обычно это магнитные карты, смарт-карты, сертификаты и устройства touch memory.

3. 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.

Пароль — это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Персональный идентификационный код PIN является испытанным способом аутентификации держателя пластиковой карты и смарт- карты. Секретное значение PIN-кода должно быть известно только держателю карты.

Динамический (одноразовый) пароль - это пароль, который после одноразового применения никогда больше не используется. На практике обычно используется регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

При сравнении и выборе протоколов аутентификации необходимо учитывать следующие характеристики:

1. Наличие взаимной аутентификации. Это свойство отражает необходимость обоюдной аутентификации между сторонами аутентификационного обмена.

2. Вычислительная эффективность. Количество операций, необходимых для выполнения протокола.

3. Коммуникационная эффективность. Это свойство отражает количество сообщений и их длину, необходимую для аутентификации.

4. Наличие третьей стороны. Примером третьей стороны может служить доверенный сервер распределения симметричных ключей или сервер, реализующий дерево сертификатов для распределения открытых ключей.

5. Гарантии безопасности. Примером может служить применение шифрования и ЭП.

2. Классификация протоколов аутентификации

Протоколы (процессы, алгоритмы) аутентификации обычно классифицируют по уровню обеспечиваемой безопасности. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы:

а) Аутентификация, использующая пароли и PIN-коды;

б) Строгая аутентификация на основе использования криптографических методов и средств;

в) Биометрическая аутентификация пользователей.

С точки зрения безопасности, каждый из перечисленных типов способствует решению своих специфических задач, поэтому процессы и протоколы аутентификации активно используются на практике.

Классификация протоколов аутентификации представлена на Рис. 14.2.

Рис. 14. 2 Классификация протоколов аутентификации

Методы аутентификации, использующие пароли и PIN-коды. Одной из распространенных схем аутентификации является простая аутентификация, которая основана на применении традиционных многоразовых и динамических (одноразовых) паролей. Аутентификация на основе паролей и PIN-кодов является простым и наглядным примером использования разделяемой информации. Пока в большинстве защищенных ИС доступ клиента к серверу разрешается по паролю. Однако все чаще применяются более эффективные средства аутентификации, например, программные и аппаратные системы аутентификации на основе одноразовых паролей, смарт- карт, PIN-кодов и цифровых сертификатов.

Процедуру простой аутентификации пользователей в сети можно представить следующим образом. При попытке входа в сеть пользователь набирает на клавиатуре ПЭВМ свой идентификатор и пароль. Эти данные поступают для обработки на сервер аутентификации. В базе данных сервера по идентификатору пользователя находится соответствующая запись, из нее извлекается пароль и сравнивается с тем паролем, который ввел пользователь. Если они совпали, то аутентификация прошла успешно, пользователь получает легальный статус, а также права и ресурсы сети, которые определены для его статуса системой авторизации.

Передача идентификатора и пароля от пользователя к системе может проводиться в открытом и зашифрованном виде.

Схема простой аутентификации с использованием пароля показана на Рис. 14.3.

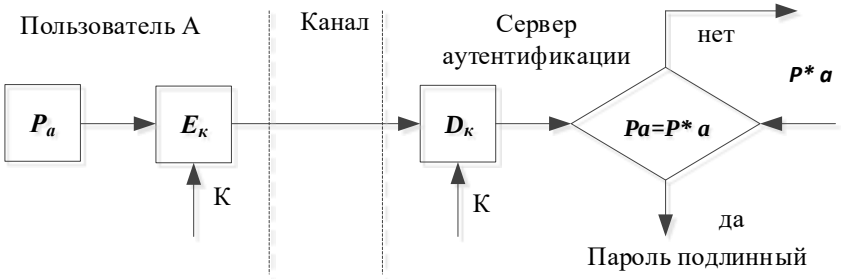

Рис. 14.3 Схема простой аутентификации с использованием пароля

Очевидно, что вариант аутентификации с передачей пароля пользователя в незашифрованном виде не гарантирует даже минимального уровня безопасности. Чтобы защитить пароль, его нужно зашифровать перед посылкой по незащищенному каналу. Для этого в схему включены средства шифрования Ек и дешифрования D_K, управляемые секретным ключом К. Проверка подлинности пользователя основана на сравнении присланного пользователем пароля Ра и исходного значения Ра*, хранящегося на сервере аутенти-

фикации. Если значения Ра и Ра* совпадают, то пароль Ра считается подлинным, а пользователь А — законным.

Наиболее распространенным методом аутентификации держателя пластиковой карты и смарт-карты является ввод секретного числа, которое обычно называют PIN-кодом. Защита PIN-кода карты является критичной для безопасности всей системы.

Строгая аутентификация на основе использования криптографических методов и средств. Идея строгой аутентификации, реализуемая в криптографических протоколах, заключается в следующем. Проверяемая (доказывающая сторона) доказывает свою подлинность проверяющей стороне, демонстрируя знание некоторого секрета.

Например, этот секрет может быть предварительно распределен безопасным способом между сторонами обмена. Доказательство знания секрета осуществляется с помощью последовательности запросов и ответов с использованием криптографических методов и средств.

Существенным является тот факт, что доказывающая сторона демонстрирует только знание секрета, но сам секрет в ходе аутентификационного обмена не раскрывается. Это обеспечивается посредством ответов доказывающей стороны на различные запросы проверяющей стороны. При этом результирующий запрос зависит только от пользовательского секрета и начального запроса, который обычно представляет произвольно выбранное в начале протокола большое число.

В большинстве случаев строгая аутентификация заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. Иначе говоря, пользователь имеет возможность определить, владеет ли его партнер по связи надлежащим секретным ключом и может ли он использовать этот ключ для подтверждения того, что он действительно является подлинным партнером и по информационному обмену.

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

а) односторонняя аутентификация;

б) двусторонняя аутентификация;

в) 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 стороны, которой были предназначены аутентификационные данные.

Трехсторонняя аутентификация содержит дополнительную передачу данных от доказывающей стороны проверяющей. Этот подход позволяет отказаться от использования меток времени при проведении аутентификации.

Биометрическая аутентификация. Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т.п.). Привычные системы аутентификации не всегда удовлетворяют современным требованиям в области информационной безопасности, особенно если речь идет об ответственных приложениях (онлайновые финансовые приложения, доступ к удаленным базам данных и т.п.).

В последнее время все большее распространение получает биометрическая аутентификация пользователя, позволяющая уверенно аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

В качестве биометрических признаков, которые активно используются при аутентификации потенциального пользователя, можно выделить следующие: отпечатки пальцев; геометрическая форма кисти руки; форма и размеры лица; особенности голоса; узор радужной оболочки и сетчатки глаз; «клавиатурный почерк»; расположение зубов (стоматологическая матрица ротовой полости человека) и др.

Аутентификация по отпечаткам пальцев. Большинство систем используют отпечаток одного пальца, который пользователь предоставляет системе. Дактилоскопическая система работает следующим образом. Сначала производится регистрация пользователя. Как правило, производится несколько вариантов сканирования в разных положениях пальца на сканере. Понятно, что образцы будут немного отличаться и требуется сформировать некоторый обобщенный образец, «паспорт». Результаты сохраняются в базе данных аутентификации. При аутентификации производится сравнение от-

сканированного отпечатка пальца с «паспортами», хранящимися в базе данных.

Аутентификация по лицу и голосу. Данные системы наиболее доступны из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса применяются при удаленной идентификации субъекта доступа в телекоммуникационных сетях.

В технологии сканирования черт лица используются особенности глаз, носа и губ. Далее проводятся некоторые математические алгоритмы для идентификации пользователя. Большая часть алгоритмов распознавания черт лица чувствительна к колебаниям освещения помещения. Изменения в положении в 15% между запрашиваемым изображением и изображением, которое находится в базе данных, напрямую сказываются на эффективности.

Системы аутентификации по голосу при записи образца и в процессе последующей идентификации опираются на такие уникальные для каждого человека особенности голоса, как высота, модуляция и частота звука. Эти показатели определяются характеристиками голосового тракта и уникальны для каждого человека. Однако голос можно записать на пленку или другие носители. Поэтому для предотвращения подлога голоса в алгоритм аутентификации включается операция запроса отклика. Эта функция предлагает пользователю при входе в систему ответить на предварительно подготовленный и регулярно меняющийся запрос, например такой: «Повторите числа 0, 1,5».

Системы аутентификации по голосу не обеспечивают достаточной точности, и их следует сочетать с другими биометрическими методами.

Системы аутентификации по узору радужной оболочки и сетчатки глаз можно разделить на два класса:

а) Использующие рисунок радужной оболочки глаза;

б) Использующие рисунок кровеносных сосудов сетчатки глаза.

Сетчатка человеческого глаза представляет собой уникальный объект для аутентификации. Рисунок кровеносных сосудов глазного дна отличается даже у близнецов. Поскольку вероятность повторения параметров радужной оболочки и сетчатки глаза имеет порядок 10^{78}, такие системы являются наиболее надежными среди всех биометрических систем.

Контрольные вопросы

1. Пояснить сущность процедур идентификации и аутентификации.
2. Процесс идентификации и аутентификации.

3. Что такое авторизация и администрирование.
4. Категории процесса аутентификации в зависимости от предъявляемых субъектом сущностей.
5. Типы процессов аутентификации.
6. Основные характеристики протоколов аутентификации.
7. Классификация основных протоколов аутентификации.

ТЕМА 15. РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ

1. **Ограничение доступа**
2. **Контроль доступа к аппаратуре**
3. **Разграничение и контроль доступа к информации ИС**
4. **Разграничение привилегий на доступ**

Литература:

1. Сычев Ю.Н. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007. – 300 с.

