Федеральное государственное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

В. В. Подтопельный

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем", специализация «Безопасность открытых информационных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент

Доцент кафедры информационной безопасности института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» А. Г. Жестовский.

Подтопельный, В. В.
Безопасность вычислительных сетей: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 " Информационная безопасность автоматизированных систем ", специализация «Безопасность открытых информационных систем. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 130 с.

Учебное пособие включает в себя рассмотрение теоретических вопросов в области защиты информации по дисциплине «Безопасность вычислительных сетей». В учебно-методическом пособии приведен тематический план изучения дисциплины. Представлены методические указания по изучению дисциплины. Даны рекомендации по подготовке к промежуточной аттестации в форме зачета и экзамена, и по выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины «Безопасность вычислительных сетей».

Пособие предназначено для студентов 3 – 4 курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей.

Рис. – 59, табл. - 11, список лит. – 5 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 19.05.2022 г., протокол № 7

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28.06.2022 г., протокол № 4

ОГЛАВЛЕНИЕ

1.ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 " Информационная безопасность автоматизированных систем ", специализация «Безопасность открытых информационных систем», изучающих дисциплину «**Безопасность вычислительных сетей».**

Цель изучения дисциплины: обучить студентов выявлять и противодействовать сетевым атакам вредоносных программ и злоумышленников в распределенных системах обработки информации**.**

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют «Безопасность систем баз данных», «Безопасность операционных систем».

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных/практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе Содержание дисциплины приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

В разделе «Балльно-рейтинговая система» приведен порядок применения балльно-рейтинговой системы контроля успеваемости.

Помимо данного пособия студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение:

1. Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения (Microsoft Office), по соглашению V9002148 Open Value Subscription (срок действия: три года)

2. Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU, по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);

– Ethereal (Программы перехвата и анализа сетевых пакетов);

Типовое ПО на всех ПК:

1. Microsoft Desktop Education (операционные системы Microsoft Windows Desktop operating system, офисные приложения Microsoft Office, по соглашению V9002148 Open Value Subscription). Дата заключения контракта 05.07.2018. Номер контракта 0335100016118000073-0484577-02.

2. Антивирусное программное обеспечение Kaspersky Total Space Security Russian Edition, лицензия 17EO-171225-104659-470-270, срок использования с 2017-12-26 до 2020-03-13

Специализированное ПО и программно-обеспечение:

Лабораторный стенд: «Сетевая безопасность»

2.ТЕМАТИЧЕСКИЙ ПЛАН

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Лекции (6-й семестр -34 ч ауд.)		
1.1	Сетевые угрозы	Тема 1. Принципы многоуровневой защиты корпоративной информации. Основы сетевого и межсетевого взаимодействия	4	14
1.2	Сетевые угрозы	Тема 1.2 Политика безопасности. Структура политики безопасности	4	14
1.3	Сетевые угрозы	Тема 1.3 Симметричные и ассиметричные системы шифрования. Функции хеширования. Электронная подпись	4	
1.4	Сетевые угрозы	Тема 1.4 Идентификация, аутентификация и управление доступом	5	
2.1	Защита от сетевых угроз	Тема 2.1 Доменные службы Active Directory. Структуры леса, доменных деревьев. Проектирование отношений и оптимизация аутентификации внутри леса	4	
2.2	Защита от сетевых угроз	Тема 2.2 Корпоративная информационная система. Сети периметра и стратегии удаленного доступа	2	16
		итого	34	84,85
		Лекции (7-й семестр -34 ч ауд.)		
2.3	Защита от сетевых угроз	Тема 2.3 Обеспечение безопасности операционных систем. Локальные политики безопасности. Встроенные системы защиты операционных систем. Модель взаимодействия си-	2	

		стем. Стек протоколов TCP/IP		
2.4	Защита от сетевых угроз	Тема 2.4 Защита на канальном уровне – протоколы удаленного доступа	2	
2.5	Защита от сетевых угроз	Тема 2.5 Протоколы IPSec, SSL, TSL, SOCKS. Защита на сетевом и сеансовом уровнях	2	16
2.6	Защита от сетевых угроз	Тема 2.6 Функционирование межсетевых экранов на различных уровнях модели OSI	2	12
2.7	Защита от сетевых угроз	Тема 2.7 Виртуальные частные сети	3	
		Итого	34	33,75
		Итого за курс	68	118,5

		лабораторные занятия (6-й семестр 34 ч)		
1.	Сетевые угрозы	Аудит безопасности протокола SNMP	6	-
2.	Сетевые угрозы	Аудит безопасности протокола STP	6	-
3.	Сетевые угрозы	Виртуальные локальные сети IEEE 802.1	6	-
4.	Сетевые угрозы	Базовые механизмы безопасности коммутаторов	6	-
5.	Сетевые угрозы	Безопасность на основе сегментации трафика	6	-
6.	Сетевые угрозы	Безопасность на основе протокола IEEE 802.1x	4	-
		Итого:	34	

1		**лабораторные занятия (7-й семестр 34 ч)**		
7.	Сетевые угрозы	Списки контроля доступа ACL	4	-
8.	Сетевые угрозы	Контроль доступа к коммутатору	4	-
9.	Защита от сетевых угроз	Шифрование канала с использованием протокола WEP	4	-
10.	Защита от сетевых угроз	Шифрование канала с использованием протокола WEP	4	-
11.	Защита от сетевых угроз	Аутентификация беспроводных клиентов на основе учѐтных записей пользователей и аппаратных адресов компьютеров	4	-
12.	Защита от сетевых угроз	Обнаружение атак диссоциации с использованием ОС Linux	4	-
13.	Защита от сетевых угроз	Протокол PPPoE	4	
14.	Защита от сетевых угроз	Технология Network Address Translation	4	
15.	Защита от сетевых угроз	Виртуальные частные сети	2	
		Итого:	34	
		Всего за семестр:	**68**	

*Лабораторные работы приведены в соответствии с лабораторным практикумом, входящим в обучающий стенд DLink

	Курсовая работа (проект) (7-й семестр)		
Название первого раздела	Контрольная точка 1. Раздел проекта 1	10,0	-
Название третьего раздела	Контрольная точка 2. Раздел проекта 2	23,75	-
	Оформление проекта. Защита	-	-
		33,75	**0**

	Рубежный (текущий) и итоговый контроль		

Название второго раздела	Контроль 1 (не предусмотрен)	-	-
Название третьего раздела	Контроль 2 (не предусмотрен)	-	-
	Итоговый контроль (зачет)		
	Итоговый контроль (экзамен)		
		0	**0**
	Всего	**169,75**	**130,85**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1. Раздел 1. Сетевые угрозы

3.1.1 Тема 1. Принципы многоуровневой защиты корпоративной информации. Основы сетевого и межсетевого взаимодействия

Перечень изучаемых вопросов:

Основные положения для планирования безопасности сети

Функции уровней защиты.

Происхождение угроз

Основные причины утечки информации.

Виды утечек информации.

Методические указания к изучению:

1. Основные положения для планирования безопасности сети

Объектами угроз для информационной безопасности могут служить следующие уровни управления КИС:

– централизованное управление всей системой предприятия;
– управление подразделениями;
– управление всей сетью;
– управление конечными пользователями.

2. В соответствии с этим система информационной безопасности КИС должна включать в себя защиту:

– централизованного управления;
– приложений и соответствующих серверов;
– сети;
– конечных пользователей.

3. Для обеспечения санкционированного доступа требуется:

– обеспечение единого механизма доступа;
– создание единой политики безопасности и защиты информации;
– централизация и непрерывный контроль за использованием ресурсов и управления ими.

4. Функции централизованного управления:

– авторизация и управление распределенной информацией в масштабах всего предприятия;

– возможность централизованной аутентификации и управление доступом во всем веб-сервисам в независимости от их платформ;

– управление доступом к персональной информации пользователей;

– централизованное кросс-платформенное управление учетными записями пользователей и информационными ресурсами;

– управление рисками на предприятии, позволяющее системным администраторам контролировать все несанкционированные вторжения на предприятие (в корпоративную сеть).

2. Функции уровней защиты

2.1. Централизованное управление рисками и администрирование системы безопасности:

– централизованное администрирование;

– административный контроль полномочий главным администратором;

– делегирование части полномочий младшим администраторам отдельных ресурсов;

– управление событиями;

– принятие решений по управлению рисками;

– долговременное хранение статистики тревог и вторжений;

– управление атрибутами пользователей (учетными записями) и обслуживание пользователей в распределенных сетях;

– осуществление централизованной аутентификации;

– управление пользовательскими группами, ролями, каталогами, привилегиями пользователей.

2.2. Защита управления приложениями.

– защита доступа к ресурсам приложений;

– установление и контроль связи учетных записей пользователей с различными типами ресурсов (файлами, каталогами, принтерами, приложениями);

– предотвращение неправомочного доступа к информационным ресурсам и критическим сервисам.

2.3. Защита систему сетей:

– защита внутреннего обмена (локальные вычислительные сети, интранет);

– защита межсетевого обмена (глобальные вычислительные сети, экстранет);

– защита обмена через Интернет;

– осуществление распределенной нагрузки для улучшения производительности и восстановления после сбоев.

2.4. Защита конечных пользователей:

– установление авторизации;

– установление правил обращения пользователей с информацией;

– сертификация открытых ключей PKI;

– мониторинг угроз безопасности и отражение их в журналах регистрации;

– контроль соблюдения требований политики секретности.

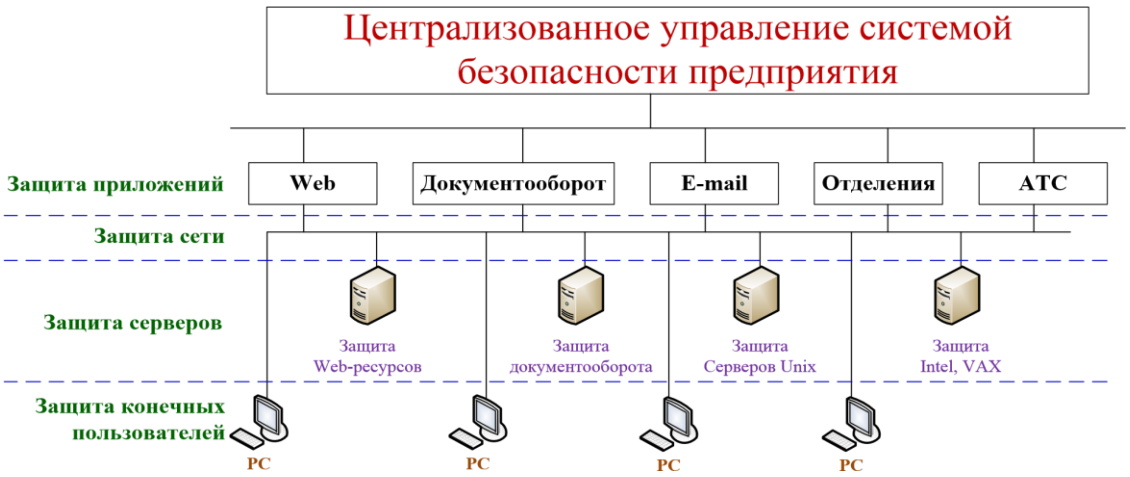

Рисунок 1. Структурная схема системы защиты информации КИС

Современные вычислительные сети организаций – это сложные системы, состоящие из следующих компонентов:

– компьютеры;

– системное и прикладное программное обеспечение (ПО);

– сетевые адаптеры;

– концентраторы;

– коммутаторы;

– маршрутизаторы и соединительные (кабельные) системы.

Корпоративные сети подразделяются на:

– интранет сеть – это сеть на уровне компании, в которой используются программные средства, основанные на стеке протоколов TCP/IP.

– экстранет сеть – это интранет сеть, подключенная к Интернету, с предоставлением доступа к ее ресурсам определенной категории пользователей, наделенной соответствующими полномочиями.

Межсетевое взаимодействие – это взаимодействие двух локальных сетей, при котором они функционируют как самостоятельные единицы объединенной сети.

Взаимодействие сетей – это методы решения, сегментации и объединения локальных сетей таким образом, чтобы общая пропускная способность была как можно выше.

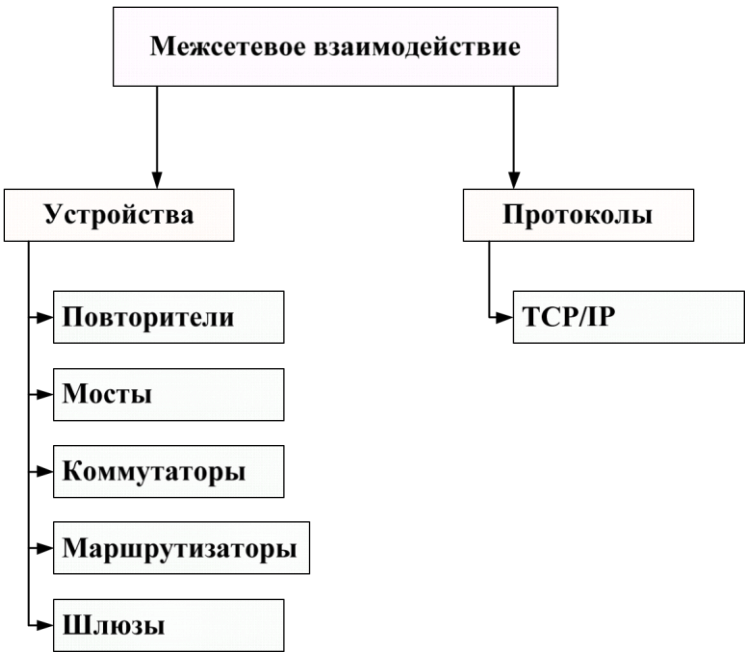

Рисунок 2. Составляющие межсетевого взаимодействия

Совокупность протоколов межсетевого взаимодействия позволяет организовать обмен данными между различными сетями.

Одним из наиболее востребованных наборов протоколов является протокол TCP/IP.

Взаимодействие сетевой инфраструктуры основывается на уровневой структуре модели OSI (Open System Interconnection) – эталонная модель взаимодействия открытых систем (рисунок 3).

Модель OSI используется как при работе сети Интернет, так и в корпоративных сетях.

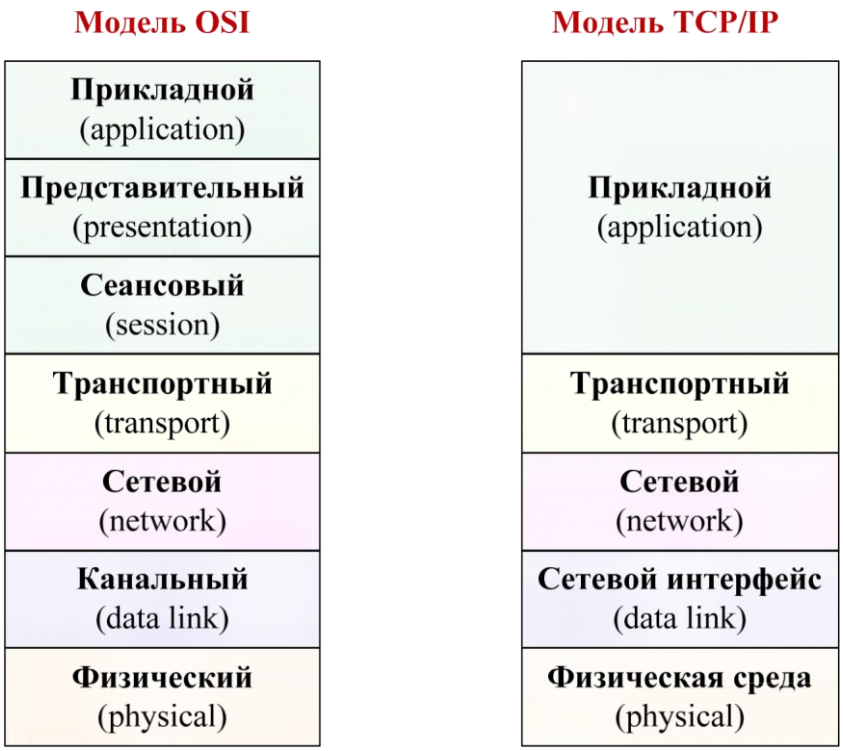

Рисунок 3. Уровневые структуры стеков

Количество инцидентов информационной безопасности (ИБ) тесно связано с количеством обнаруженных уязвимостей.

Уязвимость информационной системы – это любая характеристика, использование которой нарушителем может привести к реализации угрозы.

Угроза информационной системе – это потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы.

Виды угроз – это основополагающий параметр, определяющий целевую направленность защиты информации.

Случайные угрозы – это угрозы, появление которых является спонтанным и не зависящим от воли людей, возникающие в системе обработки данных в процессе ее функционирования, например, отказы, сбои, ошибки, стихийные бедствия и побочные явления.

Таблица 1. Система классификации угроз

Параметры	Значения	Содержание значения
Виды угроз	Физическая целостность	Уничтожение (искажение)
	Логическая структура	Искажение структуры
	Содержание	Несанкционированная модифика-

Параметры	Значения	Содержание значения
		ция
	Конфиденциальность	Несанкционированное получение, утечка информации,
	Право собственности	Присвоение чужого труда
Происхождение угроз	Случайное	Отказы, сбои, ошибки
		Стихийные бедствия
		Побочные явления
	Преднамеренное	Умышленное действие людей
Предпосылки появления угроз	Объективное	Количественная и качественная недостаточность элементов системы
	Субъективное	Промышленный шпионаж
		Недобросовестные сотрудники
		Криминальные элементы
		Службы других государств
Источники угроз	Люди	Пользователи
		Персонал
		Посторонние
	Технические устройства	Регистрации, ввода, обработки, хранения, передачи и выдачи
	Модели, алгоритмы программы	Общего назначения
		Прикладные
		Вспомогательные
	Технологические схемы обработки данных	Ручные, интерактивные, внутри машинные, сетевые

Происхождение угроз:

1. Отказ.
2. Сбой.
3. Ошибка.
4. Побочное явление.
5. Преднамеренное.

Предпосылки появления угроз:

1. Количественная недостаточность – это физическая нехватка одного или нескольких элементов системы обработки данных, вызывающая нарушения технологического процесса и перегрузку имеющихся элементов.

2. Качественная недостаточность – это несовершенство конструкции элементов системы, в силу чего могут появиться возможности для случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию.

3. Промышленный шпионаж – это негласная деятельность организации по добыче информации, специально охраняемой от несанкционированной утечки или похищения, а также по созданию для себя благоприятных условий в целях получения максимальной выгоды.

4. Действия недобросовестных сотрудников – это хищение (копирование), уничтожение информационных массивов и программ вследствие корыстных мотивов.

5. Действия криминальных элементов – это хищение информации или компьютерных программ в целях наживы или разрушения их в интересах конкурентов.

6. Деятельность разведывательных служб иностранных государств – это специально организуемая деятельность государственных органов, профессионально ориентированных на добычу необходимой информации всеми доступными способами и средствами.

Источники угроз:

1. Люди.
2. Технические устройства.
3. Модели, алгоритмы и программы.

Основные причины утечки информации:

− несоблюдение персоналом норм, требований, правил эксплуатации;

− ошибки в проектировании системы и систем защиты;

− введение противостоящей стороной технической и агентурной разведок.

Виды утечек информации:

1. Разглашение информации.
2. Несанкционированный доступ.
3. Получение защищаемой информации разведкой.
4. Канал утечки информации.

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Основные положения для планирования безопасности сети.
2. Функции уровней защиты.
3. Происхождение угроз.
4. Основные причины утечки информации.
5. Виды утечек информации.

3.1.2 Политика безопасности. Структура политики безопасности

Перечень изучаемых вопросов:

Политика безопасности.

Шаблоны политик безопасности.

Сетевая политика безопасности.

Эшелонированная оборона.

Стандарты ISO/IEC 17799:2002 Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Методические указания к изучению:

Политика безопасности. Структура политики безопасности

1. Политика безопасности

Основополагающим элементом защиты является определение политики безопасности защищаемой системы.

Определение политики информационной безопасности сводится к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, в том числе:

− управление доступом к средствам вычислительной техники, программам и данным;

− антивирусная защита;

− вопросы резервного копирования;

− проведение ремонтных и восстановительных работ; − информирование об инцидентах в области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Определение требований к режиму информационной безопасности.

4. Структуризация контрмер по уровням.

5. Определение порядка сертификации на соответствие стандартам в области ИБ.

6. Определение периодичности проведения совещаний по тематике информационной безопасности на уровне руководства, включая периодический

пересмотр положений политики информационной безопасности, а также порядок обучения всех категорий пользователей информационной системы по вопросам информационной безопасности.

Рисунок 4. Разделы политики безопасности организации

Одним из методов пересмотра политики безопасности является аудит информационных систем.

Регламента по срокам жизненного цикла не существует, однако установлена рекомендация, чтобы срок составлял от *шести месяцев до одного года*.

После разработки и внедрения правил безопасности пользователи должны быть ознакомлены с требованиями информационной безопасности, а персонал пройти соответствующее обучение. При возникновении инцидентов работа должна вестись в соответствии с планами.

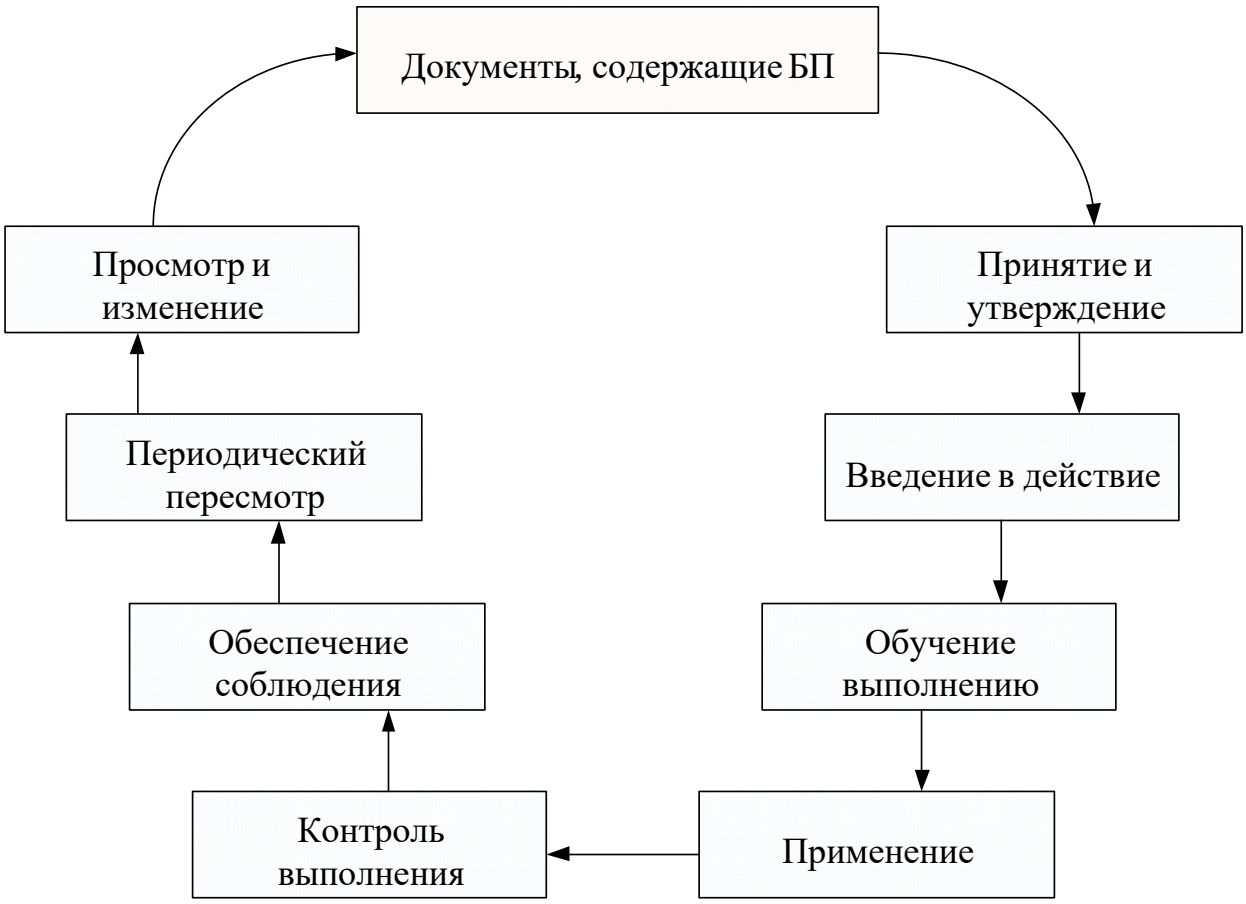

Рисунок 5. Жизненный цикл политики безопасности

2. Шаблоны политик безопасности

Политика безопасности организации – это документ, описывающий специфические требования или правила, которые должны выполняться.

Стандарт – это набор системно-специфических или процедурноспецифических требований, которые должен выполнять каждый пользователь.

Шаблоны политик безопасности

1. *Допустимая политика шифрования* – определяет требования к криптографическим алгоритмам, используемым в организации.

2. *Допустимая политика использования* – определяет использование оборудования и компьютерных служб для защиты пользователей, ресурсов организации и информации.

3. *Антивирусная защита* – определяет основные принципы эффективного уменьшения угрозы компьютерных вирусов для сети организации.

4. *Политика оценки потребностей* – определяет возможности покупок средств защиты организацией и определяет минимальные требования к оценке покупок, выполняемых группой информационной безопасности;

5. *Политика аудита сканирования уязвимостей* – определяет требования и назначает ответственного для сопровождения аудита и оценки риска, чтобы удостовериться в целостности информационных ресурсов, исследовать инци-

денты, устанавливать соответствие политикам безопасности или проводить мониторинг пользовательской и системной активности.

6. *Политика автоматически передаваемой почты* – документирует требования того, что никакая почта не может быть автоматически перенаправлена внешнему источнику без соответствующей санкции менеджера или директора.

7. *Политика кодирования полномочий к базе данных* – определяет требования для безопасного хранения и извлечения имен пользователей и паролей базы данных.

8. *Политика критичной информации* – определяет требования к классификации и безопасности информации организации путем присвоения соответствующих уровней конфиденциальности.

9. *Политика удаленного доступа* – определяет стандарты соединения с сетью организации из любого хоста или сети, являющимися внешними для организации.

10. *Политика оценки риска* – определяет требования и назначает ответственного для идентификации, оценки и уменьшения риска информационной инфраструктуры организации.

11. *Политика безопасности маршрутизатора* – определяет стандарты конфигурации минимальной безопасности для маршрутизаторов и коммутаторов внутри сети организации.

12. *Политика безопасности сервера* – определяет стандарты конфигурации минимальной безопасности для серверов внутри сети организации.

13. *Политика безопасности VPN* – определяет требования для удаленного доступа IPSec или L2TP VPN соединений с сетью организации.

14. *Политика безопасных соединений* – определяет стандарты для беспроводных систем, используемых для соединения с сетью организации.

Для обеспечения безопасности межсетевого взаимодействия особую роль играет сетевая политика безопасности.

3. Сетевая политика безопасности

При задании сетевой политики безопасности необходимо определить процедуры защиты своей сети, ее содержимого и пользователей от ущерба и потерь.

Сетевая безопасность концентрируется на контроле сетевого трафика и его использования. Она определяет сетевые ресурсы и угрозы, использование и возможности сети, а также детальные планы и действия при нарушении политики безопасности.

При применении сетевой политики безопасности необходимо установить уровни безопасности сетевых параметров, которые позволят осуществить множественный контроль безопасности сетевого трафика.

Сетевые параметры применяются к:

− защищаемые компьютеры;

− защищаемые сети;

− защищаемые механизмы (межсетевой экран).

Межсетевой экран должен являться шлюзом для всех соединений между доверенными сетями и *неизвестными*.

Маршрутизатор используется для разделения своей сети от провайдера интернета.

Внутренний сетевой периметр – это дополнительная граница, в которой размещаются другие механизмы безопасности:

− межсетевые экраны;

− фильтрующие маршрутизаторы

Расположение межсетевого экрана между внутренним и внешним маршрутизатором дает наибольшую дополнительную защиту от атак с обеих сторон, но значительно уменьшает трафик, который должен исследовать межсетевой экран, так как ему не нужно просматривать пакеты, циркулирующие внутри сети.

Внешний сетевой периметр включает в себя:

− маршрутизаторы;

− межсетевой экран;

− общедоступные Интернет-серверы (HTTP, FTP, e-mail).

Использование нескольких внутренних межсетевых экранов позволяет ограничить доступ к совместно используемым внутренним ресурсам сети.

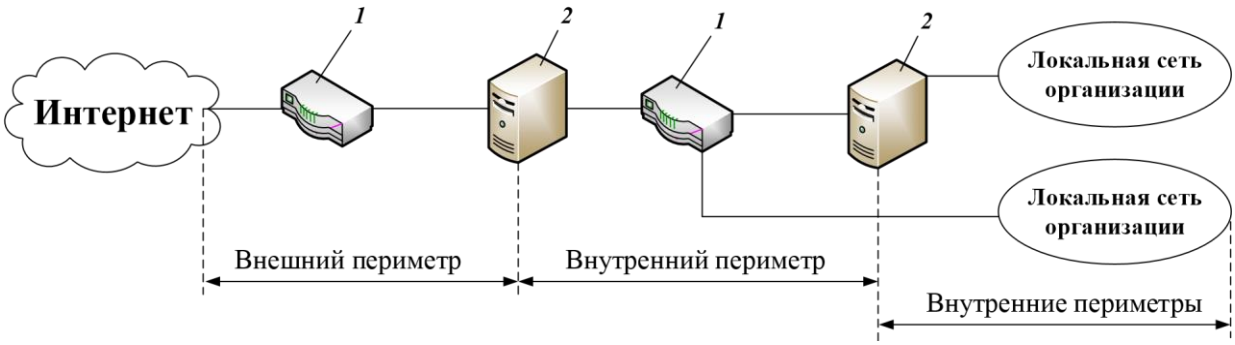

Рисунок 6. Множество внутренних сетевых параметров:
1 – маршрутизатор; *2* – межсетевой экран

Доверенными сетями являются сети внутри сетевого периметра безопасности.

