МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

Государственное бюджетное профессиональное образовательное учреждение РД
«Технический колледж имени Р.Н Ашуралиева»

Рабочая программа профессионального модуля

ПМ.02. Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи

индекс и наименование профессионального модуля

Код и наименование специальности: 11.02.11 «Сети связи и системы коммутации»

входящей в состав УГС 11.00.00 Электроника, радиотехника и системы связи

код и наименование укрупненной группы специальностей

Квалификация выпускника: Техник

2021 г.

ОДОБРЕНО

предметно-цикловой комиссией по УГС 11.00.00 Электроника, радиотехника и системы связи

Протокол № 10 от 04 06 2021 г.

Председатель П(Ц)К

Мирзаев З.Н

Подпись

УТВЕРЖДАЮ

Зам. директора по учебной работе

Ф.Р.Ахмедова

Подпись

10 06 2021 г.

Рабочая программа профессионального модуля «ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.11 Сети связи и системы коммутации (базовой подготовки), входящей в состав укрупненной группы специальностей 11.00.00 Электроника, радиотехника и системы связи, утвержденного приказом Министерства Образования и науки Российской Федерации № 813 от 28 июля 2014 г., (зарегистрирован Министерством юстиции 19 августа 2014 г. рег. № 33646);

с учетом:

- Методических рекомендаций по разработке рабочих программ профессиональных модулей в пределах освоения основной профессиональной образовательной программы среднего профессионального образования (ППКРС и ППССЗ), разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан

в соответствии с рабочим учебным планом образовательной организации на 2021/2022 учебный год

Разработчики:

- Багаутдинова Зарема Магомедзапировна преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева»

- Джамалутдинова М.Д преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева»

Рецензенты / эксперты:

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.

1.1. Область применения программы

Примерная программа профессионального модуля (далее примерная программа) – является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО / профессии (профессиям) НПО **11.02.11«Сети связи и системы коммутации»** в части освоения основного вида профессиональной деятельности (ВПД):

Выявления каналов утечки, установки и настройки специализированного оборудования по защите информации, проверки защищенности автоматизированных систем и информационно-коммуникационных сетей.

1. Выполнять монтаж и производить настройку сетей проводного и беспроводного абонентского доступа.
2. Осуществлять работы с сетевыми протоколами.
3. Обеспечивать работоспособность оборудования мультисервисных сетей.
4. Выполнять монтаж и первичную инсталляцию компьютерных сетей.
5. Инсталлировать и настраивать компьютерные платформы для организации услуг связи.
6. Производить администрирование сетевого оборудования.
7. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
8. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
9. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.
10. Выполнять монтаж оборудования телекоммуникационных систем.
11. Проводить мониторинг и диагностику телекоммуникационных.
12. Управлять данными телекоммуникационных систем.
13. Устранять аварии и повреждения оборудования телекоммуникационных систем, выбирать методы восстановления его работоспособности.
14. Выполнять монтаж и обеспечивать работу линий абонентского доступа и оконечных абонентских устройств.
15. Решать технические задачи в области эксплуатации телекоммуникационных систем.
16. Планировать и организовывать работу структурного подразделения.
17. Руководить работой структурного подразделения.
18. Анализировать процесс и результаты деятельности подразделения.
19. Проводить маркетинговые исследования рынка услуг связи для формирования бизнес-планов и бизнес-процессов.

20. Выбирать технологии для предоставления различных услуг связи в соответствии с заказами потребителей.
21. Заключать торговые сделки, коммерческие и страховые договоры при осуществлении деятельности организации связи.
22. Определять стратегию жизненного цикла услуг.
23. Выполнять монтаж, установку и настройку современного оборудования связи.
24. Проводить мониторинг информационно-коммуникационных сетей связи.
25. Управлять информационно-коммуникационными сетями связи.
26. Повышать компьютерную и технологическую грамотность персонала.

Примерная программа профессионального модуля может быть использована в программе профессиональной подготовки монтажника оборудования радио и телефонной связи, монтажника связи, электромонтера оборудования электросвязи и проводного вещания, электромонтера по ремонту линейно-кабельных сооружений телефонной связи и проводного вещания.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- выявления каналов утечки информации; определения необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности); разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы; установки и настройки программных средств защиты автоматизированных систем и информационно- коммуникационных сетей;
- конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
- проверки защищенности автоматизированных систем и информационно-коммуникационных сетей; защиты баз данных;
- организации защиты в различных операционных системах и средах; шифрования информации;

уметь:

- классифицировать угрозы информационной безопасности; [1] проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;

осуществлять мероприятия по проведению аттестационных работ;

- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;

- использовать программные продукты, выявляющие недостатки систем защиты; производить установку и настройку средств защиты; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

- выполнять тестирование систем с целью определения уровня защищенности;

- использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации;

знать:

- каналы утечки информации; назначение, классификацию и принципы работы специализированного оборудования;

- принципы построения информационно-коммуникационных сетей;

— возможные способы несанкционированного доступа; нормативно-правовые и законодательные акты в области информационной безопасности;

- правила проведения возможных проверок; этапы определения конфиденциальности документов объекта защиты;

- технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов;

- конфигурации защищаемых сетей; алгоритмы работы тестовых программ; собственные средства защиты различных операционных систем и сред;

- способы и методы шифрования информации выявления каналов утечки информации; определения необходимых средств защиты;

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 432 часов, в том числе:

максимальной учебной нагрузки обучающегося – **432** часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 240 часа;

самостоятельной работы обучающегося – 120 часов;

учебной практики – 36 часа.

Производственная практика -36 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности, **Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК.2.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
ПК.2.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению
ПК 2.3.	Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

3. СТРУРКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля *(вариант для НПО)*

Коды профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов**	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**			***Практика***	
			Обязательная аудиторная учебная нагрузка обучающегося		**Самостоятельная работа обучающегося,** часов	**Учебная,** часов	***Производственная,*** *часов*
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов			
1	**2**	**3**	**4**	**5**	**6**	**7**	***8***
ПК1 ПК 2 ПК3	**Раздел 1.** Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**192**	**128**	48	**64**		
ПК1 ПК 2 ПК3	**Раздел 2** Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**168**	**112**	48	**56**		
	Учебная практика					**36**	
	Производственная практика, часов						36
	Всего:	**432**	**240**	96	**120**	**36**	**36**

* Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов	Коды компетенций, умений и знаний, формированию которых способствует элемент программы
1	2	3	4
Раздел. 1	**ПМ2. Обеспечение информационной безопасности телекоммуникационных систем и информационно- коммуникационных сетей связи.**	432	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.	**128**	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
Тема 1.1. Основные понятия и анализ угроз информационной безопасности сетей. Стандарты информационной безопасности.	Содержание учебного материала	24	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1. Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.		
	2. Введение в сетевой информационный обмен. Использование сети Интернет Проблемы безопасности IP-сетей		
	3. Угрозы и уязвимости беспроводных сетей		
	4. Международные стандарты информационной безопасности		
	Лабораторные работы	8	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1. Модель ISO/OSI и стек протоколов TCP/IP		
	2. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)		
	3. Стандарты информационной безопасности в Интернете		
	4. Отечественные стандарты безопасности информационных технологий		
	Практические занятия.		
	1.		
Тема 1.2. Принципы криптографической защиты информации	Содержание учебного материала	14	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1. Основные понятия криптографической защиты информации		
	2. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования		
	3. Комбинированная криптосистема шифрования		
	4. Электронная цифровая подпись и функция хэширования Функция хэширования Управление крипто ключами Классификация криптографических алгоритмов.		
	Лабораторные работы	14	ПК.2.1ПК.2.2ПК2.3.

	1.	Алгоритм шифрования RSA		ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	2.	Алгоритмы цифровой подписи		
	3.	Изучение простейшего криптоанализашифротекста.		
	4.	Исследование средств двухключевого шифрования данных.		
	5.	Исследование электронной цифровой подписи информации с использованием PGP.		
	6.	Изучение способов защиты информации в системах поддержки принятия решений.		
	Практические занятия			
	1.			
Тема 1.3. Технология аутентификации обеспечение безопасности операционных систем. Технологии межсетевых экранов.	**Содержание учебного материала**		24	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1	Основные понятия аутентификации и идентификации. Аутентификация, авторизация и администрирование действий пользователей		
	2	Методы аутентификации, использующие пароли и PIN-коды		
	3	Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах Проблемы обеспечения безопасности ОС Угрозы безопасности ОС Понятие защищенной ОС Архитектура подсистемы защиты ОС.		
	4.	Функции межсетевых экранов Фильтрация трафика. Особенности функционирования МЭ на различных уровнях модели OSI		
	5.	Прикладной шлюз. Варианты исполнения МЭ. Формирование политики межсетевого взаимодействия		
	6.	Основные понятия и функции сети VPN. Персональные и распределенные сетевые экраны. Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей		
	Лабораторные работы			ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Биометрическая аутентификация пользователя		
	2.	Аутентификация на основе PIN-кода		
	3.	Аутентификация на основе многоразовых паролей и одноразовых паролей		
	4.	Исследование средств двухключевого шифрования данных.		
	5.	Исследование электронной цифровой подписи информации с использованием PGP.		
	6.	Схемы сетевой защиты на базе МЭ.		
	7.	Схемы сетевой защиты на базе МЭ Классификация сетей VPNОсновные варианты архитектуры VPN		
	Практические занятия			
	1.			
Тема 1.4. Технологии обнаружения атак. Управление сетевой безопасностью.	**Содержание учебного материала**		18	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8.
	1.	Анализ защищенности и обнаружение атак Средства анализа защищенности сетевых протоколов, сервисов и ОС. Методы		

		анализа сетевой информации. Классификация систем обнаружения атак IDS Компоненты и архитектура IDS. Методы реагирования		ОК 9.ОК 10.
	2.	Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ Антивирусные программы и комплексы. Построение системы антивирусной зашиты корпоративной сети.		
	3	Концепция глобального управления безопасностью. Функционирование системы управления средствами безопасности.		
	Лабораторные работы			ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Установление и настраивание антивирусной программы DoctorWeb.		
	2.	Установление и настраивание антивирусной программы Avast.		
	3.	Архитектура управления средствами сетевой безопасности.		
	4.	Аудит и мониторинг безопасности		
	5.	Глобальная и локальная политики безопасности		
	Практические занятия			
	1.			
		Всего 128 в том числе 48 лаб		
Раздел 2		**МДК02.02. Технология применения комплексной системы защиты информации в телекоммуникационных системах и сетях связи.**	**112**	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
Тема 2.1. Построение и организация комплексной системы защиты информации	**Содержание учебного материала**		16	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Виды и свойства защищаемой информации. Факторы, воздействующие на защищаемую информацию. Сущность и задачи комплексной системы защиты информации		
	2.	Принципы организации КСЗИ. Роль системного подхода в создании КСЗИ		
	3.	Обобщенная модель защищенной системы. Концепция информационной безопасности. Этапы разработки и жизненный цикл КСЗИ. Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты.		
	Лабораторные работы		2	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Требования КСЗИ		
	Практические занятия			
	1.			