1. ОГРАНИЧЕНИЕ ДОСТУПА

Ограничение доступа заключается в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям. Ограничение доступа к комплексам средств автоматизации (КСА) обработки информации заключается:

- в выделении специальной территории для размещения КСА;
- в сооружении по периметру зоны ограждений с охранной сигнализацией;
- в сооружении специальных зданий или других сооружений;
- в выделении специальных помещений в здании;
- создание контрольно-пропускного режима на территорию (здание, помещение).

Цель ограничения доступа — исключить случайный и преднамеренный доступ посторонних лиц на территорию размещения КСА и непосредственно к аппаратуре. Для этого создается защитный контур, замыкаемый двумя видами преград: физической и контрольно-пропускной. Такие преграды часто называют системой охранной сигнализации и системой контроля доступа.

Традиционные средства контроля доступа в защищаемую зону: изготовление и выдача допущенным лицам специальных пропусков с размещенной на них фотографией личности владельца и сведений о нем. Данные пропуска могут

храниться у владельца или непосредственно в пропускной кабине охраны. В последнем случае допущенное лицо называет фамилию и свой номер либо набирает его на специальной панели кабины при проходе через турникет; пропускное удостоверение выпадает из гнезда и поступает в руки работника охраны, который визуально сверяет личность владельца с изображением на фотографии, названную фамилию с фамилией на пропуске. Эффективность защиты данной системы выше первой. При этом исключаются: потеря пропуска, его перехват и подделка. Кроме того, есть резерв в повышении эффективности защиты с помощью увеличения количества проверяемых параметров. Однако основная нагрузка по контролю при этом ложится на человека, а он, как известно, может ошибаться.

Физическая преграда защитного контура, размещаемая по периметру охраняемой зоны, снабжается охранной сигнализацией.

Следить за состоянием датчиков может автоматическая система, расположенная в центре управления, или сотрудник охраны, который находится на объекте и при световом или звуковом сигнале принимает соответствующие меры. В первом случае местные охранные устройства подключаются к центру через телефонные линии, а специализированное цифровое устройство осуществляет периодический опрос состояния датчиков, автоматически набирая номер приемоответчика, расположенного на охраняемом объекте. При поступлении в центр сигнала тревоги автоматическая система включает сигнал оповещения.

Датчики сигналов устанавливаются на ограждениях, внутри помещений, непосредственно на сейфах и т. д. При разработке комплексной системы охраны конкретного объекта учитывают его специфику: внутреннюю планировку здания, окон, входной двери, размещение наиболее важных технических средств.

Все эти факторы влияют на выбор типа датчиков, их расположение и определяют ряд других особенностей данной системы. По принципу действия системы тревожной сигнализации можно классифицировать следующим образом:

• традиционные (обычные), основанные на использовании цепей сигнализации и индикации в комплексе с различными контактами (датчиками);

• ультразвуковые; прерывания луча; телевизионные; радиолокационные; микроволновые и прочие.

2. КОНТРОЛЬ ДОСТУПА К АППАРАТУРЕ

В целях контроля доступа к внутреннему монтажу, линиям связи и технологическим органам управления используется аппаратура контроля вскрытия аппаратуры. Это означает, что внутренний монтаж аппаратуры и технологические органы и пульты управления закрыты крышками, дверцами или кожухами, на

которые установлены датчики. Датчики срабатывают при вскрытии аппаратуры и выдают электрические сигналы, которые по цепям сбора поступают на централизованное устройство контроля. Установка такой системы имеет смысл при наиболее полном перекрытии всех технологических подходов к аппаратуре, включая средства загрузки программного обеспечения, пульт управления ЭВМ и внешние кабельные соединители технических средств, входящих в состав вычислительной системы. В идеальном случае для систем с повышенными требованиями к эффективности защиты информации целесообразно закрывать крышками под механический замок с датчиком или ставить под контроль включение также штатных средств входа в систему — терминалов пользователей.

Контроль вскрытия аппаратуры необходим не только в интересах защиты информации от НСД, но и для соблюдения технологической дисциплины в целях обеспечения нормального функционирования вычислительной системы, потому что часто при эксплуатации параллельно решению основных задач производится ремонт или профилактика аппаратуры, и может оказаться, что случайно забыли подключить кабель или с пульта ЭВМ изменили программу обработки информации. **Основная цель систем контроля вскрытия аппаратуры** — перекрытие на период эксплуатации всех нештатных и технологических подходов к аппаратуре. Если последние потребуются в процессе эксплуатации системы, выводимая на ремонт или профилактику аппаратура перед началом работ отключается от рабочего контура обмена информацией, подлежащей защите, и вводится в рабочий контур под наблюдением и контролем лиц, ответственных за безопасность информации.

Доступ к штатным входам в систему — терминалам контролируется с помощью контроля выдачи механических ключей пользователям, а доступ к информации — с помощью системы опознания и разграничения доступа, включающей применение кодов паролей, соответствующие функциональные задачи программного обеспечения и специального терминала службы безопасности информации

Указанный терминал и устройство контроля вскрытия аппаратуры входят в состав рабочего места службы безопасности информации, с которого осуществляются централизованный контроль доступа к аппаратуре и информации и управление ее защитой на данной вычислительной системе.

3. РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ ИС

Разграничение доступа в ИС заключается в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

Цель разграничения доступа: сокращение количества должностных лиц, не имеющих к ней отношения при выполнении своих функций, т. е. защита информации от нарушителя среди допущенного к ней персонала.

При этом деление информации может производиться по степени важности, конфиденциальности, по функциональному назначению, по документам и т. д.

Принимая во внимание, что доступ осуществляется с различных технических средств, начинать разграничение можно путем разграничения доступа к техническим средствам, разместив их в отдельных помещениях. Все подготовительные функции технического обслуживания аппаратуры, ее ремонта, профилактики, перезагрузки ПО и т. д. должны быть технически и организационно отделены от основных задач системы. КСА и организация его обслуживания должны быть построены следующим образом:

- техническое обслуживание КСА в процессе эксплуатации должно выполняться отдельным персоналом без доступа к информации, подлежащей защите;
- перезагрузка ПО и всякие его изменения должны производиться специально выделенным для этой цели проверенным специалистом;
- функции обеспечения безопасности информации должны выполняться специальным подразделением в организации — владельцем КСА или ИС;
- организация доступа пользователей к памяти КСА обеспечивала возможность разграничения доступа к информации, хранящейся в ней, с достаточной степенью детализации и в соответствии с заданными уровнями полномочий пользователей;
- регистрация и документирование технологической и оперативной информации должны быть разделены.

Разграничение доступа пользователей — потребителей КСА может осуществляться также по следующим параметрам:

- по виду, характеру, назначению, степени важности и секретности информации;
- по способам ее обработки: считать, записать, внести изменения и др.;
- по условному номеру терминала;
- по времени обработки и др.

Принципиальная возможность разграничения по указанным параметрам должна быть обеспечена проектом КСА. А конкретное разграничение при экс-

плуатации КСА устанавливается потребителем и вводится в систему его подразделением, отвечающим за безопасность информации.

В указанных целях при проектировании базового вычислительного комплекса для построения КСА производятся:

- разработка операционной системы с возможностью реализации разграничения доступа к информации, хранящейся в памяти ЭВМ;
- изоляция областей доступа;
- разделение базы данных на группы;
- процедуры контроля перечисленных функций.

При проектировании КСА и ИС на их базе производятся:

- разработка и реализация функциональных задач по разграничению и контролю доступа к аппаратуре и информации как в рамках КСА, так и ИС в целом;
- разработка аппаратных средств идентификации и аутентификации пользователя;
- разработка программных средств контроля и управления разграничением доступа;
- разработка отдельной эксплуатационной документации на средства идентификации, аутентификации, разграничения и контроля доступа.

В качестве идентификаторов личности для реализации разграничения широко распространено применение кодов паролей, которые хранятся в памяти пользователя и КСА. В помощь пользователю в системах с повышенными требованиями большие значения кодов паролей записываются на специальные носители — электронные ключи или карточки.

4. РАЗДЕЛЕНИЕ ПРИВИЛЕГИЙ НА ДОСТУП

Разделение привилегий на доступ к информации заключается в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Цель указанного метода — существенно затруднить преднамеренный перехват информации нарушителем. Примером такого доступа может быть сейф с несколькими ключами, замок которого открывается только при наличии всех ключей. Аналогично в ИС может быть предусмотрен механизм разделения привилегий при доступе к особо важным данным с помощью кодов паролей.

Данный метод несколько усложняет процедуру, но обладает высокой эффективностью защиты. На его принципах можно организовать доступ к данным с санкции вышестоящего лица по запросу или без него.

Сочетание двойного криптографического преобразования информации и метода разделения привилегий позволяет обеспечить высокоэффективную защиту информации от преднамеренного НСД.

Кроме того, при наличии дефицита в средствах, а также в целях постоянного контроля доступа к ценной информации со стороны администрации потребителя ИС в некоторых случаях возможен вариант использования права на доступ к информации нижестоящего руководителя только при наличии его идентификатора и идентификатора его заместителя или представителя службы безопасности информации.

При этом информация выдается на дисплей только руководителя, а на дисплей подчиненного — только информация о факте ее вызова.

Контрольные вопросы

1. В чём заключается ограничение доступа к комплексам средств автоматизации?
2. Цели ограничения доступа и способы их реализации.
3. Контроль доступа к аппаратуре.
4. Основные принципы контроля доступа к аппаратуре.
5. Разделение привилегий на доступ.

ТЕМА 16. ТЕХНОЛОГИИ МЕЖСЕТЕВЫХ ЭКРАНОВ

1. Основные понятия технологии межсетевых экранов

2. Функции межсетевых экранов

3. Ориентация МЭ на уровни эталонной модели

Литература:

1. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М. ДМК Пресс, 2010. - 544 с. ил.

2. Домарев В.В. Безопасность информационных технологий. Системный подход: К.: ООО «ТИД «ДС», 2004. – 992 с.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. —944 с.