Специалисты организации должны обладать полным сетевым контролем доверенных сетей.

Область внешнего сетевого периметра является демилитаризованной.

Демилитаризованная зона (DMZ) – область, в которой возможно использовать один либо несколько *адресов IP* или *портов* с настройками сетевого экрана. Она является незащищенной часть локальной сети.

В данной зоне располагаются: Proxy-сервера, Web-, почтовые ресурсы и т. д.

Локальная внутренняя сеть отделена от демилитаризованной зоны и защищена сетевым экраном.

Политикой сетевого подключения должны быть определены типы устройств, разрешенные для подключения к сети, настройки систем, которые могут быть подключены к сети.

Разделы политики сетевого подключения.

− описание процесса установки и настройки операционной системы и приложений, а также их функциональных возможностей, которые разрешено использовать;

− местоположение в сети (физической подсети) систем определенного типа и процедура разрешения вопросов адресации в сети;

− требования по установке и регулярном обновлении антивирусного программного обеспечения;

− описание настройки прав пользователей и защиты ресурсов, обеспечиваемых операционной системой;

− процедуры для создания новой учетной записи пользователя, и аналогичные процедуры для ее удаления;

− запрет на установку дополнительных аппаратных или программных компонентов без одобрения сетевого администратора. −

4 Эшелонированная оборона

Эшелонированная оборона – это стратегия достижения информационной гарантии в сетевом оборудовании, то есть обеспечение баланса между средствами защиты и стоимостью, производительностью и функциональными характеристиками.

Баланс компонентов информационной гарантии.

1. Персонал – распределение ролей персонала по работе с защищаемой информацией и определение мер ответственности за ее утрату;

2. Технология – настройка политики безопасности, архитектуры, стандартов системного уровня, критериев выбора необходимых продуктов, конфигурации компонентов систем, оценка рисков.

3. Функциональные операции:

3.1. Разработка, установка и поддержание политики безопасности.

3.2. Проверка и сертификация изменений в используемых информационных технологиях.

3.3. Управление установленными средствами обеспечения безопасности.

3.4. Контроль и реакция на текущие угрозы.

3.5. Обнаружение атак и защита от них.

3.6. Процедуры восстановления и перестановки компонент информационных технологий.

Принципы информационной гарантии

− применение защиты в различных точках;

− защитных механизмов между злоумышленником и целью;

− оценка защитных возможностей каждого компонента;

Применение инфраструктуры обнаружения атак и вторжений, использование методов и средств анализа и корреляции получаемых результатов.

Контрольные вопросы:

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Охарактеризуйте методы защиты ПО от несанкционированного использования.
2. Охарактеризуйте методы, используемые нападающими для проникновения в интернет-сети. Приведите ошибки в программном обеспечении.
3. Приведите классификации программных средств защиты.
4. Охарактеризуйте классификации, категории ФСТЭК уязвимости системных утилит, команд и сетевых служб.

3.1.3 Тема 1.3 Симметричные и ассиметричные системы шифрования. Функции хеширования. Электронная подпись

Перечень изучаемых вопросов:

Основные понятия криптографической защиты информации.
Симметричные криптосистемы шифрования.
Алгоритмы шифрования DES и 3-DES.
Стандарт шифрования ГОСТ 28147-89.
Асимметричные криптосистемы шифрования.
Функция хеширования.
Отечественный стандарт хеширования ГОСТ З 34.11-94.
Электронная подпись.

Методические указания к изучению:

Требуется обратить внимание на:

1. Основные понятия криптографической защиты информации.
2. Симметричные криптосистемы шифрования.
3. Алгоритмы шифрования DES и 3-DES.

4. Стандарт шифрования ГОСТ 28147-89
5. Асимметричные криптосистемы шифрования
6. Функция хеширования
7. Отечественный стандарт хеширования ГОСТ З 34.11-94
8. Электронная подпись
9. Управление крипто ключами и открытыми ключами PKI
10. Сертификаты открытых ключей

1. Основные понятия криптографической защиты информации

Функции обеспечения безопасности

– защита конфиденциальности передаваемых или хранимых в памяти данных;

– подтверждение целостности и подлинности данных;

– аутентификация абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются:

– криптографические технологии шифрования,

– цифровая подпись; □ аутентификация.

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

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

Основой большинства криптографических средств защиты информации является шифрование данных.

Шифрование данных – это совокупность процедур и правил криптографических преобразований, используемых для шифрования и расшифрования информации по ключу шифрования.

Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования E_{k1} с получением в результате *шифротекста C*.

Шифротекст C является криптограммой и содержит исходную информацию M в полном объеме. Последовательность знаков в криптограмме внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования k1.

Ключ шифрования должен принадлежать конкретному пользователю и быть уникальным.

− *бесключевые КА* – не используют в вычислениях ключи;

− *одноключевые КА* – работают с одним ключевым параметром (секретным ключом);

− *двухключевые КА* – на различных стадиях работы в них применяется два ключевых параметра: секретный и открытые ключи.

Хэширование – это метод криптозащиты, представляющий собой контрольное преобразование информации. Из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хэшзначение фиксированной длинны, однозначно соответствующее исходным данным.

Симметричное шифрование использует один и тот же ключ как для зашифрования, так и для расшифрования информации.

Блочное шифрование – это процесс, при котором информация предварительно разбивается на блоки фиксированной длины (64 или 128 бит). Блоки могут шифроваться как независимо друг от друга, так и «со сцеплением».

Поточное шифрование – это процесс при котором информацию невозможно разбить на блоки, шифрование происходит поблочно или посимвольно.

Асимметричное шифрование – характеризуется применением двух типов ключей: открытого – для зашифрования информации и секретного – для ее расшифрования.

Электронная цифровая подпись (ЭЦП) используется для подтверждения целостности и авторства данных.

2. Симметричные криптосистемы шифрования

В симметричной криптосистеме шифрования используется один и тоже ключ для зашифрования и расшифрования информации. Ключ шифрования должен быть доступен только тем, кому предназначено сообщение.

Целостность данных обеспечивается присоединением к передаваемым данным специального кода (имитоприставки), вырабатываемого по секретному ключу. Имитовставка является разновидностью контрольной суммы, т.е. эталонной характеристики сообщения, по которой проверяется целостность сообщения.

Проверка целостности сообщения выполняется получателем сообщения, путем выработки по *секретному ключу имитовставки*, соответствующей полученному сообщению и ее сравнения с полученным значением имитовставки.

При совпадении делается вывод, что информация *не была модифицирована* на пути от отправителя к получателю.

3. Алгоритмы шифрования DES и 3-DES

Алгоритм DES осуществляет шифрование 64-битных блоков данных с помощью 64-битного ключа, в котором значащими являются 56 бит, а остальные 8 бит являются проверочными для контроля на четность.

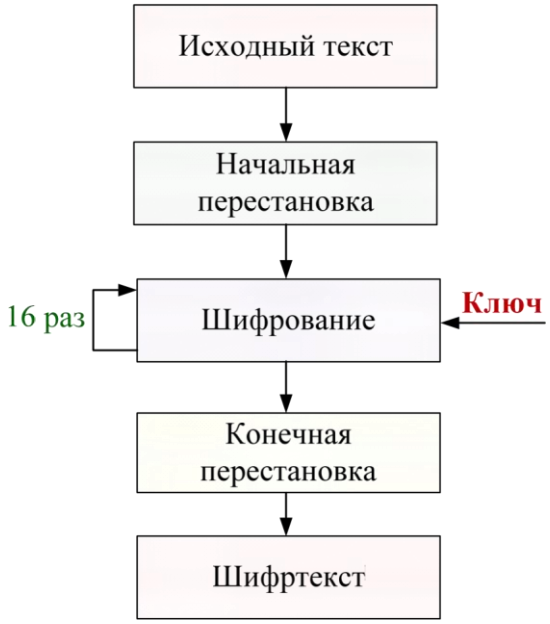

Рисунок 7. Обобщенная схема шифрования в алгоритме DES

Процесс шифрования заключается в начальной перестановке битов 64битного блока, шестнадцати циклах шифрования и в итоге в конечной перестановке битов.

Ключ шифра DES имеет 2^{56} возможных значений.

Для того, чтобы повысить качество шифрования DES был реализован алгоритм многократного шифрования с разными ключами для шифрования одного и того же блока открытого текста.

Для этого требуется шифрование открытого текста P три раза с помощью двух ключей K_1 и K_2. симметричного шифрования с двумя различными ключами

Блок открытого текста P сначала шифруется ключом K_1, затем расшифровывается ключом K_2 и окончательно зашифровывается ключом K_1.

Введение в данную систему операции расшифрования $D_{к2}$ позволяет обеспечить совместимость этой системы со схемой однократного использования блочного кода.

4. Стандарт шифрования ГОСТ 28147-89

Данный алгоритм представляет собой 64-битный блочный алгоритм с 256-битным ключом.

Данные, подлежащие зашифрованную, разбивают на 64-разрядные блоки, а они разбиваются на два субблока N1 и N2 по 32 бит.

Субблок N1 складывается по модулю 2 (исключающее ИЛИ), затем субблоки меняются местами. Данное преобразование выполняется 16 или 32 раза.

В каждом раунде выполняются две операции:

Первая операция – наложение ключа. Содержимое субблока N1 складывается по модулю 2^{32} с 32-битной частью ключа K_x. Полный ключ шифрования представляется в виде 32-битных ключей: K0, K1, K2, K3, K4, K5, K6, K7.

В процессе шифрования используется один из этих ключей в зависимости от номера раунда и режима работы алгоритма.

Вторая операция – табличная замена. После наложения ключа субблок N1разбивается на 8 частей по 4 бита, значения каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитный циклический сдвиг субблока влево на 11 бит.

5. Асимметричные криптосистемы шифрования

Для шифрования информации и ее последующего расшифрования в ассиметричных криптографических системах используются различные ключи:

− *открытый ключ K:* используется для шифрования информации, вычисляется из секретного ключа k;

− *секретный ключ k:* используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа K.

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

Для криптографического закрытия и последующего расшифрования передаваемой информации используются открытый и секретный ключи получателя B. В качестве ключа зашифрования должен использоваться открытый ключ получателя, а в качестве расшифрования – его секретный ключ.

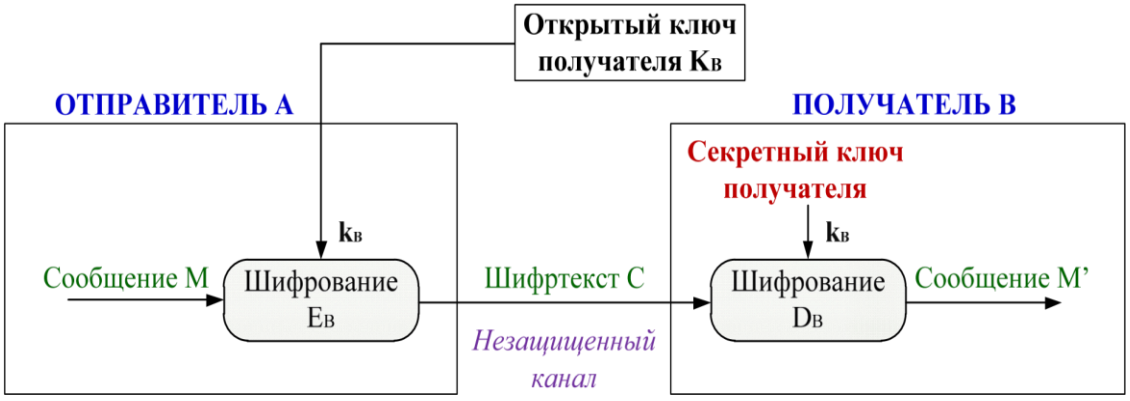

Рисунок 8. Обобщенная схема ассиметричной криптосистемы шифрования

Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у него владельца, он должен быть надежно защищен от несанкционированного доступа. Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

6. Функция хеширования

Функция хеширования (хэш-функция) – это процесс преобразования, на вход которого подается сообщение переменной длинны M, а выходом является строка фиксированной длины h(M).

Хэш-значение h(M) – это дайджест сообщения M, т. е. сжатое двоичное представление основного сообщения M произвольной длины. Хэш-значение h(M) формируется функцией хеширования.

Одним из свойств хеширования является чувствительность к возможным изменениям в тексте M, таким как вставки, удаления, перестановки.

Хэш-функция должна быть однонаправленной, т. е. обладать свойством необратимости.

7. Отечественный стандарт хеширования ГОСТ Э 34.11-94

Данный стандарт является обязательным для применения в качестве алгоритма хеширования в государственных организациях РФ и ряде коммерческих организаций.

Алгоритм шифрования.

Шаг 1. Инициализация регистра хэш-значения. Если длина сообщения не превышает 256 бит – переход к *шагу 3*, если превышает, переход к *шагу 2*.

Шаг 2. Итеративное вычисление хэш-значения блоков хэшируемых данных по 256 бит с использованием хранящегося в регистре хэш-значения предыдущего блока.

− Генерация ключей шифрования на основе блока хэшируемых данных;

− Зашифрование, хранящегося в регистре хэш-значения в виде четырех блоков по 64 бит по алгоритму ГОСТ 28147-89 в режиме простой замены; − Перемещение результата.

Вычисление производиться до тех пор, пока длинна необработанных входных данных не станет меньше или равной 256 бит. В этом случае выполняется переход к *шагу три*.

Шаг 3. Дополнение битными нулями необработанной части сообщения до 256 бит. Вычисление хэш-значения аналогично *шагу 2*. В результате в регистре оказывается искомое хэш-значение.

Рисунок 9. Хеширование по алгоритму ГОСТ Э 34.11-94

8. Электронная подпись

Электронная подпись (ЭП) используется для аутентификации текстов, передаваемых по телекоммуникационным каналам.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий.

Процедура формирования подписи

На подготовительном этапе абонент А – отправитель сообщения – генерирует пару ключей: секретный ключ k_A и открытый ключ K_A.

Открытый ключ K_A рассылается остальным абонентам сети для использования при проверке подписи.

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

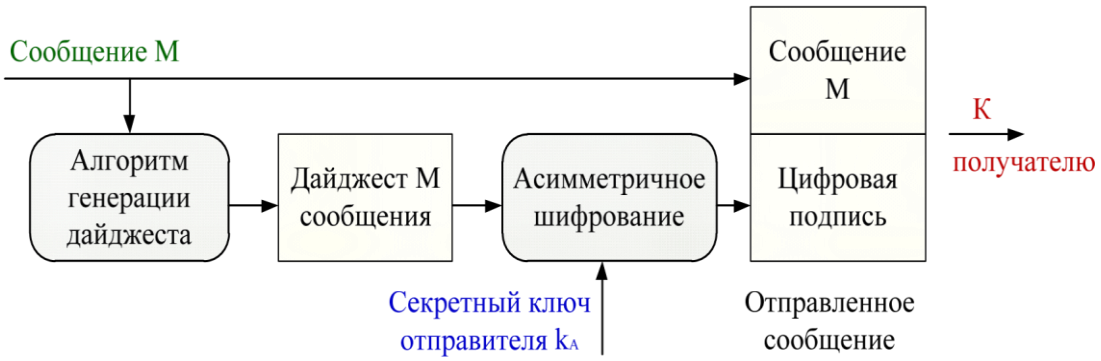

Рисунок 10. Схема формирования ЭП

Хэш-функция служит для сжатия исходного подписываемого текста М в дайджест m. Отправитель А шифрует дайджест m своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста М.

Процедура проверки подписи

Абоненты сети могут проверить подпись полученного сообщения М с помощью открытого ключа отправителя K_A этого сообщения.

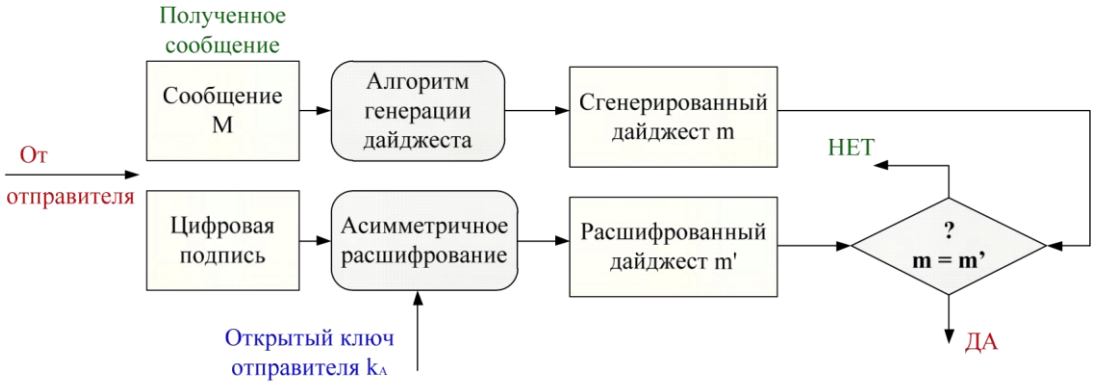

Рисунок 11. Схема проверки ЭП

При проверке ЭП абонент В – получатель сообщения М – расшифровывает принятый дайджест m открытым ключом K_A отправителя А.

Получатель вычисляет с помощью хэш-функции h(M) дайджест m’ принятого сообщения М и сравнивает его с расшифрованным. Если два дайджеста m и m’ совпадают, то подпись является подлинной. В противном случае либо подпись подделана, либо изменено

Управление крипто ключами и открытыми ключами PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) предназначена для надежного обмена информацией с помощью цепочки доверительных отношений. Инфраструктура открытых ключей PKI основывается на цифровых сертификатах, связывающим индивидуальный секретный ключ пользователя с его открытым ключом.

1. Защита от атаки «человек-в-середине»

При осуществлении атаки «человек-в-середине» атакующий может незаметно подменить передаваемые по открытому каналу открытые ключи законных участников взаимодействия на свой открытый ключ, создать разделяемые секреты с каждым из законных участников и затем перехватывать, и расшифровывать все их сообщения.

Два пользователя *i* и *j*, каждый из которых имеет по паре ключей, при этом у пользователя *j* есть открытый ключ *Kpi* для проверки ЭЦП пользователя *i*. Можно предположить, что злоумышленник может перехватить этот ключ *Kpi* в процессе его передачи от пользователя *i* пользователю *j* или получить доступ к этому ключу, хранящемуся у пользователя *j*.

Злоумышленник считает из ключа реквизиты (например, фамилию владельца, место работы и т. д.) и создаст свою пару ключей, *Ksi'* и *Kpi'*, в которые запишет известные ему реквизиты пользователя *i*. Затем он подменит посланный пользователю *j* открытый ключ *Kpi* своим фальшивым открытым ключом *Kpi'*, имеющим реквизиты пользователя *i*.

Любое сообщение злоумышленник будет подписывать своим секретным ключом *Ksi'* (для пользователя *j* эта подпись выглядит так, как если бы она бы-

ла поставлена пользователем *i*). Подпись такого сообщения, проверяемая пользователем *j*, будет верна, поскольку ему был послан фальшивый ключ *Kpi'*, парный столь же фальшивому ключу *Ksi'*.

Подмена открытого ключа раскроется только после того, как настоящий пользователь *i* пошлет пользователю *j* сообщение, подписанное истинным ключом *Ksi*. Но ситуация может находиться под контролем злоумышленника достаточно долго, тем более что он вполне может заранее оценить необходимое время сеансов связи, проанализировав интенсивность документооборота между пользователями *i* и *j*, а также рассчитать время, в течение которого подмена ключа не будет обнаружена. Проблема также существенно усугубляется, если злоумышленник имеет техническую возможность перехватывать сообщения, посылаемые пользователем *i* пользователю *j*.

Устранить данную угрозу можно с помощью использования сертификатов открытых ключей.

2. Сертификаты открытых ключей

Основное назначение – сделать доступным и достоверным открытый ключ пользователя.

В основу формирования сертификатов открытых ключей положены принципы строгой аутентификации, рекомендованные стандартом X.509 и базирующиеся на свойствах криптосистем с открытым ключом.

Криптосистемы с открытым ключом предполагают наличие у пользователя парных ключей – секретного и открытого (общедоступного). Каждый пользователь идентифицируется с помощью своего секретного ключа. С помощью парного открытого ключа любой другой пользователь имеет возможность определить, является ли его партнер по связи подлинным владельцем секретного ключа.

Процедура, позволяющая каждому пользователю устанавливать однозначное и достоверное соответствие между открытым ключом и его владельцем, обеспечивается с помощью механизма сертификации открытых ключей.

Степень достоверности факта установления подлинности (аутентификации) пользователя зависит от надежности хранения секретного ключа и надежности источника поставки открытых ключей пользователей. Чтобы пользователь мог доверять процессу аутентификации, он должен извлекать открытый ключ другого пользователя из надежного источника, которому он доверяет.

Таким источником согласно стандарту, X.509 является центр сертификации CA (Certification Authority).

Центр сертификации CA является доверенной третьей стороной, которая обеспечивает аутентификацию открытых ключей, содержащихся в сертификатах. CA имеет собственную пару ключей (открытый/секретный), где секретный ключ CA используется для подписывания сертификатов, а открытый ключ CA публикуется и применяется пользователями для проверки подлинности открытого ключа, содержащегося в сертификате.

Сертификация открытого ключа – это подтверждение подлинности открытого ключа и хранимой совместно с ним служебной информации, в частности о принадлежности ключа. Сертификация ключа выполняется путем вычисления ЭЦП сертифицируемого ключа и служебной информации с помощью специального секретного ключа-сертификата, доступного только центру сертификации CA. Сертификация открытого ключа – это подписывание открытого ключа электронной подписью, вычисленной на секретном ключе центра сертификации.

Открытый ключ совместно с сертифицирующей его ЭЦП часто называют сертификатом открытого ключа или просто сертификатом.

Открытый ключ сертификационного центра (парный секретному, на котором проводится сертификация других открытых ключей) используется для проверки целостности сертифицированных открытых ключей. Его обычно называют ключом-сертификатом.

Центр сертификации CA формирует сертификат открытого ключа пользователя путем заверения цифровой подписью CA определенного набора данных.

В соответствии с форматом X.509 в этот набор данных включаются:

– период действия открытого ключа, состоящий из двух дат: начала и конца периода;

– номер и серия ключа;

– уникальное имя пользователя;

– информация об открытом ключе пользователя: идентификатор алгоритма, для которого предназначен данный ключ, и собственно открытый ключ; ЭЦП и информация, используемая при проведении процедуры проверки ЭЦП (например, идентификатор алгоритма генерации ЭЦП); уникальное имя сертификационного центра.

5. Таким образом, цифровой сертификат содержит три главные составляющие:

– информацию о пользователе-владельце сертификата;

– открытый ключ пользователя;

– сертифицирующую ЭЦП двух предыдущих составляющих, вычисленную на секретном ключе CA.

– Сертификат открытого ключа обладает следующими свойствами:

– каждый пользователь, имеющий доступ к открытому ключу центра сертификации CA, может извлечь открытый ключ, включенный в сертификат;

– ни одна сторона, помимо центра сертификации, не может изменить сертификат так, чтобы это не было обнаружено (сертификаты нельзя подделать).

Так как сертификаты не могут быть подделаны, их можно опубликовать, поместив в общедоступный справочник и не предпринимая специальных усилий по их защите.

Создание сертификата открытого ключа начинается с создания пары ключей (открытый/секретный).

1. CA создает пару ключей. Открытый ключ заносится в сертификат, а парный ему секретный ключ передается пользователю с обеспечением аутентификации пользователя и конфиденциальности передачи ключа.

2. Пользователь сам создает пару ключей. Секретный ключ сохраняется у пользователя, а открытый ключ передается по защищенному каналу в CA.

Каждый пользователь может быть владельцем одного или нескольких сертификатов, сформированных сертификационным центром CA пользователя. Пользователь может владеть сертификатами, полученными из нескольких разных сертификационных центров.

3. Логическая структура и компоненты PKI

Инфраструктура открытых ключей PKI (Public Key Infrastructure) – это набор программных агентов и правил, предназначенных для управления ключами, политикой безопасности и собственно обменом защищенными сообщениями.

Основными задачами PKI являются:

– поддержка жизненного цикла цифровых ключей и сертификатов (то есть генерация ключей, создание и подпись сертификатов, их распределение и пр.);

– регистрация фактов компрометации и публикация черных списков отозванных сертификатов;

– поддержка процессов идентификации и аутентификации пользователей таким образом, чтобы сократить по возможности время допуска каждого пользователя в систему;

– реализация механизма интеграции (основанного на PKI) существующих приложений и всех компонентов подсистемы безопасности;

– предоставление возможности использования единственного токена безопасности, единообразного для всех пользователей и приложений и содержащего все необходимые ключевые компоненты и сертификаты.

Токен безопасности – это индивидуальное средство безопасности, определяющее все права и окружение пользователя в системе, например, USB-ключ или смарт-карта.

Для предоставления удаленного доступа мобильным пользователям центр управления должен допускать подключение компьютеров, IP-адрес которых ему заранее неизвестен. Участники информационного обмена опознаются по их криптографическим сертификатам. Так как криптографический сертификат пользователя является должен соответствовать стандарту X.509.

Концепция инфраструктуры открытых ключей PKI подразумевает, что все сертификаты конкретной PKI (своя PKI может быть у любой организации или организационной единицы) организованы в иерархическую структуру.

Иерархическая схема PKI предусматривает существование четырех типов сертификатов:

1. Сертификат конечного пользователя.

2. Сертификат CA. Должен быть доступен для проверки ЭЦП сертификата конечного пользователя и подписан секретным ключом CA верхнего уровня, причем эта ЭЦП также должна проверяться, для чего должен быть доступен сертификат CA верхнего уровня, и т. д.

3. Самоподписанный сертификат. Является корневым для всей PKI и доверенным по определению. Если в результате проверки цепочки сертификатов CA выяснится, что один из них подписан корневым секретным ключом, тогда процесс проверки ЭЦП сертификатов заканчивается.

4. Кросс-сертификат. Кросс-сертификаты позволяют расширить действие конкретной PKI путем взаимоподписания корневых сертификатов двух разных PKI.

Процедура проверки ЭЦП электронного документа:

- проверяется ЭЦП конкретного документа;
- проверяется ЭЦП сертификата, с помощью которого проверялась предыдущая ЭЦП. Последняя проверка повторяется в цикле до тех пор, пока цепочка сертификатов не приведет к корневому.

ЭЦП документа признается верной лишь в том случае, если верна не только она, но и все проверяемые в данном процессе ЭЦП сертификатов. При обнаружении неверной ЭЦП любого из сертификатов неверными считаются все ЭЦП, проверенные на предыдущих шагах.

Компоненты этой структуры имеют следующее назначение:

Каталог сертификатов – общедоступное хранилище сертификатов пользователей. Доступ к сертификатам производится обычно по стандартизованному протоколу доступа к каталогам LDAP.

Центр регистрации RA – организационная единица, назначение которой - регистрация пользователей системы.

Пользователь – владелец какого-либо сертификата (такой пользователь подлежит регистрации) или любой пользователь, запрашивающий сертификат, хранящийся в каталоге сертификатов.

Центр сертификации CA – организационная единица, назначение которой – сертификация открытых ключей пользователей (здесь из открытого ключа получается сертификат формата X.509) и их опубликование в каталоге сертификатов.

Схема работы центра сертификации CA:

– CA генерирует собственные ключи и формирует сертификаты CA, предназначенные для проверки сертификатов пользователей;

– пользователи формируют запросы на сертификацию и доставляют их

– CA тем или иным способом;

– CA на основе запросов пользователей формирует сертификаты пользователей;

– CA формирует и периодически обновляет списки отмененных сертификатов CRL (Certificate Revocation List);

– сертификаты пользователей, сертификаты CA и списки отмены CRL публикуются CA (рассылаются пользователям либо помещаются в общедоступный справочник).

Функции, выполняемые PKI в целом, можно условно разделить на несколько групп:

- функции управления сертификатами;
- функции управления ключами;
- дополнительные функции (службы).

Дополнительные компоненты, входящие в состав системы управления инфраструктурой открытых ключей:

- модули интеграции – программные агенты для прикладных и клиентских систем, программные интерфейсы к сетевым приложениям и вебсервисам;
- средства хранения ключевой информации и сертификатов пользователя – аппаратные токены, смарт-карты, USB-ключи.
- служба каталога может служить доверенным источником информации о сертификатах других участниках криптографического обмена.
- состав физической системы управления инфраструктурой открытых ключей:
- корневой узел в составе центра сертификации, хранилища сертификатов (служба каталогов) и средств администрирования;
- периферийный узел, включающий центр регистрации, используется при географической распределенности подразделений организации и большом количестве пользователей;
- клиентские станции с необходимыми программными компонентами.

Изолированный корневой удостоверяющий центр издает сертификаты только для нижестоящих УЦ. Применение изолированного корневого УЦ позволяет уменьшить риск компрометации всей инфраструктуры открытых ключей в случае успешной атаки на УЦ.

Издающий удостоверяющий центр в данном решении интегрирован в среду MS Active Directory, что позволяет ему автоматически публиковать списки отозванных сертификатов в службе каталога, а также автоматически обслуживать клиентов Active Directory

Контрольные вопросы:

1. Функционирование сканирование карты сети.
2. Принципы SYN-бомбардировки.
3. Приведите порядок реализации спуффинга.

3.1.4 Тема 1.4 Идентификация, аутентификация и управление доступом. Управление доступом по схеме однократного входа с авторизацией Single Sign-On

Перечень изучаемых вопросов:

1. Общие сведения об аутентификации.
2. Парольная аутентификация.
3. Аутентификация на основе открытого пароля.
4. Аутентификация на основе хешированного пароля.
5. Парольные политики.
6. Недостатки методов аутентификации с запоминаемым паролем.
7. Простая система однократного входа Single Sign-On.