Тема 2.2 Законодательный уровень информационной безопасности.	**Содержание учебного материала**		4	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Основные непреднамеренные и преднамеренные искусственные угрозы		
	2	Описание модели гипотетического нарушителя. Определение потенциальных каналов, методов и возможностей НСД к информации.		ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	Лабораторные работы		6	
	1.	Классификация угроз безопасности. Изучение путей реализации угроз безопасности		
	2.	Источники, виды и способы дестабилизирующего воздействия на информацию.		
	Практические занятия			
	1.			
Тема 2.3. Защита информации в распределенных КС.	**Содержание учебного материала**		2	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Физические меры. Технические (программно-аппаратные) меры		
	Лабораторные работы		6	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Нормативно-правовые меры		
	2.	Морально-этические меры Административные меры		
	Практические занятия			
	1.			
Тема 2.4. Определение компонентов КСЗИ	**Содержание учебного материала**		16	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1	Подсистема управления доступом (идентификации и аутентификации пользователей). Подсистема регистрации и учета. Подсистема обеспечения целостности. Криптографическая подсистема. Подсистема антивирусной защиты.		
	2	Подсистема резервного копирования и архивирования. Подсистема обнаружения атак. Подсистема обеспечения отказоустойчивости Подсистема централизованного управления ИБ.		
	Лабораторные работы		10	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Требования к подсистемам ЗИ.		
	2.	Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации. Планирование восстановительных работ.		
	3.	Подсистема межсетевого экранирования		
	4.	Сетевое сканирование		
	Практические занятия			
	1.			
Тема 2.5. Определение условий функционирования КСЗИ	**Содержание учебного материала**		16	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Определение условий функционирования КСЗИ. Технологическое и организационное построение КСЗИ. Кадровое обеспечение функционирования КСЗИ		

	2.	Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ		
	3.	Назначение, структура и содержание управления КСЗИ Принципы и методы планирования функционирования КСЗИ Сущность и содержание контроля функционирования КСЗИ		
	4.	Управление КСЗИ в условиях чрезвычайных ситуаций. Состав методов и моделей оценки эффективности КСЗИ		
	Лабораторные работы		10	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Разработка модели КСЗИ		
	2.	Анализ трафика и сбор критичной информации программами пассивного анализа		
	3.	Обнаружение уязвимостей по сигнатурам		
	4.	Оценка уязвимости коммутируемого доступа		
	Практические занятия			
	1.			
Тема 2. 6 Технические средства комплексной системы защиты информации	**Содержание учебного материала**			
		Причины, виды, каналы утечки и искажения информации. Технические средства и методы защиты информации.	10	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
		Анализ сетевой топологии и установленных сервисов.		
	Лабораторные работы		14	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
	1.	Изучение Системы активной защиты (САЗ) ВОЛНА-3М		
	2.	«Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)».		
	3.	Тестовые испытания программных средств защиты.		
	4.	Методы и технологии испытания аппаратного уровня комплексной защиты информации.		
	5.	Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»		
	6.	Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»		
	7.	Аудит комплексной защиты информации предприятия		
		Практические занятия		
		Всего 112 в том числе 48 ч лаб		
Самостоятельная работа при изучении раздела ПМ . Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите			120	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4. ОК 5.ОК 6.ОК 7.ОК 8. ОК 9.ОК 10.
Примерная тематика домашних заданий Основные программно-технические меры, управление Идентификация и аутентификация Стандарты и спецификации в области информационной безопасности**.**				

Законодательный уровень информационной безопасности. Административный уровень информационной безопасности.			
Учебная практика Изучение Защита информации в операционной системе Изучение стандартных настроек BIOS Setur Установление и настраивание антивирусной программы Doctor Web Установление и настраивание антивирусной программы Avest Изучение простейшего криптоанализа шифротекста. Исследование средств двухключевого шифрования данных Исследование электронной цифровой подписи информации. Изучение способов защиты информации в системах поддержки принятия. Изучение стандарта ISO/IEC 15408 «Критерии оценки» Технические средства комплексной системы защиты информации Изучение Системы активной защиты (САЗ) ВОЛНА-3М «Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)». Тестовые испытания программных средств защиты. Методы и технологии испытания аппаратного уровня комплексной защиты информации. Изучение технического регулирования в области защиты информации Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф» Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор» Аудит комплексной защиты информации предприятия		36	
Производственная практика *(для СПО –* **(по профилю специальности)** **Виды работ**	Общие сведения о предприятии. Требования охраны труда и пожарной безопасности. Изучение отраслевой принадлежности и организационной структуры предприятия Выявление каналов утечки информации; определения необходимых средств защиты. Классификация угроз информационной безопасности; проведение выборки средств защиты в соответствии с выявленными угрозами Проведение аттестации объекта защиты (проверки уровня защищенности); разработки политики безопасности для объекта защиты Определение возможных видов атак; осуществление мероприятиий по проведению аттестационных работ; Установка, настройка специализированного оборудования по защите информации. Разработка политики безопасности объекта; Выполнение расчетов и установка специализированного оборудования для максимальной защищенности объекта	36	ПК.2.1ПК.2.2ПК2.3. ОК 1ОК 2 ОК 3.ОК 4.ОК 5.ОК 6.ОК 7.ОК 8. ОК 9. ОК 10.

	Выявление возможных атак на автоматизированные системы; установки и настройки программных средств защиты автоматизированных систем и информационно- коммуникационных сетей Использование программных продуктов, выявляющих недостатки систем защиты; производение установки и настройки средств защиты; конфигурирование автоматизированных систем и информационно-коммуникационных сетей в соответствии с политикой информационной безопасности; Конфигурирование автоматизированных систем и информационно-коммуникационных сетей Выполнение тестирования систем с целью определения уровня защищенности; Оформление отчета Определение состава и содержания отчета Оформление отчета. Сдача отчета в соответствии с содержанием тематического плана практики		
	Всего	432	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лабораторий информационной безопасности телекоммуникационной системы и информационно-коммуникационных сетей связи, полигона вычислительной техники.

Оборудование лабораторий и рабочих мест лабораторий:
- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальную сеть, проектор, экран, плазменная панель, комплект учебно-методической документации.

Оборудование полигона вычислительной техники:
- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальную сеть.

Реализация программы модуля предполагает обязательную учебную практику, которую рекомендуется проводить рассредоточенно.

Оборудование и технологическое оснащение рабочих мест:
- компьютеры (рабочие станции), локальная сеть, выход в глобальную сеть.

4.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Основы информационной безопасности : учебное пособие / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина — 4-е изд. —М.: 2008. — 205 с. : ил.
2. Галатенко В. А. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с. — ISBN 5-9556-0053-1.
3. Малюк А. А., Горбатов В. С , Королев В. И. и др. Введение в информационную безопасность: Учебное пособие для вузов/ Под ред.В. С. Горбатова. - М.: Горячая линия – Телеком, 2011. – 288 с.: ил. Дополнительные источники:

4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с. — ISBN 5-94074-383-8.
5. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. — 176 с. — ISBN 978-985-463-258-2.
6. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.

Дополнительные источники:

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с. — ISBN 978-5-8041-0378-2.
2. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
3. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.

4. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. — 428 с. — ISBN 5-93598-030-4.
5. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с. — ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.
6. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
7. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005).
8. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005.
9. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
10. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1 — 2006).
11. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
12. Словарь терминов по безопасности и криптографии. Европейский институт стандартов по электросвязи
13. Поиск. Глоссарий.ru
14. Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005).
15. Государственный стандарт РФ «Аспекты безопасности. Правила включения в стандарты» (ГОСТ Р 51898-2002).
16. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.

Интернет ресурсы:
Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, WWW.twirpx.com, WWW.referent.ru, WWW.kodeks-luks.ru/dws, WWW.Consultant.ru/online.

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к учебной практике в рамках профессионального модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля «Разработка программных модулей программного обеспечения для компьютерных систем».

Перед изучением модуля обучающиеся изучают следующие дисциплины «Компьютерное моделирование», «Теория электрических цепей», «Технология монтажа телекоммуникационных систем и информационно-коммуникационных сетей связи», «Основы программирования», «Правовое обеспечение профессиональной деятельности», «Безопасность жизнедеятельности».

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам)**:** наличие высшего

профессионального образования, соответствующего профилю модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» по специальности «Сети связи и системы коммутации».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: высшее инженерное образование, соответствующее профилю модуля.

Мастера: обязательная стажировка в профильных организациях не реже 1-го раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК.2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.	- Установление и настройка специализированного оборудования по защите информации; - Установление и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей связи; - Выявление возможных атак на автоматизированные системы; - Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей - Организация защиты в различных операционных системах и средах, шифрования информации.	- Текущий контроль в форме:- защиты лабораторных занятий;- тестирования;- контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий;- тестирования. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.

ПК.2.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению	- Классифицировать угрозы информационной безопасности; - проводить выборку средств защиты в соответствии с выявленными угрозами; определять возможные виды атак; - осуществлять мероприятия по проведению аттестационных работ; - разрабатывать политику безопасности объекта; выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта; - использовать программные продукты, выявляющие недостатки систем защиты; - производить установку и настройку средств защиты; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; - выполнять тестирование систем с целью определения уровня защищенности;	- Текущий контроль в форме:- защиты лабораторных занятий;- тестирования; - - контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий; - - тестирования. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий; - - тестирования; - - контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.

	- использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации;	- Текущий контроль в форме: - - защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессиональног о модуля.
ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.	- классификацию и принципы работы специализированного оборудования;	Текущий контроль в форме:- защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК. Экзамены по разделу профессионального модуля.
	- принципы построения информационно-коммуникационных сетей;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования.
	- возможные способы несанкционированного доступа; нормативно-правовые и законодательные акты в области информационной безопасности;	Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля.
	- правила проведения возможных проверок; этапы определения конфиденциальности документов объекта защиты;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК. Экзамены по разделу профессионального модуля. Текущий контроль в форме:

		- защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля.
	- технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов;	Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля.
	- конфигурации защищаемых сетей; алгоритмы работы тестовых программ; собственные средства защиты различных операционных систем и сред;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК.
	- способы и методы шифрования информации выявления каналов утечки информации; определения необходимых средств защиты;	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	– демонстрация интереса к будущей профессии	Интерпретация результатов наблюдений за деятельностью обучающегося в

		процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	– выбор и применение методов и способов решения профессиональных задач в области разработки и администрирования баз данных; – оценка эффективности и качества выполнения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– решение стандартных и нестандартных профессиональных задач в области разработки и администрирования баз данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	– эффективный поиск необходимой информации; – использование различных источников, включая электронные	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– разрабатывать, программировать и администрировать базы данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	– самоанализ и коррекция результатов собственной работы	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	– организация самостоятельных занятий при изучении профессионального модуля	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	– анализ инноваций в области разработки и администрирования баз данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	– решение ситуативных задач, связанных с использованием профессиональных компетенций	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

Разработчики:

ГБПОУ РД Технический колледж имени Р.Н Ашуралиева	*Преподаватель*	*Багаутдинова З.М*
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*

ГБПОУ РД Технический колледж имени Р.Н Ашуралиева	*Преподаватель*	*Джамалутдинова М.Д*
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*

Эксперты:

_____	_____	_____
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*
_____	_____	_____
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н АШУРАЛИЕВА».

УТВЕРЖДАЮ

Заместитель директора по УР

_____ Ф.РАхмедова
Подпись ФИО

«____» _____2021г

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

По специальности 11.02.11 Сети связи и системы коммутации

Разработчик:

Багаутдинова З.М

Рассмотрено на заседании предметной (цикловой) комиссии УГС 11.00.00. Электроника, радиотехника и системы связи специальности 11.02.11 Сети связи и системы коммутации

Протокол № 1 от 3 сентября 2021г

Председатель П(Ц)К З.Н.Мирзаев _____
ФИО подпись

Махачкала 2021г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН
Государственное бюджетное профессиональное образовательное учреждение РД
«Технический колледж имени Р.Н Ашуралиева».

УТВЕРЖДАЮ

Заместитель директора
по учебной работе.

_____ Ф.Р Ахмедова
подпись ФИО

«____» _____ 20__ г.

КАЛЕНДАРНО–ТЕМАТИЧЕСКИЙ ПЛАН

По профессиональному модулю ПМ02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.
индекс и наименование ПМ

в том числе:
по междисциплинарному курсу МДК 02.01 Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

Составлен в соответствии с рабочей программой профессионального модуля, утвержденной «__» _____20___ г.

Рассмотрен на заседании предметной (цикловой) комиссии по УГС 11.00.00 Электроника, радиотехника и системы связи.

« _3 » _сентября 2021__ г., председатель П(Ц)К _____Мирзаев З,Н
подпись ФИО

Специальность 11. 02. 11 Сети связи и системы коммутации.
код и наименование специальности

Коды формируемых компетенций _____ОК1-ОК10 ПК1-ПК3_____

Преподаватель _____Багаутдинова З.М_____
ФИО

Общие (ОК) и профессиональные (ПК) компетенции
формируемые при изучении профессионального модуля

Код компетенции	Содержание компетенции
ПК.2.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
ПК.2.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению
ПК 2.3.	Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

Распределение часов по профессиональному модулю Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.

Междисциплинарный курс (индекс и наименование МДК)	Курс,	семестр	Форма промежуточной аттестации	Всего часов (максимальная учебная нагрузка и практика)	Объем времени, отведенный на освоение междисциплинарного курса							Практика	
					Максимальная учебная нагрузка	Обязательная аудиторная учебная нагрузка обучающегося					Самостоятельная работа обучающегося, часов	Учебная, часов	Производственная, (по профилю специальности) часов
						Всего, часов	в т.ч.						
							Теоретические занятия	Лабораторные работы, часов	Практические занятия, часов	Курсовая работа (проект), часов			
1	2	3		4	5	6	7	8	9	10	11	12	13
Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.	*3*	*5*	*Зачет*		*178*	*128*	*80*	*48*					
Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.	*3*	*5*	*Экзамен*		*144*	*112*	*52*	*44*			*48*		
Учебная практика	*2*	*4*	*Зачет*									*36*	
Всего по модулю				***324***	***288***	***192***	*104*	*88*			***96***	***36***	

Содержание обучения по профессиональному модулю ПМ02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.