1. Основные понятия технологии межсетевых экранов

Межсетевой экран (МЭ) - это специализированный комплекс межсетевой защиты, называемый также брандмауэром или файрволом. (Firewall - в переводе – стена, сделанная из негорючих материалов, препятствующая распространению пожара, брандмауэр – перегородка в поезде, отделяющая область топки паровоза от пассажирского отделения).

МЭ позволяет разделить общую сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов с данны-

ми через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной сетью предприятия и глобальной сетью Интернет. Обычно МЭ защищают внутреннюю сеть предприятия от вторжений из глобальной сети Интернет, хотя они могут использоваться и для защиты от нападений из корпоративной интрасети, к которой подключена локальная сеть предприятия.

Технология МЭ стала одной из самых первых технологий защиты корпоративных сетей от внешних угроз. Для большинства организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети.

МЭ может быть маршрутизатором, персональным компьютером, хостом или группой хостов, созданной специально для защиты сети или подсети от неправильного использования протоколов и служб хостами, находящимися вне этой подсети.

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 16.1). При этом все взаимодействия между этими сетями должны осуществляться только через МЭ. Организационно МЭ входит в состав защищаемой сети.

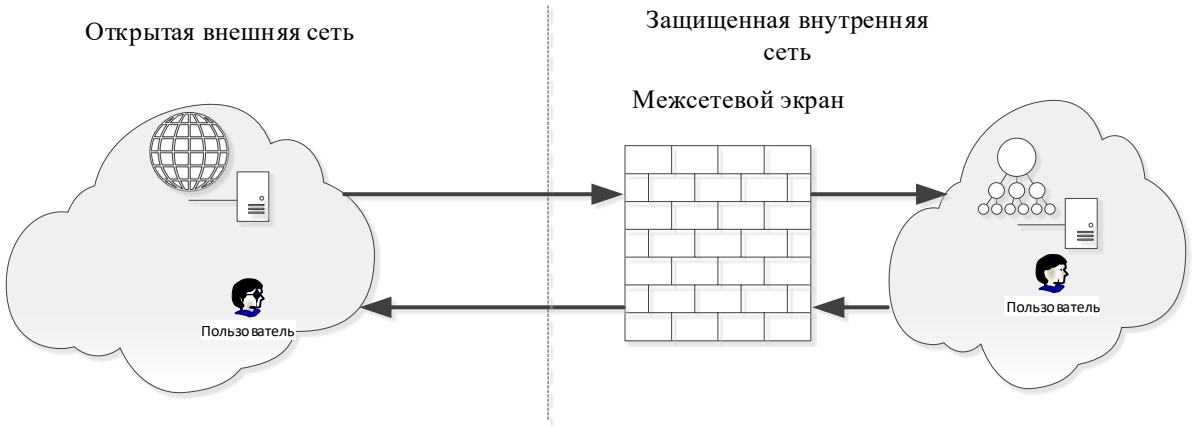

Рис. 16.1. Схема подключения межсетевого экрана МЭ

МЭ можно классифицировать по следующим основным признакам:

А). *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).

Б). *По используемой технологии.*

- контроль состояния протокола (stateful inspection);
- на основе модулей посредников (proxy).

В*). По исполнению:*

- аппаратно-программный;
- программный.

Г). *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.

МЭ первого поколения, известные также как маршрутизаторы с фильтрацией пакетов, проверяют адреса отправителя и получателя в проходящих пакетах TCP/IP. Пакеты проверяются по списку доступа на наличие "дружественного адреса", и, если он обнаружен, пакетам разрешается вход в сеть (в противном случае — запрещается). Эти МЭ служат больше средством устрашения, чем оплотом безопасности. При их использовании хакеры могут легко имитировать дружественные адреса — этот процесс называется "спуфингом" (spoofing — обман, подлог) — и получить доступ к intranet.

Следующее поколение МЭ - "уполномоченные серверы" (proxy servers) было создано именно для решения проблемы с имитацией IP-адресов. Эти МЭ могут фильтровать пакеты на уровне приложений, что особенно важно для безопасности в intranet.

Как уполномоченные представители Web-сервера, такие брандмауэры могут связываться с запросом доступа системы. Кроме того, они проверяют законность пользовательского имени, пароля и передаваемых данных, а не только заголовка пакета. Например, уполномоченное приложение HTML "знает", как должны выглядеть 'правильные" данные HTML, и способно определить, можно ли разрешить доступ.

МЭ третьего поколения, используют для фильтрации специальные многоуровневые методы анализа состояния пакетов SMLT (Stateful Multi-Layer Technique). В отличие от брандмауэров уровня приложений, брандмауэры на основе SMLT используют ПО для анализа данных, способное создавать мгновенную копию целого пакета. Эти брандмауэры быстро сравнивают проходящие пакеты с известным состоянием (state) дружественных пакетов,

позволяя значительно сократить время обработки по сравнению с медленными брандмауэрами уровня приложений.

2. Функции межсетевых экранов

2.1. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований. Фильтрация осуществляется на основе набора предварительно загруженных в МЭ правил, соответствующих принятой политике безопасности. Поэтому МЭ удобно представлять как последовательность фильтров, обрабатывающих информационный поток (Рис 16.2).

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 пропускать данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например, преобразование данных, регистрацию событий и др.

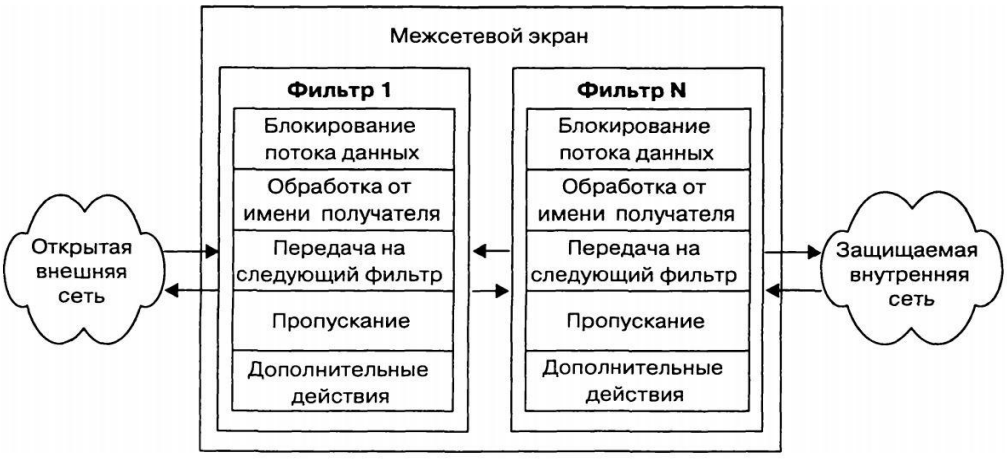

Рис. 16.2 Структура межсетевого экрана

Соответственно, правила фильтрации определяют перечень условий, по

которым осуществляется:

- разрешение или запрещение дальнейшей передачи данных;
- выполнение дополнительных защитных функций.

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.

2.2 Выполнение функций посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. 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 через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует иметь в виду, что МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетями. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

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 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.

МЭ с посредниками позволяют также организовывать защищенные виртуальные сети VPN (Virtual Private Network), например, безопасно объединить несколько локальных сетей, подключенных к Интернету, в одну виртуальную сеть.

2.3 Дополнительные возможности МЭ

Помимо выполнения фильтрации трафика и функций посредничества некоторые МЭ позволяют реализовать ряд других, не менее важных функций, без которых обеспечение защиты периметра внутренней сети было бы неполным.

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

Идентификация и аутентификация пользователей являются важными компонентами концепции МЭ. Авторизация пользователя обычно рассматривается в контексте аутентификации - как только пользователь аутентифицирован, для него определяются разрешенные ему сервисы.

Так как МЭ могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств уси-

ленной аутентификации. Хотя средства усиленной аутентификации могут использоваться на каждом хосте, более практично их размещение на МЭ. При отсутствии МЭ, использующего меры усиленной аутентификации, не аутентифицированный трафик таких приложений, как Telnet или FTP, может напрямую проходить к внутренним системам в сети.

Ряд МЭ поддерживают Kerberos - один из распространенных методов аутентификации. Как правило, большинство коммерческих МЭ поддерживает несколько различных схем аутентификации, позволяя администратору сетевой безопасности сделать выбор наиболее приемлемой схемы для своих условий.

- **Трансляция сетевых адресов.** Для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, МЭ выполняют очень важную функцию - трансляцию внутренних сетевых адресов (network address translation).

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.

- **Администрирование, регистрация событий и генерация отчетов.** Простота и удобство администрирования является 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 МЭ 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.

При правильно настроенной системе фиксации сигналов о подозрительных событиях (alarm) МЭ может дать детальную информацию о том, были ли МЭ или сеть атакованы либо зондированы. Собирать статистику использования сети и доказательства ее зондирования важно по ряду причин.

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, то есть выдача предупредительных сигналов. Любой МЭ, который не способен посылать предупредительные сигналы при обнаружении нападения, нельзя считать эффективным средством межсетевой защиты.

3. Ориентация МЭ на уровни эталонной модели

3.1 Эталонная сетевая модель OSI

OSI расшифровывается как Open System Interconnection. На русском языке это звучит следующим образом: Сетевая модель взаимодействия открытых систем (эталонная модель). Эту модель можно смело назвать стандартом. Именно этой модели придерживаются производители сетевых устройств, когда разрабатывают новые продукты.

Сетевая модель OSI состоит из 7 уровней, причем принято начинать отсчёт с нижнего. Перечислим их:

7. Прикладной уровень (application layer).
6. Представительский уровень или уровень представления (presentation layer).
5. Сеансовый уровень (session layer).
4. Транспортный уровень (transport layer).
3. Сетевой уровень (network layer).
2. Канальный уровень (data link layer).
1. Физический уровень (physical layer).