Методические указания к изучению:

Требуется обратить внимание на:

Процесс регистрации пользователя в любой системе состоит из трех взаимосвязанных, последовательно выполняемых процедур:

− идентификации; − аутентификацией; − авторизации.

Идентификация – это процедура распознавания субъекта по его идентификатору.

В процессе регистрации субъект объединяет свой идентификатор системе, которая проверяет его наличие в базе данных. Субъект, с известным в системе идентификатором, считается легальным (законными), остальные относятся к нелегальным.

Аутентификация – это процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.

Для этого он должен потвердеть факт обладания некоторой информацией, которая может быть доступна только ему.

Авторизация – это процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации.

Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

Администрирование – это процесс управления доступом к ресурсам системы.

Процесс администрирование включает:

− создание идентификатора субъекта (учетной записи пользователя) в системе;

− управление данными субъекта, используемыми для его аутентификации (смена пароля, создание сертификата и т. д.);

− управление правами доступа субъекта к ресурсам системы.

Аудит – это процесс контроля (мониторинга) доступа субъектов к ресурсам системы, включающий протоколирование действий субъектов при их доступе к ресурсам системы в целях обнаружения несанкционированных действий.

Общие сведения об аутентификации

1. Задачи аутентификации

Элементы аутентификации

− *Субъект доступа* – это конкретный человек или процесс, который должен проходить аутентификацию;

− *Идентификатор* – это опознавательный знак, выделяющий субъекта среди других.

− *Аутентификатор* – отличительная характеристика, подтверждающая принадлежность идентификатора субъекту доступа.

− *Администратор* – владелец системы, который несет ответственность за использование системы, и в разграничении авторизованных пользователей и остальных полагается на механизм аутентификации.

− *Механизм аутентификации*, который позволяет проверить присутствие отличительной характеристики.

Механизм управления доступом – это процесс, в котором субъект, при успешном прохождении аутентификации, получает некоторые права (привилегии), а при неудачном лишается их.

В вычислительной системе целью владельца системы является предоставление доступа только авторизованных (законным) пользователям.

Процесс аутентификации позволяет потвердеть подлинность имени пользователя, а управление доступом, осуществляется путем сравнения имени пользователя с правами доступа, связанными с конкретным файлом или другим ресурсом.

2. Факторы аутентификации

Фактор аутентификации – это определенный вид информации, предоставляемый субъектом системе при его аутентификации.

Таблица 2. Факторы аутентификации

Фактор аутентификации	Параметры
На основе знания чего-либо	- пароль или парольная фаза; - PIN-Код (Personal Identification Number)
На основе обладания чем-либо	- физический ключ; - карта с магнитной полосой; - OTP-Токен, генерирующий одноразовый пароль
На основе биометрических характеристик	- отпечаток пальцы; - рисунок сетчатки глаза; - голос

На основе места проверки процедуры	- строго определенное помещение; - строго определенный компьютер со статическим IP; - строго определенное время

3. Парольная аутентификация

Парольная аутентификация – это аутентификация на основе обладания неким секретным знанием.

3.1. Аутентификация на основе открытого пароля

Сервер База данных Пользователь Рабочая станция

Рисунок 12. Аутентификация на основе открытого пароля

3.2. Аутентификация на основе хешированного пароля

Однонаправленные хеш-функции – это функции, которые принимают на входе строку переменной длины и преобразуют ее в выходную строку фиксированной (обычно меньшей) длины.

Сервер База данных

ПользовательРабочая станция

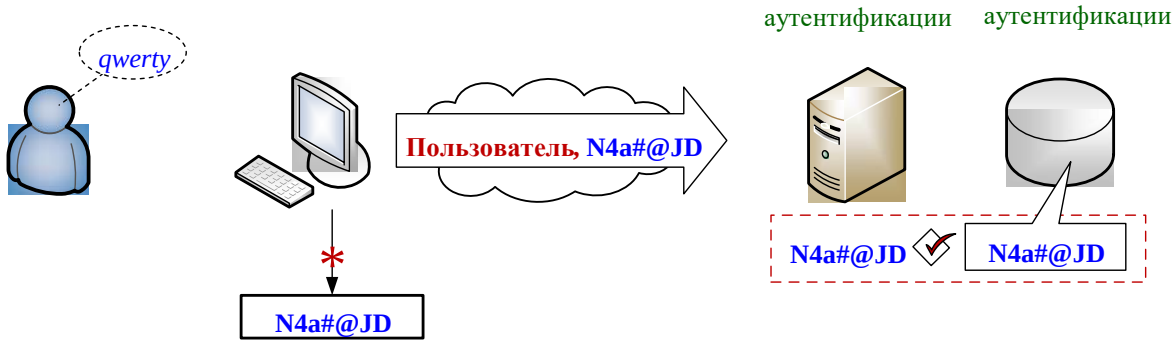

Рисунок 13. Аутентификация на основе хешированного пароля

Основным свойством однонаправленных хеш-функций является невозможность восстановления исходной информации при обладании полученным из нее хеш-значением.

Восстановить открытое значение пароля из файла паролей, где он храниться в виде хеш-значения, практически невозможно.

4. Аутентификация на основе PIN-кода

PIN-код – это разновидность пароля, обычно используемом для аутентификации в локальном устройстве.

Область применения PIN-кода:

− В локальном устройстве, в котором осуществляется аутентификация, с помощью PIN-кода, имеется интерфейс для пользователя, а не для программ.

Никто не может ввести PIN-код, не используя клавиатуру данного устройства.

− PIN-код не передается по сети и не может быть перехвачен.

5. Парольные политики

1. Политика паролей для администраторов со строгими параметрами.

Например, наименьшая длинна пароля – 12 знаков, максимальный срок действия пароля – 28 дней, включены требования сложности: Пароль должен содержать не менее *x* символов; пароль не может повторять ни один из *x* предыдущих паролей; должен состоять из заглавных букв, цифр или знаков пунктуации; не должен включать имя учетной записи или полное имя пользователя.

2. Политика паролей для пользователей.

Например, наименьшая длинна пароля – 6 знаков, максимальный срок действия – 90 дней, требования сложности отключены.

3. Политика паролей учетных записей служб с наименьшей длинной пароля 32 знака и включенными требованиями сложности.

Недостатки методов аутентификации с запоминаемым паролем

Таблица 3. Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
Кража парольного файла	Хэширование пароля
Атака со словарем	Безопасность доступа к файлу; Хеширование с шумами (помехами); Правила формата паролей
Подбор пароля	Правила формата паролей; Автоматическое блокирование
Социотехника	Политика несанкционированных паролей; Политика смены паролей

Принуждение	Сигнал о принуждении
Троянский конь	Особый режим интерактивного взаимодействия для механизма аутентификации; Антивирусное ПО; Средства обеспечения контроля целостности файлов
Аппаратный сниффер клавиатуры	Безопасность рабочих помещений; Безопасность рабочих мест
Регистрация излучения	Не отображение пароля Безопасность излучений
Анализ сетевого трафика	Шифрование Одноразовые пароли

7. Аутентификация с помощью биометрических характеристик

Биометрическая характеристика — это измеримая физиологическая или поведенческая черта живого человека, которую можно использовать для установления личности или проверки декларируемых личных данных.

Работа биометрической системы основана на предоставление *пользователем образца* – опознаваемое, необработанное изображение или запись физиологической, или поведенческой характеристики.

К физиологическим биометрическим характеристикам относят:

4. Радужную оболочку глаза.
5. Отпечаток пальца.
6. Лицо.
7. Кисть.
8. Сетчатку.

К поведенческим биометрическим характеристикам относят:

− голос;
− подпись;
− ритм работы сердца.

С помощью регистрирующего устройства (сканера, камеры) этот биометрический образец обрабатывается для получения информации об отличительных признаках, в результате чего получается контрольный шаблон.

Шаблон – это большая числовая последовательность, сам образец невозможно восстановить из шаблона.

Недостатки методов аутентификации с запоминаемым паролем

Таблица 4. Атаки на биометрические системы и защита от них

Описание атаки	Защита от данной атаки
Подделка личностной чер-	Снятие показателей с высоким уровнем детали-

ты	зации
Воспроизведение поведения пользователя	Изменяемое поведение
Перехват биометрических показателей	Шифрование биометрических данных
Воспроизведение биометрической «подписи»	Использование ЭЦП для обеспечения целостности биометрической подписи

9. Аутентификация с помощью одноразовых паролей

Одноразовые пароли – это динамическая аутентификационная информация, генерируемая для единичного использования с помощью аутентификационных ключей (программных или аппаратных.)

В качестве возможных устройств для генерации одноразовых паролей обычно используют OTP-токены.

OTP-токен – это мобильное персональное устройство, которое принадлежит определенному пользователю и генерирует одноразовые пароли, используемые для аутентификации данного пользователя.

Преимущества аутентификационных устройств в виде введения PIN-кода:

− для активации OTP-токена;

− в качестве дополнительной информации, используемой при генерации OTP;

− для предъявления серверу аутентификации вместе с OTP.

OTP-токены имеют небольшой размер и выпускается в виде:

− смарт-карты;

− устройства, комбинированного с USB-ключом.

10. Методы аутентификации с помощью OTP-токенов

В OTP-токенах применяется симметричная криптография. Устройство каждого пользователя содержит уникальный, персональный секретный ключ, используемый для шифрования некоторых данных и для генерации OTP.

Этот же ключ храниться на сервере аутентификации, который выполняет аутентификацию данного пользователя.

Сервер шифрует те же данные и сравнивает два результата шифрования:

полученный им и присланный от клиента. Если результаты совпадают, то пользователь успешно проходит аутентификацию.

10.1. Метод «Запрос-ответ»

В методе «запрос-ответ» OTP является ответом пользователя на случайный запрос от сервера.

Пример аутентификации пользователя при использовании OTP-токеном метода «только ответ»:

1. Пользователь активизирует свой OTP-токен, который вычисляет и отображает ответ на «скрытый» запрос.

2. Пользователь вводит свое «имя пользователя» и этот ответ («66260689») на рабочей станции.

3. Имя пользователя и ответ («66260689») передаются по сети в открытом виде.

4. Сервер находит запись пользователя, генерирует такой же скрытый запрос и шифрует его с помощью секретного ключа пользователя, получая ответ на свой запрос.

5. Сервер сравнивает представленный ответ от пользователя («66260689») с вычисленным им самим ответом («66260689»).

6. При совпадении значений аутентификация считается успешной.

10.2. Метод «только ответ»

В методе «только ответ» аутентификационное устройство и сервер аутентификации генерируют «скрытый» запрос, используя значение предыдущего запроса.

Для начальной инициализации данного процесса используется уникальное случайное начальное значение, генерируемое по инициализации OTP-токена.

Пример аутентификации пользователя при использовании OTP-токеном метода «запрос-ответ»:

1. Пользователь вводит свое имя пользователя на рабочей станции.

2. Имя пользователя передается по сети в открытом виде.

3. Сервер аутентификации генерирует случайный запрос («31415926»).

4. Запрос передается по сети в открытом виде.

5. Пользователь вводит запрос в свой OTP-токен.

6. OTP-токен шифрует запрос с помощью секретного ключа пользователя («cft6yhnj»), в результате получается ответ («27182818»), который отображается на экране OTP-токена.

7. Пользователь вводит этот ответ на рабочей станции.

8. Ответ передается по сети в открытом виде.

9. Аутентификационный сервер находит запись пользователя в аутентификационной базе данных и с помощью хранимого им секретного ключа пользователя зашифровывает тот же запрос.

10. Сервер сравнивает представленный ответ от пользователя («27182818») с вычисленным им самим ответом («27182818»).

При совпадении значений аутентификация считается успешной.

Управление доступом по схеме однократного входа с авторизацией Single Sign-On

Управление доступом по схеме однократного входа с авторизацией SSO дает возможность пользователям корпоративной сети при их входе в сеть пройти одну аутентификацию, предъявив только один раз пароль (или иной требуемый аутентификатор), и затем без дополнительной аутентификации получить доступ ко всем авторизованным сетевым ресурсам, которые им нужны для выполнения их работы. Такими сетевыми ресурсами могут быть принтеры, при-

ложения, файлы и другие данные, размещаемые по всему предприятию на серверах различных типов, которые работают на базе разных операционных систем. Управление доступом по схеме однократного входа SSO позволяет повысить производительность труда пользователей сети, уменьшить стоимость сетевых операций и улучшить сетевую безопасность.

С помощью аутентификации система проверяет подлинность пользователя, в то время как авторизация определяет, какими ролями и правами доступа пользователь обладает.

Большинство подходов SSO централизованно осуществляют аутентификацию пользователя. Авторизацию обычно выполняют на ресурсах целевых объектов, хотя некоторые продвинутые SSO-решения централизованно осуществляют и авторизацию – при этом используются продукты централизованного администрирования безопасности, которые осуществляют администрирование полномочий пользователей.

Схему однократного входа SSO поддерживают протоколы:

– LDAP (Lightweight Directory Access Protocol);
– протокол SSL (Secure Sockets Layer);
– система Kerberos;
– инфраструктура управления открытыми ключами PKI;
– также средства интеграции сервисов каталогов и безопасности.

1. Простая система однократного входа Single Sign-On

Самое простое SSO-решение состоит в автоматизации процесса предъявления пароля. Для многих продуктов SSO информация входа (то есть имя пользователя и пароль) и любые необходимые записи хранятся на специальном сервере аутентификации. Используя клиентское программное обеспечение, пользователь предъявляет серверу аутентификации пароль, и этот сервер сообщает клиентскому программному обеспечению, к каким ресурсам пользователь может получить доступ. Клиентское программное обеспечение представляет пользователю допустимые опции. Когда пользователь выберет ресурс, клиентское программное обеспечение использует мандат входа и сценарии, предоставленные сервером аутентификации, чтобы установить от имени пользователя соединение с соответствующим ресурсом целевого объекта (сервера, хоста, домена или приложения).

При автоматизации процедуры входа выполняются следующие шаги:

1. Пользователь предъявляет серверу аутентификации пароль, используя специальное клиентское программное обеспечение на своем персональном компьютере.

2. Сервер аутентификации проверяет, к каким ресурсам может получить доступ этот пользователь, и отправляет эту информацию обратно на клиентское SSO-приложение совместно с необходимым мандатом входа и сценариями для соединения с каждым разрешенным ресурсом.

3. Клиентское SSO-приложение представляет пользователю доступные ресурсы и входит от имени пользователя в выбранные приложения.

Автоматизация процедуры входа позволяет получить простую схему SSO, но при этом еще больше децентрализуется администрирование безопасностью. Ряд поставщиков предлагают дополнительные средства централизованного администрирования безопасностью. Эти средства используют агентов в целевых системах и обеспечивают основанное на ролях (role-based) централизованное администрирование учетных записей пользователей и информации об их полномочиях. В некоторых случаях эти средства администрирования полностью отделены от схемы SSO; в других случаях они интегрированы с SSO.

При формировании современного решения SSO применяются также такие средства аутентификации пользователя, как токены, цифровые сертификаты PKI, смарт- карты и биометрические устройства.

Более совершенный подход к аутентификации обычно основан на использовании токенов.

Наиболее известной системой аутентификации является Kerberos (в качестве механизма аутентификации Kerberos поддерживают IBM, Майкрософт, CyberSafe и ряд других компаний).

Продвинутые SSO-решения также предоставляют больше контроля над полномочиями пользователя, поддерживаемыми обычно на прикладном уровне.

Такие решения включают агентов для общего сервера и сред приложений, которые обеспечивают централизованное, основанное на ролях администрирование полномочий пользователя по нескольким ресурсам. Целевой ресурс доверяет SSO-системе идентифицировать конкретных пользователей и их роли; SSO эффективно доставляет доверенные мандаты к приложению, скрывая от приложения процесс аутентификации.

2. Системы однократного входа Web SSO . Cookie – это часть информации, которую веб-сервер хранит на ПК пользователя с помощью браузера и которую можно использовать при принятии решения о предоставлении пользователю доступа. Если имя пользователя хранится в cookie на компьютере пользователя, серверное приложение может проверить, кем является этот пользователь, не предлагая ему предъявлять пароль снова, независимо от того, на какую страницу сайта переходит этот пользователь.

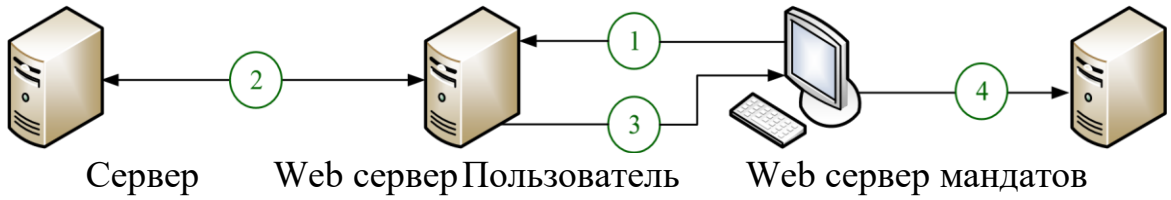

Рисунок 14. Схема Web SSO, основанная на использовании cookie

В схеме Web SSO, основанной на использовании cookie, при реализации процедуры входа выполняются следующие шаги:

1. Пользователь, применяя специальное клиентское программное обеспечение на своем персональном компьютере, передает на веб-сервер имя пользователя и пароль.

2. Агент веб-сервера извлекает мандат пользователя с сервера мандатов (Cre-dentials Server). Веб-сервер предоставляет пользователю ресурсы в соответствии с его мандатом.

3. Агент веб-сервера сохраняет зашифрованный мандат в качестве cookie на компьютере пользователя.

4. Когда пользователь переходит на другую страницу на веб-сайте, которая может быть на другом веб-сервере, последний просто читает мандат пользователя из его cookie.

Вскоре после своего появления cookie стали подвергаться атакам, но, поскольку теперь cookie могут передаваться с помощью шифрованной SSLсессии, эта проблема практически исключена. Позднее Java обеспечил гибкость программирования на стороне браузера, что образует базу для других SSOподходов в Сети.

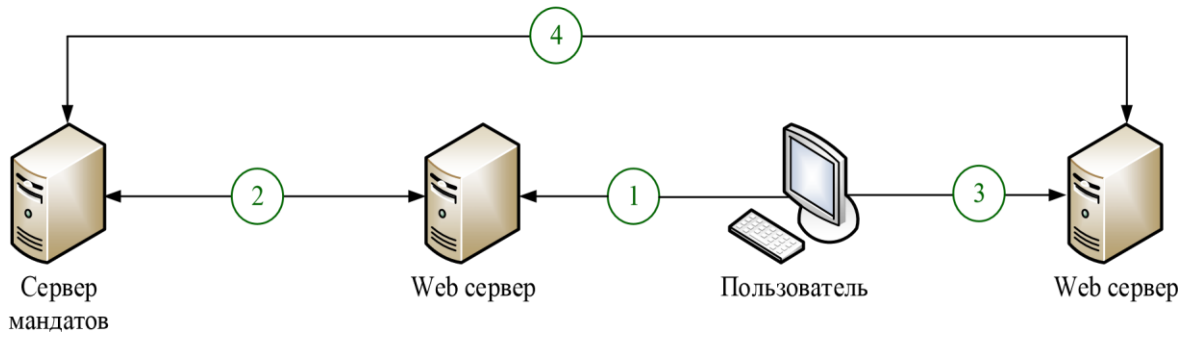

Рисунок 15. Схема Web SSO, не использующая cookie

В схеме Web SSO, не использующей cookie, при реализации процедуры входа выполняются следующие шаги:

1. Пользователь передает на веб-сервер имя пользователя и пароль.

2. Агент на веб-сервере извлекает мандат пользователя с сервера мандатов. Веб-сервер предоставляет пользователю ресурсы в соответствии с его мандатом.

3. Если пользователь пытается получить доступ к защищенным ресурсам на другом веб-сервере...

4. ...агент на этом веб-сервере должен снова запрашивать мандат пользователя на сервере мандатов.

Коммерческие решения Web SSO используют ряд подходов. Почти во всех подходах требуется использование агентов, установленных на вебсерверы, которые связываются с отдельным мандатным сервером, чтобы проверить подлинность пользователя. Некоторые варианты также требуют собственного клиентского программного обеспечения. Такой подход может дать более высокий

уровень безопасности при использовании технологий аутентификации на основе одноразовых токенов или возможностей PKI.

Безопасность корпоративной сети, подключений к интернету, реализуется по периметру между корпоративной сетью и открытым Интернетом. Поэтому при рассмотрении проблемы безопасности корпоративной сети пользователей разделяют на внутренних и внешних.

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Охарактеризовать ложный ARP- сервер., IP Hijacking.
2. Привести методы распределенных атаки "отказ в обслуживании".
3. Привести классификацию распределенных атаки "отказ в обслуживании".

3.2 Защита от сетевых угроз

3.2.1 Тема 2.1 Доменные службы Active Directory. Структуры леса, доменных деревьев. Проектирование отношений и оптимизация аутентификации внутри леса

Перечень изучаемых вопросов:

Назначение службы каталогов Active Director.

LDAP (Lightweight Directory Access Protocol)ка.

Основные функции контроллеров домена:

Логическая структура Active Directory.

Протокол Kerberos.

Методические указания к изучению:

Служба каталогов Active Directory является основой логической структуры корпоративных сетей, базирующихся на системе Windows.

Модели управления безопасностью:

1. «Рабочая группа»
2. Централизованная доменная модель.

Основное назначение служб каталогов – управление сетевой безопасностью.

Основа сетевой безопасности - база данных учетных записей (accounts) пользователей, групп пользователей и компьютеров, с помощью, которой осуществляется управление доступом к сетевым ресурсам.

1. Модель «Рабочая группа»

Предназначена для использования в небольших одноранговых сетях (310 компьютеров). Каждый компьютер в сети с операционными системами Windows имеет свою собственную локальную базу данных учетных записей и с помощью нее осуществляется управление доступом к ресурсам данного компьютера.

Компьютеры рабочей группы совместно используют общие ресурсы, такие как файлы и принтеры.

При администрировании каждого компьютера определяют:

– какие ресурсы этого компьютера будут разделяемыми (общими),

– какие пользователи сети будут иметь доступ к этим ресурсам, с какими правами.

Локальная БД учетных записей называется база данных SAM (Security Account Manager – Диспетчер учётных записей безопасности) и хранится в реестре операционной системы.

Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.

Достоинство: удобная сетевая среда для небольшого числа компьютеров, расположенных недалеко друг от друга.

Недостаток: сложность управления ресурсами; большая избыточность; высокая трудоемкость.

2. Доменная модель

В доменной модели существует единая база данных служб каталогов, доступная всем компьютерам сети.

В сети устанавливаются специализированные серверы - контроллеры домена, которые хранят на своих жестких дисках эту базу.

Серверы DC-1 и DC-2 – контроллеры домена, они хранят доменную базу данных учетных записей (каждый контроллер хранит у себя свою собственную копию БД, но все изменения, производимые в БД на одном из серверов, реплицируются на остальные контроллеры).

С помощью доменной базы данных осуществляется централизованное управление доступом к сетевым ресурсам независимо от количества компьютеров в сети.

3. Назначение службы каталогов Active Directory

Объекты AD – это информация, относящаяся к пользователям, группам, компьютерам, сетевым принтерам, общим файловым ресурсам.

Атрибуты AD – это информация о самом объекте, или его свойствах.

Например,

Атрибутами являются: имя руководителя пользователя, номер телефона, адрес, имя для входа в систему, пароль, группы, в которые он входит, и т. д.

Функции AD:

− единая регистрация в сети.

Пользователи могут регистрироваться в сети с одним именем и паролем и получать при этом доступ ко всем сетевым ресурсам и службам (службы сетевой инфраструктуры, службы файлов и печати, серверы приложений и баз данных и т. д.);

− безопасность информации.

Средства аутентификации и управления доступом к ресурсам, встроенные в службу Active Directory, обеспечивают централизованную защиту сети; − централизованное управление.

Администраторы могут централизованно управлять всеми корпоративными ресурсами;

− администрирование с использованием групповых политик.

При загрузке компьютера или регистрации пользователя в системе выполняются требования групповых политик; их настройки хранятся в объектах групповых политик (GPO) и применяются ко всем учетным записям пользователей и компьютеров, расположенных в сайтах, доменах или организационных подразделениях;

− интеграция с DNS.

Серверы DNS могут хранить информацию о зонах в базе данных Active Directory;

− расширяемость каталога.

Администраторы могут добавлять в схему каталога новые классы объектов или добавлять новые атрибуты к существующим классам; − масштабируемость.

Служба Active Directory может охватывать как один домен, так и множество доменов, объединенных в дерево доменов, а из нескольких деревьев доменов может быть построен лес;

− репликация информации.

В службе Active Directory используется репликация служебной информации в схеме со многими ведущими (multi-master), что позволяет модифицировать БД Active Directory на любом контроллере домена. Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость и возможность распределения сетевой нагрузки;

− гибкость запросов к каталогу.

БД Active Directory может использоваться для быстрого поиска любого объекта AD, используя его свойства (например, имя пользователя или адрес его электронной почты, тип принтера или его местоположение и т. п.); − стандартные интерфейсы программирования.

Для разработчиков программного обеспечения служба каталогов предоставляет доступ ко всем возможностям (средствам) каталога и поддерживает принятые стандарты и интерфейсы программирования (API).

Объект AD – это уникальную сущность внутри Каталога и обычно обладает многими атрибутами, которые помогают описывать и распознавать его.

Например,

Тип объекта - Учетная запись пользователя

Атрибуты типа объекта: имя, фамилия, пароль, номер телефона, адрес и многие другие.

Протоколы и службы, используемые в AD:

– LDAP
– Kerberos
– DNS

3. LDAP (Lightweight Directory Access Protocol)

Протокол прикладного уровня для доступа к службе каталогов X.500, использующий TCP/IP и позволяющий производить операции авторизации *(bind)*, поиска *(search)* и сравнения *(compare)*, а также операции добавления, изменения или удаления записей.

Свойства протокола LDAP:

− иерархическая система построения справочника
− масштабируемость
− расширяемость

Операции над каталогами со стороны клиентского приложения:

− установление связи с каталогом;
− поиск в нем информации;
− модификация его содержимого;
− добавление объекта; − удаление объекта.

4. Kerberos

Сетевой протокол аутентификации, позволяющий передавать данные через незащищённые сети для безопасной идентификации. Ориентирован на клиент-серверную модель и обеспечивает взаимную аутентификацию – оба пользователя через сервер подтверждают личности друг друга.

5. Домен

Формирует область административной ответственности.

База данных домена содержит учетные записи пользователей, групп и компьютеров.

Имена доменов Active Directory формируются по той же схеме, что и имена в пространстве имен DNS. Служба DNS является средством поиска компонент домена – в первую очередь контроллеров домена.

Контроллеры домена - специальные серверы, которые хранят соответствующую данному домену часть базы данных Active Directory.

Основные функции контроллеров домена:

1) хранение БД Active Directory (организация доступа к информации, содержащейся в каталоге, включая управление этой информацией и ее модификацию);

2) синхронизация изменений в AD (изменения в базу данных AD могут быть внесены на любом из контроллеров домена, любые изменения, осуществляемые на одном из контроллеров, будут синхронизированы с копиями, хранящимися на других контроллерах);

3) аутентификация пользователей (любой из контроллеров домена осуществляет проверку полномочий пользователей, регистрирующихся на клиентских системах).

В каждом домене рекомендуется устанавливать не менее двух контроллеров домена:

− для защиты от потери БД Active Directory в случае выхода из строя какого-либо контроллера.

− для распределения нагрузки между контроллерами.

6. Дерево

Дерево – это набор доменов, которые используют единое связанное пространство имен.

Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом.

Доверительные отношения означают, что ресурсы одного из доменов могут быть доступны пользователям других доменов.

7. Лес

Лес объединяет деревья, которые поддерживают единую схему.

Схема – это набор определений типов, или классов, объектов в БД Active Directory.

В лесу между всеми доменами установлены двухсторонние транзитивные доверительные отношения, что позволяет пользователям любого домена получать доступ к ресурсам всех остальных доменов, если они имеют соответствующие разрешения на доступ.

По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD:

Свойства доменного леса:

− первое созданное в лесу доменов дерево является корневым деревом, первый созданный в дереве домен называется корневым доменом дерева (tree root domain);

− первый домен, созданный в лесу доменов, называется корневым доменом леса (forest root domain), данный домен не может быть удален (он хранит информацию о конфигурации леса и деревьях доменов, его образующих).

8. Организационные подразделения (ОП).

Организационные подразделения - контейнеры внутри AD, которые создаются для объединения объектов в целях делегирования административных прав и применения групповых политик в домене.

ОП существуют только внутри доменов и могут объединять только объекты из своего домена.

ОП могут быть вложенными друг в друга, что позволяет строить внутри домена сложную древовидную иерархию из контейнеров и осуществлять более гибкий административный контроль.

9.Глобальный каталог

Глобальный каталог – это перечень всех объектов, которые существуют в лесу Active Directory.

Сервер Глобального каталога является контроллером домена, в котором содержится информация о каждом объекте, находящемся в данном лесу.

10. Именование объектов

В каталогах на базе протокола LDAP для идентификации объекта в масштабе всего леса используется механизм именования объектов отличительных имен (Distinguished Name, DN).

В Active Directory учетная запись пользователя с именем User домена company.ru, размещенная в стандартном контейнере Users, будет иметь уникальное имя: «DC=ru, DC=company, CN=Users, CN=User».

Обозначения:

DC (Domain Component) – указатель на составную часть доменного имени; OU (Organizational Unit) – указатель на организационное подразделение (ОП); CN (Common Name) – указатель на общее имя.

Для идентификации объекта контейнера, в котором данный объект хранится, существует относительное отличительное имя (Relative Distinguished Name, RDN).