(индекс и наименование ПМ)

Междисциплинарный курс: МДК02.01 Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи

(индекс и наименование МДК)

Преподаватель: Багаутдинова З.М

№	Наименование разделов профессионального модуля, тем и занятий по МДК	Обязательная учебная нагрузка		Материально-техническое обеспечение занятий, Интернет-ресурсы (№ позиции из табл.2а, 2г)	Внеаудиторная самостоятельная работа обучающихся		
		кол-во часов	вид занятия		вид задания	информа-ционное обеспечение (№ из табл. 2б,2в,2г)	кол-во часов
1	2	3	4	5	6	7	8
Раздел 1. Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи							
Тема 1.1.Основные понятия и анализ угроз информационной безопасности сетей. Стандарты информационной безопасности 18 (8) часов.							
1	Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.	2	Лекция	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
2	Анализ угроз информационной безопасности	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
3	Введение в сетевой информационный обмен. Использование сети Интернет	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
4	Проблемы безопасности IP-сетей Угрозы и уязвимости беспроводных сетей	2	Комб.урок	1, 2	Подготовка реферата (компьютерной презентации) на	ОИ 1, ОИ 2	1

					тему: « Организация совместного использования линий связи»		
5	Международные стандарты информационной безопасности	4	Комб.урок	1, 2	Подготовка реферата (компьютерной презентации)		1
6	Модель ISO/OSI и стек протоколов TCP/IP	4	Л.р.№1	1, 2	Подготовка к лабораторным работам с использованием методических рекомендаций, оформление отчета по лабораторной работе, подготовка к защите.	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
7	Стандарты ISO/IEC 17799:2002 (BS 7799:2000)	4	Л.р.№2	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
8	Стандарты информационной безопасности в Интернете	4	Л.р.№3	1, 2	Подготовка к лабораторным работам с использованием методических рекомендаций, оформление отчета по лабораторной работе, подготовка к защите.	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
9	Отечественные стандарты безопасности информационных технологий	2	Л.р.№4	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
			Практическое занятие				
			Контрольная работа				1
Тема 1.2.Принципы криптографической защиты информации							
10	Основные понятия криптографической защиты информации	2	Лекция	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
11	Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической	ОИ 1, ОИ 2	1

					литературы (по вопросам к параграфам учебника).		
12	Комбинированная криптосистема шифрования	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
13	Электронная цифровая подпись и функция хэширования Функция хэширования Управление крипто ключами	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
14	Классификация криптографических алгоритмов	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
15	Алгоритм шифрования RSA	2	Л.р.№5	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
16	Алгоритмы цифровой подписи	2	Л.р.№6	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
17	Изучение простейшего криптоанализашифротекста.	2	Л.р.№7	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
18	Одноключевые криптографические системы.	2	Л.р.№8	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
19	Исследование электронной цифровой подписи информации с использованием PGP.	2	Л.р.№97	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
20	Изучение способов защиты информации в системах поддержки принятия решений.	2	Л.р.№10	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
			Практическое занятие				

			Контрольная работа				
Тема 1.3.Технология аутентификации обеспечение безопасности операционных систем. Технологии межсетевых экранов.							
21	Основные понятия аутентификации и идентификации.	2	Лекция	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
22	Аутентификация, авторизация и администрирование действий пользователей	2	Лекция	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
23	Методы аутентификации, использующие пароли и PIN-коды	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
24	Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах Проблемы обеспечения безопасности ОС Угрозы безопасности ОС Понятие защищенной ОС Архитектура подсистемы защиты ОС.	6	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
25	Функции межсетевых экранов Фильтрация трафика. Особенности функционирования МЭ на различных уровнях модели OSI	6	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
26	Прикладной шлюз. Варианты исполнения МЭ. Формирование политики межсетевого взаимодействия	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
27	Основные понятия и функции сети VPN. Персональные и распределенные сетевые экраны.	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1

28	Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
29	Биометрическая аутентификация пользователя	2	Л.р.№11	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
30	Аутентификация на основе PIN-кода	2	Л.р.№12	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
31	Аутентификация на основе многоразовых паролей и одноразовых паролей	2	Л.р.№13	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
32	Исследование средств двухключевого шифрования данных.	2	Л.р.№14	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
33	Исследование электронной цифровой подписи информации с использованием PGP.	2	Л.р.№15	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
34	Схемы сетевой защиты на базе МЭ.	2	Л.р.№16	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
35	Схемы сетевой защиты на базе МЭ Классификация сетей VPNОсновные варианты архитектуры VPN	2	Л.р.№17	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
Теиа 1.4. Технология обнаружения атак . Управление сетевой безопасностью							
36	Анализ защищенности и обнаружение атак Средства анализа защищенности сетевых протоколов, сервисов и ОС.	4	Лекция	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
37	Методы анализа сетевой информации. Классификация систем обнаружения атак IDS Компоненты и архитектура IDS. Методы реагирования.	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической	ОИ 1, ОИ 2	1

					литературы (по вопросам к параграфам учебника).		
38	Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов.	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
39	Основные каналы распространения вирусов и других вредоносных программ	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
40	Антивирусные программы и комплексы. Построение системы антивирусной зашиты корпоративной сети.	4	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
41	Задачи управления системой сетевой безопасности.	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
42	Концепция глобального управления безопасностью.	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	1
43	Функционирование системы управления средствами безопасности.	2	Комб.урок	1, 2	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам учебника).	ОИ 1, ОИ 2	Комб.урок
44	Установление и настраивание антивирусной программы DoctorWeb.	2	Л.р.№18	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
45	Установление и настраивание антивирусной программы Avast.	2	Л.р.№19	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1

46	Архитектура управления средствами сетевой безопасности.	2	Л.р.№20	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
47	Аудит и мониторинг безопасности Глобальная и локальная политики безопасности	2	Л.р.№21	1, 2	Оформление лабораторно-практических работ, отчетов и подготовка к их защите	ОИ 1,ОИ 5, ОИ 6, ДИ 3	1
							1
ВСЕГО 128 часа из них 48 часа лабораторных.							

Виды работ по учебной практике _____

№ п/п	Раздел ПМ. Виды работ	Количество часов	Коды формируемых компетенций		Материально-техническое и информационное обеспечение занятий (№ позиций из табл. 2а, 2б, 2в, 2г)
			ОК	ПК	
1	2	3	4	5	6
	Раздел ПМ 2. **Обеспечение информационной безопасности телекоммуникационных систем и информационно- коммуникационных сетей связи.**				
Тема 1. Обеспечение информационной безопасности телекоммуникационных систем и информационно- коммуникационных сетей связи.			ОК 1. ОК 2. ОК 3. ОК 4. ОК 5.	ПК.2.1	
1	Изучение Защита информации в операционной системе	2			Табл.2а 1, 2; Табл.2б ОИ 7
2	Изучение стандартных настроек BIOS Setup.	2			Табл.2а 1, 2; Табл.2б ОИ 7
3	Защита от Макрос.				Табл.2а 1, 2; Табл.2б ОИ 7
4	Установление и настраивание антивирусной программы Doctor Web.	2			Табл.2а 1, 2; Табл.2б ОИ 7
5	Установление и настраивание антивирусной программы Avest.	2			Табл.2а 1, 2; Табл.2б ОИ 7
Тема 2. Изучение простейшего криптоанализа шифротекста.					
6	Исследование средств двухключевого шифрования данных.	2			Табл.2а 1, 2; Табл.2б ОИ 7
7	Исследование электронной цифровой подписи информации.	2			Табл.2а 1, 2; Табл.2б ОИ 7
8	Изучение способов защиты информации в системах поддержки принятия.	2			Табл.2а 1, 2; Табл.2б ОИ 7
9	Изучение стандарта ISO/IEC 15408 «Критерии оценки»	2			Табл.2а 1, 2; Табл.2б ОИ 7

Тема 3. Изучение руководящих документов Гостехкомиссии России.					
10	Ознакомление с интерпретацией «Оранжевой книги» для сетевых конфигураций.	2			Табл.2а 1, 2; Табл.2б ОИ 7
11	Изучение руководящих документов. Гостехкомиссии России.	2			Табл.2а 1, 2; Табл.2б ОИ 7
12	Изучение сетевых сервисов безопасности.	2			Табл.2а 1, 2; Табл.2б ОИ 7
13	Ознакомление с администрированием средств безопасности.	2			Табл.2а 1, 2; Табл.2б ОИ 7
Тема 4. Изучение функциональных подсистем КСЗИ.					Табл.2а 1, 2; Табл.2б ОИ 7
14	Изучение технической защиты конфиденциальной информации.	2			Табл.2а 1, 2; Табл.2б ОИ 7
15	Изучение организационной структуры объектового уровня.	2			Табл.2а 1, 2; Табл.2б ОИ 7
16	Изучение технического регулирования в области защиты информации.	2			Табл.2а 1, 2; Табл.2б ОИ 7
17	Комплексная проверочная работа по УП *(по окончанию УП)*	4			Табл.2а 1, 2; Табл.2б ОИ 7
	ВСЕГО 36 часов				

Материально–техническое обеспечение занятий

по профессиональному модулю _____

Таблица 2а

№ п/п	Материально–техническое обеспечение занятий
1	Интерактивная доска
2	Персональный компьютер

Информационное обеспечение обучения
Основные источники (ОИ)

Таблица 2б

№ п/п	Наименование	Автор	Издательство, год издания
ОИ 1	Защита информации в компьютерных системах и сетях.	Шаньгин В.Ф	Москва.ДМКПресс, 2012г.
ОИ 2	Современная компьютерная безопасность. Теоретические основы. Практические аспекты. —	Щербаков А. Ю.	М.: Книжный мир, 2009. — 352 с. — ISBN 978-5-8041-0378-2.
ОИ 3	Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.	Петренко С. А. Курбатов В. А.	— М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
ОИ 4	Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.	Петренко С. А.	М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.
ОИ5	Инструкции к лабораторным работам.	Магомедалиева Х.Б.	
ОИ 6	Методические указания к выполнению лабораторных работ	Магомедалиева Х.Б.	
ОИ 7	Методические указания к выполнению лабораторных работ по практике	Магомедалиева Х.Б.	

Дополнительные источники (ДИ)

Таблица 2в

№ п/п	Наименование	Автор	Издательство, год издания

ДИ 1	Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества.	Лопатин В. Н.	М.: 2000. — 428 с. — ISBN 5-93598-030-4.
ДИ 2	Разработка правил информационной безопасности.	Бармен Скотт	М.: Вильямс, 2002. — 208 с. — ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.
ДИ 3	Национальный стандарт РФ «Защита информации. Основные термины и определения»		(ГОСТ Р 50922-2006).
ДИ 4	Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью»		(ГОСТ Р ИСО/МЭК 17799—2005).
ДИ 5	Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»		(ГОСТ Р ИСО/МЭК 13335-1 — 2006).
ДИ 6	Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации»		(Р 50.1.053-2005).
ДИ 7	Словарь терминов по безопасности и криптографии. Европейский институт стандартов по электросвязи		

Интернет-ресурсы (ИР)

Таблица 2г

ИР 1	WWW.twirpx.com, ,
ИР 2	WWW.referent.ru
ИР 3	WWW.kodeks-luks.ru/dws
ИР 4	WWW.Consultant.ru/online.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н АШУРАЛИЕВА».

УТВЕРЖДАЮ

Заместитель директора по УР

_____ Ф.РАхмедова
Подпись ФИО

«____» _____2021г

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

По специальности 11.02.11 Сети связи и системы коммутации

Разработчик:

Багаутдинова З.М

Рассмотрено на заседании предметной (цикловой) комиссии УГС 11.00.00. Электроника, радиотехника и системы связи специальности 11.02.11 Сети связи и системы коммутации

Протокол № 1 от 3 сентября 2021г

Председатель П(Ц)К З.Н.Мирзаев _____
ФИО подпись

Махачкала 2021г.

Перечень вопросов для подготовки студентов к зачёту

МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

1. Основные понятия защиты информации и информационной безопасности.
2. Анализ угроз информационной безопасности.
3. Введение в сетевой информационный обмен.
4. Использование сети Интернет Проблемы безопасности IP-сетей
5. Актуальность проблемы обеспечения безопасности информационных технологий.
6. Место и роль информационных систем в управлении бизнес-процессами.
7. Основные причины обострения проблемы обеспечения безопасности информационных технологий Основные понятия в области безопасности информационных технологий.
8. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.
9. Угрозы безопасности информационных технологий.
10. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности.
11. Принципы обеспечения безопасности информационных технологий.
12. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты.
13. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
14. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация.
15. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.
16. Международные стандарты информационной безопасности
17. Государственная система защита информации.
18. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.
19. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
20. Обеспечение безопасности компьютерных систем и сетей
21. Технология аутентификации обеспечение безопасности операционных систем.
22. Основные понятия аутентификации и идентификации. Аутентификация, авторизация и администрирование действий пользователей
23. Проблемы обеспечения безопасности в компьютерных системах и сетях.
24. Типовая корпоративная сеть. Уязвимости и их классификация.
25. Назначение, возможности и защитные механизмы межсетевых экранов.
26. Угрозы, связанные с периметром сети.
27. Типы межсетевых экранов. Сертификация межсетевых экранов.
28. Назначение, возможности и защитные механизмы межсетевых экранов.