Как говорилось выше, сетевая модель – это модель взаимодействия сетевых протоколов (стандартов), вот на каждом уровне и присутствуют свои протоколы.

Прикладной уровень

Прикладной уровень или уровень приложений (application layer) – это самый верхний уровень модели. Он осуществляет связь пользовательских приложений с сетью. Эти приложения нам всем знакомы: просмотр веб-страниц (HTTP), передача и приём почты (SMTP, POP3), приём и получение файлов (FTP, TFTP), удаленный доступ (Telnet) и т.д.

Представительский уровень

Представительский уровень или уровень представления данных (presentation layer) – он преобразует данные в соответствующий формат. На примере понять проще: те картинки (все изображения) которые вы видите на экране, передаются при пересылке файла в виде маленьких порций единиц и ноликов (битов). Так вот, когда Вы отправляете своему другу фотографию по электронной почте, протокол Прикладного уровня SMTP отправляет фотографию на нижний уровень, т.е. на уровень Представления. Где Ваше фото преобразуется в удобный вид данных для более низких уровней, например в биты (единицы и нолики).

Именно таким же образом, когда Ваш друг начнет получать Ваше фото, ему оно будет поступать в виде все тех же единиц и нулей, и именно уровень Представления преобразует биты в полноценное фото, например JPEG.

Вот так и работает этот уровень с протоколами (стандартами) изображений (JPEG, GIF, PNG, TIFF), кодировок (ASCII, EBDIC), музыки и видео (MPEG) и т.д.

Сеансовый уровень

Сеансовый уровень или уровень сессий (session layer) – как видно из названия, он организует сеанс связи между компьютерами. Хорошим примером будут служить аудио и видеоконференции, на этом уровне устанавливается, каким кодеком будет кодироваться сигнал, причем этот кодек должен присутствовать на обеих машинах. Еще примером может служить протокол SMPP (Short message peer-to-peer protocol), с помощью него отправляются хорошо известные нам СМС-ки и USSD запросы. И последний пример: PAP (Password Authentication Protocol) – это старенький протокол для отправки имени пользователя и пароля на сервер без шифрования.

Транспортный уровень

Транспортный уровень (transport layer) – этот уровень обеспечивает надёжность передачи данных от отправителя к получателю. На самом деле всё очень просто, например вы общаетесь с помощью веб-камеры со своим другом или преподавателем. Нужна ли здесь надежная доставка каждого бита переданного изображения? Конечно нет, если потеряется несколько битов из потокового видео Вы даже этого не заметите, даже картинка не изменится (м.б. изменится цвет одного пикселя из 900000 пикселей, который промелькнет со скоростью 24 кадра в секунду).

А теперь приведем такой пример: Вам друг пересылает (например, через почту) в архиве важную информацию или программу. Вы скачиваете себе на компьютер этот архив. Вот здесь надёжность нужна 100%, т.к. если пару бит при закачке архива потеряются – Вы не сможете затем его разархивировать, т.е. извлечь необходимые данные. Или представьте себе отправку пароля на сервер, и в пути один бит потерялся – пароль уже потеряет свой вид и значение изменится.

Таким образом, когда мы смотрим видеоролики в интернете, иногда мы видим некоторые артефакты, задержки, шумы и т.п. А когда мы читаем текст с веб-страницы – потеря (или искажение) букв не допустима, и когда скачиваем программы – тоже все проходит без ошибок.

На этом уровне я выделю два протокола: UDP и TCP. UDP протокол (User Datagram Protocol) передает данные без установления соединения, не подтверждает доставку данных и не делает повторы. TCP протокол (Transmission Control Protocol), который перед передачей устанавливает соединение, подтверждает доставку данных, при необходимости делает повтор, гарантирует целостность и правильную последовательность загружаемых данных.

Следовательно, для музыки, видео, видеоконференций и звонков используем UDP (передаем данные без проверки и без задержек), а для текста, программ, паролей, архивов и т.п. – TCP (передача данных с подтверждением о получении, затрачивается больше времени).

Сетевой уровень

Сетевой уровень (network layer) – этот уровень определяет путь, по которому данные будут переданы. И, между прочим, это третий уровень Сетевой модели OSI, а ведь существуют такие устройства, которые как раз и называют **устройствами третьего уровня – маршрутизаторы**.

Все мы слышали об IP-адресе, вот это и осуществляет протокол IP (Internet Protocol). IP-адрес – это логический адрес в сети.

На этом уровне достаточно много протоколов и все эти протоколы мы разберем более подробно позже, в отдельных статьях и на примерах. Сейчас же только перечислим несколько популярных.

Как об IP-адресе все слышали и о команде ping – это работает протокол ICMP. Те самые маршрутизаторы (с которыми мы и будет работать в дальнейшем) используют протоколы этого уровня для маршрутизации пакетов (RIP, EIGRP, OSPF).

Канальный уровень

Канальный уровень (data link layer) – он нам нужен для взаимодействия сетей на физическом уровне. Наверное, все слышали о MAC-адресе, вот он является физическим адресом. **Устройства канального уровня – коммутаторы, концентраторы** и т.п.

IEEE (Institute of Electrical and Electronics Engineers - Институт инженеров по электротехнике и электронике) определяет канальный уровень двумя подуровнями: LLC и MAC.

LLC – управление логическим каналом (Logical Link Control), создан для взаимодействия с верхним уровнем.

MAC – управление доступом к передающей среде (Media Access Control), создан для взаимодействия с нижним уровнем.

Пример: в Вашем компьютере (ноутбуке, коммуникаторе) имеется сетевая карта (или какой-то другой адаптер), так вот для взаимодействия с ней (с картой) существует драйвер. Драйвер – это некоторая **программа** - верхний подуровень канального уровня, через которую как раз и можно связаться с нижними уровнями, а точнее с микропроцессором (**железо**) – нижний подуровень канального уровня.

Типичных представителей на этом уровне много. PPP (Point-to-Point) – это протокол для связи двух компьютеров напрямую. FDDI (Fiber Distributed Data Interface) – стандарт передаёт данные на расстояние до 200 километров. CDP (Cisco Discovery Protocol) – это проприетарный (собственный) протокол принадлежащий компании Cisco Systems, с помощью него можно обнаружить соседние устройства и получить информацию об этих устройствах.

Физический уровень

Физический уровень (physical layer) – самый нижний уровень, непосредственно осуществляющий передачу потока данных. Протоколы нам всем хорошо известны: Bluetooth, IRDA (Инфракрасная связь), медные провода (витая пара, телефонная линия), Wi-Fi, и т.д.

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 (рис. 16.3), как: - **экранирующий маршрутизатор**; - **шлюз сеансового уровня**; - **шлюз прикладного уровня**.

Используемые в сетях протоколы (TCP/IP, SPX/IPX) не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, **прикладной шлюз** может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI.

МЭ указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечивая полную безопасность межсетевого взаимодействия.

Надежную же защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

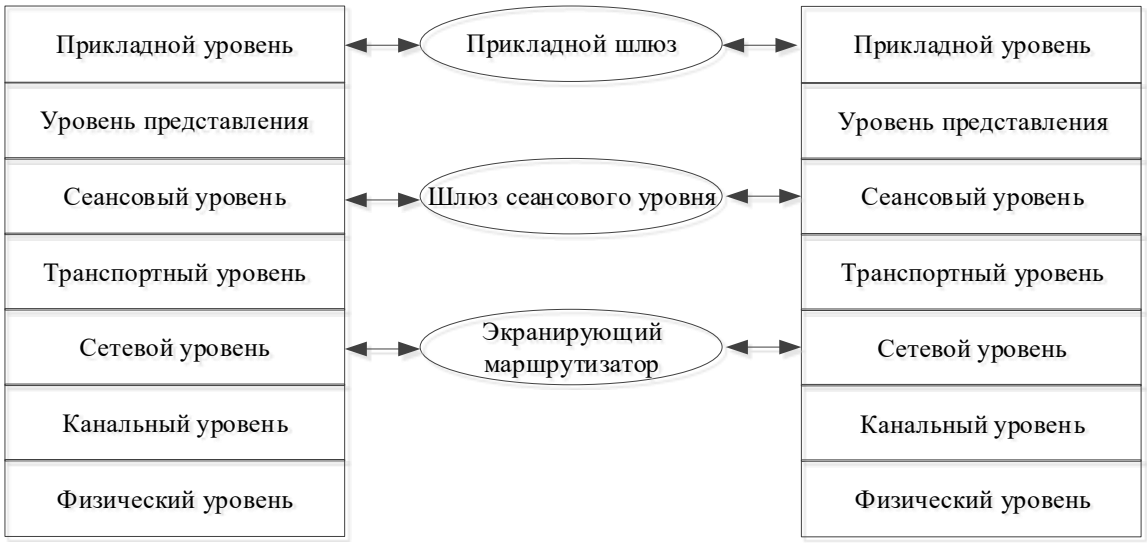

Рис. 16.3 Типы МЭ, функционирующих на различных уровнях модели OSI

3.2 Экранирующий маршрутизатор

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 OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели.

Решение о том, пропустить или отбраковать данные, принимается для каждого пакета независимо на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней. В качестве анализируемых полей IP - и TCP (UDP)- заголовков каждого пакета могут использоваться (адрес отправителя; адрес получателя; тип пакета; флаг фрагментации пакета; номер порта источника; номер порта получателя).

Первые четыре параметра относятся к IP - заголовку пакета, а следующие - к TCP - или UDP - заголовку. Адреса отправителя и получателя явля-

ются IP-адресами. Эти адреса заполняются при формировании пакета и остаются неизменными при передаче его по сети.