Для пользователя User из предыдущего примера RDN-имя будет иметь вид «CN=User».

Основное имя объекта (User Principal Name, UPN).

Оно имеет формат <имя субъекта>@<суффикс домена>.

Для пользователя основное имя будет выглядеть: User@company.ru.

Имена DN, RDN могут меняться, если объект перемещается из одного контейнера AD в другой.

Для того чтобы не терять ссылки на объекты при их перемещении в лесу, всем объектам назначается глобально уникальный идентификатор (Globally Unique Identifier, GUID), представляющий собой 128-битное число.

11. Планирование пространства имен AD При планировании AD необходимо:

− тщательный выбор имен доменов верхнего уровня;

− качество коммуникаций в компании (связь между отдельными подразделениями и филиалами);

− организационная структура компании;

− количество пользователей и компьютеров в момент планирования; − прогноз темпов роста количества пользователей и компьютеров.

12. Логическая структура Active Directory

Служба каталогов Active Directory организована в виде иерархической структуры, построенной из различных компонентов, которые представляют элементы корпоративной сети.

Логическая структура AD – это способ организации элементов корпоративной сети. Она состоит из леса, деревьев, доменов.

Домен – логическая группа пользователей и компьютеров, которая поддерживает централизованное администрирование и управление безопасностью.

Домен также является основной единицей для репликации – все контроллеры одного домена должны участвовать в репликации друг с другом. Домены в одном лесу имеют автоматически настроенные доверительные отношения, что позволяет пользователям из одного домена получать доступ к ресурсам в другом. Можно создавать доверительные отношения с внешними доменами, не входящими в лес.

Дерево – это набор доменов, которые связаны отношениями «дочерний» / «родительский», а также используют связанные (смежные, или прилегающие) пространства имен. При этом дочерний домен получает имя от родительского.

Лес – это одно или несколько деревьев, которые разделяют общую схему, серверы Глобального каталога и конфигурационную информацию. В лесу все домены объединены транзитивными двухсторонними доверительными отношениями.

Каждая конкретная инсталляция Active Directory является лесом, даже если состоит всего из одного домена.

Организационное подразделение (ОП) – это контейнер, который помогает группировать объекты для целей администрирования или применения групповых политик.

13. Физическая структура Active Directory

Служит для связи между логической структурой AD и топологией корпоративной сети.

Основные элементы физической структуры Active Directory – контроллеры домена и сайты.

Сайт – группа IP-сетей, соединенных быстрыми и надежными коммуникациями.

Назначение сайтов – управление процессом репликации между контроллерами доменов и процессом аутентификации пользователей.

Быстрый канал – имеет скорость передачи данных не менее 512 Кбит/с.

Структура сайтов не зависит от структуры доменов. Один домен может быть размещен в нескольких сайтах, и в одном сайте могут находиться несколько доменов.

Поскольку сайты соединяются друг с другом медленными линиями связи, механизмы репликации изменений в AD внутри сайта и между сайтами различные.

Внутри сайта контроллеры домена соединены линиями с высокой пропускной способностью. Поэтому репликация между контроллерами произво-

дится каждые 5 минут, данные при передаче не сжимаются, для взаимодействия между серверами используется технология вызова удаленных процедур (RPC).

Для репликации между сайтами кроме RPC может использоваться также протокол SMTP, данные при передаче сжимаются (в результате сетевой трафик составляет от 10 до 40 % от первоначального значения), передача изменений происходит по определенному расписанию. Если имеется несколько маршрутов передачи данных, то система выбирает маршрут с наименьшей стоимостью.

Сайты используются при аутентификации пользователей в домене. При входе пользователя в сеть его аутентификация осуществляется ближайшим контроллером домена. В процессе поиска «ближайшего» контроллера используется информация о сайте, к которому принадлежит компьютер пользователя.

На каждом сайте необходимо размещать минимум один сервер глобального каталога и контроллер домена.

В самом начале создания леса автоматически создается сайт по умолчанию с именем Default-First-site-Name.

При создании нового контроллера на основании выделенного ему IPадреса служба каталога автоматически отнесет его к соответствующему сайту.

14. Репликация, управление топологией репликации

Репликация внутри сайта

Топологию репликации, т. е. порядок, в котором серверы опрашивают друг друга для получения изменений в базе данных, серверы строят автоматически (эту задачу выполняет компонента служб каталогов, называемая Knowledge Consistency Checker, или KCC).

При достаточно большом количестве контроллеров KCC строит кольцевую топологию репликации, для надежности образует несколько колец, по которым контроллеры передают данные репликации.

Репликация между сайтами

Использует межсайтовый транспорт: IP (RPC), SMTP.

Для каждого вида межсайтового транспорта определяется «соединение сайтов», с помощью которого строится управление репликацией между двумя и более сайтами.

15. Серверы Глобального каталога

Глобальный каталог – это перечень всех объектов леса Active Directory. Он является контроллером домена, в котором содержится информация о каждом объекте, находящемся в данном лесу.

Функции сервера глобального каталога: − поиск объектов в масштабах всего леса; − аутентификация пользователей.

По умолчанию самый первый контроллер домена в лесу является сервером глобального каталога.

16. Учетные записи и группы

Типы пользовательских учетных записей:

1. Локальные учетные записи пользователей. Эти учетные записи существуют в локальной базе данных SAM (Security Accounts Manager) на каждой системе, работающей под управлением Windows 2003.

2. Учетные записи пользователей домена. Эти учетные записи хранятся в Active Directory и могут использоваться для входа в систему и доступа к ресурсам по всему лесу AD.

3. Встроенные учетные записи. Эти учетные записи создаются самой системой и не могут быть удалены.

Основное имя пользователя (UPN, User Principle Name) включает в себя имя входа пользователя, затем значок «@» и имя домена.

Все UPN в лесу должны быть уникальными.

Типы групп Active Directory

Группы безопасности – используются для назначения разрешений при определении прав доступа к различным сетевым ресурсам.

Группы распространения – предназначены для организации списков рассылки для почтовых программ.

17. Маркер доступа.

Маркер доступа состоит из набора идентификаторов безопасности - идентификатора безопасности (SID) самого пользователя и идентификаторов безопасности тех групп, членом которых он является.

18. Управление Организационными подразделениями, делегирование полномочий

Организационные подразделения – организация иерархической структуры объектов AD внутри домена.

Задачи ОП:

1. делегирование административных полномочий на управление объектами ОП пользователю или группе пользователей;

2. применение групповых политик к объектам, входящим в ОП.

Делегирование административных полномочий позволяет распределить нагрузку по администрированию учетными записями между различными сотрудниками, не увеличивая при этом количество пользователей, имеющих административные права на уровне всего домена.

Механизм Групповых политик позволяет автоматизировать настройку параметров компьютеров и пользовательской рабочей среды сразу в масштабах сайта AD, домена, организационного подразделения.

Каждый объект групповых политик состоит из двух частей:

1) контейнера групповых политик, хранящегося в БД AD

2) шаблона групповых политик, хранящегося в файловой системе контроллера домена.

Групповые политики могут использоваться для установки прикладных программ в масштабах всего домена или отдельного организационного подразделения.

19. Протокол Kerberos

Протокол Kerberos предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Другими словами, протокол идеально подходит для применения в Интернет и аналогичных сетях.

Участники сеанса связи обмениваются криптографическим ключом, знание которого подтверждает личность собеседника.

Чтобы доказать своё право на вход, пользователь предъявляет аутентификатор в виде набора данных, зашифрованного секретным ключом. Получив аутентификатор, «привратник» расшифровывает его и проверяет полученную информацию, чтобы убедиться в успешности дешифрования.

Участника безопасной связи по протоколу Kerberos:

Клиент - система (пользователь), делающий запрос;

Сервер - система, которая обеспечивает сервис для систем, чью подлинность нужно подтвердить.

Центр распределения ключей - сторонний посредник между клиентом и сервером, который ручается за подлинность клиента. В среде Windows , выступает контроллер домена со службой каталогов Active Directory.

В среде Kerberos для входа в систему пользователь должен предоставить свое имя пользователя, пароль и имя домена, в который он хочет войти. Эта информация посылается KDC, который устанавливает подлинность пользователя. Если пользователь подлинный, ему предоставляется статус ticket-granting ticket, TGT.

Для получения доступа к серверу, требуется обратиться к KDC, предъявить свой билет TGT, как подтверждение подлинности, а затем уже запросить «билет сеанса» для сервера, с которым вам необходим контакт.

Корпоративная информационная система:

1. Основные положения для планирования безопасности сети

Объектами угроз для информационной безопасности могут служить следующие уровни управления КИС:

– централизованное управление всей системой предприятия;
– управление подразделениями;
– управление всей сетью;
– управление конечными пользователями.

2.В соответствии с этим система информационной безопасности КИС должна включать в себя защиту:

– централизованного управления;

– приложений и соответствующих серверов;
– сети;
– конечных пользователей.

3.Для обеспечения санкционированного доступа требуется:
– обеспечение единого механизма доступа;
– создание единой политики безопасности и защиты информации;
– централизация и непрерывный контроль за использованием ресурсов и управления ими.

4. Функции централизованного управления:
– авторизация и управление распределенной информацией в масштабах всего предприятия;
– возможность централизованной аутентификации и управление доступом во всем веб-сервисам в независимости от их платформ;
– управление доступом к персональной информации пользователей;
– централизованное кросс-платформенное управление учетными записями пользователей и информационными ресурсами;
– управление рисками на предприятии, позволяющее системным администраторам контролировать все несанкционированные вторжения на предприятие (в корпоративную сеть).

5. Централизованное управление рисками и администрирование системы безопасности:
централизованное администрирование;
– административный контроль полномочий главным администратором;
– делегирование части полномочий младшим администраторам отдельных ресурсов;
– управление событиями;
– принятие решений по управлению рисками;
– долговременное хранение статистики тревог и вторжений;
– управление атрибутами пользователей (учетными записями) и обслуживание пользователей в распределенных сетях;
– осуществление централизованной аутентификации;
– управление пользовательскими группами, ролями, каталогами, привилегиями пользователей.

6. Защита управления приложениями.
– защита доступа к ресурсам приложений;
– установление и контроль связи учетных записей пользователей с различными типами ресурсов (файлами, каталогами, принтерами, приложениями);
– предотвращение неправомочного доступа к информационным ресурсам и критическим сервисам.

7. Защита систему сетей:
– защита внутреннего обмена (локальные вычислительные сети, интранет);

– защита межсетевого обмена (глобальные вычислительные сети, экстранет);

– защита обмена через Интернет;

– осуществление распределенной нагрузки для улучшения производительности и восстановления после сбоев.

8. Защита конечных пользователей:

– установление авторизации;

– установление правил обращения пользователей с информацией;

– сертификация открытых ключей PKI;

– мониторинг угроз безопасности и отражение их в журналах регистрации;

– контроль соблюдения требований политики секретности.

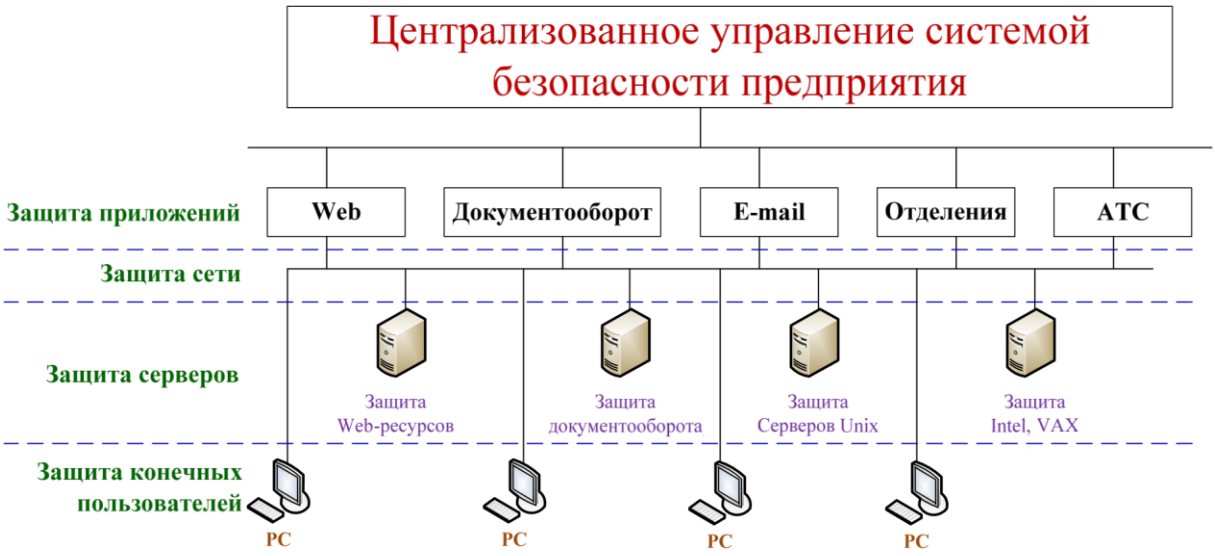

Рисунок 16. Структурная схема системы защиты информации КИС

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Охарактеризуйте системы обнаружения вторжений.
2. Охарактеризуйте межсетевые экраны.
3. Охарактеризуйте системы шифрования трафика.

3.2.2 Тема 2.2 Корпоративная информационная система. Сети периметра и стратегии удаленного доступа

Перечень изучаемых вопросов:
Основные положения для планирования безопасности сети.
Функции уровней защиты.
Сети периметра и стратегия удаленного доступа.
Сеть периметра.
Обеспечение безопасности сети периметра.
Обнаружение вторжений.

Методические указания к изучению:
1. Основные положения для планирования безопасности сети
Объектами угроз для информационной безопасности могут служить следующие уровни управления КИС:
- централизованное управление всей системой предприятия;
- управление подразделениями;
- управление всей сетью;
- управление конечными пользователями.
В соответствии с этим система информационной безопасности КИС должна включать в себя защиту:
- централизованного управления;
- приложений и соответствующих серверов;
- сети;
- конечных пользователей.
Для обеспечения санкционированного доступа требуется:
- обеспечение единого механизма доступа;
- создание единой политики безопасности и защиты информации;
- централизация и непрерывный контроль за использованием ресурсов и управления ими.
Функции централизованного управления:
– авторизация и управление распределенной информацией в масштабах всего предприятия;
– возможность централизованной аутентификации и управление доступом во всем веб-сервисам в независимости от их платформ;
– управление доступом к персональной информации пользователей;
– централизованное кросс-платформенное управление учетными записями пользователей и информационными ресурсами;

– управление рисками на предприятии, позволяющее системным администраторам контролировать все несанкционированные вторжения на предприятие (в корпоративную сеть).

Функции уровней защиты.

2.1. Централизованное управление рисками и администрирование системы безопасности:

- централизованное администрирование;
- административный контроль полномочий главным администратором;
- делегирование части полномочий младшим администраторам отдельных ресурсов;
- управление событиями;
- принятие решений по управлению рисками;
- долговременное хранение статистики тревог и вторжений;
- управление атрибутами пользователей (учетными записями) и обслуживание пользователей в распределенных сетях;
- осуществление централизованной аутентификации;
- управление пользовательскими группами, ролями, каталогами, привилегиями пользователей.

2.2. Защита управления приложениями.

– защита доступа к ресурсам приложений;

– установление и контроль связи учетных записей пользователей с различными типами ресурсов (файлами, каталогами, принтерами, приложениями);

– предотвращение неправомочного доступа к информационным ресурсам и критическим сервисам.

2.3. Защита систему сетей:

– защита внутреннего обмена (локальные вычислительные сети, интранет);

– защита межсетевого обмена (глобальные вычислительные сети, экстранет);

– защита обмена через Интернет;

– осуществление распределенной нагрузки для улучшения производительности и восстановления после сбоев.

2.4. Защита конечных пользователей:

9. установление авторизации;
10. установление правил обращения пользователей с информацией;
11. сертификация открытых ключей PKI;
12. мониторинг угроз безопасности и отражение их в журналах регистрации;
13. контроль соблюдения требований политики секретности.

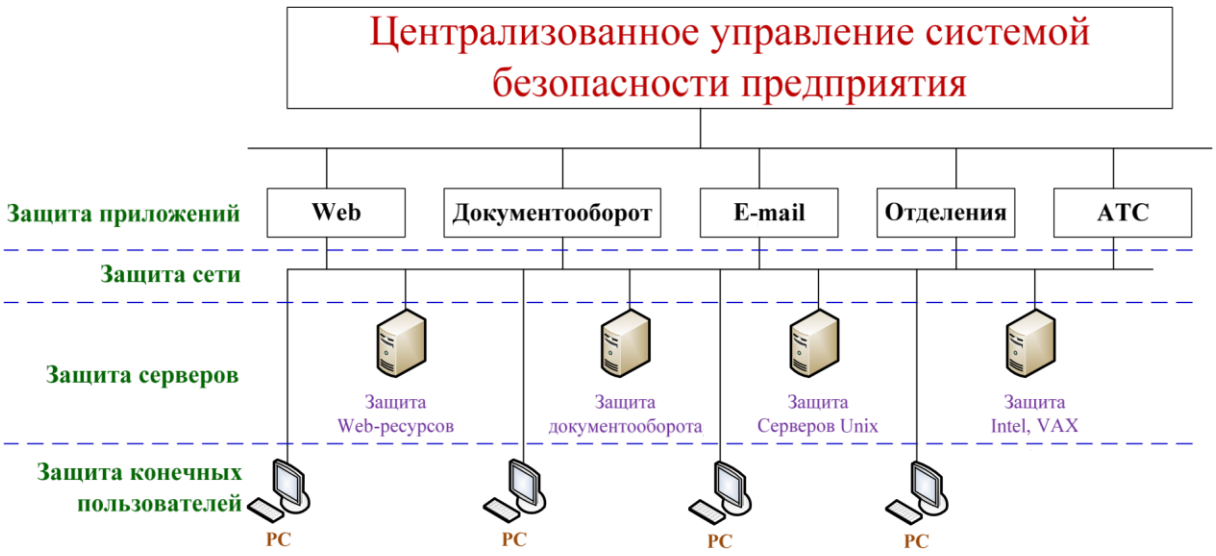

Рисунок 17. Структурная схема системы защиты информации КИС

Защита сетей от атак постоянно совершенствуется, начиная с момента появления брандмауэров, поддерживающих отслеживание состояния соединения, до появления комплексных служб безопасности. При попытках подключения атакующего компьютера к безопасным сетям доступ этого компьютера должен быть заблокирован, как на уровне аппаратно-программной защиты.

Сначала проектируется безопасная сеть периметра и решается, какие службы будут находиться в ней.

1. Сети периметра и стратегия удаленного доступа

Безопасность удаленного взаимодействия обеспечивается проектированием доступа сети периметра.

Компоненты служб сети периметра:

− RADIUS;
− VPN-серверы;
− общедоступные серверы приложений;
− беспроводные устройства;
− вспомогательные устройства сетевой инфраструктуры

По соображениям безопасности в сети должны присутствовать:

1) брандмауэр;
2) *устройства:*
− коммутаторы;
− маршрутизаторы;
− серверы приложений;
− служба RADIUS

2. Сеть периметра

Для защиты сети периметра используются один или два аппаратных брандмауэра.

Входящий трафик должен проходить один или более пунктов контроля, прежде чем попасть в сеть периметра получить доступ к развернутой в ней службам и безопасной среде.

В типовой схеме содержатся одно устройство периметра с двумя или более интерфейсами, либо два пункта контроля с двумя устройствами обеспечения безопасности. На одном из них проверяется трафик из не доверенной внешней среды в сеть периметра, а на втором – трафик на входе в безопасную среду из сети периметра.

Администратор предприятия должен определить трафик допустимый в сети периметра и трафик, разрешенный в защищенной сети.

Типы архитектуры сетей периметра

Сетевая архитектура состоит из трех областей или зон:

− пограничная сеть;

− сеть периметра;

− внутренняя сеть.

Пограничная сеть обеспечивает подключение к внешней среде, и подключена к Интернет-провайдеру через маршрутизатор.

Пограничный маршрутизатор выполняет защитные функции – содержит списки доступа для управления нежелательным трафиком определенных команд протокола ICMP (Например, эхо-запросами PING)

Брандмауэр периметра сети, совместно с устройствами и службами безопасности обеспечивает основную защиту пограничной сети.

Сеть периметра – это частично защищенная брандмауэром периметра область, в которой располагаются следующие службы: общедоступные webсерверы, способные обращаться к внутренним SQL-серверам и другим серверам приложений.

Внутренняя сеть – это безопасная среда, где размещается корпоративная пользовательская, и серверная среда.

В некоторых проектах обеспечения безопасности присутствует дополнительный брандмауэр, отделяющий сеть внутренних пользователей от ферм серверов.

На Рисунок 18 представлена типовая архитектура сетевой среды, состоящей из трех зон, где задействовано два брандмауэра.

Если брандмауэр периметра содержит три или более сетевых интерфейса, внутренний брандмауэр – это логическая связь с физическим устройством, представляющим службы брандмауэра периметра, а не физическая связь с его сетевыми интерфейсами.

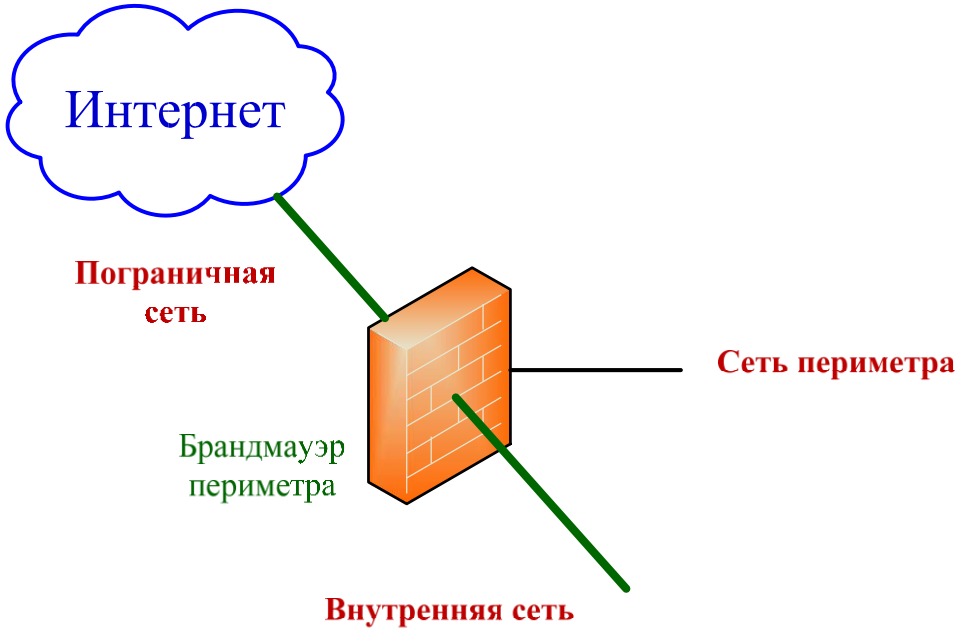

Рисунок 18. Схема сети периметра с одним брандмауэром

3. Обеспечение безопасности сети периметра

Функции устройств уровня безопасности на предприятии

– преобразование сетевых адресов (Network Address Translation, NAT);
– проверка отслеживанием состояния;
– проверка на уровне канала;
– функции прокси;
– брандмауэры уровня приложений.

В протоколе NAT используются частные IP-адреса, которые применяются только внутри организации. Когда трафик передается в Интернет, они преобразуются в допустимые общие IP-адреса.

Одно из преимуществ использования NAT в системе с брандмауэром состоит в сокрытии внутренней структуры адресов от злоумышленников извне.

Недостаток в использовании NAT заключается в том, что он нарушает работу некоторых служб. Например, для поддержки PPTP-туннелей потребуются редакторы NAT, а для туннелей IPseci L2TP нужен NAT-T (NAT Traversal).

Брандмауэры, поддерживающие состояние, отображают весь исходящий трафик интерфейса в таблице состояния. При возврате трафика таблица состояния позволяет установить, откуда поступил трафик – с данного интерфейса или другого источника.

Брандмауэры канального уровня обеспечивают более глубокую проверку трафика, по сравнению с брандмауэрами, поддерживающими состояния соединений. Брандмауэры канального уровня обслуживают сеанс и позволяют использовать протоколы с вторичными подключениями, такие как FTP.

Прокси-серверы играют роль посредника, запрашивая службу от имени клиента. Клиент не подключается к службе напрямую. Служба прокси-сервера может проверять все заголовки транзакции, обеспечивая дополнительный уровень защиты. Часто используемое содержимое для сокращения трафика кэшируется и используется повторно. Прокси-серверы поддерживают запросы на проверку подлинности, NAT и пересылку запросов на проверку подлинности.

Наивысший уровень защиты – брандмауэр уровня приложения. Кроме проверки заголовков всех входящих и исходящих пакетов и ведения таблиц состояния, он позволяет проверить потоки данных, обеспечивая защиту от атак, скрытых в полезной нагрузке обычных пакетов веб-службы (HTTP), других веб-запросах и пакетах данных, и прочих пакетах и ответов приложений.

4. ISA-серверы

Основная задача ISA-сервера – защита сети периметра. Версия ISAServer 2006 – позволяет реализовать интегрированный в периметр шлюз защиты, удаленный доступ, подключение филиалов и защиту доступа в Интернет.

ISA-сервер легко интегрируется в любые решения на основе продуктов Microsoft благодаря хорошей поддержке служб удаленного доступа Microsoftи безопасных VPN-туннелей типа «сеть-сеть».

В сети периметра ISA-сервер используется в схеме «back-to-back» спаренных брандмауэров. Действуя, как брандмауэр, ISA-сервер защищает сеть периметра от внешних угроз, одновременно играя роль фильтра и обратного прокси-сервера для служб, работающих в сети периметра. Второй сервер на основе ISA-сервера располагается между сетью периметра и внутренней сетью и выполняет функции брандмауэра прикладного уровня и прокси-сервера, проверяя и защищая все запросы на пути к внутренней сети. На Рисунок 19 приведены некоторые роли, выполняемые ISA-сервером в сети периметра.

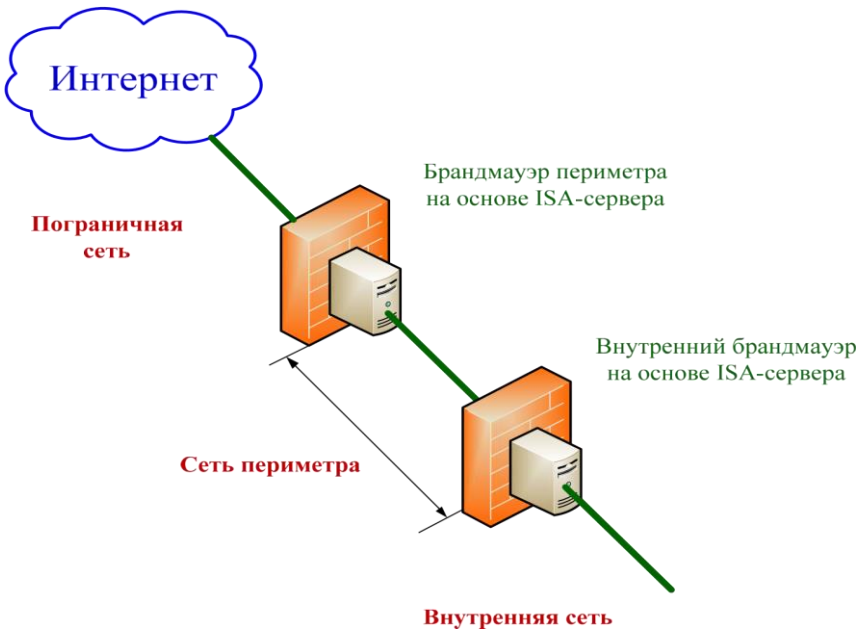

Рисунок 19. Сдвоенный брандмауэр на основе ISA-серверов

Дополнительные функции брандмауэров

− отслеживание состояния соединений;

− защита от вторжения;

− защита от вредоносных программ; службы брандмауэра прикладного уровня.

Аппаратный брандмауэр должен предоставлять службы канального уровня, а также модуль защиты от входящих вторжений для проверки приходящих из пограничной сети запросов на прикладном уровне.

В сети периметра могут содержаться следующие компоненты:

− серверы приложений для экстрасетей;

− VPN-серверы для удаленного доступа;

− беспроводные точки доступа для обеспечения общего доступа на предприятии, а также в беспроводных локальных сетях (WLAN)? Использующихся внутри корпорации;

− серверная роль шлюза служб терминалов;

− компоненты RADIUS, обеспечивающие проверку подлинности для беспроводного доступа, VPN и серверов приложений;

− серверы OCSP, предоставляющие сведения о статусе отзыва действующих сертификатов. −

В сети периметра обычно развертываются следующие веб-службы:

− Веб-серверы для доступа в интернет и экстрасеть;

− FTP-серверы;

− Общедоступные FTP-серверы.

5. Технологии идентификации – RADIUS

Технологии RADIUS реализованы на уровне ISA-сервера. Проверка клиентов, получивших доступ по VPN можно организовать через NSP-сервер (VPN+RADIUS), настроенный как RADIUS клиент.

Служба удаленной аутентификации пользователей RADIUS позволяет централизованно управлять большим числом удаленных пользователей, получающих доступ к сети из самых различных мест.

Во время процедуры аутентификации сервер доступа к сети передает на сервер RADIUS идентифицирующие пользователя данные. Если право пользователя на доступ подтверждается, сервер выдает разрешение на доступ и сообщает необходимую дополнительную информацию о параметрах сеанса связи, в частности назначенный клиенту IP-адрес и время максимальной продолжительности самого сеанса. В противном случае, т. е. если пользователь в системе не зарегистрирован, сервер выдает сообщение об отказе в доступе и по возможности указывает причину отказа. Используемые во время обмена информацией между серверами доступа и RADIUS атрибуты и их значения, хранятся в специальном файле-словаре.