Перечень вопросов для подготовки студентов к экзамену

МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

1. Основные понятия защиты информации и информационной безопасности.
2. Анализ угроз информационной безопасности.
3. Введение в сетевой информационный обмен.
4. Использование сети Интернет Проблемы безопасности IP-сетей
5. Актуальность проблемы обеспечения безопасности информационных технологий.
6. Место и роль информационных систем в управлении бизнес-процессами.
7. Основные причины обострения проблемы обеспечения безопасности информационных технологий Основные понятия в области безопасности информационных технологий.
8. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.
9. Угрозы безопасности информационных технологий.
10. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности.
11. Принципы обеспечения безопасности информационных технологий.
12. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты.
13. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
14. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация.
15. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.
16. Международные стандарты информационной безопасности
17. Государственная система защита информации.
18. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.
19. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
20. Обеспечение безопасности компьютерных систем и сетей
21. Технология аутентификации обеспечение безопасности операционных систем.
22. Основные понятия аутентификации и идентификации. Аутентификация, авторизация и администрирование действий пользователей
23. Проблемы обеспечения безопасности в компьютерных системах и сетях.
24. Типовая корпоративная сеть. Уязвимости и их классификация.
25. Назначение, возможности и защитные механизмы межсетевых экранов.
26. Угрозы, связанные с периметром сети.
27. Типы межсетевых экранов. Сертификация межсетевых экранов.
28. Назначение, возможности и защитные механизмы межсетевых экранов.
29. Угрозы, связанные с периметром сети. Виртуальные частные сети
30. VPN на основе криптошлюза.
31. Методы аутентификации, использующие пароли и PIN-коды
32. Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах.
33. Проблемы обеспечения безопасности ОС Угрозы безопасности ОС.
34. Понятие защищенной ОС Архитектура подсистемы защиты ОС.
35. Функции межсетевых экранов Фильтрация трафика.
36. Особенности функционирования МЭ на различных уровнях модели OSI
37. Прикладной шлюз. Варианты исполнения МЭ.
38. Формирование политики межсетевого взаимодействия
39. Основные понятия и функции сети VPN.

40. Персональные и распределенные сетевые экраны.
41. Средства обеспечения безопасности VPN. VPN-решения для построения защищенных сетей
42. Технологии обнаружения атак.
43. Управление сетевой безопасностью программно-аппаратными средствами.
44. Анализ защищенности и обнаружение атак.
45. Средства анализа защищенности сетевых протоколов, сервисов и ОС.
46. Методы анализа сетевой информации.
47. Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS.
48. Методы реагирования. Компьютерные вирусы и проблемы антивирусной защиты.
49. Классификация компьютерных вирусов. Жизненный цикл вирусов.
50. Основные каналы распространения вирусов и других вредоносных программ
51. Антивирусные программы и комплексы.
52. Построение системы антивирусной зашиты корпоративной сети.
53. Концепция глобального управления безопасностью.
54. Функционирование системы управления программными средствами безопасности.
55. Функционирование системы управления аппаратными средствами безопасности.

МДК03.02. Технология применения комплексной системы защиты информации в телекоммуникационных системах и сетях связи.

1. Значение информационной безопасности и ее место в системе национальной безопасности.
2. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.
3. Виды и источники угроз информационной безопасности Российской Федерации.
4. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.
5. Структура правовой защиты информации.
6. Организационные основы защиты информации. Принципы организационной защиты информации.
7. Обзор стандартов и методических документов в области защиты информации.
8. Регулирующие организации в области защиты информации.
9. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность.
10. Виды ответственности за правонарушения в информационной сфере.
11. Общая характеристика комплексной защиты информации.
12. Основы обеспечения комплексной защиты информации.
13. Сущность и задачи комплексной защиты информации.
14. Структура и основные характеристики комплексной защиты информации.
15. Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.
16. Подсистема инженерной защиты.
17. Периметровая сигнализация и ограждение. Периметровое освещение.
18. Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.
19. Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.
20. Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.
21. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.
22. Классификация каналов утечки информации.
23. Основные способы и средства НСД к защищаемой информации.
24. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации.
25. Защита информации в каналах связи.

26. Акустический контроль. Понятие разборчивости речи при перехвате информации.
27. Способы и средства информационного скрытия речевой информации от подслушивания.
28. Классификация средств обнаружения неизлучающих закладок.
29. Контроль слаботочных цепей. Принципы контроля линий заземления.
30. Нелинейные радиолокаторы. Современные средства радиолокации.
31. Основные методы криптографического преобразования данных.
32. Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись.
33. Безопасные хеш-функции, алгоритмы хеширования.
34. Контрольное значение циклического избыточного кода CRC.
35. Цифровые сертификаты.
36. Отечественный стандарт цифровой подписи. Понятие криптоанализа.
37. Общие вопросы по аттестации ОИ по требованиям безопасности информации.
38. Основные стадии создания системы защиты информации на ОИ.
39. Порядок проведения аттестации объектов информатизации.
40. Организационная структура системы аттестации объектов информатизации.
41. Программа и методика проведения аттестационных испытаний.
42. Лицензирование деятельности в области защиты конфиденциальной информации.
43. Документы, разрабатываемые на объектах информатизации.
44. Документы, разрабатываемые на аттестуемое помещение.
45. Порядок действий при лицензировании

Разработчик преподаватель _____ М.Д.Джамалутдинова

Разработчик преподаватель _____ З.М Багаутдинова

ПЦК УГС 11.00.00 _____ З.Н Мирзаев

Перечень тем для написания рефератов

1. Основные понятия защиты информации и информационной безопасности.
2. Анализ угроз информационной безопасности.
3. Введение в сетевой информационный обмен.
4. Использование сети Интернет Проблемы безопасности IP-сетей
5. Угрозы безопасности информационных технологий.
6. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
7. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация.
8. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.
9. Международные стандарты информационной безопасности
10. Государственная система защита информации.
11. Проблемы обеспечения безопасности в компьютерных системах и сетях.
12. Типовая корпоративная сеть. Уязвимости и их классификация.
13. Назначение, возможности и защитные механизмы межсетевых экранов.
14. Угрозы, связанные с периметром сети.
15. Типы межсетевых экранов. Сертификация межсетевых экранов.
16. Назначение, возможности и защитные механизмы межсетевых экранов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н АШУРАЛИЕВА».

УТВЕРЖДАЮ

Заместитель директора по УР

_____ Ф.РАхмедова
Подпись ФИО

«____» _____2021г

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

По специальности 11.02.11 Сети связи и системы коммутации

Разработчик:

Багаутдинова З.М

Рассмотрено на заседании предметной (цикловой) комиссии УГС 11.00.00. Электроника, радиотехника и системы связи специальности 11.02.11 Сети связи и системы коммутации

Протокол № 1 от 3 сентября 2021г

Председатель П(Ц)К З.Н.Мирзаев _____
ФИО подпись

Махачкала 2021г.

Методические указания для выполнения лабораторных работ студентами

(цели, задачи, рекомендации)

Быстрый рост глобальной сети Internet и стремительное развитие информационных технологий привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Новые технологические возможности облегчают распространение информации, повышают эффективность производственных процессов, способствуют расширению деловых отношений. Однако несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. Поэтому проблемы обеспечения информационной безопасности привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса

Создаваемая СИБ предприятия должна учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к любым элементам КИС, таким как:
применение открытых стандартов;
использование интегрированных решений;
обеспечение масштабирования в широких пределах.
Переход на открытые стандарты составляет одну из главных тенденций развития средств информационной безопасности.
Для того чтобы обеспечить надежную защиту ресурсов КИС, в СИБ должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. К ним относятся:
криптографическая защита данных для обеспечения конфиденциальности, целостности и подлинности информации;
технологии аутентификации для проверки подлинности пользователей и объектов сети;*технологии межсетевых экранов* для зашиты корпоративной сети от внешних угроз при подключении к общедоступным сетям связи;
технологии виртуальных защищенных каналов и сетей VPN для защиты информации, передаваемой по открытым каналам связи;
гарантированная идентификация пользователей путем применения токенов (смарт-карт, touch-memory, ключей для USB-портов и т. п.) и других средств аутентификации;
управление доступом на уровне пользователей и защита от несанкционированного доступа к информации;
поддержка инфраструктуры управления открытыми ключами PKI;
технологии обнаружения вторжений (Intrusion Detection) для активного исследования защищенности информационных ресурсов;
технологии защиты от вирусов с использованием специализированных комплексов антивирусной профилактики и защиты;
централизованное управление СИБ на базе единой политики безопасности предприятия;
комплексный подход к обеспечению информационной безопасности, обеспечивающий рациональное сочетание технологий и средств информационной защиты.

Содержание лабораторно-практических занятий по дисциплине

Лабораторная работа №1: «Модель ISO/OSI и стек протоколов TCP/IP**».**

Цель: Изучить модели и стеки ISO/OSI, стек протоколов TCP/IP.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.На какие уровни делятся модели ISO?
2.Как происходит обмен данными?
3.Что нужно для обеспечения совместимости?
4.Что такое *«стек коммуникационных протоколов»*?
5.Различия между стеком протоколов и моделями ISO/OSI.
6.Что такое «*межуровневый интерфейс*»?
7.Что такое и для чего используют «*TCP/IP*»?
8.Особенности TCP/IP

Лабораторная работа №2: «Стандарты ISO/IEC 17799:2002 (BS 7799:2000)**».**

Цель: Изучить стандарты ISO/IEC
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Какие вопросы информационной безопасности организаций и предприятий рассматривает ISO/IEC 17799:2000 (BS 7799—1:2000)?
2.Какие дополнительные рекомендации содержит руководство Британского института стандартов?
3.Что было изменено в международном стандарте ISO 17799 (BS 7799)?

Лабораторная работа №3: «Стандарты информационной безопасности в Интернете»

Цель: Изучить стандарты информационной безопасности в Интернете
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1.Что такое термин «открытые системы»?
2.Протокол SSL его использование.
3.Протокол SET, сфера его использования и преимущества.
4.Использование и преимущества протокола IPSec.
5.Предназначение открытых ключей PKI.

Лабораторная работа №4: «Отечественные стандарты безопасности информационных технологий»

Цель: Изучить виды отечественной безопасности и его преимущества.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Основные проблемы защиты информации в коммерческой АС.
2. Что такое: ГОСТ Р ИСО/МЭК 15408—2002.
4. Из каких частей состоит ГОСТ Р ИСО/МЭК 15408—2002.
5. Главные достоинства ГОСТ Р ИСО/МЭК 15408—2002.

Лабораторная работа №5: «Проблемы создания защищенных информационных систем»

Цель: Обеспечение информационной безопасности на всех уровнях.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Как обеспечить информационную безопасность.
2. Дать пояснение что такое комплексная защита и что она в себя включает.
3. Кто или что является возможным источником угрозы, какого рода атаки на безопасность системы могут быть предприняты?
4. Какие средства использовать для защиты каждого вида информации?
5. Какую информацию защищать?
6. Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?

Лабораторная работа №6: «Определение защищенной информационной системы»

Цель: Изучить системы защиты информации.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.

Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Как обеспечить информационную безопасность.
2. Дать подробное пояснение для чего и как работает защищенная информационная система.
3. Для чего служит функция монитора и как она работает.
4. Кто или что является возможным источником угрозы, какого рода атаки на безопасность системы могут быть предприняты.
5. Для чего нужна политика безопасности.

Лабораторная работа №7: «Обзор и сравнительный анализ стандартов информационной безопасности»

Цель: Изучить стандарты информационной безопасности.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение защищенной вычислительной системе.
2. Для чего нужны стандарты информационной безопасности.
3. Перечислите какие вы знаете стандарты информационной безопасности.
4. Какой бы выбрали стандарт информационной безопасности для своей организации и почему.

Лабораторная работа №8: «Требования к архитектуре информационной системы для обеспечения безопасности ее функционирования»

Цель: Изучить требования к архитектуре информационной безопасности.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение информационной безопасности.
2. Перечислить требования к архитектуре информационной системы для обеспечения безопасности.
3. Перечислить основные требования к информационной безопасности.
4. Этапы построения системы безопасности ИС.
5. Что значит надежная информационная система.

Лабораторная работа №9: «Этапы построения системы безопасности ИС»

Цель: Изучить этапы построения системы безопасности.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309

Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение информационной безопасности.
2. Перечислить основные этапы построения системы безопасности.
3. Что включает в себя аудит безопасности.
4. Что означает техническая поддержка и сопровождение.

Лабораторная работа №10: «Анализ стандартов информационной безопасности»
Цель: Изучить анализ стандартов информационной безопасности.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение информационной безопасности.
2. Перечислите основные показатели сопоставления стандартов.
3. Перечислите основные риски в области информационной безопасности.
4. Цели аудита информационной безопасности.