Пакетные фильтры могут быть реализованы как аппаратно, так и программно. В качестве пакетного фильтра могут быть использованы как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Современные маршрутизаторы, в частности компаний Cisco и BayNetworks, позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе.

Обладая положительными качествами, пакетные фильтры не лишены серьезных недостатков. Они не обеспечивают высокой степени безопасности, так как проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты, например, **аутентификацию конечных узлов, криптографическое закрытие** пакетов сообщений, а также **проверку их целостности и подлинности**. Пакетные фильтры уязвимы для таких распространенных сетевых атак, как подмена исходных адресов и несанкционированное изменение содержимого пакетов сообщений.

«Обмануть» МЭ данного типа не составляет труда - достаточно сформировать заголовки пакетов, которые удовлетворяют разрешающим правилам фильтрации.

Однако такие достоинства пакетных фильтров, как простота реализации, высокая производительность, прозрачность для программных приложений и малая цена, обусловленная тем, что любой маршрутизатор в той или иной степени предоставляет возможность фильтрации пакетов, - перевешивают указанные недостатки и обуславливают их повсеместное распространение и **использование как обязательного элемента системы сетевой безопасности**. Кроме того, они являются составной частью практически всех межсетевых экранов, использующих контроль состояния.

3.3 Шлюз сеансового уровня

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.

Шлюз сеансового уровня обеспечивает также трансляцию внутренних адресов сетевого уровня (IP-адресов) при взаимодействии с внешней сетью.

Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP - адреса компьютеров-отправителей внутренней сети автоматически преобразуются в один IP-адрес, ассоциируемый с экранирующим транспортом. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными межсетевым экраном, что исключает прямой контакт между внутренней и внешней сетями. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

Трансляция адресов вызвана необходимостью усиления защиты путем сокрытия от внешних пользователей структуры защищаемой внутренней сети. При трансляции внутренних IP-адресов шлюз сеансового уровня экранирует, то есть заслоняет внутреннюю сеть от внешнего мира.

С другой стороны, трансляция адресов вызвана тем, что канальные посредники создают новое соединение каждый раз, когда они активизируются. Посредник принимает запрос от рабочей станции внутренней сети и затем инициирует новый запрос к компьютеру внешней сети. Поэтому компьютер внешней сети воспринимает запрос как исходящий от посредника, а не от действительного клиента.

С точки зрения реализации шлюз сеансового уровня представляет собой довольно простую и относительно надежную программу. Он дополняет экранирующий маршрутизатор функциями контроля виртуальных соединений и трансляции внутренних IP-адресов.

Недостатки у шлюза сеансового уровня те же, что и у экранирующего маршрутизатора, - не обеспечиваются контроль и защита содержимого пакетов сообщений, не поддерживаются аутентификация пользователей и конечных узлов, а также другие функции защиты локальной сети. У данной технологии есть еще один серьезный недостаток - невозможность проверки содержимого поля данных. В результате злоумышленнику представляется возможность передачи в защищаемую сеть «троянских коней» и других вредоносных программ. Кроме того, при перехвате TCP-сессии злоумышленник может реализовывать свои атаки даже в рамках разрешенной сессии.

На практике большинство шлюзов сеансового уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня.

3.4 Прикладной шлюз

Прикладной шлюз, называемый также экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывая также уровень

представления, и обеспечивает наиболее 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.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) - по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, то есть прикладной шлюз функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетями.

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP - серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP. Трафик UDP обслуживается специальным транслятором содержимого UDP-пакетов.

Как и в случае шлюза сеансового уровня, для связи между рабочей станцией внутренней сети и компьютером внешней сети соответствующий посредник прикладного шлюза образует два соединения: от рабочей станции до МЭ и от МЭ до места назначения. Но, в отличие от канальных посредников, посредники прикладного шлюза пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать.

Например, программа-посредник службы HTTP может обрабатывать лишь трафик, генерируемый этой службой.

Если для какого-либо из приложений отсутствует свой посредник приложений, то прикладной шлюз не сможет обрабатывать трафик такого приложения и он будет блокирован. Например, если прикладной шлюз использует только программы-посредники HTTP, FTP и Telnet, то он будет обрабатывать лишь пакеты, относящиеся к этим службам, блокируя при этом пакеты всех остальных служб.

Фильтрация потоков сообщений реализуется прикладными шлюзами на прикладном уровне модели OSI. Соответственно, посредники прикладного шлюза, в отличие от канальных посредников, обеспечивают проверку содержимого обрабатываемых пакетов. Они могут фильтровать отдельные виды команд или информации в сообщениях протоколов прикладного уровня, которые им поручено обслуживать.

При настройке прикладного шлюза и описании правил фильтрации сообщений используются такие параметры, как название сервиса, допустимый временной интервал его использования, ограничения на содержимое сообщений, связанных с данным сервисом, компьютеры, с которых можно пользоваться сервисом, идентификаторы пользователей, схемы аутентификации и др.

Шлюз прикладного уровня обладает следующими достоинствами:

- обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;
- защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, основанных на недостатках программного обеспечения;
- при нарушении работоспособности прикладного шлюза блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам прикладного шлюза относятся:

- относительно высокая стоимость;
- довольно большая сложность самого firewall, а также процедур его установки и конфигурирования;
- высокие требования к производительности и ресурсоемкости компьютерной платформы;
- отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

3.5 Шлюз экспертного уровня

Для устранения такого существенного недостатка прикладных шлюзов, как отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий, компании Check Point и ON Technology разработали технологию фильтрации пакетов, которую иногда называют **фильтрацией с контролем состояния соединения** (stateful inspection) или фильтрацией экспертного уровня.

Такая фильтрация осуществляется на основе специальных методов многоуровневого анализа состояния пакетов SMLT (Stateful MultiLayer Technique).

Эта гибридная технология позволяет отслеживать состояние сетевого соединения, перехватывая пакеты на сетевом уровне и извлекая из них информацию прикладного уровня, которая используется, для контроля за соединением. Быстрое сравнение проходящих пакетов с известным состоянием (state) «дружественных» пакетов позволяет значительно сократить время обработки по сравнению с МЭ уровня приложений.

МЭ экспертного уровня также выполняют все функции прикладного шлюза, касающиеся фильтрации пакетов на прикладном уровне модели OSI. Они оценивают содержимое каждого пакета в соответствии с заданной политикой безопасности.

Достоинством МЭ экспертного уровня является прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения. Помимо прозрачности для пользователей и более высокой скорости обработки информационных потоков к достоинствам МЭ экспертного уровня относится также то, что эти МЭ не изменяют IP -адресов проходящих через них пакетов. Это означает, что любой протокол прикладного уровня, использующий IP -адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программирования.

Поскольку данные МЭ допускают прямое соединение между авторизованным клиентом и компьютером внешней сети, они обеспечивают менее высокий уровень защиты.

Поэтому на практике технология фильтрации экспертного уровня используется для повышения эффективности функционирования комплексных МЭ.

В настоящее время фильтрация экспертного уровня становится одной из функций новых маршрутизаторов.

Контрольные вопросы

1. Что понимается под технологией межсетевого экранирования?
2. Классификация межсетевых экранов.
3. Основные функции межсетевых экранов.
4. Структура межсетевого экрана.
5. Функции посредничества межсетевых экранов.
6. Эталонная сетевая модель OSI.
7. Типы межсетевых экранов, функционирующих на различных уровнях модели OSI.

ТЕМА 17. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)

1. Основные понятия и функции виртуальных сетей
2. Специфика построения VPN
3. Туннелирование в виртуальных частных сетях
4. Схема виртуальной частной сети
5. Политики безопасности в виртуальных частных сетях
6. Цифровые сертификаты
7. Примеры отечественного построения VPN

Литература:

1. Информационная безопасность открытых систем: учебник для вузов по спец. 075500 (090105) - "Комплексное обеспечение информационной безопасности автоматизированных систем": в 2 т. /Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. - М.: Горячая линия-Телеком, 2008. - 558 с.

1. Основные понятия и функции виртуальных сетей

Благодаря развитию криптографических технологий появился способ решить задачи ЗИ в современной сетевой среде за счет использования технологии защищенных виртуальных частных сетей (Virtual Private Network —

VPN), надежно шифрующих информацию, передаваемую по дешевым открытым сетям, включая Internet.

Открытая сеть может служить основой для одновременного сосуществования множества виртуальных сетей, количество которых определяется пропускной способностью открытых каналов. связи.

Можно встретить и такие общие подходы к определению VPN:

- VPN — это защита трафика, основанная на криптографии;
- VPN — это средство коммуникации, так как гарантия защиты доступа к внутренним ресурсам из любой точки мира инициирует применение ИС для удаленного доступа.

Под VPN понимают потоки данных одного предприятия, которые существуют в публичной сети с коммутацией пакетов и в достаточной степени защищены от влияния потоков данных других пользователей этой публичной сети.

Другими словами, **VPN — это некоторая имитация сети, построенной на выделенных каналах.** Если публичная сеть предоставляет такой сервис, то в ней одновременно сосуществуют несколько VPN, разделяющих общие коммутаторы и физические каналы связи.

Сети VPN решают задачи подключения корпоративного пользователя к удаленной сети и соединения нескольких ЛВС (интрасетей) (рис. 17.1).

Цель VPN-технологий состоит в максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей публичной сети.