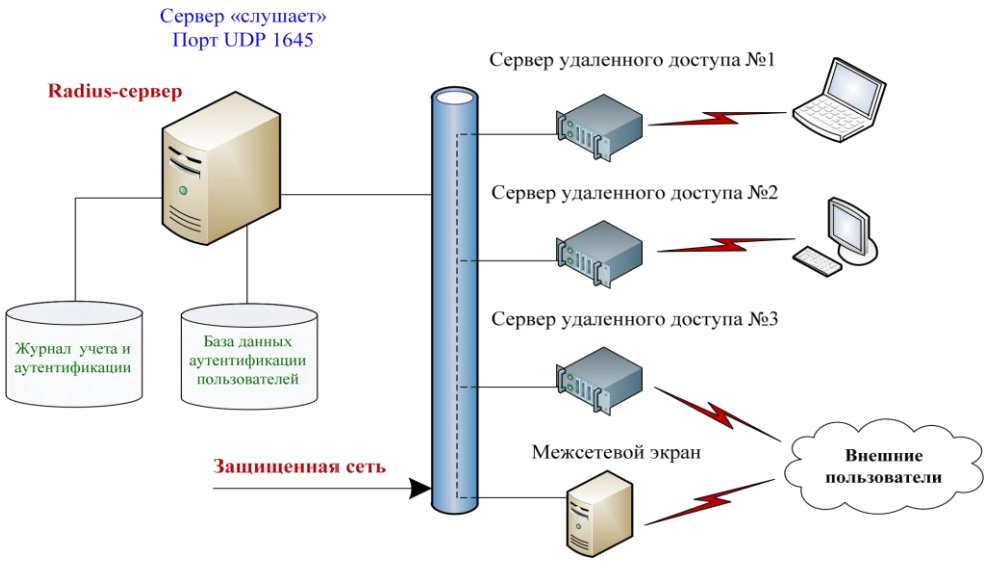

Рисунок 20. Архитектура сервера аутентификации RADIUS

Дальнейшие действия NAS предпринимает только после получения информации от RADIUS сервера. RADIUS сервер работает с одним или несколькими серверами NAS, он отвечает за прием запросов на установление соединения, процедуру аутентификации, и возврат всей необходимой информации авторизованной информации серверу NAS. Обычно под сервер RADIUS выделяют отдельную машину в сети. Для связи между серверами NAS и RADIUS используется протокол UDP.

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Приведите специфику методы предотвращения вторжения.
2. Приведите общие методы отклонения вторжения, принципы обнаружение вторжений.

3.2.3 Тема 2.3. Обеспечение безопасности операционных систем. Локальные политики безопасности. Встроенные системы защиты операционных систем

Перечень изучаемых вопросов:

Сетевые уровни

Административные меры защиты

Методические указания к изучению:

Защищенные операционные системы относятся к базовым средствам многоуровневой комплексной защиты корпоративные информационные системы (КИС).

Окружение, в котором функционирует ОС, называется доверенной вычислительной базой (ДВБ).

Состав ДВБ:

- операционная система;
- программное обеспечение;
- сетевое оборудование;
- средства физической защиты;
- организационные процедуры.

1. Угрозы безопасности операционной системы

Угрозы безопасности операционной системы зависят от того, какая информация хранится и обрабатывается в системе, и т. д.

Например:

Если операционная система используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же операционная система используется как платформа провайдера интернет-услуг, очень опасны атаки на сетевое программное обеспечение.

Активное воздействие на операционную систему – это несанкционированные действия злоумышленника в системе;

Пассивное воздействие на операционную систему – это несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Рисунок 21. Классификация угроз безопасности операционных систем

Атаки на операционную систему:

– сканирование файловой системы. Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. При обнаружении ошибки, злоумышленник получает доступ к информации, который должен быть ему запрещен; подбор пароля.

Методы подбора паролей пользователей:

− *тотальный перебор*, оптимизированный по статистике встречаемости символов или с помощью словарей;

− *подбор пароля с использованием знаний о пользователе* (его имени, фамилии, даты рождения, номера телефона и т. д.);

– кража ключевой информации. Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарт-карта, Touch Memory и т. д.) может быть просто украден;

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

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

– программные закладки.

– жадные программы – это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху операционной системы.

Защищенной операционная система – это такая система, в которой предусмотрены средства защиты от основных классов угроз.

Виды защищенных операционных систем:

Фрагментарный подход, при котором вначале организуется защита от одной угрозы, затем от другой и т. д.

Например, берется незащищенная операционная система, на нее устанавливают антивирусный пакет, систему шифрования, систему регистрации действий пользователей и т. д.

Средства защиты работают независимо друг от друга, при этом практически невозможно организовать их тесное взаимодействие, т.е. могут возникать конфликты ПО и оборудования.

2. Административные меры защиты

Состав административных мер защиты

1. Постоянный контроль корректности функционирования операционной системы. Необходима автоматическая регистрация наиболее важных событий (event logging) в специальном журнале.

2. Организация и поддержание адекватной политики безопасности. Оперативная реакция и корректировка на попытки злоумышленников преодолеть защиту операционной системы.

3. Осведомление пользователей операционной системы о необходимости соблюдении мер безопасности при работе с ОС и контроль за соблюдением этих мер.

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

5. Постоянный контроль изменений в конфигурационных данных и политый безопасности ОС.

Этапы формирования и поддержания адекватной политики безопасности ОС:

1. Анализ угроз. Мониторинг и выявление угроз, являющихся наиболее опасными. Организация защиты от них.

2. Формирование требований к политике безопасности. Администратор определяет, какие средства и методы будут применяться для защиты от тех или иных угроз.

3. Формальное определение политики безопасности. Формулируются необходимые требования к конфигурации ОС, а также требования к конфигурации дополнительных пакетов защиты, если установка таких пакетов необходима. *Результатом данного этапа* является развернутый перечень настроек конфигурации ОС и дополнительных пакетов защиты с указанием того, в каких ситуациях какие настройки должны быть установлены.

4. Введение в эксплуатацию политики безопасности. *Задачей* данного этапа является приведение конфигурации ОС и дополнительных пакетов защиты в соответствие с политикой безопасности, формально определенной на предыдущем этапе.

5. *Поддержание и коррекция политики безопасности.* В задачу администратора входит контроль соблюдения политики безопасности и внесение в нее необходимых изменений по мере появления изменений в функционировании ОС.

Сертификация операционной системы по некоторому классу защиты сопровождается составлением требований к адекватной политике безопасности, при безусловном выполнении которой защищенность конкретного экземпляра операционной системы будет соответствовать требованиям соответствующего класса защиты.

Основные функции подсистемы защиты операционной системы

1. Идентификация и аутентификация. Информация, подтверждающая, что пользователь действительно является тем, кем он себя заявляет.2. Разграничение доступа. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

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

4. Управление политикой безопасности. Политика безопасности должна постоянно поддерживаться в адекватном состоянии, то есть должна гибко реагировать на изменения условий функционирования ОС.

5. Криптографические функции. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

6. Сетевые функции.

Объект доступа – это любой элемент ОС, доступ к которому пользователей или других субъектов доступа может быть произвольно ограничен.

Метод доступа – это операция, определенная для объекта.

Субъект доступа – это сущность, способная инициировать выполнение операций над объектами, с учетом прав доступа.

Правила разграничения доступа

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

Модели разграничения доступа

Избирательное разграничение доступа (Discretionary Access Control) определенные операции над конкретным ресурсом запрещаются или разреша-

ются субъектам, или группам субъектов. Большинство операционных систем реализуют именно избирательное разграничение доступа.

Полномочное разграничение доступа заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации.

Система правил избирательное разграничение доступа:

1. Для любого объекта операционной системы существует владелец

Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой тройки субъект-объект-метод возможность доступа определена однозначно.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

При создании объекта его владельцем назначается субъект, создавший данный объект.

В дальнейшем субъект, обладающий необходимыми правами, может назначить объекту *нового владельца*. При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя.

Такое ограничение вводится для того, чтобы владелец объекта не мог отдать владение объектом другому субъекту и тем самым снять с себя ответственность за некорректные действия с объектом.

Для определения прав доступа субъектов к объектам при избирательном разграничении доступа используются такие понятия, как матрица доступа и домен безопасности.

Домен безопасности (Protection Domain) определяет набор объектов и типов операций, которые могут производиться над каждым объектом операционной системы.

Избирательное разграничение доступа описывается матрицей, в *строках* которой перечислены субъекты доступа, в *столбцах* – объекты доступа, а в *ячейках – операции*, которые субъект может выполнить над объектом.

Расширением модели избирательного разграничения доступа является изолированная (или замкнутая) программная среда.

При использовании изолированной программной среды права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту. Например, разрешить обращаться к файлам с расширением doc только программам Word, Word Viewer.

Система правил разграничения доступа для модели изолированной программной среды:

1. Для любого объекта операционной системы существует владелец

2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой четверки субъект-объект-метод-процесс возможность доступа определена однозначно.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу.

5. Для каждого субъекта определен список программ, которые этот субъект может запускать

Изолированная программная среда существенно повышает защищенность операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы, повышается защищенность целостности данных, хранящихся в системе.

Изолированная программная среда не защищает от утечки конфиденциальной информации.

Полномочное, или мандатное, разграничение доступа (Mandatory Access Control) обычно применяется в совокупности с избирательным разграничением доступа.

Полномочное разграничение доступа с контролем информационных потоков

1. Для любого объекта операционной системы существует владелец.

2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой четверки субъект-объект-метод-процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Права процесса на доступ должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.

5. Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен

6. Каждый субъект доступа имеет уровень допуска. Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.

7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

– объект является объектом полномочного разграничения доступа;

– гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему;

– субъект открывает объект в режиме, допускающем чтение информации.

Это правило называют правилом NRU (Not Read Up - не читать выше).

8. Каждый процесс операционной системы имеет уровень конфиденциальности, равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования. Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.

9. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

– объект является объектом полномочного разграничения доступа;

– гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему;

– субъект собирается записывать в объект информацию.

Это правило разграничения доступа предотвращает утечку секретной информации – правило NWD (Not Write Down - не записывать ниже).

1. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:

– имеет доступ к объекту согласно правилу 7;

– обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

При использовании данной модели разграничения доступа существенно страдает производительность операционной системы, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтения/записи.

Если уровень конфиденциальности процесса строго выше нуля, то вся информация в памяти процесса фактически является секретной и не может быть записана в несекретный объект.

При чтении секретного файла процесс должен считать содержимое такого файла в секретную область памяти, используя для этого функции операционной системы, гарантирующие невозможность утечки информации.

Таблица 5. Сравнительные анализ моделей разграничения доступа

Свойства модели	Тип разграничения доступа		
	Избирательная	Изолированная среда	Полномочное с контролем потоков
Защита от утечки информации	отсутствуют	отсутствуют	имеется

Защищенность от разрушающих воздействий	низкая	высокая	низкая
Сложность реализации	низкая	средняя	высокая
Сложность администрирования	низкая	средняя	высокая
Затраты ресурсов компьютера	низкая	низкая	высокая
Использование ПО,разработанного для других систем	возможно	возможно	проблематично

Модель взаимодействия систем. Стек протоколов TCP/IP

1. Сетевые уровни

Сетевые уровни предназначены для осуществления этапов сетевой связи, выполняемых с помощью протоколов.

В компьютерных сетях для описания связи используется набор протоколов TCP/IP, условно привязанный к модели OSI

Рисунок 22. Соответствие уровней TCP/IP и OSI

2. Уровни сетевой модели TCP/IP

Принцип многослойной сетевой модели позволяет заменять отдельные протоколы на любом уровне другими протоколами, совместимыми с протоколами на соседних уровнях.

Рисунок 23. Протоколы, используемые на четырех уровнях модели TCP/IP в сетях Microsoft

Уровень сетевого интерфейса

Уровень сетевого интерфейса предназначен для:

– связи сетевых интерфейсов, которые идентифицируются по фиксированным аппаратным адресам. (Например, MAC-адреса);

– определения физических требований для обмена сигналами сегментов сети.

Сегмент сети включает в себя сетевые интерфейсы, отделенные кабелями, коммутаторами, концентраторами и беспроводными точками доступа.

Технология передачи данных: Ethernet, Token Ring, Point-to-Point Protocol (PPP).

Уровень Интернета

Уровень Интернета предназначен для взаимодействия между устройствами, расположенными в разных сетевых сегментах.

Протокол: IP

Устройство: маршрутизатор

Маршрутизаторы читают адрес назначения в пакете уровня Интернета, а затем перенаправляют сообщение по соответствующему пути в пункт назначения. Если адрес в пакете относиться к локальной сети или является широковещательным адресом в локальной сети, маршрутизатор по умолчанию отбрасывает такой пакет.

Транспортный уровень

Транспортный уровень модели TCP/IP предназначен для отправки и получения, данных устройствами, а так же для отметки предназначения данных для определенного приложения (Например, электронная почта, вебприложение).

В набор TCP/IP входят протоколы транспортного уровня: TCP и UDP.

При получении потока данных с сетевого хоста протокол TCP посылает их приложению на указанный TCP-порт.

TCP-порты позволяют различным приложениям и программам использовать TCP-службы на одном хосте.

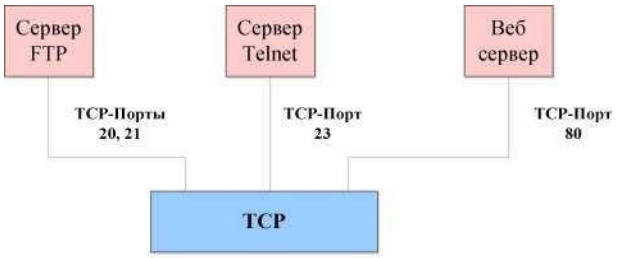

Рисунок 24. TCP-порты

Прикладной уровень

Прикладной уровень предназначен для осуществления такого этапа связи, на котором сетевые сервисы стандартизированы.

3. Инкапсуляция TCP/IP

Инкапсуляция данных на уровнях стека TCP/IP создает пакет, пригодный для передачи другому сегменту сети.

Рисунок 25. Пример пакета TCP-IP

Пакеты могут использовать как меньшим числом протоколов, за счет сквозной связи для нижерасположенных уровней (TCP), так и использовать более четырех протоколов, если используют по несколько протоколов на каждом уровне (на уровне 4 часто используются несколько прикладных протоколов и сервисов более высокого уровня).

4. Сетевые подключения.

Сетевые мосты

Предназначены для комбинирования множества сетевых подключений, для интерпретации системой их как одну сеть (в одном широковещательном домене).

Например, к одной точке беспроводного доступа (WAP) можно назначить общий доступ с множеством различных топологий подключений.

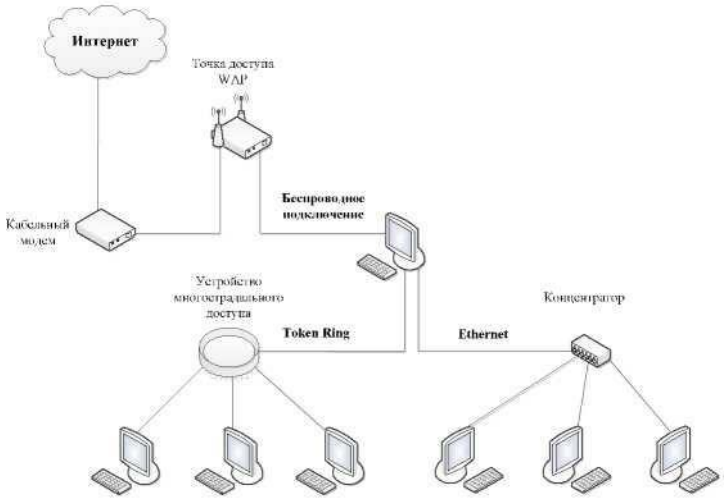

Рисунок 26. Пример сетевого моста

Подключение к интернету привязано к одной точке беспроводного доступа WAP. Точка WAP осуществляет связь через беспроводную сетевую интерфейсную карту.

При включении сетевого моста все точки входа на сервер (беспроводной доступ, Token Ring и Ethernet) объединяются в одну сеть.

Настройка IP-конфигурации

1. Статические. Адрес остается неизменным после перезапуска компьютера. Предназначен для идентификации серверного оборудования и сетевого оборудования.

2. Динамические. При автоматическом назначении параметров все сетевые подключения получают 1РУ4 от DHCP-сервера.

Адреса DHCP всегда обладают более высоким приоритетом по отношению к другим методам автоматической настройки конфигурации IPv4. Хост может получить IP-адрес от DHCP-сервера, если в пределах широковещательного диапазона находиться DHCP-сервер.

Сетевое широковещание – это режим передачи данных по всем локальным адресам. Транслируется через все устройства уровня 1 и 2 (например, кабели, повторители, концентраторы, мосты и коммутаторы) и блокируется устройствами на уровне 3 (маршрутизаторами).

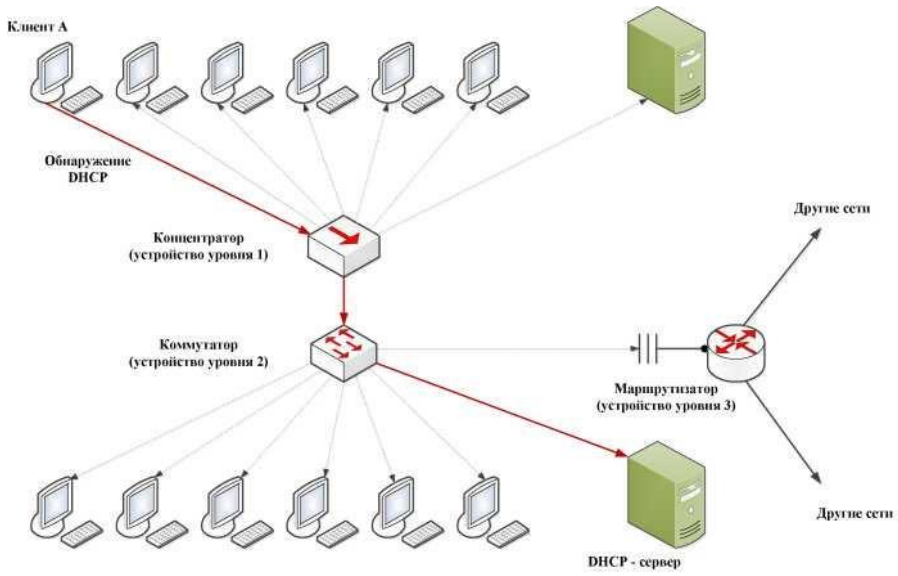

Рисунок 27. Пример сетевого широковещания

5. Адресация IP версии 4

Структура IPv4-адресов

Система адресации IPv4 обеспечивает уникальность и возможность поиска устройств, разделяя адреса на 2 части: идентификаторы сети и идентификаторы узла.

Идентификатор сети идентифицирует конкретную сети в инфраструктуре Ipv4 (например, Интернет)

Идентификатор узла идентифицирует узел IPv4 (например, компьютер, маршрутизатор или другое IPv4 устройство) в сети.

Суммарное количество бит в идентификаторе сети и идентификаторе узла

Рисунок 28. Идентификаторы сети и узла

6. Маска подсети

Маска подсети используется для определения части 32-битового IPv4адреса, которая представляет идентификатор сети.

192.168.23.254/24 - запись IP адреса с маской подсети /24.

/24 указывает, что первые 24 или 32 бита в этом IPv4-адресе должны представлять идентификатор сети.

Маршрутизация и основные шлюзы.

7. Блоки адресов и подсети

Адресация бывает публичной и частной.

Публичные адреса назначаются доступным из интернета серверам.

Частные адреса назначаются внутренним маршрутизаторам, серверам и клиентам.

Блок адресов – это готовая группа, образующих непрерывное пространство IP-адресов, у которых один идентификатор сети. Адреса в блоке составляют отдельную сеть.

8. Определение количества адресов в блоке сети /п

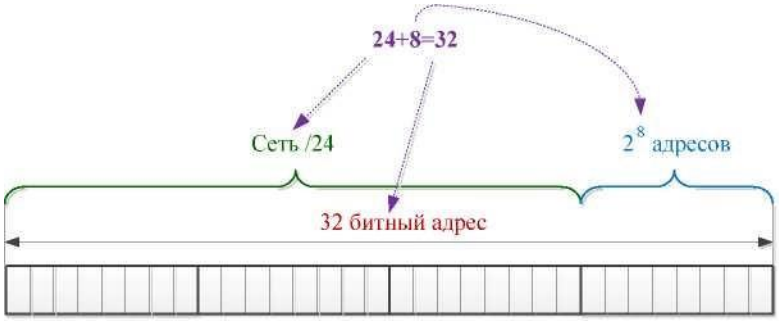

Рисунок 29. Математическая связь между значением /п и числом адресов

9. Разбиение адресного пространства на подсети

Разбиение на подсеть - это способ деления адресного пространства путем расширения строки битов, которая используется в маске подсети.

Предназначено для создания в исходном адресном пространстве сети множество подсетей или широковещательных доменов.

1. Использование маски подсети выданной провайдером. Используются только внутренние устройства данной сети (коммутаторы, концентраторы) 2. Использование маски подсети организации

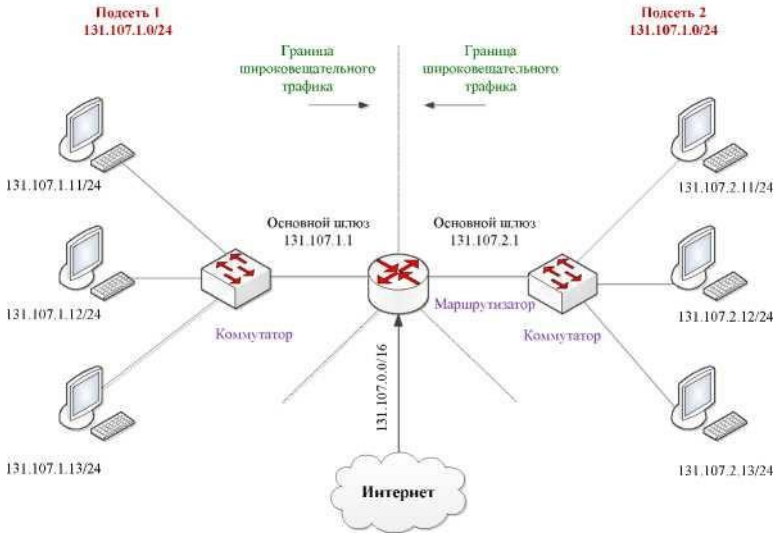

Рисунок 30. Разбиение на подсети адресного пространства

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Охарактеризуйте идентификацию и аутентификацию пользователей с использованием технических устройств.

2. Охарактеризуйте идентификацию и аутентификацию с использованием индивидуальных биометрических характеристик пользователя.

Тема 2.4 Защита на канальном уровне – протоколы удаленного доступа

Перечень изучаемых вопросов:

Протокол PPTP.

Протокол L2TP

Методические указания к изучению:

Защита на канальном уровне – протоколы удаленного доступа:

Протоколы PPTP (Point-to-Point Tunneling Protocol) и L2TP (Layer-2 Tunneling Protocol) являются протоколами туннелирования канального уровня модели OSI. Эти протоколы используются для организации защищенного мно-

гопротокольного удаленного доступа к ресурсам корпоративной сети через открытую сеть, например, через Интернет.

Клиентское программное обеспечение обычно использует для удаленного доступа стандартный протокол канального уровня PPP (Point-to-Point Protocol).

В набор PPP входят протокол управления соединением LCP (Link Control Protocol), ответственный за конфигурацию, установку, работу и завершение соединения точка-точка, и протокол управления сетью NCP (Network Control Protocol), способный инкапсулировать в PPP протоколы сетевого уровня для транспортировки через соединение точка-точка. Это позволяет одновременно передавать пакеты Novell IPX и Microsoft IP по одному соединению PPP.

Для доставки конфиденциальных данных из одной точки в другую через сети общего пользования сначала производится инкапсуляция данных с помощью протокола PPP, затем протоколы PPTP и L2TP выполняют шифрование данных и собственную инкапсуляцию.

После того как туннельный протокол доставляет пакеты из начальной точки туннеля в конечную, выполняется деинкапсуляция.

На физическом и канальном уровнях протоколы PPTP и L2TP идентичны.

1. Протокол PPTP. Протокол PPTP, предназначен для создания защищенных виртуальных каналов при доступе удаленных пользователей к локальным сетям через Интернет. Протокол PPTP предполагает создание криптозащищенного туннеля на канальном уровне модели OSI для случаев как прямого соединения удаленного компьютера с открытой сетью, так и подсоединения его к открытой сети по телефонной линии через провайдера.

Пакеты, передаваемые в рамках сессии PPTP, имеют следующую структуру:

- заголовок канального уровня, используемый внутри Интернета, например, заголовок кадра Ethernet;
- заголовок IP, содержащий адреса отправителя и получателя пакета;
- заголовок общего метода инкапсуляции для маршрутизации GRE
- (Generic Routing Encapsulation);
- исходный пакет PPP, включающий пакет IP, IPX или NetBEUI.

Рисунок 31. Структура пакета для пересылки по туннелю PPTP

Принимающий узел сети извлекает из пакетов IP кадры PPP, а затем извлекает из кадра PPP исходный пакет IP, IPX или NetBEUI и отправляет его по локальной сети конкретному адресату. Многопротокольность инкапсулирующих протоколов канального уровня, к которым относится протокол PPTP, явля-

ется их важным преимуществом перед протоколами защищенного канала более высоких уровней.

Данный способ инкапсуляции обеспечивает независимость от протоколов сетевого уровня модели OSI и позволяет осуществлять защищенный удаленный доступ через открытые IP-сети к любым локальным сетям (IP, IPX или NetBEUI). Протокол PPTP при создании защищенного виртуального канала производит аутентификацию удаленного пользователя и шифрование передаваемых данных.

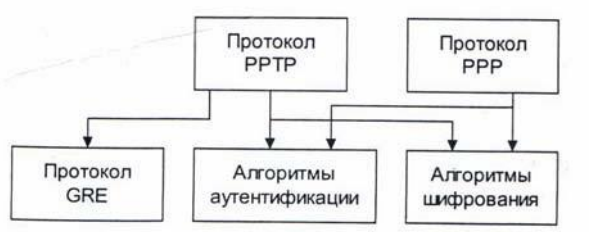

Рисунок 32. Архитектура протокола PPTP

Для аутентификации удаленного пользователя в реализации PPTP поддерживаются следующие протоколы аутентификации:

– протоколаутентификации по паролю PAP (Password Authentication Protocol);

– протокол аутентификации при рукопожатии MSCHAP (Microsoft Challenge-Handshaking Authentication Protocol);

– протокол аутентификации EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).

При использовании протокола PAP идентификаторы и пароли передаются по линии связи в незашифрованном виде, при этом только сервер проводит аутентификацию клиента.

При использовании протоколов MSCHAP и EAP-TLS обеспечиваются защита от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем и взаимная аутентификация клиента и VPNсервера.

Протокол PPTP изменяет значение ключа шифрования после каждого принятого пакета.

Протокол PPTP применяется в схеме туннелирования при прямом подсоединении компьютера удаленного пользователя к Интернету.

Рисунок 33. Схема туннелирования при прямом подсоединении компьютера удаленного пользователя к Интернету

1. Удаленный пользователь устанавливает удаленное соединение с локальной сетью с помощью клиентской части сервиса удаленного доступа RAS (Remote Access Service), входящего в состав Windows.

2. Удаленный пользователь обращается к серверу удаленного доступа локальной сети, указывая его IP-адрес, и устанавливает связь по протоколу PPTR.

Функции сервера удаленного доступа может выполнять пограничный маршрутизатор локальной сети.

Служебные сообщения передаются по протоколу TCP.

После успешной аутентификации начинается процесс защищенного информационного обмена.

2. Протокол L2TP. Протокол L2TP – протокол защищенного туннелирования PPP-трафика через сети общего назначения с произвольной средой. L2TP не привязан к протоколу IP, поэтому он может быть использован в сетях с коммутацией пакетов, например, в сетях ATM (Asynchronous Transfer Mode) или в сетях с ретрансляцией кадров (Frame Relay). Кроме того, в протокол L2TP добавлена функция управления потоками данных.

В протокол L2TP включена возможность работы с протоколами AH и ESP стека протоколов IPSec.

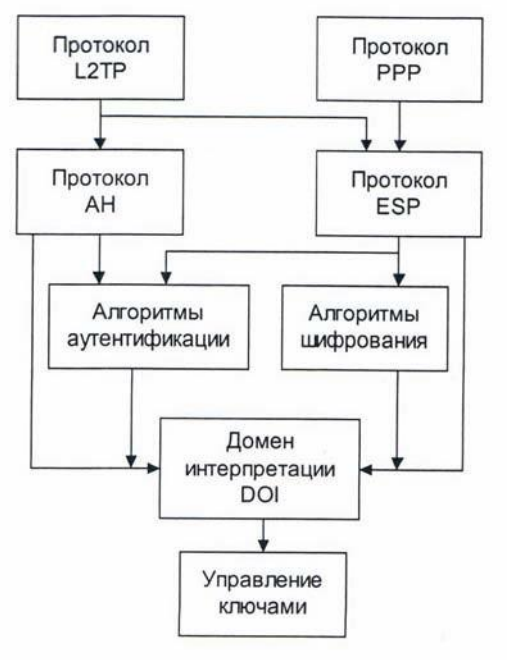

Рисунок 34. Архитектура протокола L2TP

Протокол L2TP применяет в качестве транспорта протокол UDP и использует одинаковый формат сообщений как для управления туннелем, так и для пересылка данных.

В реализации Microsoft протокол L2TP использует в качестве контрольных сообщений пакеты UDP, содержащие шифрованные пакеты PPP. Надежность доставки гарантирует контроль последовательности пакетов.