Лабораторная работа №11: «Защита персональных данных»
Цель: Изучить способы защиты информации.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Перечислите общие требования при обработке персональных данных.
2. Методы защиты персональных данных.
3. Средства защиты персональных данных.
4. Какой способ используете вы и почему именно этот описать.

Лабораторная работа №12: «Защита компьютерной информации на уроне доступа в систему»
Цель: Изучить способы защиты информации.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309

Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение информационной безопасности.
2. Какие признаки компьютерных преступлений вы знаете перечислить.
3. Перечислить четыре уровня защиты компьютерных и информационных ресурсов.
4. Перечислить какие меры защиты информационной безопасности компьютерных систем вы знаете дать подробную характеристику.

Лабораторная работа №13: «Защита от атак по локальным и глобальным сетям»
Цель: Изучить способы защиты информации.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение что такое сетевая атака.
2. Способы и методы защиты информации от сетевых атак.
3. Перечислить методы обнаружения DoS атак.
4. Как защититься от несанкционированного доступа изнутри ЛВС организации.

Лабораторная работа №14: «Алгоритм шифрования RSA»
Цель: Изучить алгоритм шифрования RSA.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1.Для чего нужен открытый ключ $K_в$?
2.Сколько ключей использует крипто алгоритм RSA?
3.Различия RSA и DES, преимущества и недостатки.

Лабораторная работа №15: «Алгоритмы цифровой подписи»
Цель: Изучить алгоритм цифровой подписи.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30

Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Какие параметры используются в цифровой подписи ГОСТ Р 34.10—94?
2.Что нужно сделать для того чтобы подписать сообщение?
3.Преимущества ГОСТ Р 34**.**10—2001 над ГОСТ Р 34.10—94**.**

Лабораторная работа №16: «Изучение простейшего криптоанализашифротекста.»
Цель: Изучить простейшего криптоанализашифротекста. .
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Дать определение что такое криптография и криптоанализ.
2. Перечислить какие методы вы знаете при шифровании данных.

Лабораторная работа №17: «Исследование средств двухключевого шифрования данных..»
Цель: Изучить исследование средств двухключевого шифрования данных..
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Дать определение что такое шифрование.
2. Перечислить какие методы вы знаете при шифровании данных.
3. Дать определение что значит двухключевое шифрование данных как оно работает.
4. Привести пример двухключевого шифрования.

Лабораторная работа №18: «Исследование электронной цифровой подписи информации с использованием PGP».
Цель: Изучить электронную цифровую подпись информации с использованием PGP...
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:

Составить отчет в письменном виде.

Контрольные вопросы:

1. Чем обусловлена актуальность внедрения электронного документооборота.
2. Что такое электронная цифровая подпись.
3. Расскажите алгоритм подписывания документа.
4. Что такое дайджест сообщения?
5. Какими ключами подписывается и проверяется сообщение.

Лабораторная работа №19: «Изучение способов защиты информации в системах поддержки принятия решений.

Цель: Изучение способов защиты информации в системах поддержки принятия решений.

Оборудование: Персональный компьютер

Место проведения: Технический колледж кабинет №309

Время: 8:30

Учебные вопросы:

Порядок выполнения работ:

Изучить теоретическую часть и ответить на вопросы.

Отчет о проделанной работе:

Составить отчет в письменном виде.

Контрольные вопросы:

1.Перечислить способы защиты информации.
2. Дать определение что такое защита информации.
3. Что значит система поддержки принятия решений.
4. Как можно классифицировать систему поддержки принятия решений.

Лабораторная работа №20: «Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения». несанкционированного доступа.

Цель: Изучение различных видов шифрования информации.

Оборудование: Персональный компьютер

Место проведения: Технический колледж кабинет №309

Время: 8:30

Учебные вопросы:

Порядок выполнения работ:

Изучить теоретическую часть и ответить на вопросы.

Отчет о проделанной работе:

Составить отчет в письменном виде.

Контрольные вопросы:

1.От каких угроз информации нужна защита.
2. Методы защиты информации.
3. Перечислить виды шифрования информации.
4. Что значит техническая защита информации от несанкционированного доступа.

Лабораторная работа №21: «Разработка комплекса организационно-административной защиты от вредоносных программ»

Цель: Изучение комплексной защиты и нформации.

Оборудование: Персональный компьютер

Место проведения: Технический колледж кабинет №309

Время: 8:30

Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Методы и технологии защиты от вредоносных программ.
2. Что значит легитимное программное обеспечение.
2.Дать определение антивирусная защита и как она работает.
3. Объяснить принцип работы межсетевого экрана.

Лабораторная работа №22: «Биометрическая аутентификация пользователя»
Цель: Изучение биометрической аутентификация пользователя.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Достоинства биометрических методов защиты.
2.Какими параметрами характеризуется эффективность биометрической аутентификационной системы?
3.Какие технологии аутентификации разработаны и используются к настоящему времени?
4. Где используются дактилоскопические системы аутентификации? Основные элементы дактилоскопической системы аутентификации.
5.Сканеры отпечатков пальцев, как происходит их регистрация и как можно их использовать?
6.Системы аутентификации по форме ладони, их использование и преимущества.
7. Системы аутентификации по лицу, их использование и преимущества.
8. Системы аутентификации по голосу, их преимущества и недостатки.

Лабораторная работа №23: «Аутентификация на основе PIN-кода.»
Цель: Изучение аутентификации на основе PIN-кода..
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Зачем нужен PIN-код в пластиковой карте?
2.Как происходит ввод PIN-кода?
3.Неалгоритмический способ проверки PIN-кода, как осуществляется?
4.Алгоритмический способ проверки PIN-кода, его преимущества.

Лабораторная работа №24: «Аутентификация на основе многоразовых паролей и одноразовых паролей».
Цель: Изучение аутентификации на основе многоразовых паролей и одноразовых паролей
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309

Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Для чего нужна база данных (Б.Д.), что в ней хранится.
2.Описать процедуру простой аутентификации многоразового пароля, пользователя в сети.
3.Однонапрвленность хеш-функции, недостатки и преимущества.
4.По каким формам представления объектов, аутентифицируется пользователь, чем может являться внешним объектом?
5.Какиее параметры использует схема аутентификации одноразового пароля?
6.Процес аутентификации одноразового пароля.
7.Различия, недостатки и достоинства между одноразовыми и многоразовыми паролями.

Лабораторная работа №25: «Исследование средств шифрования данных.».
Цель: Изучение средств шифрования данных.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Назовите и охарактеризуйте методы шифрования.
2. Дать определение криптостойкость.

Лабораторная работа №26: «Исследование средств двухключевого шифрования данных.
Цель: Изучение средств двухключевого шифрования данных..
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Дать определение ассиметричному шифрованию данных.
2. Дать определение симметричному шифрованию данных.
3. Дать характерные особенности асимметричных криптосистем.
4. Преимущества ассиметричных криптосистем.

Лабораторная работа №27: «Исследование электронной цифровой подписи информации»
Цель: Изучение электронной цифровой подписи информаци .
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30

Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Дать определение ассиметричному шифрованию данных.
2. Дать определение симметричному шифрованию данных.
3. Дать характерные особенности асимметричных криптосистем.
4. Преимущества ассиметричных криптосистем.

Лабораторная работа №28: «Биометрическая аутентификация пользователя»
Цель: Изучение биометрической аутентификации пользователя.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Достоинства биометрических методов защиты.
2.Какими параметрами характеризуется эффективность биометрической аутентификационной системы?
3.Какие технологии аутентификации разработаны и используются к настоящему времени?
4. Где используются дактилоскопические системы аутентификации? Основные элементы дактилоскопической системы аутентификации.
5.Сканеры отпечатков пальцев, как происходит их регистрация и как можно их использовать?
6.Системы аутентификации по форме ладони, их использование и преимущества.
7. Системы аутентификации по лицу, их использование и преимущества.
8. Системы аутентификации по голосу, их преимущества и недостатки.

Лабораторная работа №29: «Аутентификация на основе PIN-кода»
Цель: Изучение аутентификации на основе PIN-кода.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Зачем нужен PIN-код в пластиковой карте?
2.Как происходит ввод PIN-кода?
3.Неалгоритмический способ проверки PIN-кода, как осуществляется?
4.Алгоритмический способ проверки PIN-кода, его преимущества.

Лабораторная работа №30: «Аутентификация на основе одноразовых и многоразовых паролей»

Цель: Изучение аутентификация на основе одноразовых и многоразовых паролей.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Для чего нужна база данных (Б.Д.), что в ней хранится.
2.Описать процедуру простой аутентификации многоразового пароля, пользователя в сети.
3.Однонапрвленность хеш-функции, недостатки и преимущества.
4.По каким формам представления объектов, аутентифицируется пользователь, чем может являться внешним объектом?
5.Какиее параметры использует схема аутентификации одноразового пароля?
6.Процес аутентификации одноразового пароля.
7.Различия, недостатки и достоинства между одноразовыми и многоразовыми паролями.

Лабораторная работа №31: «Исследование средств шифрования данных»
Цель: Изучение средств шифрования данных.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Перечислить какие методы криптографии вы знаете дать объяснение каждому методу.
2. Что собой представляет алгоритм.
3. Дать определение что такое криптография.
4. Что означает криптостойкость шифра.
5. Дать определение что такое шифратор и дешифратор.

Лабораторная работа №32: «Исследование средств двухключевого шифрования данных.»
Цель: Исследование средств двухключевого шифрования данных..
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Что значит комбинированные шифры.
2. Как работают двухключевые несимметричные криптосистемы.
3. Какие три основные функции используются в криптографии.
4. Дать подробный ответ что значит открытый и закрытый ключ.
5. Что собой представляет шифр.

Лабораторная работа №33: «Исследование электронной цифровой подписи информации»
Цель: Исследование электронной цифровой подписи информации
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Дать определение ассиметричному шифрованию данных.
2. Дать определение симметричному шифрованию данных.
3. Дать характерные особенности асимметричных криптосистем.
4. Преимущества ассиметричных криптосистем.

Лабораторная работа №34: «Исследование электронной цифровой подписи информации с использованием PGP»
Цель: Исследование электронной цифровой подписи информации с использованием PGP.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1Для чего нужен публичный ключ и как он выглядит?
2.Уязвимые места PGP, описание.
3.Перечислить некоторые рекомендации по защите пароля.

Лабораторная работа №35: «Схемы сетевой защиты на базе МЭ.»
Цель: Изучение схемы сетевой защиты на базе МЭ.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1Дать определение что значит межсетевой экран firewall или брандмауэр и как он работает.
2. Какие два важных аспекта используются при установки межсетевого экрана.
3. Какие два принципа используются в политике работы межсетевого экрана.
4. Дать определение что такое маршрутизатор.
5.Нарисовать схему с защищаемой закрытой сетью и не защищаемой открытой сетью.
6. Что значит распределительный межсетевой экран дать подробный ответ с определением.

Лабораторная работа №36: «Классификация сетей VPN.»

Цель: Изучение сетей VPN.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Что такое удаленный доступ?
2. Назовите виды удаленного доступа.
3. Перечислите протоколы удаленного доступа.
4. Для чего нужна аутентификация при удаленном доступе?
5. Что такое VPN?
6. Каким образом сети VPN обеспечивают безопасную передачу пакетов?
7. Назовите виды VPN-соединений.
8. По каким признакам классифицируют сети VPN?

Лабораторная работа №37: «Основные варианты архитектуры VPN»
Цель: Изучение архитектуры VPN»
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1 .Что служит фундаментом для построения защищённой сети?
2. Какие функции, обеспечивающие защиту информации, реализуются VPN-сетями?
3. В каких случаях защита информации с помощью технологии VPN окажется не эффективной?
4. Каковы сильные стороны защищённых сетей?
5. Каковы слабые стороны защищённых сетей?

Лабораторная работа №38: «Аутентификация, авторизация и администрирование действий пользователей»
Цель: Изучение аутентификации, авторизации и администрирования действий пользователей.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:
Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Дать полное определение аутентификации идентификации и авторизации.

2. Что значит комбинированные методы идентификации.
3. В чем заключается механизм идентификации и аутентификации.
4. Перечислите способы создания учетных записей пользователей на ПК
5. Какие существуют способы аутентификации пользователей?
6. В чем слабость парольной аутентификации?
7. Как может быть повышена надежность аутентификации с помощью паролей?
8. Какой может быть реакция системы на попытку подбора паролей?

Лабораторная работа №39: «Типовая корпоративная сеть**».**

Цель: Изучить типовую корпоративную сеть.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1.Дать определение корпоративной сети.
2. Какие вы знаете корпоративные сети?
3. Способы защиты корпоративных сетей от несанкционированного доступа?
4. Что значит Инранет.
5. Что значит технология «клиент-сервер» и как она работает.
6. Перечислите технические средства для создания корпоративной сети?
7. Какие топологии используются в корпоративной сети?