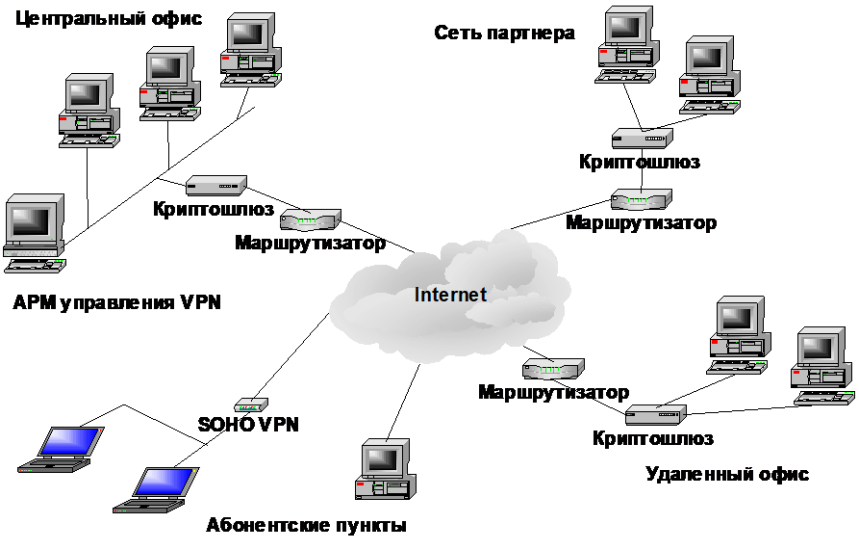

Рис. 17.1. Пример VPN.

Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в конфиденциальности передаваемых данных.

Таким образом, основными задачами технологий VPN являются обеспечение в публичной сети гарантированного качества обслуживания для потоков пользовательских данных, а также защита их от возможного НСД или разрушения.

VPN-технологии обеспечивают:

- защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
- защиту внутренних сегментов сети от НСД со стороны сетей общего пользования;
- контроль доступа в защищаемый периметр сети;
- сокрытие внутренней структуры защищаемых сегментов сети;
- идентификацию и аутентификацию пользователей сети;
- централизованное управление политикой корпоративной сетевой безопасности и настройками VPN-сети;
- криптографическую защиту данных, передаваемых по каналам связи сетей общего пользования между защищаемыми сегментами сети;
- безопасный доступ пользователей VPN к ресурсам сетей общего пользования.

Термин «private» имеет два основных значения: частный (собственный) и конфиденциальный (закрытый). Если делать акцент на первом значении, то частная сеть — это такая сеть, в которой все оборудование (включая территориальные кабельные системы, коммутирующие устройства, средства управления и т.п.) являются собственностью предприятия. На рис. 17.2 приведен пример сети, в которой связи между филиалами построены на основе собственного оборудования данного предприятия. Три территориальных канала связывают центральную интрасеть предприятия с тремя интрасетями удаленных филиалов. Каждый территориальный канал образован отрезками кабеля, проложенного между устройствами регенерации, необходимыми для усиления сигналов и восстановления их формы после прохождения определенного расстояния по пассивному кабелю. Вся пропускная способность территориальных каналов находится в полном распоряжении предприятия.

Потоки данных отдельного предприятия образуют виртуальные каналы частной сети (рис.17.2).

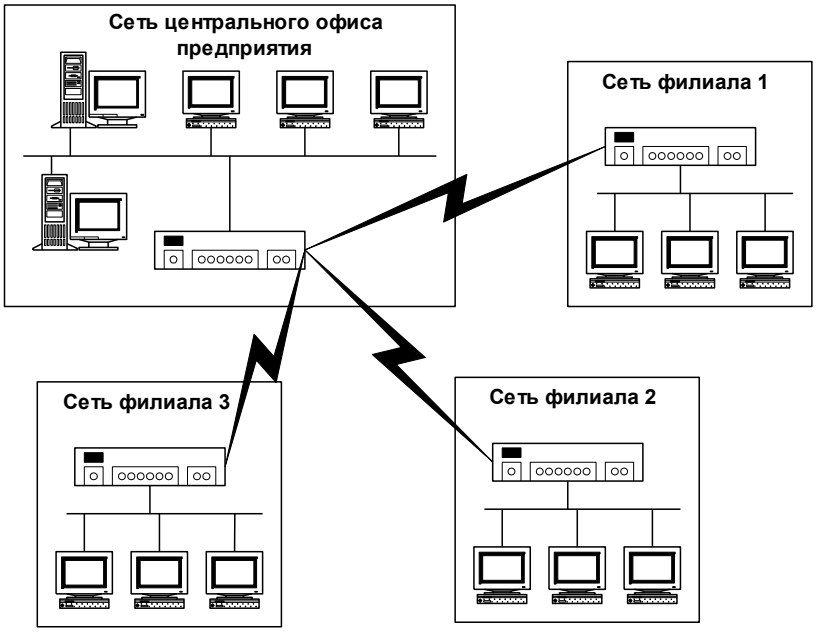

Рис. 17.2. Частная сеть с собственными территориальными каналами

Следует заметить, что сетей, являющихся абсолютно частными, в мире не так уж много. Использовать собственные территориальные каналы связи могут только те предприятия, для которых такие каналы являются органической частью собственной инфраструктуры, обусловленной основной производственной деятельностью. Например, для передачи технологической информации железнодорожные компании прокладывают линии связи вдоль полотна, а нефтяные — вдоль трубопроводов, поэтому они могут использовать свободную часть своих линий для построения каналов связи.

Понятно, что сеть, построенная целиком на собственном оборудовании предприятия, соответствует и второму определению термина "private" - в собственной сети легче соблюдать конфиденциальность, поскольку все ресурсы сети используются только сотрудниками предприятия-владельца.

С точки зрения конечных пользователей их обычно интересуют ответы на следующие вопросы о VPN.

1. Как мне защитить удаленный филиал своей организации или подключиться к сети из дома или с переносного компьютера?
2. Если я использую МЭ, то нужна ли мне VPN?
3. Защищает ли VPN от внешних и внутренних атак?
4. Насколько медленнее будет работать моя сеть после установки VPN?
5. Отличие сертифицированного и несертифицированного VPN-устройства?
6. Почему VPN-устройства сертифицируются по классу МЭ?

2. Специфика построения VPN

Как правило, построение VPN для распределенных компаний даже с небольшим количеством удаленных подразделений (филиалов) является достаточно трудоемкой задачей, сложность которой обуславливается следующими основными причинами:

- гетерогенностью используемых аппаратно-программных платформ;
- разнообразием задач (защищенный обмен между головным офисом и филиалами, офисом и мобильными или удаленными сотрудниками, сегментами внутренней сети компании);
- необходимостью построения централизованной системы управления всей корпоративной VPN;
- наличием узкой полосы пропускания и откровенно плохим качеством существующих каналов связи, особенно с региональными подразделениями.

Одним из требований к VPN является обеспечение масштабируемости конкретной VPN. Многолетний опыт показывает, что наиболее успешно для этого применяются **программные VPN-агенты, которые:**

- могут обеспечить защиту трафика на всех типах компьютеров — рабочих станциях, серверах и шлюзах (на выходе из локальной в открытые сети);
- работают на всех популярных ОС.

3. Туннелирование в виртуальных частных сетях

VPN состоит из каналов глобальной сети, защищенных протоколов и маршрутизаторов (рис. 17.3). Для объединения удаленных ЛВС в VPN используются так называемые виртуальные выделенные каналы. Для организации подобных соединений применяется механизм туннелирования, или инкапсуляции.

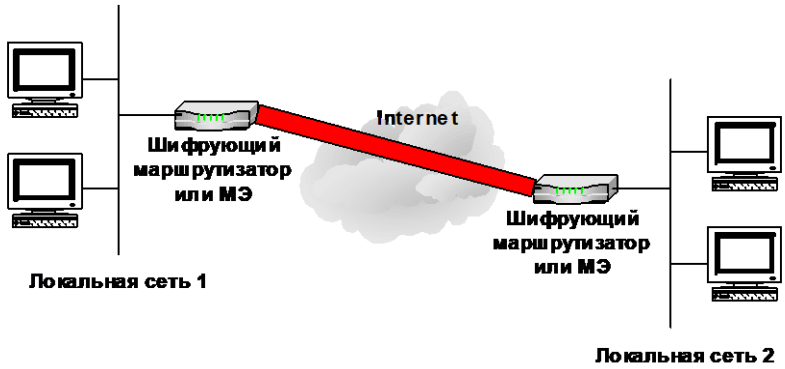

Рис. 17.3 Структура VPN

При туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня.

Например, при туннелировании кадр Ethernet может быть размещен в пакете IP, пакет IPX — в пакете IP. Возможен и такой вариант: пакет IP размещается в пакете IP.

Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть. Инициатор туннеля инкапсулирует пакеты ЛВС (в том числе пакеты немаршрутизируемых протоколов) в IP-пакеты, содержащие в заголовке адреса инициатора и терминатора туннеля. Терминатор туннеля извлекает исходный пакет. Естественно, при подобной передаче требуется решать проблему конфиденциальности и целостности данных, что не обеспечивается простым туннелированием.

Конфиденциальность передаваемой корпоративной информации достигается шифрованием (алгоритм одинаков на обоих концах туннеля).

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных.

Исходный пакет зашифровывают полностью, вместе с заголовком, и этот зашифрованный пакет помещают в другой, внешний пакет с открытым заголовком. Для транспортировки данных по "опасной" сети используются открытые поля заголовка внешнего пакета, а при прибытии внешнего пакета в конечную точку защищенного канала из него извлекают внутренний пакет, расшифровывают и используют его заголовок для дальнейшей передачи уже в открытом виде по сети, не требующей защиты. При этом для внешних пакетов используются адреса пограничных маршрутизаторов, установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних пакетах в защищенном виде (рис. 17.4).

Механизм туннелирования можно представить как результат работы протоколов трех типов: - протокола-пассажира; - несущего протокола; - протокола туннелирования.