Протокол L2TP начинает сборку пакета для передачи в туннель с добавления к полю информационных данных заголовка PPP, а затем заголовка L2TP. Полученный пакет инкапсулируется протоколом UDP. В качестве порта отправителя и получателя протокол L2TP использует UDP-порт 1701.

Рисунок 35. Структура пакета для пересылки по туннелю L2TP

В зависимости от выбранного типа политики безопасности стека протоколов IPSec протокол L2TP может шифровать UDP-сообщения и добавлять к ним заголовок и окончание ESP (Encapsulating Security Payload), а также окон-

чание IPSec ESP Authentication. Затем производится инкапсуляция в IP. Добавляется IP-заголовок, содержащий адреса отправителя и получателя. В завершение L2TP выполняет вторую PPP-инкапсуляцию для подготовки данных к передаче.

Компьютер-получатель принимает данные, обрабатывает заголовок и окончание PPP, убирает заголовок IP. При помощи IPSec ESP Authentication проводится аутентификация информационного поля IP, а протокол ESP IPSec помогает расшифровать пакет. Далее компьютер обрабатывает заголовок UDP и использует заголовок L2TP для идентификации туннеля. Теперь пакет PPP содержит только полезные данные, которые обрабатываются или пересылаются указанному получателю.

Протокол L2TP поверх IPSec обеспечивает аутентификацию на уровнях «пользователь» и «компьютер», а также выполняет аутентификацию и шифрование данных. На первом этапе аутентификации клиентов и серверов VPN протокол L2TP использует локальные сертификаты, полученные от службы сертификации. Клиент и сервер обмениваются сертификатами и создают защищенное соединение ESP SA (Security Association).

После того как L2TP (поверх IPSec) завершает процесс аутентификации компьютера, выполняется аутентификация на уровне пользователя. Для этой аутентификации используется протокол, даже PAP, передающий имя пользователя и пароль в открытом виде. L2TP (поверх IPSec) шифрует всю сессию, что делает процесс передачи безопасным.

Проведение аутентификации пользователя при помощи MSCHAP, применяющего различные ключи шифрования для аутентификации компьютера и пользователя, может повысить безопасность.

Протокол L2TP предполагает использование схемы, в которой туннель образуется между сервером удаленного доступа провайдера и маршрутизатором корпоративной сети.

Протокол L2TP предоставляет возможность открывать между конечными абонентами сразу несколько туннелей, каждый из которых может быть выделен для отдельного приложения. Эти особенности обеспечивают гибкость и безопасность туннелирования.

Согласно спецификации протокола, L2TP роль сервера удаленного доступа провайдера должен выполнять концентратор доступа LAC (L2TP Access Concentrator), который реализует клиентскую часть протокола L2TP и обеспечивает удаленному пользователю сетевой доступ к его локальной сети через Интернет. В качестве сервера удаленного доступа локальной сети должен выступать сетевой сервер LNS (L2TP Network Server), функционирующий на совместимых с протоколом PPP платформах.

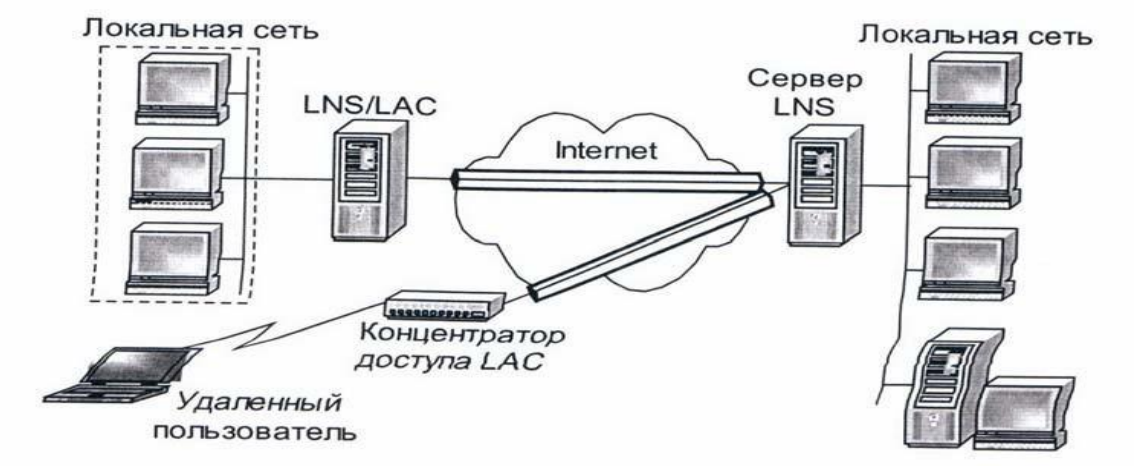

Рисунок 36. Схемы туннелирования по протоколу L2TP

Этапы формирования защищенного виртуального канала в протоколе L2TP:

– установление соединения с сервером удаленного доступа локальной
14. сети;
– аутентификация пользователя;
– конфигурирование защищенного туннеля.

15. На первом этапе для установления соединения с сервером удаленного доступа локальной сети удаленный пользователь инициирует PPP-соединение с провайдером ISP. Концентратор доступа LAC, функционирующий на сервере провайдера ISP, принимает это соединение и устанавливает канал PPP. Концентратор доступа LAC выполняет частичную аутентификацию конечного узла и его пользователя. Используя только имя пользователя, провайдер ISP решает, нужен ли пользователю сервис туннелирования L2TP. Если такой сервис нужен, то следующим шагом для концентратора доступа LAC будет выяснение адреса сетевого сервера LNS, с которым нужно установить туннельное соединение. Для удобства определения соответствия между пользователем и сервером LNS, обслуживающим сеть пользователя, может использоваться база данных, поддерживаемая провайдером ISP для своих клиентов.

После выяснения IP-адреса сервера LNS производится проверка, не существует ли уже туннель L2TP с этим сервером. Если такого туннеля нет, то он устанавливается. Между концентратором доступа провайдера LAC и сетевым сервером LNS локальной сети устанавливается сессия по протоколу L2TP.

При создании туннеля между LAC и LNS новому соединению в рамках этого туннеля присваивается идентификатор, называемый идентификатором вызова Call ID. Концентратор LAC отправляет сетевому серверу LNS пакет с уведомлением о вызове с данным Call ID. Сервер LNS может принять этот вызов или отклонить его.

На втором этапе после установления сессии L2TP сетевой сервер LNS локальной сети выполняет процесс аутентификации пользователя. Для этого может быть использован один из стандартных алгоритмов аутентификации, в частности CHAP. В случае применения протокола аутентификации CHAP пакет уведомления включает слово-вызов, имя пользователя и его ответ. Для протокола PAP эта информация состоит из имени пользователя и незашифрованного пароля. Сетевой сервер LNS может сразу использовать эту информацию для выполнения аутентификации, чтобы не заставлять удаленного пользователя повторно вводить свои данные и не осуществлять дополнительный цикл аутентификации.

При отправке результата аутентификации сетевой сервер LNS может также передать концентратору доступа LAC сведения об IP-адресе узла пользователя. Концентратор доступа LAC работает как посредник между узлом удаленного пользователя и сетевым сервером LNS локальной сети.

На третьем этапе в случае успешной аутентификации пользователя создается защищенный туннель между концентратором доступа LAC провайдера и сервером LNS локальной сети. В результате инкапсулированные кадры PPP могут передаваться по туннелю между концентратором LAC и сетевым сервером LNS в обоих направлениях. При поступлении кадра PPP от удаленного пользователя концентратор LAC удаляет из него байты обрамления кадра, байты контрольной суммы, затем инкапсулирует его с помощью протокола L2TP в сетевой протокол и отправляет по туннелю сетевому серверу LNS. Сервер LNS, используя протокол L2TP, извлекает из прибывшего пакета кадр PPP и обрабатывает его стандартным образом.

Настройка необходимых значений параметров туннеля производится помощью управляющих сообщений. Протокол L2TP может работать поверх любого транспорта с коммуникацией пакетов. Транспорт, например, протокол UDP, не обеспечивает гарантированной доставки пакетов. Поэтому протокол L2TP самостоятельно решает эти вопросы, используя процедуры установления соединения внутри туннеля для каждого удаленного пользователя.

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Охарактеризуйте IPSec протокол.
2. Охарактеризуйте концентратор доступа LAC.
3. Поясните принципы построения сервер LNS

3.2.5 Тема 2.5 Протоколы IPSec, SSL, TSL, SOCKS. Защита на сетевом и сеансовом уровнях

Перечень изучаемых вопросов:
Классификация систем обнаружения вторжений.
Перечень изучаемых вопросов:
Протокол Internet Protocol Security (IPSec).
Протокол SSL.
Протокол TSL.
Протокол SOCKS.

Методические указания к изучению:

Протокол Internet Protocol Security (IPSec) обеспечивает защиту сетей, выполняя шифрование пакетов IP и используя безопасные подключения.

Протокол IPSec можно применять для обеспечения безопасности связи между двумя узлами или для защиты трафика через Интернет в сценариях, с использованием виртуальной частной сети (VPN).

1. Проверка подлинности данных. Обеспечение аутентификации данных в виде проверки подлинности данных, целостности данных и защиты от повторного воспроизведения.

Проверка подлинности приходящих данных. При наличии протокола IPSec можно гарантировать, что каждый пакет, получаемый от доверенной стороны, предоставляет подлинные данные доверенной стороны, а не искажен на пути следования.

Целостность данных. Можно гарантировать, что данные не будут изменены во время передачи. Защита от повторного воспроизведения. Позволяет проверять уникальность каждого пакета, чтобы предотвратить дублирование.

2. Шифрование. С помощью протокола IPSec можно шифровать сетевые данные, чтобы их нельзя было прочитать или перехватить во время передачи.

1. Сопоставление безопасности

Безопасность обмена данными обеспечивается «сопоставлением безопасности» (SecurityAssociation, SA).

В SA безопасность обеспечивается с помощью протоколов:

Протоколом проверки подлинности заголовка (AuthenticationHeader, AH) обеспечивает аутентичность и целостность данных, а также защиту от повторного воспроизведения для всего IP-пакета. Протоколом безопасности инкапсуляции данных

(EncapsulatingSecurityPayload, ESP) обеспечивает шифрование, аутентификацию источника и целостность данных, а также защиту от повторного воспроизведения для передаваемого потока ESP.

2. Протокол аутентификации заголовка

Протокол АН – это IP-протокол 51. Он поддерживает функциональные возможности аутентификации и проверки целостности, но не поддерживает конфиденциальность содержимого пакета.

Обеспечение аутентификации и защиты целостности достигается добавлением дополнительного заголовка к IP-пакету. Этот заголовок содержит цифровую подпись, называемую *значением проверки целостности* (IntegrityCheckValue, ICV), которая является значением хеш-функции, подтверждающей, что пакет был изменен во время транспорта.

Протокол АН просматривает заголовок IP-пакета при вычислении цифровой подписи, и определяет подлинность IP-адреса отправителя, и самого отправителя.

Использование информации IP-заголовка протоколом АН делает его несовместимым с использованием NAT.

Структура заголовка АН-пакета представлена на Рисунок 15.1.

Следующий заголовок	Длинна содержимого пакета	Зарезервировано
Индекс параметра обеспечения безопасности (SPI)		
Порядковый номер		
Информация аутентификации (переменная длинна, кратная 32 байтам)		

Рисунок 37. Структура заголовка АН-пакета

Поле *следующего заголовка* содержит идентификатор, определяющий тип заголовка АН-пакета: транспортный, туннельный.

Индекс периметра предназначен для обеспечения безопасности и показывает, частью какого уникального потока связи является рассматриваемый пакет.

Порядковый номер - это уникальное увеличивающееся значение, которое предназначено для противодействия повторному использованию пакета.

Поле *информации аутентификации* содержит значение проверки целостности и цифровую подпись, подтверждающую подлинность рассматриваемого пакета.

3. Протокол безопасности инкапсуляции содержимого пакета

Протокол ESP – это IP-протокол 50. Он обеспечивает конфиденциальность при помощи полного шифрования содержимого IP-пакетов.

Протокол ESP реализован в виде модулей и может использовать любое количество доступных симметричных алгоритмов шифрования.

Применение протокола ESP различается в зависимости от используемого режима протокола IPSec.

В транспортном режиме протокол ESP добавляет свой заголовок после IP-заголовка и зашифровывает остальную часть сетевого пакета, начиная с транспортного уровня. Если при этом определена служба аутентификации, то протокол ESP добавляет концевую метку (trailer).

Концевая метка предназначена для подтверждения целостности пакета и аутентификации (в отличие от протокола AH значение проверки целостности вычисляется без использования информации из IP-заголовка).

При использовании туннельного режима протокол ESP инкапсулирует оригинальный пакет полностью, шифруя его целиком и создавая новый IPзаголовок и ESP-заголовок в устройстве туннелирования.

Концевая метка добавляется в случае выбора аутентификационного сервиса протокола ESP.

Структура заголовка пакета ESP приведена на Рисунок 15.2.

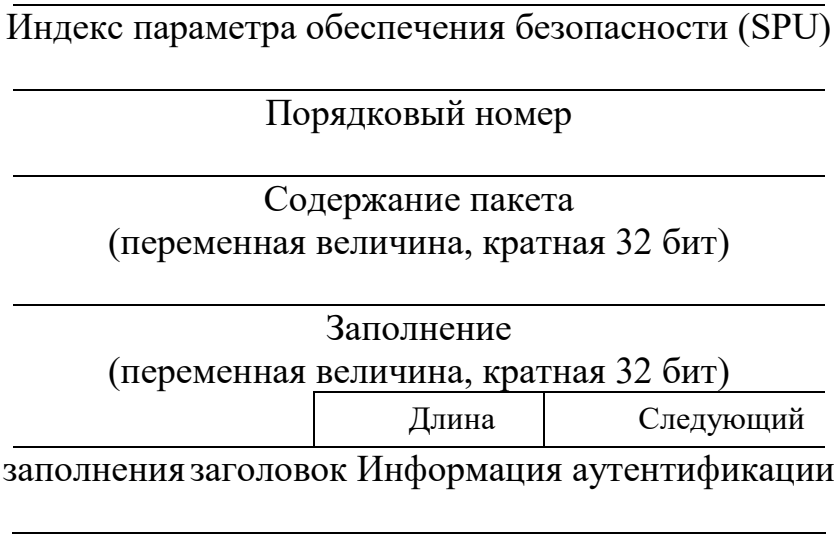

Рисунок 38. Структура заголовка пакета ESP

В любом режиме протокол ESP использует в каждом сетевом пакете порядковые номера. При работе протокола ESP в туннельном режиме

можно использовать NAT.

Поле длины заполнения указывает, насколько заполнено содержимое пакета, чтобы длина содержимого пакета и последующие поля заголовка соответствовали требованию *выравнивания длины* сетевого пакета.

Поле следующего заголовка сообщает номер протокола пакета, который инкапсулирован внутри пакета протокола ESP.

Поле информации аутентификации содержит дополнительное значение проверки целостности, которое доступно для пакетов протокола ESP.

4. Особенности реализации средств IPSec

Протоколы AH или ESP могут защищать передаваемые данные в двух режимах:

 туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки;

 транспортном, обеспечивающем защиту только содержимого IPпакетов.

Основным режимом является туннельный. В туннельном режиме исходный пакет помещается в новый IP-пакет, и передача данных по сети выполняется на основании заголовка нового IP-пакета.

При работе в этом режиме каждый обычный IP-пакет помещается целиком в криптозащищенном виде в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой защищенный IP-пакет. Туннельный режим обычно реализуют на специально выделенных шлюзах безопасности, в роли которых могут выступать маршрутизаторы или межсетевые экраны. Между такими шлюзами и формируются защищенные туннели IPSec.

После приема на другой стороне туннеля защищенные IP-пакеты распаковываются, и полученные исходные IP-пакеты передаются компьютерам приемной локальной сети по стандартным правилам.

В транспортном режиме передача IP-пакета через сеть выполняется с помощью исходного заголовка этого пакета. В конверт IPSec в криптозащищенном виде помещается только содержимое исходного IP-пакета, и к полученному конверту добавляется исходный IP-заголовок. Транспортный режим быстрее туннельного и разработан для применения на оконечных системах. Данный режим может использоваться для поддержки удаленных и мобильных пользователей, а также для защиты информационных потоков внутри локальных сетей.

5. Основные схемы применения IPSec

Узлом, завершающим защищенный канал, может быть хост (конечный узел) или шлюз (промежуточный узел).

Схемы применения IPSec:

a) хост-хост;

b) шлюз-шлюз; хост-шлюз.

В первой схеме защищенный канал, устанавливается между двумя конечными узлами сети, то есть хостами H1 и H2.

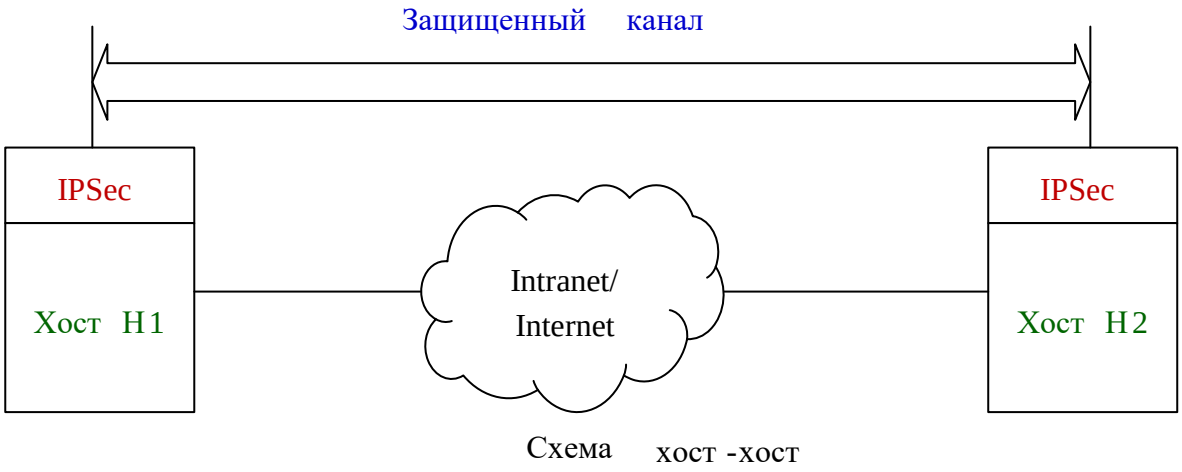

Рисунок 39. Схема хост-хост

Протокол IPSec работает на конечном узле и защищает данные, поступающие на него. Для хостов, поддерживающих IPSec, разрешается использовать как транспортный режим, так и туннельный.

В соответствии со второй схемой защищенный канал устанавливается между двумя промежуточными узлами, называемыми шлюзами безопасности SG1 и SG2, на каждом из которых работает протокол IPSec.

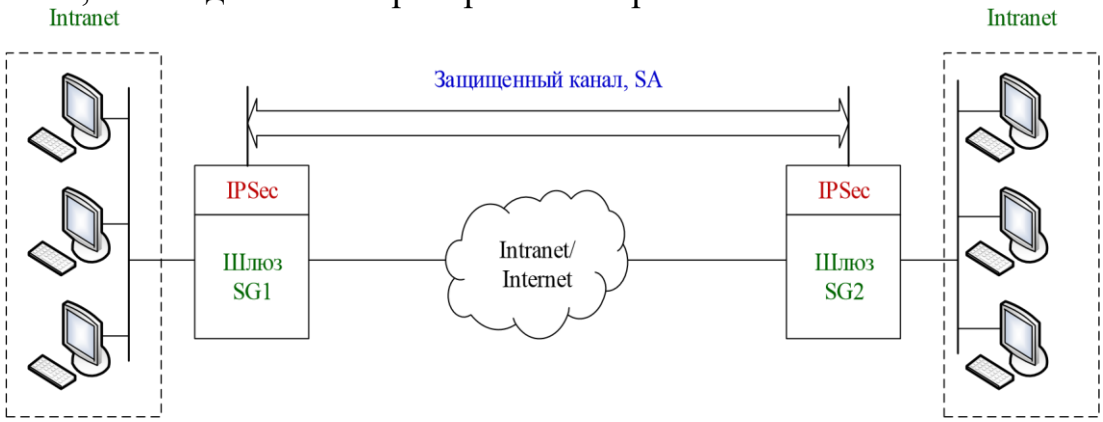

Рисунок 40 Схема шлюз-шлюз

Шлюз безопасности – это сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для хостов, расположенных позади него.

Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, которые расположены позади шлюзов безопасности. При защищенном удаленном доступе часто применяется схема хост-шлюз.

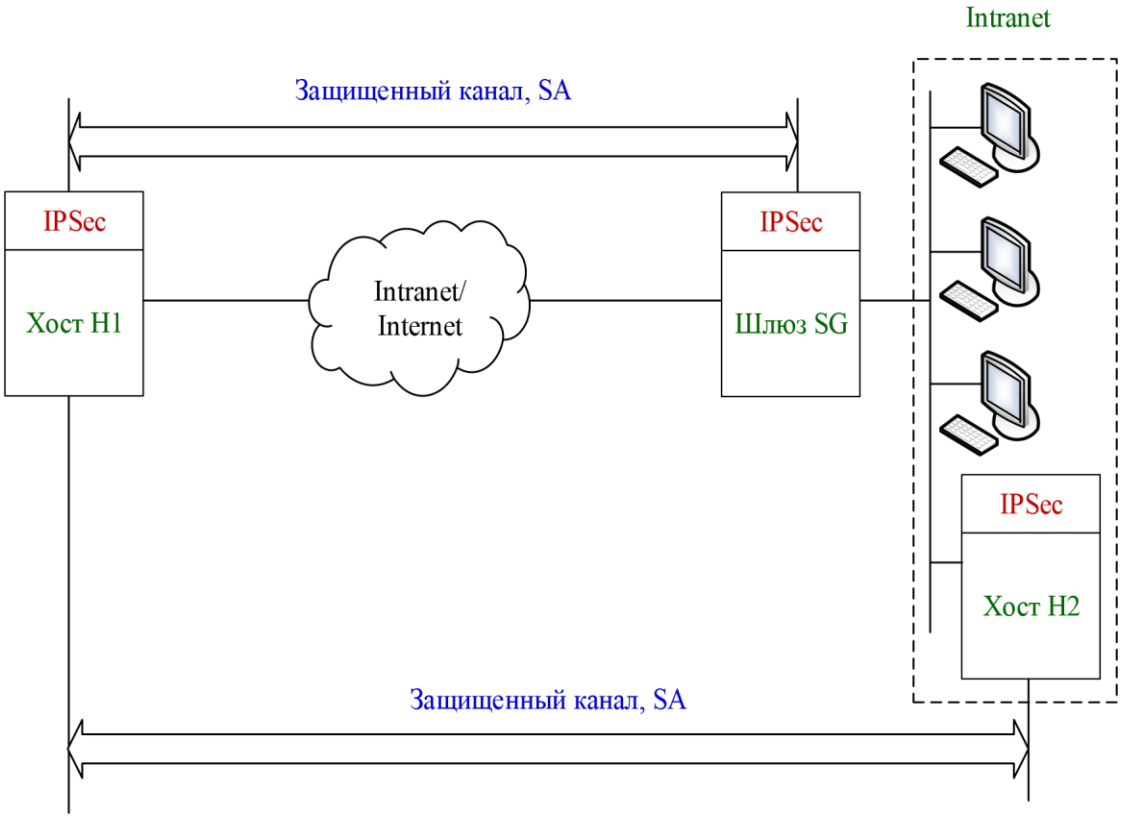

Рисунок 41. Схема хост-шлюз, дополненная каналом хост-хост

Здесь защищенный канал организуется между удаленным хостом H1, на котором работает IPSec, и шлюзом SG, защищающем трафик для всех хостов, входящих в сеть интранет предприятия. Удаленный хост может использовать при отправке пакетов шлюзу как транспортный, так и туннельный режим, шлюз же отправляет пакеты хосту только в туннельном режиме.

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

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, соответствующие общепринятому стандарту X.509, а также стандарты инфраструктуры открытых ключей PKI (Public Key Infrastructure), с помощью которой организуются выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей.

Подлинность и целостность циркулирующей информации обеспечиваются за счет формирования и проверки электронной цифровой подписи. Для цифровых подписей и обмена ключами шифрования используются алгоритмы с открытым ключом.

Туннели создаются между конечными точками виртуальной сети. Инициаторами каждого защищенного туннеля являются клиент и сервер, функционирующие на компьютерах в конечных точках туннеля.

Сервер Локальная сеть

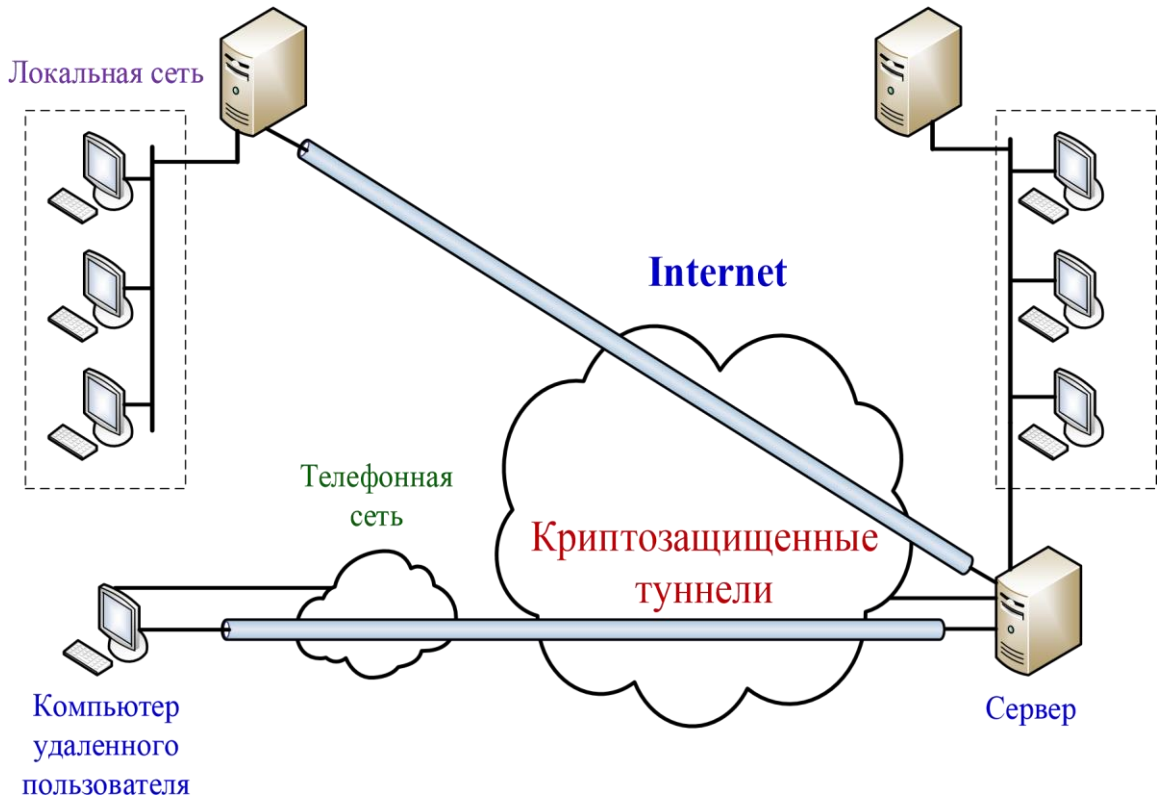

Рисунок 42. Криптозащищенные туннели, сформированные на основе протокола SSL

Этапы взаимодействия клиента и сервера при формировании и поддержке защищаемого соединения протоколом SSL:

– установление SSL-сессии;
– защищенное взаимодействие.

– В процессе установления SSL-сессии решаются следующие задачи: аутентификация сторон;

– согласование криптографических алгоритмов и алгоритмов сжатия, которые будут использоваться при защищенном информационном обмене;

– формирование общего секретного мастер-ключа;

– генерация на основе сформированного мастер-ключа общих секретных сеансовых ключей для криптозащиты информационного обмена.

Процедура установления SSL-сессии, называемая также процедурой рукопожатия, отрабатывается перед непосредственной защитой информационного обмена и выполняется по протоколу начального приветствия (Handshake Protocol), входящему в состав протокола SSL.

При установлении повторных соединений между клиентом и сервером стороны могут, по взаимному соглашению, формировать новые сеансовые ключи на основе старого общего секрета (данная процедура называется продолжением SSL-сессии).

В реализациях протокола SSL для аутентификации взаимодействующих сторон и формирования общих секретных ключей чаще всего используют алгоритм RSA.

Соответствие между открытыми ключами и их владельцами устанавливается с помощью *цифровых сертификатов*, выдаваемых специальными центрами сертификации.

Типы аутентификации в протоколе SSL: аутентификация сервера клиентом; аутентификация клиента сервером.

SSL-аутентификация сервера позволяет клиенту проверить подлинность сервера.

SSL-аутентификация клиента позволяет серверу проверить личность пользователя.