Лабораторная работа №40: «Виртуальная частная сеть VPN на основе криптошлюза**».**

Цель: Изучение виртуальной частной сети VPN на основе криптошлюза .
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:
1. Какие технологии и принципы работы виртуальной частной сети используются?
2. Перечислить типы соединений VPN ?
3. Классификация VPN?
4. Преимущества использования VPN-соединения?
5. Как защитить VPN?

Лабораторная работа №41: «Установление и настраивание антивирусной программы

Цель: Установление и настраивание антивирусной программы.
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30

Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Чем платный антивирус отличается от бесплатного?
2. Какой функционал есть у комплексного антивируса помимо антивирусного сканера (какие
3. ещё имеются механизмы защиты)?
4. Чем необходимо руководствоваться при выборе антивируса?
5. Какой антивирус для работы в «опасной среде» вы бы посоветовали использовать? Выбор объясните.
6. Для чего в антивирусе отчёты?
7. Как антивирус может обнаружить вредоносное ПО, которого нет в антивирусных базах?

Лабораторная работа №42: «Установление и настраивание безопасности с помощью маршрутизатора»

Цель: Установление и настраивание безопасности с помощью маршрутизатора
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Выполнить практическое занятие провести настройку маршрутизатора
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Описать принцип работы маршрутизатора?

Лабораторная работа №43: «Аудит и мониторинг безопасности»

Цель: Аудит и мониторинг безопасности
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение аудит и мониторинг безопасности- это?
2. Основные направления аудита безопасности?
3. Виды и цели аудита?
4. Основные этапы аудита безопасности?

Лабораторная работа №44: «Локальная политика безопасности»

Цель: Изучить локальную политику безопасности
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение что значит политика безопасности?
2. Для чего используется локальная политика безопасности?
3. Чем можно управлять с помощью локальной политики безопасности ?

Лабораторная работа №45: «Глобальная политика безопасности»

Цель: Изучить глобальную политику безопасности
Оборудование: Персональный компьютер
Место проведения: Технический колледж кабинет №309
Время: 8:30
Учебные вопросы:

Порядок выполнения работ:
Изучить теоретическую часть и ответить на вопросы.
Отчет о проделанной работе:
Составить отчет в письменном виде.
Контрольные вопросы:

1. Дать определение что такое глобальная политика безопасности?
2. Чем отличаются глобальная политика от локальной политики и могут ли они работать совместно?

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н АШУРАЛИЕВА».

УТВЕРЖДАЮ

Заместитель директора по УР

_____ Ф.РАхмедова
Подпись ФИО

«____» _____2021г

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.

По специальности 11.02.11 Сети связи и системы коммутации

Разработчик:

Багаутдинова З.М

Рассмотрено на заседании предметной (цикловой) комиссии УГС 11.00.00. Электроника, радиотехника и системы связи специальности 11.02.11 Сети связи и системы коммутации

Протокол № 1 от 3 сентября 2021г

Председатель П(Ц)К З.Н.Мирзаев _____
ФИО подпись

Махачкала 2021г.

Методические указания по выполнению самостоятельной работы студентами

Успешность освоения дисциплины во многом зависит от планирования и организации самостоятельной работы слушателя.

Изучать новый материал и закреплять ранее пройденный, можно применяя разнообразные технологии. Целесообразно исполнить следующие рекомендации:

- изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере;

- Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.

- ознакомление с нормативными документами по ИБ;

- изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности;

- составление доклада по перспективным направлениям развития средств комплексной защиты информации;

- разработка пакета документации по инженерно-технической защите информации на объекте;

- изучение возможностей инженерно-технических средств защиты информации;

- изучение технических характеристик инженерно-технических средств защиты информации;

- разработка предложений по инженерно-технической защите информации на определенном объекте;

- Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.

Наиболее эффективно изучать учебный материал в традиционном повествовательном изложении материала в учебниках и учебных пособиях, решая одновременно приведенные учебные задания.

Как правило, студентов знакомят со структурой и содержанием дисциплины, раскрывают последовательность и внутреннюю логику курса еще на вводных занятиях. Это дает возможность заблаговременно изучить необходимый материал, подготовиться к практическим занятиям.

Самостоятельно приобретать знания о специальности можно, используя разнообразные источники информации:

1. **Мельников, В.П.** Информационная безопасность: учебное пособие для студентов образовательных учреждений среднего профессионального образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 7-е изд., стер. - Москва : Академия, 2013. - 331,с. : ил., табл.; - (Среднее профессиональное образование. Информатика и вычислительная техника).; ISBN 978-5-7695-9954-5

2. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с. — ISBN 978-5-8041-0378-2.

3. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.

Научно-технические и реферативные журналы:

1. Электросвязь
2. Вестник связи
3. Сети и системы связи
4. Мобильные системы
5. Цифровая обработка сигналов
6. Сводный реферативный журнал "Связь".

Интернет ресурсы:

Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний,

WWW.twirpx.com, WWW.referent.ru, WWW.kodeks-luks.ru/dws, WWW.Consultant.ru/online.

Учебно-методическое и информационное обеспечение дисциплины «Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи».

Тема: **Основные понятия в области информационной безопасности**

Еще совсем недавно пользователи компьютеров имели туманное *представление* о том, что при выходе в *Интернет* или любую другую общедоступную *сеть* компьютеры могут "заразиться" вирусами, а *информация* в течение очень короткого времени может быть украдена или искажена. Сегодня же практически каждый *пользователь* Интернета (да и не только Интернета, но и любой компьютерной сети) знает об опасности, подстерегающей его *компьютер* и о том, что необходимо защищать информацию от воздействия на нее потенциальных атак и вирусов.

Современный IT-рынок предлагает различные варианты обеспечения безопасности пользовательских устройств и компьютерных сетей в целом. *Конечные* пользовательские устройства, как правило, довольно успешно защищаются антивирусными программами и программными межсетевыми экранами (брандмауэры, *файрволы*). *Компьютерные сети* в комплексе защитить сложнее. Одним программным обеспечением здесь не обойтись. Решением вопроса обеспечения безопасности компьютерных сетей является установка межсетевых экранов в программно-аппаратном исполнении на границе сетей.

В основные задачи межсетевых экранов входит защита компьютеров от вторжения злоумышленников из внешней сети и последствий такого вторжения – утечки/изменения информации. Устанавливая *межсетевой экран* с требуемой конфигурацией на границу с внешней сетью, можно быть уверенным в том, что Ваш *компьютер* будет "невидим" извне (если только политикой администрирования не предусмотрен *доступ* к нему). Современные межсетевые экраны работают по принципу "запрещено все, что не разрешено", то есть Вы сами решаете для какого протокола или программы разрешить *доступ* во внутреннюю *сеть*.

Помимо функций сетевой защиты, *межсетевой экран* обеспечивает возможность нормального функционирования сетевых приложений.

Безусловно, *межсетевой экран* – это не панацея от всех бед компьютерного мира. Всегда необходимо принимать во внимание "*человеческий фактор*", так как именно человек неосознанно (а порой и целенаправленно) может нанести вред информационной системе, выполнив действия, нарушающие политику безопасности. Это может быть утечка информации через подключение внешних носителей, установление дополнительного незащищенного *Интернет*-подключения, умышленное изменение информации санкционированным пользователем и т.п.

В данной книге предлагаются к рассмотрению условия и предпосылки возникновения угроз при хранении информации и передаче ее по сетям и системам связи, методы предупреждения угроз, защиты

и обеспечения безопасности информации в целом, а также технологии и методы, позволяющие обеспечивать работу и *безопасность* сетей, на примере межсетевых экранов и *Интернет*-маршрутизаторов D-Link.

Обозначения, используемые в курсе

В курсе используются следующие пиктограммы для обозначения сетевых устройств и соединений:

Термины и определения в области информационной безопасности

Прежде всего, необходимо определиться с основными понятиями и терминами, относящимися к информационной безопасности.

В широком смысле ***информационная система*** есть совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать пользователей системы нужной информацией.

Информационная безопасность – защита конфиденциальности, целостности и доступности информации.

- ***Конфиденциальность***: доступ к информационным ресурсам только авторизованным пользователям.
- ***Целостность***: неизменность информации в процессе ее передачи или хранения.
- ***Доступность***: свойство информационных ресурсов, определяющее возможность получения и использования информационных данных авторизованными пользователями в каждый момент времени.

Безопасность информации – состояние защищенности хранимой информации от негативных воздействий.

Сетевая безопасность – это набор требований, предъявляемых к инфраструктуре компьютерной сети предприятия и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа.

Под сетевой безопасностью принято понимать защиту информационной инфраструктуры объекта (при помощи аутентификации, авторизации, межсетевых экранов, систем обнаружения вторжений IDS/IPS и других методов) от вторжений злоумышленников извне, а также защиту от случайных ошибок (с применением технологий *DLP*) или намеренных действий персонала, имеющего *доступ* к информации внутри самого предприятия. *DLP* (*Data Leak Prevention*) – это современные технологии защиты конфиденциальной информации от возможных утечек из информационной системы с применением программных или программно-аппаратных средств. Каналы утечки могут быть сетевые (например, электронная *почта*) либо локальные (с использованием внешних накопителей).

Аутентификация (*Authentication*) – процедура проверки идентификационных данных пользователя (чаще всего, логина и пароля) при доступе к информационной системе.

Авторизация (*Authorization*) – предоставление определенному пользователю прав на выполнение некоторых действий. *Авторизация* происходит после аутентификации и использует *идентификатор* пользователя для определения того к каким ресурсам он имеет *доступ*. В информационных технологиях с помощью авторизации устанавливаются и реализуются *права* доступа к ресурсам и системам обработки данных.

Аутентичность в передаче и обработке данных – *целостность* информации, подлинность того, что данные были созданы законными участниками информационного процесса, и невозможность отказа от авторства.

Защита информации представляет собой *деятельность*, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных (случайных) воздействий на защищаемую информацию.

Возможные объекты воздействия в информационных системах:

- аппаратное обеспечение;
- программное обеспечение;
- коммуникации (обеспечение передачи и обработки данных через каналы связи и коммутационное оборудование);
- персонал.

Объектами воздействия с целью нарушения конфиденциальности, целостности или доступности информации могут быть не только элементы информационной системы, но и поддерживающей ее инфраструктуры, которая включает в себя сети инженерных коммуникаций (системы электро-, теплоснабжения, кондиционирования и др.). Кроме того, следует обращать внимание на территориальное *размещение* технических средств, которое следует размещать на охраняемой территории. Беспроводное оборудование рекомендуется устанавливать так, чтобы зона действия беспроводной сети не выходила за пределы контролируемой зоны.

Учитывая широкий спектр воздействия угроз, к защите информации необходим *комплексный подход*.

Контролируемая зона – это охраняемое *пространство* (территория, здание, *офис* и т.п.), в пределах которого располагается *коммуникационное оборудование* и все точки соединения локальных периферийных устройств информационной сети предприятия.

Правила разграничения доступа – совокупность правил, регламентирующих *права* доступа пользователей к ресурсам информационной системы.

Санкционированный доступ к информации не нарушает правил разграничения доступа.

Несанкционированный доступ (несанкционированные действия) – *доступ* к информации или действия с информацией, осуществляемые с нарушением установленных прав и/или правил разграничения доступа к информации.

Общая классификация угроз информационной безопасности

Угрозы безопасности информационных систем классифицируются по нескольким признакам (рис. 1.1).

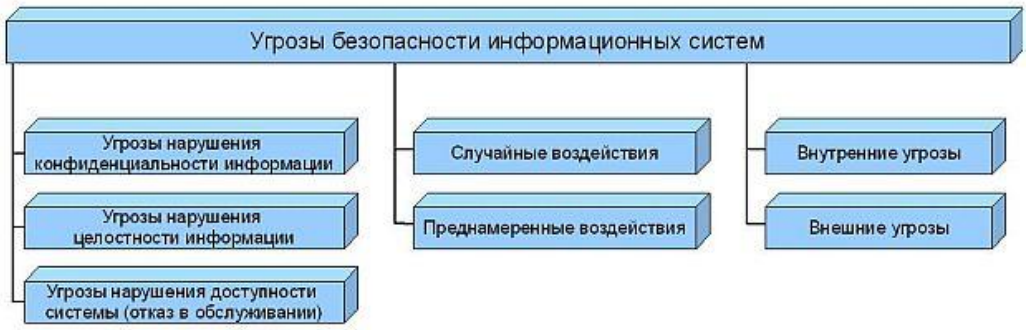


Рис. 1.1. Классификация угроз безопасности информационных систем

Угрозы нарушения конфиденциальности направлены на получение (хищение) конфиденциальной информации. При реализации этих угроз *информация* становится известной лицам, которые не должны иметь к ней *доступ*. Несанкционированный *доступ* к информации, хранящейся в информационной системе или передаваемой по каналам (сетям) передачи данных, *копирование* этой информации является нарушением конфиденциальности информации.