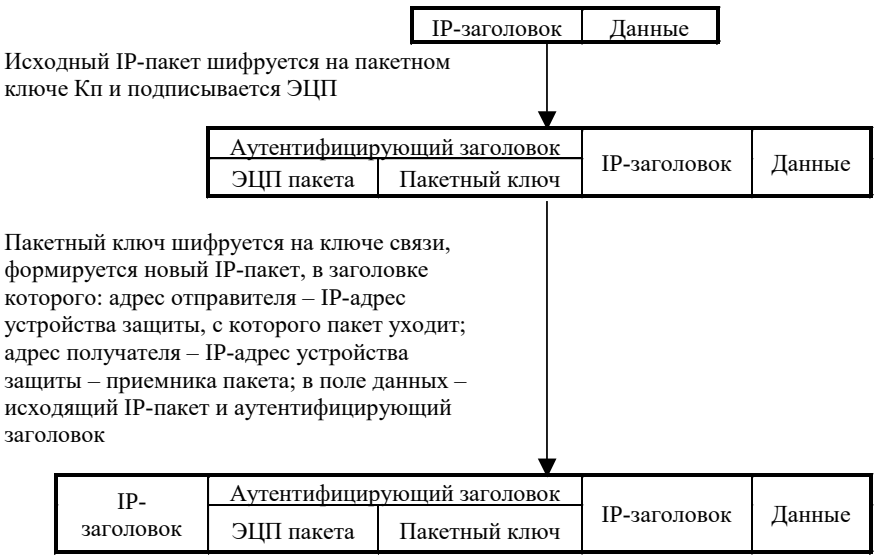

Рис. 17.4 Туннелирование пакетов

Транспортный протокол объединяемых сетей (например, протокол IPX, переносящий данные в ЛВС филиалов одного предприятия) является протоколом-пассажиром, а протокол транзитной сети (например, протокол IP сети Internet) — несущим протоколом (рис. 17.5).

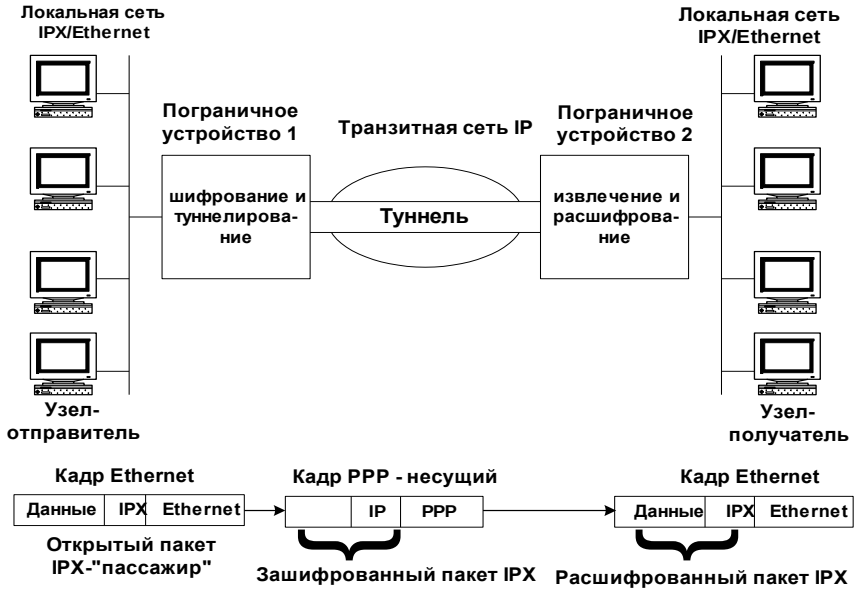

Рис. 17.5 Схема использования туннелирования для зашифрованной передачи трафика IPX через сеть IP

Процедура помещения пакетов протокола-пассажира в поле данных пакетов несущего протокола составляет суть протокола туннелирования. Пакеты протокола-пассажира никак не обрабатываются при транспортировке их по транзитной сети. Туннелирование обычно выполняет пограничное устройство (маршрутизатор или шлюз), которое располагается на границе между исходной и транзитной сетями, но этой работой может заниматься и узел-отправитель.

Извлечение пакетов-пассажиров из несущих пакетов выполняет второе пограничное устройство, которое находится на границе между транзитной сетью и сетью назначения, либо узел-получатель.

4. Схема виртуальной частной сети

Суть VPN состоит в следующем (рис. 17.6) — на все компьютеры, имеющие выход в Internet, устанавливается средство, реализующее VPN (VPN-агент).

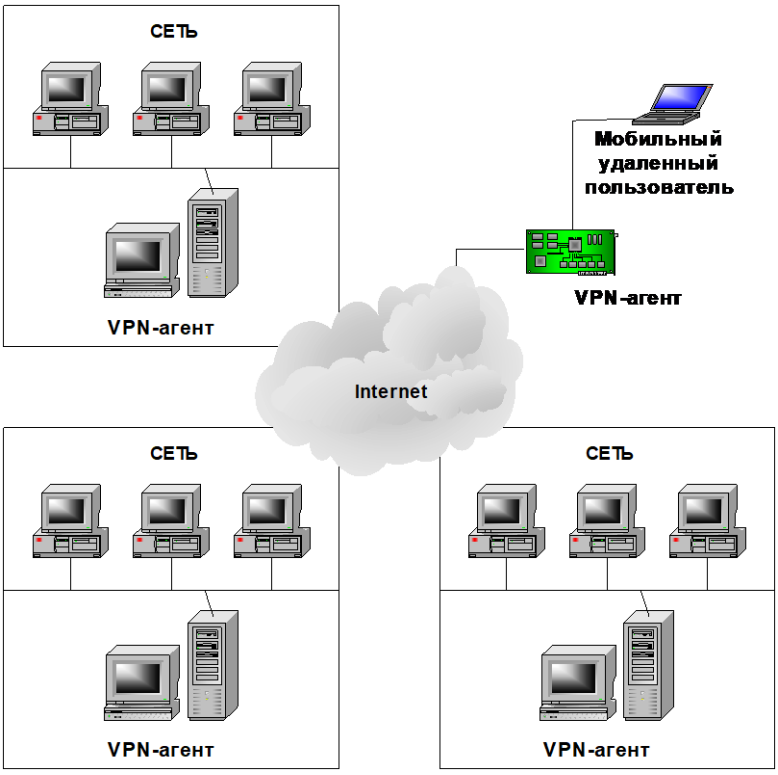

Рис. 17.6 Схема VPN

VPN-агенты автоматически шифруют всю исходящую информацию (и соответственно расшифровывают всю входящую). Они также следят за ее целостностью с помощью электронной подписи (ЭП) или имитовставок (криптографическая контрольная сумма, рассчитанная с использованием ключа шифрования). Поскольку информация, циркулирующая в Internet, представляет собой множество пакетов протокола IP, VPN-агенты работают именно с ними.

Перед отправкой IP-пакета VPN-агент действует следующим образом:

- Из нескольких поддерживаемых им алгоритмов шифрования и ЭП по IP-адресу получателя выбирает нужный для защиты данного пакета, а также

ключи. Если же в его настройках такого получателя нет, то информация не отправляется.

- Генерирует и добавляет в пакет ЭП отправителя или имитовставку.
- Шифрует пакет (целиком, включая заголовок).

Проводит инкапсуляцию, т.е. формирует новый заголовок, где указывается адрес вовсе не получателя, а его VPN-агента. Эта полезная дополнительная функция позволяет представить обмен между двумя сетями как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для злоумышленника информация, например, внутренние IP-адреса, ему уже недоступна. При получении IP-пакета выполняются обратные действия

- Заголовок содержит сведения о VPN-агенте отправителя. Если таковой не входит в список разрешенных в настройках, то информация просто отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.
- Согласно настройкам, выбираются алгоритмы шифрования и ЭП, а также необходимые криптографические ключи.
- Пакет расшифровывается, затем проверяется его целостность. Если ЭП неверна, то он отбрасывается.
- Пакет в его исходном виде отправляется настоящему адресату по внутренней сети.

Все операции выполняются автоматически. Сложной в технологии VPN является только настройка VPN-агентов.

VPN-агент может находиться непосредственно на защищаемом ПК, что полезно для мобильных пользователей, подключающихся к Internet из разных мест. В этом случае он обезопасит обмен данными только того компьютера, на котором установлен.

Возможно совмещение VPN-агента с маршрутизатором (в этом случае его называют криптографическим) IP-пакетов. Ведущие мировые производители в последнее время выпускают маршрутизаторы со встроенной поддержкой VPN, например, Express VPN от Intel, который шифрует все проходящие пакеты по алгоритму Triple DES.

Как видно из описания, **VPN-агенты создают каналы между защищаемыми сетями, которые обычно называют туннелями.** Они "прорыты" от одной сети к другой; циркулирующая внутри информация спрятана от чужих глаз.

Кроме того, все пакеты фильтруются в соответствии с настройками (рис. 17.7). Таким образом, **все действия VPN-агентов можно свести к двум механизмам: созданию туннелей и фильтрации проходящих пакетов.**

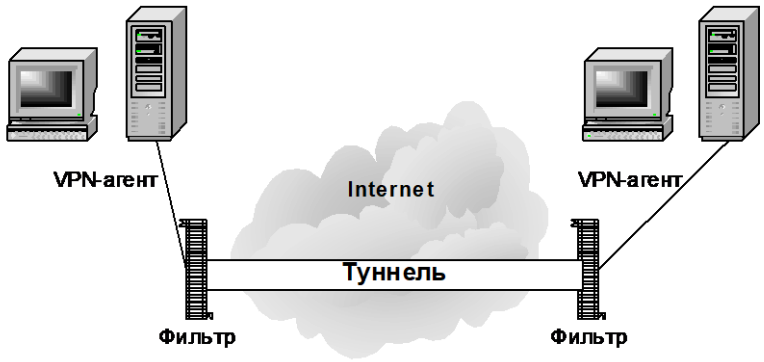

Рис. 17.7 Функции VPN-агентов

Совокупность правил создания туннелей, которая называется "политикой безопасности", записывается в настройках VPN-агентов. IP-пакеты направляются в тот или иной туннель или отбрасываются после того, как будут проверены: - IP-адрес источника (для исходящего пакета — адрес конкретного компьютера защищаемой сети); - IP-адрес назначения; - протокол более высокого уровня, которому принадлежит данный пакет (например, TCP или UDP); - номер порта, с которого или на который отправлена информация (например, 1080).