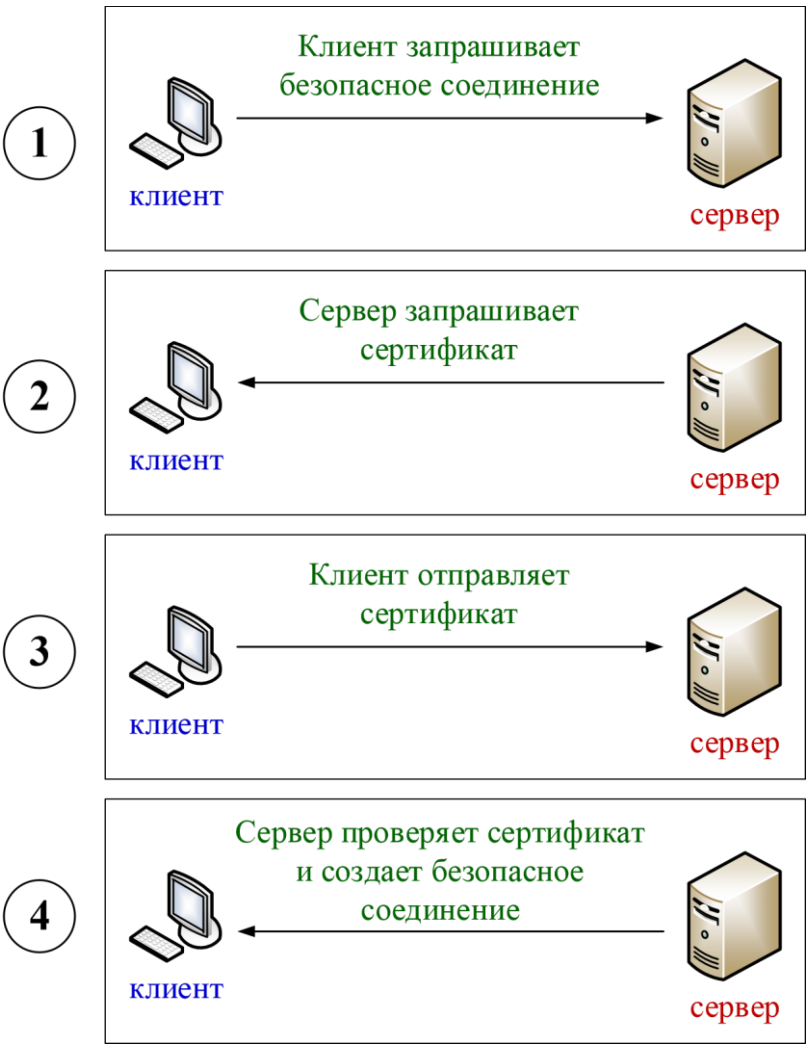

Рисунок 43. Функции безопасности, предоставляемые протоколом SSL

Функции безопасности, предоставляемые протоколом SSL:

– шифрование данных с целью предотвратить раскрытие конфиденциальных данных во время передачи;

– подписывание данных с целью предотвратить несанкционированное изменение данных во время передачи;

– аутентификация клиента и сервера, позволяющая убедиться, что общение ведется с соответствующим человеком или компьютером.

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

Функции программ-посредников:

– идентификацию и аутентификацию пользователей;

– криптозащиту передаваемых данных;

– разграничение доступа к ресурсам внутренней сети;

– разграничение доступа к ресурсам внешней сети;

– фильтрацию и преобразование потока сообщений, например, поиск вирусов и прозрачное шифрование информации;

– трансляцию внутренних сетевых адресов для исходящих потоков сообщений.

Различают SOCKS-сервер, который устанавливается на шлюз (межсетевой экран) сети, и SOCKS-клиент, который устанавливают на каждый пользовательский компьютер.

SOCKS-сервер обеспечивает взаимодействие с любым прикладным сервером от имени, соответствующего этому серверу прикладного клиента.

SOCKS-клиент предназначен для перехвата всех запросов к прикладному серверу со стороны клиента и передачи их SOCKS-серверу.

Общая схема установления соединения по протоколу SOCKS версии 5:

– запрос прикладного клиента, желающего установить соединение с каким- либо прикладным сервером в сети, перехватывает установленный на этом же компьютере SOCKS-клиент;

– соединившись с SOCKS-сервером, SOCKS-клиент сообщает ему идентификаторы всех методов аутентификации, которые он поддерживает;

– SOCKS-сервер решает, каким методом аутентификации воспользоваться (если SOCKS-сервер не поддерживает ни один из методов аутентификации, предложенных SOCKS-клиентом, соединение разрывается);

– при поддержке каких-либо предложенных методов аутентификации SOCKS- сервер в соответствии с выбранным методом аутентифицирует пользователя, от имени которого выступает SOCKS-клиент; в случае безуспешной аутентификации SOCKS-сервер разрывает соединение;

– после успешной аутентификации SOCKS-клиент передает SOCKSсерверу DNS-имя или IP-адрес запрашиваемого прикладного сервера в сети, и далее SOCKS-сервер на основе имеющихся правил разграничения доступа принимает решение об установлении соединения с этим прикладным сервером;

– в случае установления соединения прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS-сервер ретранслирует данные, а также может выполнять функции посредничества по защите сетевого взаимодействия: например, если в ходе аутентификации SOCKS-клиент и SOCKS-сервер обменялись сеансовым ключом, то весь трафик между ними может шифроваться.

Аутентификация пользователя, выполняемая SOCKS-сервером, может основываться на цифровых сертификатах в формате X.509 или паролях.

Для формирования защищенных виртуальных сетей по протоколу SOCKS в точке сопряжения каждой локальной сети с Интернетом на компьютере-шлюзе устанавливается SOCKS-сервер, а на рабочих станциях в локальных сетях и на компьютерах удаленных пользователей – SOCKS-клиенты.

Удаленные пользователи могут подключаться к Интернету любым способом – по коммутируемой или выделенной линии. При попытке пользователя защищенной виртуальной сети установить соединение с каким-либо приклад-

ным сервером SOCKS-клиент начинает взаимодействовать с SOCKS-сервером. По завершении первого этапа взаимодействия пользователь будет аутентифицирован, а проверка правил доступа покажет, имеет ли он право соединиться с конкретным серверным приложением, функционирующим на компьютере с указанным адресом. Дальнейшее взаимодействие может происходить по криптографически защищенному каналу.

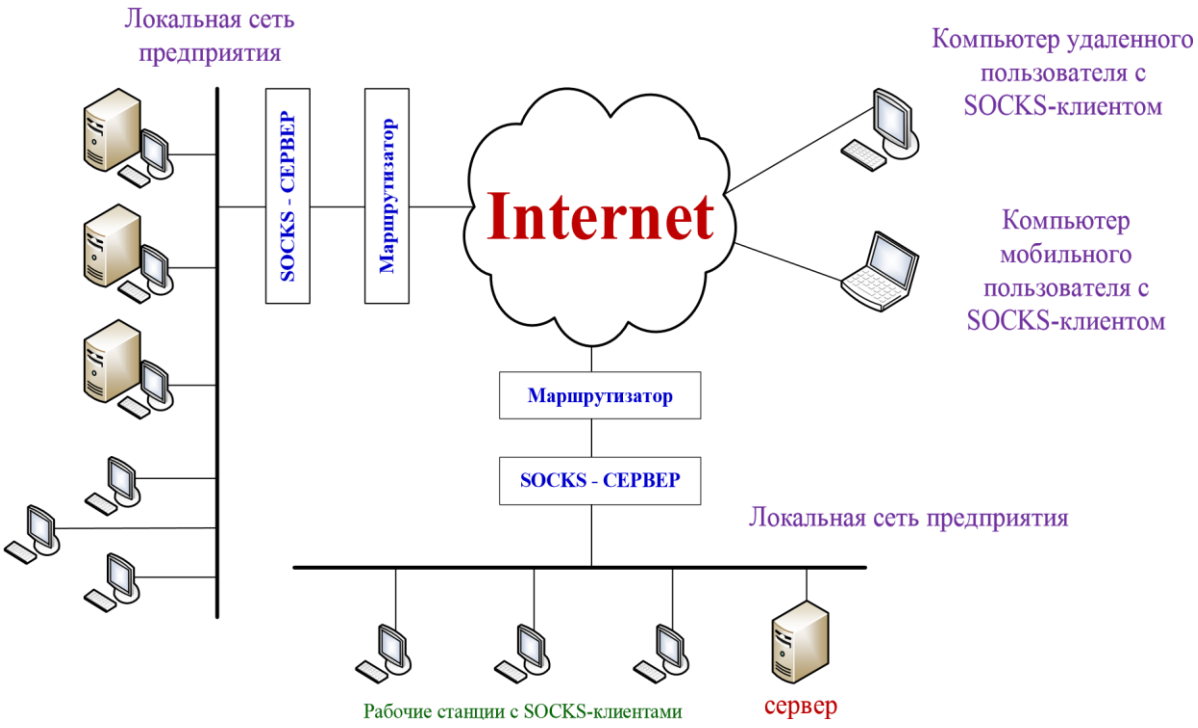

Рисунок 44. Схема взаимодействия по протоколу SOCKS

Для достижения более высокой степени безопасности сетевого взаимодействия серверы локальной сети, к которым разрешен доступ со стороны Интернета, должны быть выделены в отдельный подсоединяемый к SOCKS-серверу сегмент, образующий защищаемую открытую подсеть.

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:
1. Функции программ-посредников.
2. Общая схема установления соединения по протоколу SOCKS.
3. Типы аутентификации в протоколе SSL.

3.2.6 Тема 2.6 . Функционирование межсетевых экранов на различных уровнях модели OSI

Перечень изучаемых вопросов:
Фильтрация пакетов.
Трансляция сетевых адресов.
Межсетевые экраны уровня соединения.
Межсетевые экраны прикладного уровня.
Межсетевые экраны с динамической фильтрацией пакетов.
Межсетевые экраны инспекции состояний.

Методические указания к изучению:

Для противодействия несанкционированному межсетевому доступу межсетевой экран МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью. Все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно межсетевой экран входит в состав защищаемой сети.

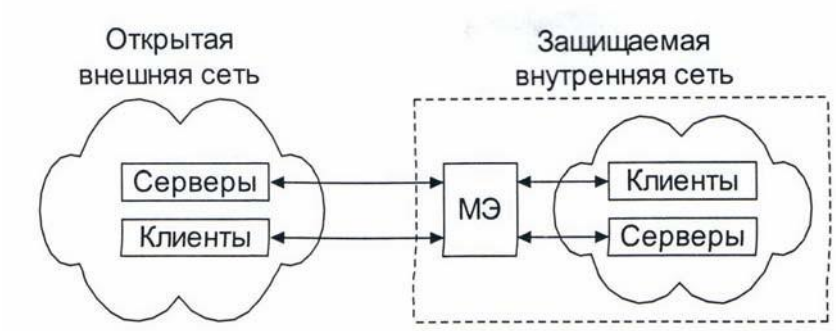

Рисунок 45. Схема подключения межсетевого экрана

Задачи межсетевого экрана:

– ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети;

– разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей.

Классификация МЭ:

По функционированию на уровнях модели OSI:

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

По используемой технологии:

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

По исполнению:

- аппаратно-программный;
- программный.

По схеме подключения:

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

1. Фильтрация трафика

Фильтрация осуществляется на основе набора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. Следовательно, межсетевой экран удобно представлять, как последовательность фильтров, обрабатывающих информационный поток.

Рисунок 46. Структура межсетевого экрана

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

1. Анализ информации по заданным в интерпретируемых правилах критериям: например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена.

2. Принятие на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;

– обработать данные от имени получателя и возвратить результат отправителю;

– передать данные на следующий фильтр для продолжения анализа; пропустить данные, игнорируя следующие фильтры.

Перечень условий, по которым осуществляется фильтрация: 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. Чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

2. Выполнение функций посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, вызываемых программами-посредниками или экранирующими агентами. Программы-посредники 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. Обмен информацией между компьютерами внутренней и внешней сетей осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

МЭ может выполнять функции фильтрации без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетями.

Программы-посредники, блокируя прозрачную передачу потока I сообщений, могут выполнять следующие функции:

– проверку подлинности передаваемых данных;

– фильтрацию и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;

– разграничение доступа к ресурсам внутренней сети;

– разграничение доступа к ресурсам внешней сети;

– кэширование данных, запрашиваемых из внешней сети.

– идентификацию и аутентификацию пользователей;

– трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;

– регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов.

Программы-посредники могут выполнять разграничение доступа к ресурсам внутренней или внешней сети, используя результаты идентификации и аутентификации пользователей при их обращении к межсетевому экрану.

При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

– разрешение доступа только по заданным адресам во внешней сети;
– фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
– накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти МЭ и полный запрет доступа во внешнюю сеть.

С помощью специальных посредников поддерживается кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на жестком диске МЭ, называемого в этом случае прокси-сервером. Поэтому если при очередном запросе нужная информация окажется на проксисервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ.

Виды 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.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например, обезвреживание обнаруженных компьютерных вирусов.

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

3. Дополнительные возможности МЭ Дополнительные возможности МЭ:

– идентификация и аутентификация пользователей;
– трансляция внутренних сетевых адресов для исходящих пакетов сообщений;
– регистрация событий;
– реагирование на задаваемые события;

– анализ зарегистрированной информации и генерация отчетов.

Идентификация и аутентификация пользователей иногда осуществляются при предъявлении обычного идентификатора (имени) и пароля. Эта схема уязвима с точки зрения безопасности – пароль может быть перехвачен и использован другим лицом. Пароль следует передавать через общедоступные коммуникации в зашифрованном виде. Это позволяет предотвратить получение несанкционированного доступа путем перехвата сетевых пакетов.

Более надежным методом аутентификации является использование одноразовых паролей. Широкое распространение получила технология аутентификации на основе одноразовых паролей SecurID.

Для безопасной авторизации также целесообразно применение цифровых сертификатов, выдаваемых доверенными органами, например, центром распределения ключей.

Трансляция сетевых адресов. Для сокрытия топологии сети межсетевые экраны выполняют трансляцию внутренних сетевых адресов (Network Address Translation).

Рисунок 47. Трансляция сетевых адресов

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

Трансляция внутренних сетевых адресов может осуществлять двумя способами: динамически и статически. В первом случае адрес выделяется узлу в момент обращения к МЭ. После завершения соединения адрес освобождается и может быть использован любым другим узлом корпоративной сети. Во втором случае адрес узла всегда привязывается к одному адресу МЭ, из которого передаются все исходящие пакеты. IP-адрес МЭ становится единственным активным IP-адресом, который попадает во внешнюю сеть. В результате все исходящие из внутренней сети пакеты оказываются отправленными МЭ, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешнем сетью.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности, трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в Интернете.

Схемы сетевой защиты на базе межсетевых экранов.

Первое появление межсетевых экранов (МЭ) как технологии связывается с маршрутизаторами, которые появились в 1983 – 1985 гг. Эти МЭ назывались фильтрами пакетов.

В 1989 – 1990 гг. появилось второе поколение архитектур МЭ, связанное с исследованием задержек в цепях.

Третье поколение – МЭ прикладного уровня, нацеленное на реализацию динамической фильтрации пакетов.

Начиная с 2000 года широкое направление исследований было нацелено на разработку персональных МЭ, т. е. использования на персональном компьютере, обеспечивая персональную защиту пользователя.

1. Фильтрация пакетов

Каждый IP-пакет исследуется на соответствие множеству правил. Эти правила устанавливают разрешение связи по содержанию заголовков сетевого и транспортного уровней модели TCP/IP, анализируется и направление передвижения пакета.

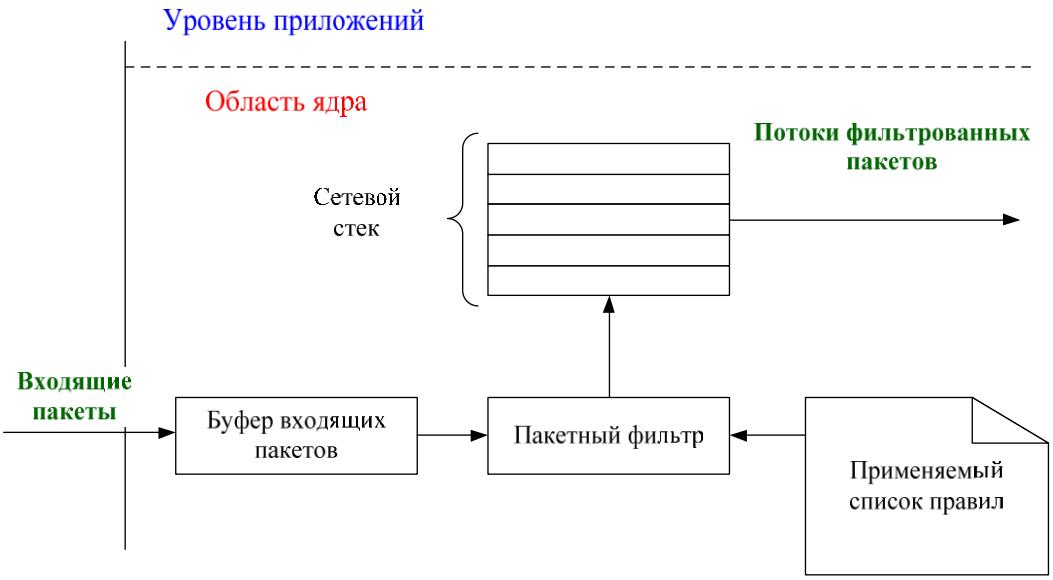

Рисунок 48. Схема архитектуры фильтров пакета

Фильтры пакетов контролируют:

− физический интерфейс, откуда пришел пакет;

− IPи (IP-адрес источника);

− IPН (IP-адрес назначения);

− тип транспортного уровня (TCP, UDP, ICMP); − транспортные порты источника и назначения.

Трансляция сетевых адресов.

Межсетевой экран, фильтрующий пакеты, часто переадресует сетевые пакеты так, что выходной трафик осуществляется с другими адресами. Такая схема называется схемой трансляции адресов (NAT).

Применение схемы NAT позволяет:

− спрятать топологию и схему адресации доверенной сети;

− использовать внутри организации пул IP-адресов меньшего размера.

При статической трансляции используется блок внешних адресов, которые назначаются запросам хостов локальной сети.

При динамической трансляции все запросы хостов локальной сети имеют один и тот же адрес. Для динамической трансляции используется форма (NAT Overloading), которая ставит в соответствие множеству адресов локальной сети единственный IP-адрес, используя различные номера портов (Port Address Translation, PAT).

При фильтрации пакетов, если пакет удовлетворяет правилам, то он (в зависимости от направления от или к удаленному хосту) перемещается по сетевому стеку для дальнейшей обработки или передачи.

Список контроля доступа содержит перечень элементов в заголовках пакетов, которые будут проверяться.

Достоинства технологии фильтрации: быстрота работы, аппаратная реализация, не требуется конфигурирование хостов пользователя.

Недостатки: Не понимает прикладные протоколы, не отслеживает соединения (нет информации о сеансе), обработка внутри пакета затруднена.

2. Межсетевые экраны уровня соединения

Данные МЭ проверяют факт, что пакет является либо запросом на TCPсоединение, либо представляет данные, относящиеся к уже установленному соединению, либо относится к виртуальному соединению между двумя транспортными уровнями.

Для проверки соединения МЭ исследует каждое установленное соединение (проверяя законное «рукопожатие» для используемого транспортного уровня (TCP)). Никакие пакеты не передаются до завершения «рукопожатия». Для этого МЭ формирует таблицу действительных (установленных) соединений, которые включают в себя полную информацию о состоянии соединения и выполнении необходимой последовательности.

Разрешается прохождение пакетов, информация в которых соответствует входу в таблицу виртуальных соединений. По окончании соединения соответствующий вход в таблицу удаляется.

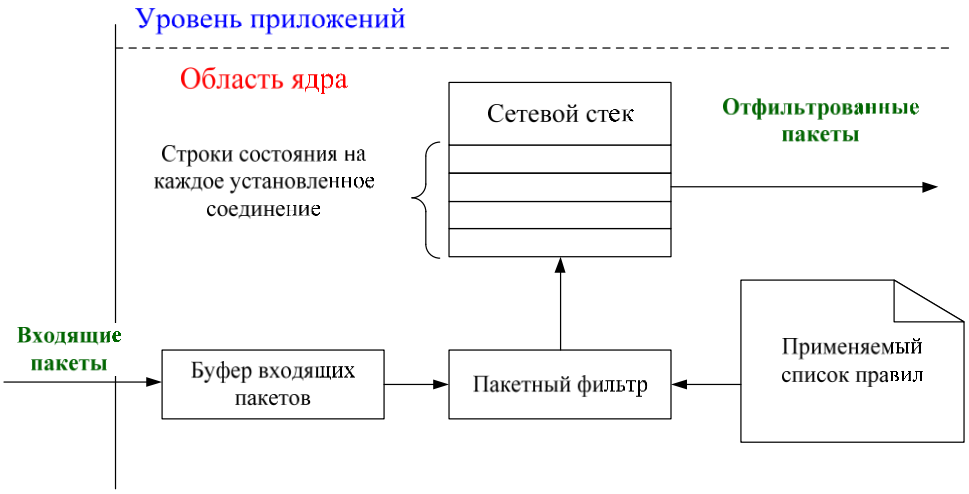

Рисунок 49. Схема функционирования МЭ уровня соединения

После установления соединения в соответствующей таблице (таблице состояний) обычно хранится следующая информация:

− идентификатор сеанса;

− состояние соединения (рукопожатие, установлено, закрыто);

− последовательная информация (последовательные номера пришедших байтов, состояния флагов и т. д.);

− IP-адрес источника и IP-адрес назначения;

− номера портов, участвующих в сеансе;

− физический интерфейс, куда прибыл пакет;

− физический интерфейс, куда передается пакет;

− временные метки начала открытия сеанса и т. д.

При функционировании такого МЭ должно обеспечиваться минимальное количество проверок, что реализуется посредством построения ограниченной формы состояний соединений.

Достоинство: Возможность запрещения соединения с определенными хостами.

Недостатки: Не могут ограничить доступ протоколов, отличных от TCP, Не осуществляют проверки для протоколов высших уровней.

3. Межсетевые экраны прикладного уровня

Данные МЭ оценивают сетевые пакеты на соответствие определенному прикладному уровню перед установкой соединения. Они исследуют данные всех сетевых пакетов на прикладном уровне и устанавливают состояние полного (завершенного) соединения и последовательной информации. Также они отслеживают параметры, содержащиеся внутри данных прикладного уровня (пароли, запросы служб).

Большинство МЭ прикладного уровня включает в себя специализированное прикладное ПО и службу proxy.

Рисунок 50. Схема функционирования служб proxy: 1 – рабочая станция; 2 – сервер

Каждая proxy-служба является специфичной для каждого протокола и может осуществлять усиленный контроль доступа, проверку данных, а также генерировать записи аудита. Службы proxy не позволяют прямого соединения пользователей с серверами и работают в прикладной области ОС.

Использование proxy позволяет проводить анализ множества команд для одного протокола и анализ содержания данных (фильтрацию URL, аутентификацию и т. д.).

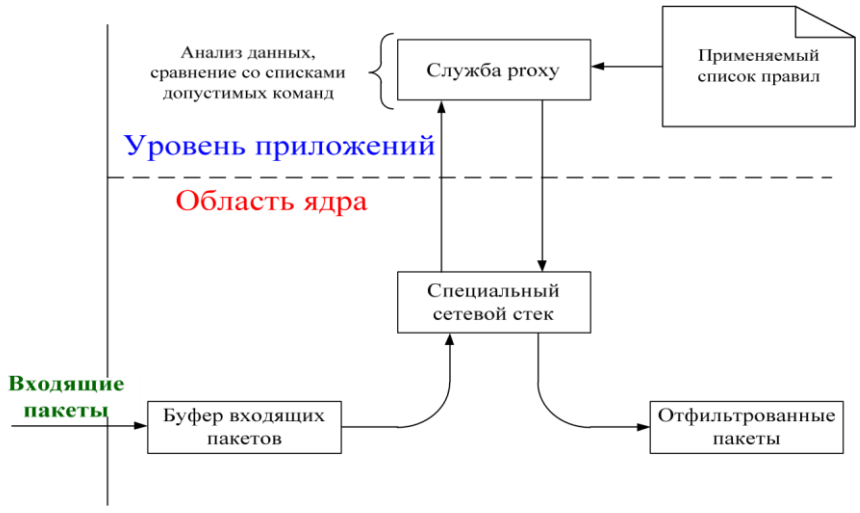

Рисунок 51. Схема функционирования МЭ прикладного уровня

Достоинства: работа с протоколами высшего уровня (HTTP, FTP). Возможность ограничения доступа к определенным сетевым службам, возможность обработки информации данных пакета, запрет прямых соединений с

внешними серверами, прозрачность proxy, фильтрация URL, аутентификации, кэширование HTTP.

Недостатки: служба proxy требует замены сетевого стека на сервере МЭ; слушает порт , но не может его использовать, большая временная задержка (входной пакет обрабатывается дважды – приложением и proxy), proxy уязвимы к ошибкам ОС и ПО прикладного уровня.

4. Межсетевые экраны с динамической фильтрацией пакетов

Данные МЭ позволяют осуществлять модификацию базы правил «на лету» (on fly). Это реализуется для протокола UDP.

МЭ осуществляет ассоциацию всех UDP пакетов, которые пересекают периметр безопасности через виртуальное соединение. Если генерируется пакет ответа и передается источнику запроса, то устанавливается виртуальное соединение и пакету разрешается пересечь сервер МЭ. Информация, ассоциированная с виртуальным состоянием, запоминается на краткий промежуток времени, поэтому если пакет ответа не получен, то соединение считается закрытым.

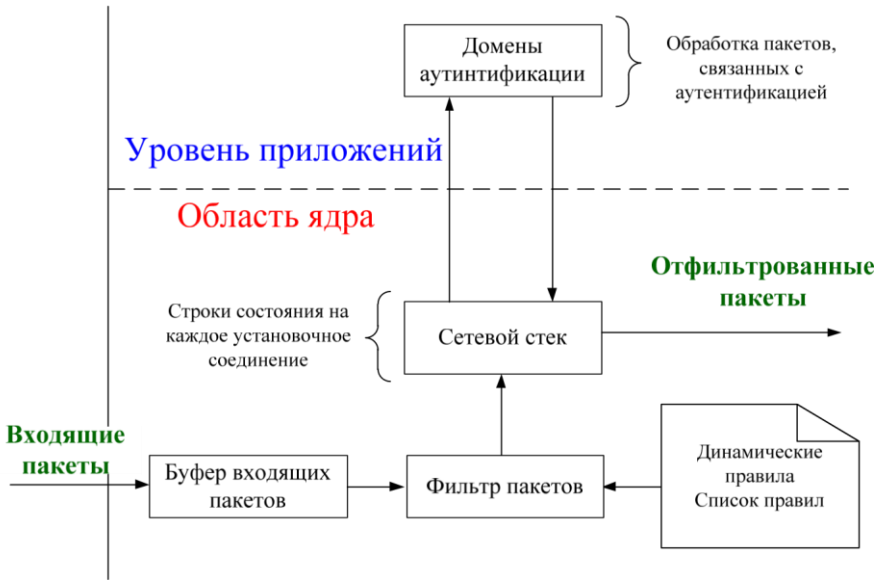

Рисунок 52. Схема функционирования МЭ с динамической фильтрацией

Главной особенностью данной схемы является наличие двух групп правил. Одна – статическая, другая – динамическая, изменяемая и ходе работы МЭ.

Достоинства: не позволяет прошедшим пакетам UDP войти во внутреннюю сеть; если запрос пакета UDP приходит из внутренней сети и направлен на не доверительный хост, то сервер МЭ позволяет появление ответного пакета, доставляемого хосту – инициатору запроса; динамический фильтр может использоваться для поддержки ограниченного множества команд ICMP.

Недостатки: не понимает прикладные протоколы, слабые возможности обработки информации внутри пакета, не может ограничивать информацию с внутренних компьютеров к службам МЭ сервера.

5. Межсетевые экраны инспекции состояний. Технология инспекции состояний осуществляет анализ пакетов на трех высших уровнях. Этот подход используется многими разработчиками.

Устройство инспекции состояний осуществляет анализ пакетов и формирование данных о «состоянии виртуального соединения».

Соединение может находиться в состоянии установки, передачи или отключения.

Вся информация, связанная с состоянием данного виртуального соединения, хранится в таблице динамических состояний, с помощью которой оценивается дальнейший обмен в рамках этого виртуального соединения, т.е. осуществляется контроль последовательности пакетов на различных уровнях.

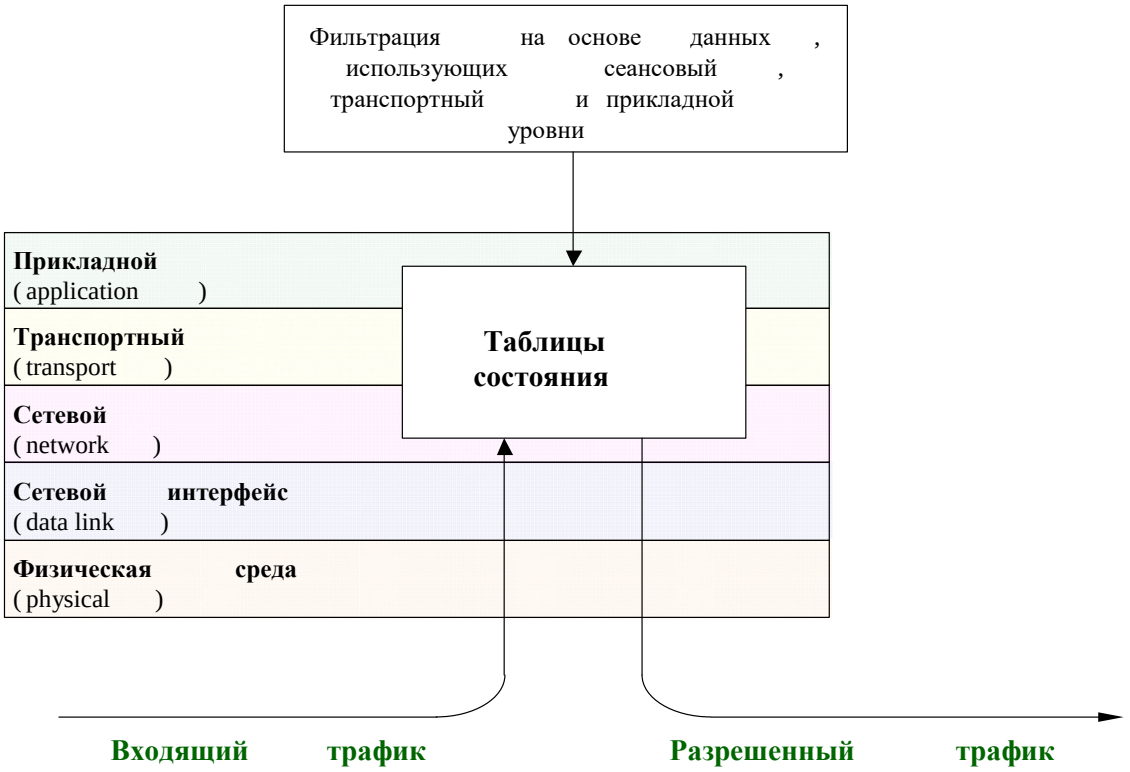

Рисунок 53. Схема фильтрации при инспекции состояний

Отслеживание информации прикладного уровня позволяет учитывать поведение нестандартных протоколов (например, FTP или H.323).