Угрозы нарушения целостности информации, хранящейся в информационной системе или передаваемой посредством *сети передачи данных*, направлены на изменение или искажение данных, приводящее к нарушению качества или полному уничтожению информации. *Целостность* информации может быть нарушена намеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему (помехи). Эта *угроза* особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется авторизованными пользователями с обоснованной целью.

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют *доступ* к некоторым её ресурсам.

Причины *случайных воздействий*:

- аварийные ситуации из-за стихийных бедствий и отключения электроэнергии;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).

Преднамеренные воздействия связаны с целенаправленными действиями злоумышленника, в качестве которого может выступить любое заинтересованное лицо (конкурент, посетитель, персонал и т.д.). Действия злоумышленника могут быть обусловлены разными мотивами: недовольством сотрудника

своей карьерой, материальным интересом, любопытством, конкуренцией, стремлением самоутвердиться любой ценой и т.п.

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения таких угроз может послужить нездоровый климат в коллективе или неудовлетворенность от выполняемой работы некоторых сотрудников, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Также имеет *место* так называемый "*человеческий фактор*", когда человек не умышленно, по ошибке, совершает действия, приводящие к разглашению конфиденциальной информации или к нарушению доступности информационной системы. Большую долю конфиденциальной информации *злоумышленник* (конкурент) может получить при несоблюдении работниками-пользователями компьютерных сетей элементарных правил защиты информации. Это может проявиться, например, в примитивности паролей или в том, что сложный *парольпользователь* хранит на бумажном носителе на видном месте или же записывает в текстовый *файл* на жестком диске и пр. Утечка конфиденциальной информации может происходить при использовании незащищенных каналов связи, например, по телефонному соединению.

Под *внешними угрозами* безопасности понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды, такие как:

- атаки из внешней сети (например, Интернет), направленные на искажение, уничтожение, хищение информации или приводящие к отказу в обслуживании информационных систем предприятия;
- распространение вредоносного программного обеспечения;
- нежелательные рассылки (спам);
- воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем;
- перехват информации с использованием радиоприемных устройств;
- воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций;
- воздействие на персонал предприятия с целью получения конфиденциальной информации.

В современном мире, когда стало возможным применять сервисы и службы с использованием информационной коммуникационной среды (электронные платежи, *Интернет*-магазины, электронные очереди и т.п.), многократно увеличивается риск именно внешних угроз.

Как правило, несанкционированный *доступ*, перехват, хищение информации, передаваемой по каналам связи, проводится средствами технической разведки, такими как радиоприемные устройства, средства съема акустической информации, системы перехвата сигналов с компьютерных сетей и контроля телекоммуникаций, средства съема информации с кабелей связи и другие.

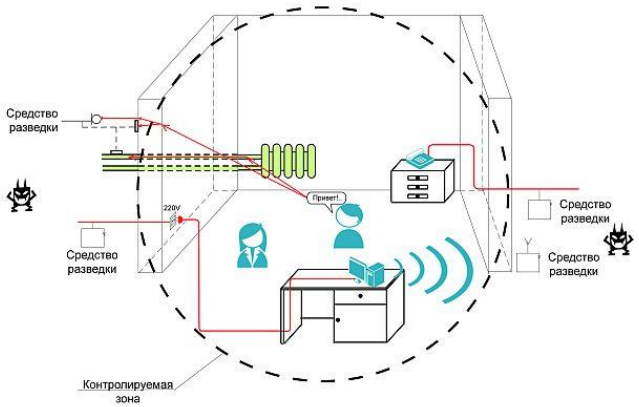


Рис. 1.2. Механизм возникновения каналов утечки информации за пределы контролируемой зоны

Контрольные вопросы

1. Что такое угроза с точки зрения ИБ?
2. Что такое атака?
3. Как можно классифицировать угрозы?
4. Какие формы утечки информации вам известны?
5. В чем выражаются угрозы информации?

Тема : Введение в сетевой информационный обмен.

Стремительное развитие ИТ привело к появлению и быстрому росту глобальной сети Internet. Развитие компьютерных сетей немыслимо без строгого соблюдения принципов стандартизации аппаратного и ПО. Днем рождения Интернета в современном понимании этого слова стала дата стандартизации в 1983 г. стека коммуникационных протоколов TCP/IP, лежащего в основе Всемирной сети Интернет. Интернет представляет собой совокупность соединенных между собой компьютерных сетей, в которых используются единые согласованные правила обмена данными между компьютерами.

Использование сети Интернет

Развитие глобальной сети Internet способствовало использованию для построения глобальных корпоративных связей более дешевого и более доступного (по сравнению с выделенными каналами) транспорта Internet. Сеть Internet предлагает разнообразные методы коммуникации и способы доступа к информации, поэтому для многих компаний она стала неотъемлемой частью их ИС.

Влияние Internet на корпоративные сети способствовало появлению нового понятия — intranet (интранет, интрасети), при котором способы доставки и обработки информации, присущие Internet, переносятся в корпоративную сеть.

Отметим основные возможности, предоставляемые сетью Internet для построения корпоративных сетей.

Дешевые и доступные коммуникационные каналы Internet. К началу XXI в. в связи с бурным развитием Internet и сетей коллективного доступа в мире произошел качественный скачок в распространении и доступности информации. Пользователи получили дешевые и доступные

коммуникационные каналы Internet. Стремясь к экономии средств, предприятия стали активно использовать эти каналы для передачи критичной коммерческой и управленческой информации.

Универсальность. Глобальная сеть Internet была создана для обеспечения обмена информацией между удаленными пользователями. Развитие Internet-технологий привело к возникновению популярной глобальной службы World Wide Web (WWW), что позволило пользователям работать с информацией в режиме прямого подключения. Эта технология подразумевает подключение пользователя к глобальной сети и использования WWW-браузе- ров для просмотра информации. Стандартизация интерфейсов обмена данными между утилитами просмотра информации и информационными серверами позволила организовать одинаковый интерфейс с пользователем для различных платформ.

Доступ к разнообразной информации и услугам в Internet. Кроме транспортных услуг по транзитной передаче данных для абонентов любых типов, сеть Интернет обеспечивает также достаточно широкий набор высокоуровневых Интернет-сервисов: всемирная паутина World Wide Web; сервис имен доменов DNS; доступ к файловым архивам FTP; электронная почта (e-mail); телеконференции (Usenet); сервисы общения ICQ, IRC; сервис Telnet; поиск информации в Интернете. Компьютеры, предоставляющие эти услуги, называются *серверами,* соответственно компьютеры, пользующиеся услугами, называются *клиентами.* Эти же термины относятся и к ПО, используемому на компьютерах-серверах и компьютерах-клиентах. Сеть Internet обеспечивает доступ к обширной и разнообразной информации с помощью огромного числа подключенных к ней хост-узлов. *Хост* — это компьютер или группа компьютеров, имеющих прямое сетевое соединение с Internet и предоставляющих пользователям доступ к своим средствам и службам. Многие из этих компьютеров выполняют роль серверов, предлагающих любому пользователю, имеющему выход в Internet, доступ к электронным ресурсам — данным, приложениям и услугам. Связав свои сети с внешними ресурсами, компании могут реализовать постоянные коммуникации и организовать эффективный поток информации между людьми. Соединение внутренних сетей с внешними организациями и ресурсами позволяет компаниям воспользоваться преимуществами этих сетей — снижением затрат и повышением эффективности.

Простота использования. При использовании Интернет-технологий не требуется специального обучения персонала.

Для объединения локальных сетей в глобальные используются специализированные компьютеры (маршрутизаторы и шлюзы), с помощью которых локальные сети подключаются к межсетевым каналам связи. Маршрутизаторы и шлюзы физически соединяют локальные сети друг с другом и, используя специальное ПО, передают данные из одной сети в другую. Глобальные сети имеют сложную разветвленную структуру и избыточные связи. Маршрутизаторы и шлюзы обеспечивают поиск оптимального маршрута при передаче данных в глобальных сетях, благодаря чему достигается максимальная скорость потока сообщений. Высокоскоростные каналы связи между локальными се-тями могут быть реализованы на основе волоконно-оптических кабелей или с помощью спутниковой связи. В качестве медленных межсетевых каналов связи используются различные виды телефонных линий.

Построение корпоративных компьютерных сетей с применением технологии интрасетей означает прежде всего использование стека TCP/IP для транспортировки данных и технологии Web для их представления.

Модель ISO/OSI и стек протоколов TCP/IP

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

Модель OSI определяет различные уровни взаимодействия систем и указывает, какие функции должен выполнять каждый уровень. В модели OSI средства взаимодействия делятся на семь уровней: прикладной (Application), представительный (Presentation), сеансовый (Session), транспортный (Transport), сетевой (Network), канальный (Data Link) и физический (Physical). Самый верхний уровень — прикладной. На этом уровне пользователь взаимодействует с приложениями. Самый нижний уровень — физический. Этот уровень обеспечивает обмен сигналами между устройствами.

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

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

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком коммуникационных протоколов.* Следует четко различать модель ISO/OSI и стек протоколов ISO/OSI. *Модель ISO/OSI*является концептуальной схемой взаимодействия открытых систем, а *стек протоколов ISO/OSI* представляет собой набор вполне конкретных спецификаций протоколов для семи уровней взаимодействия, которые определены в модели ISO/OSI.

Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней — как правило, чисто программными средствами.

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле сети, должны взаимодействовать друг с другом также в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть *межуровневым интерфейсом.* Межуровневый интерфейс определяет набор сервисов, предоставляемых данным уровнем соседнему уровню. В сущности, протокол и интерфейс являются близкими понятиями, но традиционно в сетях за ними закреплены разные области действия: *протоколы* определяют правила взаимодействия модулей одного уровня в разных узлах сети, а *интерфейсы* определяют правила взаимодействия модулей соседних уровней в одном узле.

Стек протоколов TCP/IP (Transmission Control Protocol/ Internet Protocol) является промышленным стандартом стека коммуникационных протоколов, разработанным для глобальных сетей. Стандарты TCP/IP опубликованы в серии документов, названных Request for Comment (RFC). Документы RFC

описывают внутреннюю работу сети Internet. Некоторые RFC описывают сетевые сервисы или протоколы и их реализацию, в то время как другие обобщают условия применения.

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

Большой вклад в развитие стека TCP/IP внес Калифорнийский университет в Беркли (США), который реализовал протоколы стека в своей версии ОС UNIX, сделав как сами программы, так и их исходные тексты бесплатными и общедоступными. Популярность этой ОС привела к широкому распространению протоколов IP, TCP и других протоколов стека. Сегодня этот стек используется для связи компьютеров всемирной информационной сети Internet, а также в огромном числе корпоративных сетей. Стек TCP/IP является самым распространенным средством организации составных компьютерных сетей.

Широкое распространение стека TCP/IP объясняется следующим:

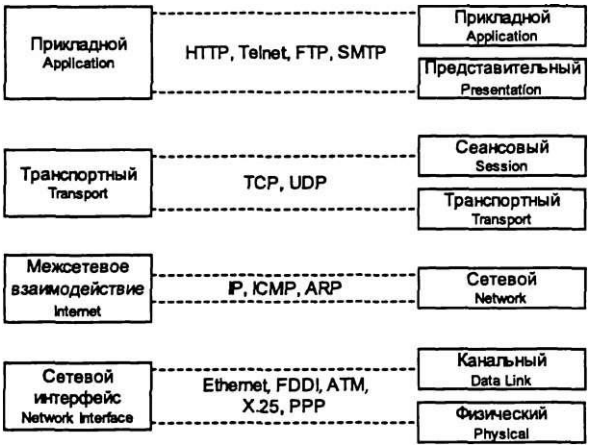
- это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю;
- почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP;
- все современные ОС поддерживают стек TCP/IP.

Кроме того, это:

- метод получения доступа к сети Internet;
- гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов;
- основа для создания intranet — корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet;
- устойчивая масштабируемая межплатформенная среда для приложений клиент—сервер [46].

Структура и функциональность стека протоколов TCP/IP

Стек TCP/IP был разработан до появления модели взаимодействия открытых систем OSI и также имеет многоуровневую структуру. Структура протоколов TCP/IP приведена на рис. 2.1. Стек протоколов TCP/IP имеет четыре уровня — прикладной (Application), транспортный (Transport), уровень межсетевого взаимодействия (Internet) и уровень сетевых интерфейсов



Уровни стека Уровни модеш

TCP/P OSI

Рис. 2.1. Уровни стека протоколов TCP/IP

(Network). Для сравнения на рис. 2.1 показаны также семь уровней модели OSI. Следует отметить, что соответствие уровней стека TCP/IP уровням модели OSI достаточно условно.