5. Политики безопасности в виртуальных частных сетях

В соответствии с общепринятым определением, безопасность данных означает их конфиденциальность, целостность и доступность. Применительно к задачам VPN критерии безопасности могут быть определены следующим образом.

• Конфиденциальность — гарантия того, что в процессе передачи по защищенным каналам VPN данные не могут быть просмотрены никем, кроме легальных отправителя и получателя.

• Целостность — гарантия сохранения неизменности передаваемых данных во время прохождения по защищенному каналу VPN.

• Доступность — гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям. Доступность средств VPN — это комплексный показатель, зависящий от нескольких факторов: надежности реализации, качества обслуживания, а также степени защищенности самого средства от внешних атак.

Существует три основных варианта создания VPN:

1. Защищенные каналы. МЭ шифрует весь трафик, передаваемый удаленному хосту (хост — это компьютер, имеющий уникальный IP-адрес) или сети, и расшифровывает весь трафик, принятый от них.

Трафик между хостами в VPN, связанными защищенными каналами, передается свободно, как будто между ними нет МЭ. На самом деле трафик маршрутизируется МЭ VPN. Его обработка прокси-серверами (proxy-сервер, или сервер полномочий, или сервер-посредник ждет директив из сети, пересылает запрос к удаленному серверу, расположенному за пределами защитной системы, получает от него ответное сообщение и передает его по назначению) и аутентификация не требуются.

Любые два хоста внутри VPN, связанные защищенными каналами, могут свободно обмениваться данными между собой, и предоставлять все сервисы TCP/IP, которые у них имеются. Защищенные каналы часто используются для соединения географически разделенных сетей, принадлежащих одной организации, каждая из которых имеет свое собственное подключение к Internet через провайдера, в одну виртуальную сеть безопасным способом.

2. Частные каналы. Трафик между МЭ и удаленным хостом шифруется так же, как и для защищенного канала. Но трафик между удаленными хостами, связанными частными каналами, не передается свободно, а должен быть обработан прокси-сервером МЭ и соединение аутентифицировано, как того требует обычная политика доступа для прокси-сервера. Этот вид канала обеспечивает аутентификацию отправителя трафика и конфиденциальность данных, но в данном случае две сети обеспечивают наличие двух различных периметров безопасности, и могут использоваться только те сервисы, для которых сконфигурирована передача прокси-серверу в МЭ. Частные каналы часто используются для организации связи между сетями различных организаций, которые не хотят предоставлять полного доступа к их сетям, и требуют конфиденциальности трафика между ними.

3. Промежуточные каналы. Эти каналы используются для промежуточной передачи зашифрованного трафика между хостами, расположенными за МЭ и входящими в состав другой VPN. Это позволяет МЭ, находящемуся между двух других VPN, быть сконфигурированным так, что он только передает зашифрованные данные. Он не расшифровывает трафик и даже не знает ключа шифрования. Ему надо лишь знать адреса хостов по обе стороны МЭ, участвующих в организации этого канала, чтобы определить, какие зашиф-

рованные пакеты пропускать. Такая архитектура позволяет использовать промежуточный МЭ как маршрутизатор.

Используя только что введенные понятия каналов VPN, приведем **примеры некоторых политик безопасности (ПБ) при использовании каналов Internet для построения VPN.**

1. **Высокая ПБ.** Для VPN, использующих Internet, МЭ организации должны работать в режиме частного канала, шифровать трафик VPN и требовать использования прокси-серверов МЭ для ограничения доступа к сервисам со стороны удаленных хостов VPN.

2. **Низкая-средняя ПБ.** Для VPN, использующих Internet, МЭ организации должны работать в режиме защищенного канала, шифровать трафик VPN и не требовать использования прокси-серверов для его обработки.

3. **Средняя-высокая ПБ.** VPN между ЛВС не должны использовать Internet для передачи критичного к оперативности передачи трафика. Если уровень надежности, предоставляемый Internet, недостаточен для обеспечения требуемого уровня сервиса, для передачи данных должны использоваться другие способы.

6. Цифровые сертификаты

Для организации защищенных связей необходимо применение шифрования, которое, в свою очередь, требует наличия у пользователя ключа шифрования. При этом возникает проблема управления ключами, которая включает в себя следующие задачи: генерацию, проверку, распространение, использование, хранение, резервирование, обновление, уничтожение ключей и установление времени жизни ключа. При использовании симметричного шифрования у пользователя должны быть ключи для всех абонентов, с которыми он должен поддерживать защищенную связь, поэтому наибольшее распространение получило асимметричное шифрование. Однако из-за трудоемкости вычислений обычно асимметричное шифрование применяется для формирования сеансового ключа, который используется для симметричного шифрования данных в текущем сеансе.

Применение асимметричного шифрования требует наличия общедоступной системы, содержащей открытые ключи абонентов. В этом случае возможна фальсификация открытого ключа. Данная проблема решается с помощью сертификатов открытых ключей. Под сертификатом понимается подписанная цифровой подписью запись данных, содержащая имя и открытый ключ абонента. Сертификат подписывается специально создаваемой службой — уполномоченным центром сертификации, который пользуется

доверием абонентов. Универсальное распространение получила схема создания сертификатов открытых ключей, основанная на стандарте X.509.

7. Примеры отечественного построения VPN

Протоколы построения защищенных виртуальных сетей могут быть реализованы различными средствами:

- серверами удаленного доступа, позволяющими создавать защищенные туннели на канальном уровне;
- маршрутизаторами, которые поддерживают протоколы создания защищенных виртуальных сетей на канальном и сетевом уровнях;
- межсетевыми экранами, возможно включающими в свой состав серверы уд. доступа и позволяющие создавать VPN на канальном, сетевом и транспортном уровнях;
- специализированным программным обеспечением для создания защищенных туннелей на сетевом и транспортном уровнях;
- программно-аппаратными средствами, позволяющими формировать защищенные туннели на канальном и сетевом уровнях.

В качестве отечественного примера построения VPN рассмотрим особенности системы «Континент-К» НИП «Информзащита» и продукты ViPNet компании Infotecs.

Основными компонентами системы «Континент-К» являются криптошлюз, центр управления сетью криптошлюзов, программное обеспечение управления сетью криптошлюзов, абонентский пункт.

Криптошлюз представляет собой программно-аппаратное устройство под управлением операционной системы FreeBSD и обеспечивает:

- прием и передачу пакетов (TCP/IP); • шифрование по ГОСТ 28147—89 в режиме гаммирования с обратной связью; • сжатие защищаемых данных; • защиту данных от искажения (имитовставка); • аутентификацию удаленных абонентов; • контроль целостности ПО криптошлюза до загрузки ОС (электронный замок «Соболь»).

Абонентский пункт служит для защищенного подключения к серверу доступа, на котором находится криптошлюз «Континент-К». После установления соединения и получения разрешения на доступ в защищаемую сеть (сервер доступа проводит идентификацию и аутентификацию удаленного пользователя и определяет его уровень доступа) весь трафик между абонентским пунктом и защищенной сетью шифруется по ГОСТ 28147—89. Комплекс использует схему сертификатов X.509.

Продукты ViPNet для организации VPN включают в себя два решения: ViPNet [Custom] и ViPNet [Tunnel].

Система ViPNet [Custom] предназначена для объединения в единую защищенную сеть произвольного числа рабочих станций и локальных сетей. В состав системы входят:

• ViPNet [Администратор] — модуль, создающий инфраструктуру сети, ведущий мониторинг сети и управляющий объектами сети. Он формирует первичную ключевую и парольную информацию для объектов сети и сертифицирует ключи, сформированные этими объектами;

• ViPNet [Координатор] — модуль, выполняющий маршрутизацию защищенных пакетов, туннелирование пакетов от обслуживаемой группы незащищенных компьютеров локальной сети. Он фильтрует трафик от источников, не входящих в VPN в соответствии с заданной ПБ, обеспечивает возможность работы защищенных компьютеров через межсетевые экраны и ргоху-серверы других производителей;

• ViPNet [Клиент] — модуль, обеспечивающий защиту информации при передаче по открытым каналам связи и защиту доступа к ресурсам компьютера из сетей общего пользования. Модуль может быть установлен как на рабочую станцию, так и на сервер (баз данных, файл-сервер, www-сервер, SMTP, SQL и т.д.).

Контрольные вопросы

1. Что понимается под технологией защищенных виртуальных частных сетей?
2. Пример частной сети с собственными территориальными каналами.
3. Специфика построения VPN. Что такое VPN-агент?
4. Механизм туннелирования (инкапсуляции).
5. Политики безопасности в виртуальных частных сетях.
6. Основные варианты построения VPN.
7. Примеры отечественных VPN.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. -392с.
2. Информационная безопасность компьютерных систем и сетей. учебное пособие / В.Ф. Шаньгин. - М.: ИД «ФОРУМ»: ИНФРА-М, 2014. - 416с.
3. Стратегия национальной безопасности Российской Федерации (Указ Президента РФ от 31.01.2015 г. № 683).
4. Доктрина ИБ информационной безопасности РФ от 05.12.2016 (Указ Президента РФ от 05 декабря 2016 г.).
5. Стратегия национальной безопасности Российской Федерации: Утв. Указом Президента РФ от 31 декабря 2015г. № 683.
6. Малюк А.А. Защита информации в информационном обществе. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2015. – 230 с.
1. Расторгуев С.П. Информационная война. - М: Радио и связь, 1999. - 416 с.