Межсетевой экран IP-tables является свободно распространяемым продуктом для Linux. При отслеживании состояния соединение регистрируется в основном на основании информации о протоколе.

Администратор имеет возможность создать правила, определяющие, какие протоколы или определенные виды трафика необходимо отслеживать. Когда соединение начинается с использованием отслеживаемого протокола, IPtables добавляет записи в таблицу состояний всего соединения.

Запись в таблице состояний включает в себя следующую информацию:

− протокол, используемый для соединения;

− IP-адреса источника и назначения;

− номера портов источника и назначения;

− листинг с обращенными адресами и номерами портов (для контроля возвращаемого трафика);

− время, по истечению которого соединение будет удалено;

− состояние TCP-соединения (только для TCP); − состояние отслеживаемого соединения.

При принятии решения о разрешении прохождения пакета межсетевой экран проверит его последовательно по следующим структурам данных:

− *таблица состояний* – зарегистрировано ли соединение для данного входящего пакета (если да, то пакет передается без дальнейшей проверки);

− *политика безопасности* – если правило разрешает прохождение пакета, то пакет будет передан, а для его сеанса соединения будет добавлена запись в таблицу состояний.

6. Межсетевые экраны уровня ядра. Межсетевой экран Cisco Centri включает в себя основные достоинства предыдущих архитектур (скорость обработки в ядре, зависимость от сессии для каждого уровня протокола и т.д.). МЭ разработан с использованием технологии автономных агентов, что позволяет легко добавлять новых агентов для решения новых задач.

Рисунок 54. Схема функционирования уровня ядра

Подсистема МЭ Cisco Centri включает в себя следующие основные модули:

− ядро безопасности;

− модуль управления хостом;

− модуль управления каналами связи МЭ;

− агент регистрации входов; − агент аутентификации.

Основным модулем является ядро безопасности. Ядро анализирует каждый входящий и исходящий пакет, проходящий через сервер МЭ, и применяет к каждому пакету заданную реализацию установленной политики безопасно-

сти. Ядро безопасности оперирует внутри ядра Windows NT, что позволяет обеспечить высокую производительность МЭ.

Модуль управления управляет созданием соединения для соответствующей сетевой карты. Каждый сетевой пакет анализируется на принадлежность к существующему соединению. Если такое соединение для пакета есть, то пакет передается в стек proxy существующего соединения. Если нет – проверяется модулем управления на наличие политики соединения. В результате пакет или удаляется, или создается динамический стек для нового соединения, и пакет передается в него.

7. Новое поколение межсетевых экранов. Для эффективного противодействия современным угрозам разработаны МЭ нового поколения, обеспечивающие:

− идентификация приложений, а не портов

− расширенная инспекция состояний – необходимо контрил ровать сеансы приложений после того, когда выбраны динамические порты

− расшифровка и шифровка SSL

− идентификация корпоративных пользователей, а не IP-адресов – это позволяет строить и применять политики безопасности, формировать отчеты для конкретных пользователей и групп пользователей (служб каталогов); − сканирование в реальном времени, высокая производительность.

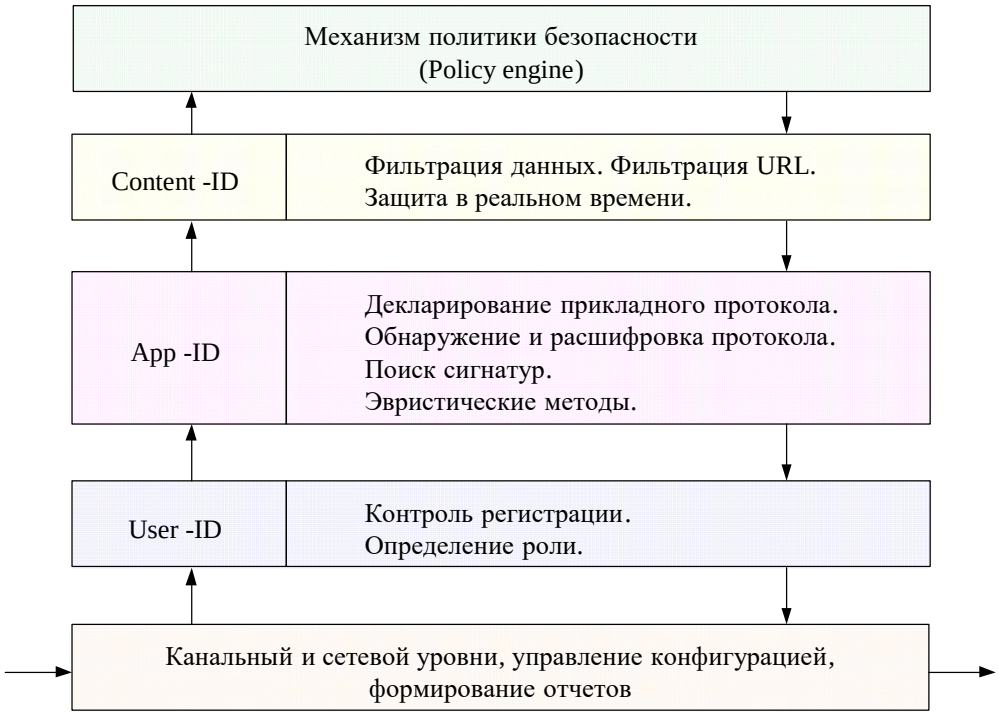

Рисунок 55. Схема функционирования МЭ нового поколения

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Фильтрация пакетов.
2. Межсетевые экраны прикладного уровня.
3. Межсетевые экраны с динамической фильтрацией пакетов.
4. Межсетевые экраны инспекции состояний.
5. Межсетевые экраны уровня ядра.

3.2.7 Тема 2.7 Виртуальные частные сети

Перечень изучаемых вопросов:

Туннелирование.

Протоколы VPN транспортного уровня

Протокол L2TP

Методические указания к изучению:

Виртуальные частные сети, или защищенные виртуальные сети (Virtual Private Network, VPN) – это подключение, установленное по существующей общедоступной инфраструктуре и использующее шифрование, и аутентификацию для обеспечения безопасности содержания передаваемых пакетов.

Виртуальная частная сеть создает виртуальный сегмент между любыми двумя точками доступа к сети. Она может проходить через общедоступную инфраструктуру локальной вычислительной сети, подключения к глобальной сети (Wide Area Network, WAN) или Интернет.

Виды конфигурации VPN:

− узел-узел (host-to-host);

− узел-шлюз (host-to-gateway);

− шлюз-шлюз (gateway-to-gateway).

Основной концепцией VPN является защита шифрованием канала связи на различных уровнях модели TCP/IP, а именно:

− прикладном (5-й уровень);

− транспортном (4-й уровень);

− сетевом (3-й уровень);

− канальном (2-й уровень).

Уровни TCP/IP	Основные протоколы
Прикладной (application)	PGP, S/MIME SSH, Kerbeors, RADIUS
Транспортный (transport)	SSL, TSL, SOCKS v5
Сетевой (network)	IPSec (AH, ESP)
Канальный (data link)	L2TP, PPTP, L2A, CHAP, PAP, MS-CHAP

Рисунок 56. Схема расположения VPN

1 Туннелирование

Туннелирование – это процесс инкапсуляции одного типа пакетов внутри другого в целях получения преимущества при транспортировке.

Туннелирование можно использовать, чтобы послать трафик через маршрутизируемую сетевую среду или чтобы применить шифрование для обеспечения безопасности IP-пакетов.

Рисунок 57. Реализация VPN типа шлюз-шлюз

Межсетевой экран преобразует все пакеты, предназначенные для удаленной сети, в зашифрованный вид и добавляет к ним новые IP-заголовки со своим собственным IP-адресом в качестве отправителя и адресом удаленного межсетевого экрана в качестве IP-адреса назначения.

В этом случае шифрование скрывает фактическую информацию, содержащуюся в оригинальном IP-пакете. Когда удаленный МЭ получает пакет, он расшифровывает его и передает узлу сети, для которого он предназначался.

Виртуальный сегмент сети, создаваемый между двумя шлюзовыми оконечными точками, называется туннелем (так как конечные узлы удаленных локальных сетей «не имеют представления» о том, что происходит с их пакетами во время доставки).

Пакет проходит от одного узла сети к другому, не будучи транслированным шлюзовыми устройствами.

Главная выгода от использования VPN для удаленного доступа – это совокупность стоимостной эффективности возможного использования общедоступной сетевой среды для транспортирования частной информации и высокого уровня безопасности.

Защищённая виртуальная сеть может предоставить множество уровней безопасности, включая усовершенствование конфиденциальности, целостности и аутентификации.

Для организации VPN туннеля нет необходимости прокладывать новые (выделенные) линии связи.

Недостатки VPN:

− использование шифрования сказывается на общей пропускной способности подключения VPN;

− необходимость фрагментации пакетов;

− проблемы реализации, сетевых адресов (NAT) для VPN;

− внутренние части структуры и содержимое инкапсулированных пакетов недоступны до момента их расшифровки;

− проблемы с функционированием сетевых систем обнаружения вторжений (закрытие содержимого пакетов).

2. Протоколы VPN канального уровня

На канальном уровне существуют два протокола для реализации VPN: протокол туннелирования типа «точка-точка» (Point-to-Point Tunneling Protocol, PPTP) и протокол туннелирования второго уровня (Layer Two Tunneling Protocol, L2TP).

Оба этих протокола включены в состав операционной системы Microsoft Windows.

Протокол PPTP

PPTP использует протоколы:

− *протокол аутентификации пароля* (Password Authentication Protocol, PAP);

− *протокол аутентификации с предварительным согласованием вызова* (Challenge Handshake Authentication Protocol, CHAP);

− *расширенный протокол аутентификации* (Extensible Authentication Protocol, EAP).

Протокол PPTP использует два канала, работающих совместно.

Первый – канал управления (порт 1723/tcp). Этот канал посылает в обе стороны все команды, которые управляют сеансом подключения.

Второй – инкапсулированный канал передачи данных, являющийся вариантом протокола общей инкапсуляции для маршрутизации (Generic Routing Encapsulation, GRE). Это протокол использует UDP в качестве транспортного протокола.

Преимущество туннеля протокола общей инкапсуляции для маршрутизации – инкапсуляция и передача протоколов, отличающиеся от протокола IP.

Достоинство: Протокол PPTP работает без помех через устройства NAT.

Недостаток: Протокол PPTP при инициализации связи использует протокол PPP, поэтому может оказаться уязвимым к атакам типа spoofing и «человек посередине».

Протокол L2TP

Протокол L2TP определен в документе RFC 2661 и фактически является гибридом двух предыдущих протоколов туннелирования:

− *протокола пересылки второго уровня* (Layer Two Forwarding, L2F) компании Cisco;

− *протокола PPTP*;

Протокол L2TP, использует при аутентификации пользователя возможности протокола PPP.

Аналогично протоколу PPTP протокол L2TP использует два канала связи:
− сообщения управления;

− сообщения туннеля для передачи данных.

Первый бит заголовка протокола PPTP служит для опознания этих типов сообщений (1 – для сообщений управления, 0 – для сообщений данных).

Сообщениям управления дается более высокий приоритет по отношению к сообщениям данных, чтобы гарантировать, что важная информация администрирования сеанса будет передана максимально быстро.

Подключение канала управления устанавливается для туннеля, который затем сопровождается инициированием сеанса протокола L2TP. После завершения инициирования обоих подключений информация в виде кадров протокола PPP начинает передаваться по туннелю.

Этапы формирование защищенного канала:

− установление соединения клиента с сервером удаленного доступа;

− аутентификация пользователя;

− конфигурирование защищенного туннеля.

Для установления соединения с сервером удаленного доступа (сетевой сервер L2TP) удаленный пользователь связывается по протоколу PPP с концентратором доступа L2TP, обычно функционирующем на сервере провайдера.

Концентратор доступа может выполнить аутентификацию пользователя от имени провайдера.

По заданному имени получателя концентратор доступа определяет адрес сетевого сервера L2TP, который защищает сеть с заданным адресом.

Между концентратором доступа и сервером L2TP устанавливается соединение.

Производится аутентификация пользователя сервером L2TP. В случае успешной аутентификации устанавливается защищенный туннель между концентратором доступа и сервером L2TP.

С помощью управляющих сообщений производится настройка параметров туннеля, причем в одном туннеле может быть несколько сеансов пользователя.

При использовании IPSec пакеты L2TP инкапсулируются в UDP-пакеты, которые передаются концентратором доступа и сервером L2TP через IPSecтуннель (порт 1701/tcp).

3. Основные виды защищенных связей

В RFC 2401 приведены четыре примера комбинации защищённых связей, которые должны поддерживаться использующими IPSec узлами или шлюзами защиты.

1. Обеспечение защиты связи между конечными системами, использующими IPSec. Эти конечные системы должны использовать общие секретные ключи. При этом допустимы следующие комбинации:

− AH в транспортном режиме;

− ESP в транспортном режиме;

− сначала AH, а затем ESP в транспортном режиме;

− любая из предыдущих связей внутри AH или ESP в туннельном режиме.

Рисунок 58. Защитная связь между конечными системами с IPSec

2. Обеспечение защиты между шлюзами. Защита организуется только между шлюзами (маршрутизаторами, межсетевыми экранами), а в конечных узлах применение IPSec не предполагается. Требуется только одна туннельная защищенная связь. Туннель может использовать AH, ESP или ESP с опцией аутентификации.

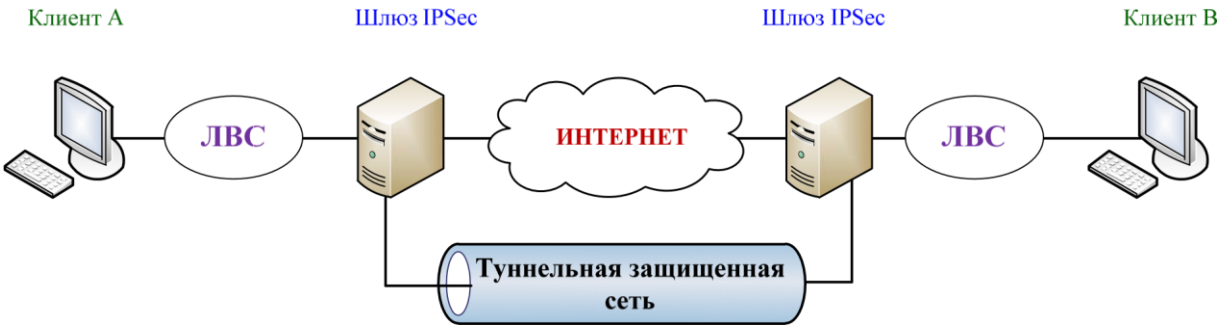

Рисунок 59. Защищенная связь между шлюзами

3. Обеспечение сквозной защиты. В этом случае используется схема защиты между шлюзами с добавлением сквозной защиты. Туннель от шлюза к шлюзу обеспечивает аутентификацию или конфиденциальность для всего трафика между конечными системами (когда туннель использует ESP, обеспечивается ограниченная конфиденциальность потока обмена данными). Конечные системы могут использовать дополнительные сервисы IPSec, необходимые для конкретных узлов.

4.Обеспечение защиты удаленного доступа. В этом случае обеспечивается защита удаленного узла, использующего Интернет для связи с межсетевым экраном организации в целях получения доступа к узлу локальной вычислительной сети, защищаемому этим межсетевым экраном. Между удаленным узлом и МЭ необходимо использовать только туннельный режим. Как и в варианте 1, между удаленным и локальным узлами можно использовать одну или две защищенные связи.

5. Протоколы VPN транспортного уровня

Протоколы транспортного уровня прозрачны для прикладных протоколов и протоколов представления сервисов (HTTP, FTP, POP3, SMTP, и др.).

Транспортный уровень отвечает за установку логических соединений и управление этими соединениями, то на этом уровне появляется возможность использования программ-посредников, которые проверяют допустимость соединений и обеспечивают выполнение других функций защиты.

Протокол SSL

Протокол ориентирован на организацию защищенного обмена между клиентом и сервером. Клиентская часть протокола включена в состав всех популярных Web-браузеров, а серверная – в большинство Web-серверов.

Формирование защищённого обмена:

− установление SSL-сеанса;

− защищенное взаимодействие.

Процедура установления SSL-сеанса представляет собой технологию, при которой клиент посылает серверу запрос на установление защищённого соединения, в котором передаются параметры соединения.

Сервер, обработав запрос, передает клиенту согласованный набор параметров.

Клиент проверяет сертификат сервера и при положительном результате проверки генерирует случайную последовательность (48 байт), шифрует ее открытым ключом сервера и посылает серверу; с помощью согласованной хэшфункции формирует сеансовые ключи.

Сервер расшифровывает последовательность ключа и выполняет аналогичные клиенту операции;

В ходе защищенного взаимодействия обе стороны при передаче формируют MAC для каждого сообщения и зашифровывают исходное сообщение MAC-кодом. При приеме сообщение расшифровывается и осуществляется проверка его целостности.

Литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

Контрольные вопросы:

1. Привести особенности порядка реагирования на вторжения в интернет-сети и организационно-правовые вопросы.
2. Указать и охарактеризовать сохранение доказательств вторжения
3. Протоколы VPN транспортного уровня

4.Требования к аттестации по дисциплине

4.1 Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации:

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная либо балльно-рейтинговая..

Выбрана традиционная зачетно-экзаменационная методика оценивания знаний

Предусматривается: зачет, экзамен, курсовой проект.

4.2 Порядок применения рейтинговой системы (не предусматривается)

В рамках балльно-рейтинговой системы выставляется оценка за качество выполнения и защиту лабораторных и контрольных работ.

Таблица 6. Оценка в балльно-рейтинговой системе

Вид деятельности	Доля	Кол-во ед.	Макс. балл за ед.	Всего
Обязательные виды деятельности				
1 семестр				
Посещаемость занятий	20%	N1	=200/N1	200
Выполнение лаб. работ (защита)	40%	2	200	400
Контрольная работа 1	40%	1	400	400
Итого:	100%			1000
2 семестр				
Посещаемость занятий	20%	N2	=200/N2	200
Выполнение лаб. работ (защита)	40%	2	200	400
Контрольная работа 2	40%	1	400	400
Итого:	100%			1000
Всего				2000
Дополнительные задания (по выбору студента в каждом семестре)				
Подготовка реферата (видео-доклада)	20%		200	200
Решение дополнительных задач контрольной работы	10%		100	100
Выполнение задания в рамках НИРС	50%		500	500

4.3 Условия получения положительной оценки

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой:

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя:

- материалы для проведения текущего контроля успеваемости – варианты заданий;
- перечень компетенций и их элементов, проверяемых на каждом мероприятии текущего контроля успеваемости;
- систему и критерии оценивания по каждому виду текущего контроля успеваемости
- описание процедуры оценивания.

Текущий контроль в форме опроса.

Текущий контроль осуществляется путем опроса по материалу, пройденному на предшествующих лекциях.

Оценивается:

- полнота усвоения пройденного материала,
- качество изложения пройденного материала (устно и письменно)

Таблица 7. Шкала оценок уровня усвоения материала обучающимся

Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не может ответить на вопросы по пройденному материалу или графически изобразить на доске	Отвечает сбивчиво, путается в определениях и обозначениях, нуждается в помощи других обучающихся	Допускает незначительные ошибки при изложении пройденного материала, не полностью представляет связи между разделами изучаемой дисциплины	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изученных разделов дисциплины

Таблица 8. Шкала оценок уровня освоения дисциплины по зачету

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Правильные ответы даны менее чем на 50% включительно. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи	Правильные ответы даны на 51-64% вопросов. Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи	Правильные ответы даны на 65-94% вопросов. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный ха-	Правильные ответы даны на 95-100% вопросов. Ответы на поставленные в билете вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие

		рактер. Соблюдаются нормы литературной речи	знания предмета. Соблюдаются нормы литературной речи

Таблица 9. Шкала оценок уровня освоения дисциплины по экзамену

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий	Твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок

Таблица 10. Шкала оценок уровня освоения дисциплины по тесту.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый

«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Менее 50% правильных ответов	50-70% правильных ответов	71-90% правильных ответов	91-100% правильных ответов

Таблица 11. Шкала оценок курсового проекта

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Работа носит реферативный характер, студент допускает существенные ошибки при защите, с большими затруднениями отвечает на вопросы, оформление работы не соответствует правилам	Работа носит реферативный характер, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении при защите, оформление работы имеет незначительные отклонения от правил	В работе углублены теоретические и практические знания, материал излагается грамотно и по существу, не допускается существенных неточностей в ответе на вопрос, оформление работы соответствует правилам	В процессе выполнения работы приобретены навыки самостоятельного планирования и выполнения научно-исследовательской работы; получен опыт сбора и обработки исходного материала, анализа научно-технической литературы, материал излагается грамотно оформление работы соответствует правилам

Критерии оценивания для проведения итоговой аттестации

Итоговая аттестация обучающихся проводится в форме зачета (8-й семестр) и экзамена (9-й семестр).

Допуск к итоговой аттестации возможен при:

- всех выполненных, сданных (проверенных, защищенных) лабораторных работах, наличии отчётов по ним;

- наличии показателей приемлемого уровня освоения материалов курса: более 50% посещений от общего числа требуемых по учебному плану.

Критерии оценивания:

- уровень усвоения материала, предусмотренного программой
- умение выполнять задания, предусмотренные программой
- уровень знакомства с дополнительной литературой
- уровень раскрытия причинно-следственных связей
- уровень раскрытия междисциплинарных связей
- стиль поведения (культура речи, манера общения, убежденность, готовность к дискуссии)
- качество ответа (полнота, правильность, аргументированность, его общая композиция, логичность)

4.4 Примерные вопросы к зачету/экзамену по дисциплине

4.4.1 Зачет с оценкой:

1. Обобщённые категории атак и х краткая характеристика.
2. Охарактеризуйте распространенные приемы хакеров и методы защиты от их реализаций.
3. Сетевые атаки. Общая классификация по технологиям.
4. Кратко охарактеризуйте известные атаки на канальном уровне OSI
5. Раскройте специфику атаки «Переполнение CAM-таблицы». Приведите способы защиты от нее.
6. Раскройте специфику атаки «VLAN Hoping». Приведите способы защиты от нее.
7. Раскройте специфику атаки на STP. Приведите способы защиты от нее.
8. Раскройте специфику атак на PVLAN, на DHCP. Приведите способы защиты от них.
9. Раскройте специфику атаки ARP-spoofing. Приведите способы защиты от нее.
10. Кратко охарактеризуйте известные атаки на сетевом уровне OSI.
11. Раскройте специфику атак на маршрутизаторы.
12. Раскройте специфику атак на среды с протоколом RIP с использованием ложных маршрутов.. Приведите способы защиты.
13. Раскройте специфику атак на среды с протоколом RIP с использованием взлома хеша MD5 и понижением версий. Приведите способы защиты.
14. Раскройте специфику атак на среды с протоколом OSPF с использованием ложных маршрутов. Приведите способы защиты.
15. Раскройте специфику атак на среды с протоколом BGP с использованием router masquerading, взлома хеша MD5. Приведите способы защиты.
16. Раскройте специфику атак на среды с протоколом BGP с «слепого DOS» и других способов (кроме использованием router masquerading, взлома хеша MD5). Приведите способы защиты.

17. Раскройте специфику атак на среды с протоколом IS-IS. Приведите способы защиты.
18. Раскройте специфику атак на среды с протоколом MPLS. Приведите способы защиты.
19. Раскройте специфику протокола IPSec.
20. Раскройте специфику защиты с сетей с учетом масштабов и конфигураций.

4.4.2 Вопросы к экзамену:

21. Обобщённые категории атак и х краткая характеристика.
22. Охарактеризуйте распространенные приемы хакеров и методы защиты от их реализаций.
23. Сетевые атаки. Общая классификация по технологиям.
24. Кратко охарактеризуйте известные атаки на канальном уровне OSI.
25. Раскройте специфику атаки «Переполнение CAM-таблицы». Приведите способы защиты от нее.
26. Раскройте специфику атаки «VLAN Hoping». Приведите способы защиты от нее.
27. Раскройте специфику атаки на STP. Приведите способы защиты от нее.
28. Раскройте специфику атак на PVLAN, на DHCP. Приведите способы защиты от них.
29. Раскройте специфику атаки ARP-spoofing. Приведите способы защиты от нее.
30. Кратко охарактеризуйте известные атаки на сетевом уровне OSI.
31. Раскройте специфику атак на маршрутизаторы.
32. Раскройте специфику атак на среды с протоколом RIP с использованием ложных маршрутов.. Приведите способы защиты.
33. Раскройте специфику атак на среды с протоколом RIP с использованием взлома хеша MD5 и понижением версий. Приведите способы защиты.
34. Раскройте специфику атак на среды с протоколом OSPF с использованием ложных маршрутов. Приведите способы защиты.
35. Раскройте специфику атак на среды с протоколом BGP с использованием router masquerading, взлома хеша MD5. Приведите способы защиты.
36. Раскройте специфику атак на среды с протоколом BGP с «слепого DOS» и других способов (кроме использованием router masquerading, взлома хеша MD5). Приведите способы защиты.
37. Раскройте специфику атак на среды с протоколом IS-IS. Приведите способы защиты.
38. Раскройте специфику атак на среды с протоколом MPLS. Приведите способы защиты.
39. Раскройте специфику протокола IPSec.
40. Раскройте специфику защиты с сетей с учетом масштабов и конфигураций.

41. Приведите классификацию МЭ. Раскройте специфику защиты с использованием МЭ пакетного типа.
42. Приведите классификацию МЭ. Раскройте специфику защиты с использованием МЭ сеансового типа.
43. Приведите классификацию МЭ. Раскройте специфику защиты с использованием МЭ сеансового типа.
44. Раскройте специфику функционирования МЭ.
45. Протоколы SSL и TLS.
46. Протокол SOCKS.
47. Протокол PPTP, L2TP.
48. Защиты трафика в WiFi-сетях .
49. Опишите способы защиты сетей с использование распределения доступа и настроек протокольных сред в сетях домен в Windows Server (по лаб. раб.).
50. Опишите способы защиты сетей с использование распределения доступа и настроек протокольных сред в сетях Cisco (по лаб. раб.)
51. Опишите способы защиты сетей с использование распределения доступа и настроек протокольных сред в сетях Cisco (по лаб. раб.)
52. Опишите способы защиты сетей с использование технологий VPN (OpenVPN) (по лаб. раб. и лек.)

4.4.3 Темы курсовых проектов:

1. IPSec протокол.
2. Протокол L2TP.
3. Концентратор доступа LAC.
4. Сервер LNS.
5. протоколом PPP.
6. Протокол Internet Protocol Security (IPSec).
7. Протокол SSL.
8. Протокол TSL.
9. Протокол SOCKS.
10. Схемы применения IPSec.
11. Система правил избирательное разграничение доступа.
12. Протокол LDAP.
13. Протокол Kerberos.
14. Протокол DNS.
15. VPN-серверы.
16. Протоколы VPN транспортного уровня.
17. ISA-серверы.
18. Протокол SOCKS. SOCKS-сервер.
19. Дополнительные возможности МЭ. Реагирование на задаваемые события.

20. Разработка схемы сетевой защиты на базе межсетевых экранов.
21. Фильтрация пакетов.
22. Межсетевые экраны прикладного уровня.
23. Межсетевые экраны с динамической фильтрацией пакетов.
24. Межсетевые экраны инспекции состояний.
25. Межсетевые экраны уровня ядра.
26. Протокол L2F.

5.ЗАКЛЮЧЕНИЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- *развивающая (*повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- *информационно-обучающая* (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- *ориентирующая и стимулирующая* (процессу обучения придается профессиональное ускорение);
- *воспитывающая* (формируются и развиваются профессиональные качества специалиста):
- *исследовательская* (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к самораз-

витию, самосовершенствованию и самореализации;

- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с *рабочей программой учебной дисциплины.* Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;

- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей);
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
- подготовка курсовых проектов и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

ЛИТЕРАТУРА

1. Гузенкова, Е. А. Безопасность сетей ЭВМ : конспект лекций / Е. А. Гузенкова. – Екатеринбург : Изд-во УрГУПС, 2016. – 151 с.

2. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 1.

3. Запечников, С. В. Информационная безопасность открытых систем: в 2 т.: учебник для вузов / С. В. Запечников, Н. Г. Милославская. - Москва: Горячая линия-Телеком, 2006. - Т. 2.

4. Подтопельный, В. В. Программно-аппаратные средства обеспечения информационной безопасности. Часть 3. Поиск и извлечение вредоносных программ в программной среде: учебное пособие / В. В. Подтопельный. - Калининград: Изд-во БГАРФ, 2020.

5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. - Москва: ИД "Форум»; Москва: ИНФРА-М, 2013. - 416 с.

Локальный электронный методический материал

Владислав Владимирович Подтопельный

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ»

Редактор Г. А. Смирнова

Уч.-изд. л. 8,25. Печ. л. 8,25

Издательство федерального государственного бюджетного образовательного учреждения
высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1

130