Прикладной уровень (Application) включает большое число прикладных протоколов и сервисов. К ним относятся такие популярные протоколы, как протокол копирования файлов FTP, протокол эмуляции терминала Telnet, почтовый протокол SMPT, используемый в электронной почте сети Internet, гипертекстовые сервисы доступа к удаленной информации, такие как WWW, и многие другие. Рассмотрим подробнее некоторые из этих протоколов [46].

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Для того чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений — TCP. Кроме пересылки файлов, протокол FTP предлагает и другие услуги. Например, пользователю предоставляется возможность интерактивной работы с удаленной машиной, в частности, он может распечатать содержимое ее каталогов. Наконец, FTP выполняет аутентификацию пользователей. Прежде чем получить доступ к файлу, в соответствии с протоколом пользователи должны сообщить свое имя и пароль. Для доступа к публичным каталогам FTP-архивов

Internet не требуется парольная аутентификация, и ее можно обойти путем использования для такого доступа предопределенного имени пользователя Anonymous.

Протокол Telnet обеспечивает передачу потока байтов между процессами, а также между процессом и терминалом. Наиболее часто этот протокол используется для эмуляции терминала удаленного компьютера. При использовании сервиса Telnet пользователь фактически управляет удаленным компьютером так же, как и локальный пользователь, поэтому такой вид доступа требует хорошей защиты. Серверы Telnet всегда используют, как минимум, аутентификацию по паролю, а иногда и более мощные средства защиты, например систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) используется для организации сетевого управления. Сначала протокол SNMP был разработан для удаленного контроля и управления маршрутизаторами Internet. С ростом популярности протокол SNMP стали применять для управления разным коммуникационным оборудованием — концентраторами, мостами, сетевыми адаптерами и др.

В стандарте SNMP определена спецификация информационной базы данных управления сетью. Эта спецификация, известная как база данных MIB (Management Information Base), определяет те элементы данных, которые управляемое устройство должно сохранять, и допустимые операции над ними.

На **транспортном уровне** (Transport) стека TCP/IP, называемом также основным уровнем, функционируют протокол TCP и протокол UDP.

Протокол управления передачей TCP (Transport Control Protocol) решает задачу обеспечения надежной информационной связи между двумя конечными узлами. Этот протокол называют протоколом «с установлением соединения». Это означает, что два узла, связывающиеся при помощи этого протокола, «договариваются» о том, что они будут обмениваться потоком данных и принимают некоторые соглашения об управлении этим потоком. Согласно протоколу TCP, отправляемые данные «нарезаются» на небольшие стандартные пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем были данные для правильной сборки документа на компьютере получателя.

Протокол дейтаграмм пользователя UDP (User Datagram Protocol) обеспечивает передачу прикладных пакетов дейта- граммным способом, т. е. каждый блок передаваемой информации (пакет) обрабатывается и распространяется от узла к узлу

3 - 3348 как независимая единица информации — дейтаграмма. При этом протокол UDP выполняет только функции связующего звена между сетевым протоколом и многочисленными прикладными процессами. Необходимость в протоколе UDP обусловлена тем, что UDP «умеет» различать приложения и доставляет информацию от приложения к приложению.

Уровень межсетевого взаимодействия (Internet) реализует концепцию коммутации пакетов без установления соединений. Основным протоколом этого уровня является *адресный протокол IP*. Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого числа локальных сетей, объединенных как локальными, так и глобальными связями.

Суть протокола IP состоит в том, что у каждого пользователя Всемирной сети Internet должен быть свой уникальный адрес (IP-адрес). Без этого нельзя говорить о точной доставке TCP-па- кетов в нужное рабочее место. Этот адрес выражается очень просто — четырьмя байтами, например: 185.47.39.14. Структура IP-адреса организована таким образом, что каждый компьютер, через который проходит какой-либо TCP-пакет, может по этим четырем числам определить, кому из ближайших «соседей» надо переслать пакет, чтобы он оказался «ближе» к получателю. В результате конечного числа перебросок TCP-пакет достигает адресата. В данном случае оценивается не географическая «близость». В расчет принимаются условия связи и пропускная способность линии. Два компьютера, находящиеся на разных континентах, но связанные высокопроизводительной линией космической связи, считаются более близкими друг другу, чем два компьютера из соседних городов, связанных обычной телефонной связью. Решением вопросов, что считать «ближе», а что «дальше» занимаются специальные средства — маршрутизаторы. Роль маршрутизатора в сети может выполнять как специализированный компьютер, так и специализированная программа, работающая на узловом сервере сети.

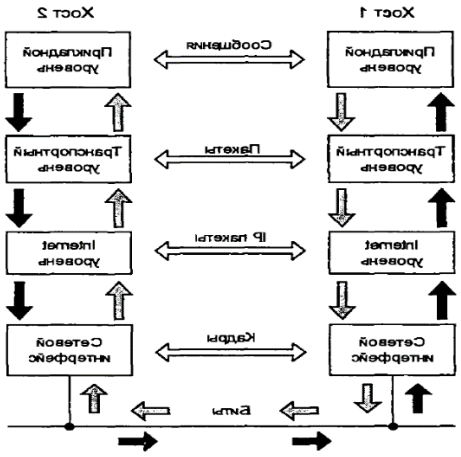
К уровню межсетевого взаимодействия относятся и протоколы, связанные с составлением и модификацией таблиц маршрутизации, такие как *протоколы сбора маршрутной информации RIP* (Routing Internet Protocol) и *OSPF* (Open Shortest Path First), а также *протокол межсетевых управляющих сообщений ICMP* (Internet Control Message Protocol). Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом — источником пакета.

Уровень сетевого интерфейса (Network) соответствует физическому и канальному уровням модели OSI. Этот уровень в протоколах TCP/IP не регламентируется, но поддерживает все популярные стандарты физического и канального уровня: для локальных сетей это Ethernet, Token Ring, FDDI, Fast Ethernet, для глобальных сетей — протоколы соединений «точка—точка» SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, frame relay. Разработана спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня. Разделенные на уровни протоколы стека TCP/IP спроектированы таким образом, что конкретный уровень хоста назначения получает именно тот объект, который был отправлен эквивалентным уровнем хоста источника. Каждый уровень стека одного хоста образует логическое соединение с одноименным уровнем стека другого хоста. При реализации физического соединения уровень передает свои данные интерфейсу уровня, расположенного выше или ниже в том же хосте (рис. 2.2). Вертикальные стрелки показывают физическое соединение в рамках одного хоста, а горизонтальные стрелки показывают логическое соединение между одноименными уровнями в различных хостах.

Следует обратить внимание на терминологию, традиционно используемую для обозначения информационных объектов, распространяющихся на интерфейсах между различными уровнями управления стека протоколов TCP/IP.

Приложение передает транспортному уровню сообщение (message), которое имеет соответствующее данному приложению размер и семантику. Транспортный уровень «разрезает» это сообщение (если оно достаточно велико) на пакеты (packets), которые передаются уровню межсетевого взаимодействия (т. е. протоколу IP). Протокол IP формирует свои IP-пакеты (еще говорят — IP-дейтаграммы) и затем упаковывает их в формат, приемлемый для данной физической среды передачи информации. Эти, уже аппаратно-зависимые, пакеты обычно называют кадрами (frame).

Когда данные передаются от прикладного уровня к транспортному уровню, затем уровню межсетевого взаимодействия и далее через уровень сетевого интерфейса в сеть, каждый протокол выполняет соответствующую обработку и инкапсулирует



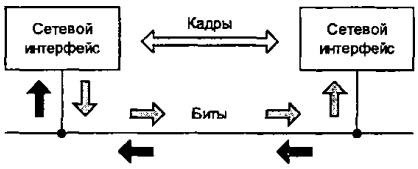


Рис. 2.2. Логические и физические соединения между уровнями стека TCP/IP

В системе, принимающей данный поток информации, эти заголовки последовательно удаляются по мере обработки данных и передачи их вверх по стеку. Такой подход обеспечивает необходимую гибкость в обработке передаваемых данных, поскольку верхним уровням вовсе не нужно касаться технологии, используемой в нижних уровнях. Например, если шифруются данные на уровне IP, уровень TCP и прикладной уровень остаются неизменными.

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

Тема 5: Проблемы безопасности IP-сетей.

Рост популярности Интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. В ближайшем будущем их число во много раз возрастет, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно возрастает.

На практике IP-сети уязвимы для многих способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется.

Наиболее распространены следующие атаки.

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

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

Изменение данных. Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг — изменить их. Данные в пакете могут быть изменены, даже если злоумышленник ничего не знает ни об отправителе, ни о получателе. Даже если вы не нуждаетесь в строгой конфиденциальности всех передаваемых данных, то наверняка не захотите, чтобы они были изменены по пути.

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

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

После получения доступа к сети атакующий злоумышленник может:

посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию

наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в результате перегрузки;

блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

Отказ в обслуживании (Denial of Service, DoS). Эта атака отличается от атак других типов: она не нацелена на получение доступа к сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, ОС или приложения. По существу, она лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Парольные атаки. Их цель — завладение паролем и логином законного пользователя.

Злоумышленники могут проводить парольные атаки, используя такие методы, как:

подмена IP-адреса (1P-спуфинг);

подслушивание (сниффинг);

простой перебор.

Часто хакеры пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой метод носит название атака полного перебора (brute force attack). Для этой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего

пользования (например, к серверу). Если в результате злоумышленнику удается подобрать пароль, он получает доступ к ресурсам на правах обычного пользователя.

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

При использовании обычных паролей необходимо придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее 8 символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, $, &, % и т. д.).

Угадывание ключа. Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа не просто и требует больших затрат ресурсов, тем не менее это возможно. В частности, для определения значения ключа может быть использована специальная программа, реализующая метод полного перебора. Ключ, к которому получает доступ атакующий, называется скомпрометированным. Атакующий использует скомпрометированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает возможность расшифровывать и изменять данные.

Атаки на уровне приложений могут проводиться несколькими способами.

Самый распространенный из них состоит в использовании известных слабостей серверного ПО (FTP, HTTP, web-сереера).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран. Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Невозможно полностью исключить атаки на уровне приложений. Хакеры постоянно открывают и публикуют на своих сайтах в Интернете все новые уязвимые места прикладных программ. 1

Здесь важно осуществлять хорошее системное администрирование.

Вопросы обеспечения безопасности IP сетей удобно рассматривать, выделив несколько уровней: Уровень персонала, Уровень приложений, Уровень СУБД, Уровень ОС, Уровень сети

К уровню сети относятся используемые сетевые протоколы (TCP/ I P, NetBEUI , IPX / SPX), каждый из которых имеет свои особенности, уязвимости и связанные с ними возможные атаки. К уровню операционных систем (ОС) относятся установленные на узлах корпоративной сети операционные системы (Windows , UNIX и т. д.). Следует также выделить уровень систем управления базами данных (СУБД). На четвертом уровне находятся всевозможные приложения, используемые в корпоративной сети. Это может быть программное обеспечение Web -серверов, различные офисные приложения, броузеры и т.п. И, наконец, на верхнем уровне находятся пользователи и

обслуживающий персонал автоматизированной системы, которому присущи свои уязвимости с точки зрения безопасности.

Можно выделить несколько общих этапов проведения атаки на IP сеть: Сбор сведений, Попытка получения доступа к наименее защищённому узлу (возможно, с минимальными привилегиями), Попытка повышения уровня привилегий или (и) использование узла в качестве платформы для исследования других узлов сети, Получение полного контроля над одним из узлов или несколькими.

Для обеспечения безопасности необходимо правильное использование протокола IPSec - это протокол транспортного уровня передачи данных, созданный для обеспечения безопасного соединения компьютеров по протоколу IP. Так как сам по себе протокол IP не имеет никаких механизмов безопасности, то при его использовании можно перехватывать IP-пакеты с последующим их анализом, уничтожением, изменением или фальсификацией. С целью предотвращения ситуаций подобного рода сообществом Internet Engineering Task Force (IETF) и был создан протокол IPSec.

IPSec устанавливает четыре основных признака безопасного соединения по IP и надежной передачи данных: конфиденциальность данных (Confidentiality), их целостность (Integrity), идентификацию другой стороны и данных (Authentification) и фиксацию авторства (от данных нельзя отказаться - Non-Repudiation).

Тема 6: Актуальность проблемы обеспечения безопасности информационных технологий.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

• обострением противоречий между объективно существующими потребностями общества *в* расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование

• расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи

• повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности

• вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса

• концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях

• количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам

• отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем

• многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации

• ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации

• увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов)

• развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин.

Прежде всего - это *расширение сферы применения средств вычислительной техники и возросший уровень доверия к автоматизированным системам* управления и обработки информации. Компьютерным системам доверяют самую ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, управляют движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию.

Изменился подход и к самому понятию "информация". Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в рамках которой он существует. Осуществляется переход к рыночным отношениям в области создания и предоставления информационных услуг, с присущей этим отношениям *конкуренцией и промышленным шпионажем.*

Проблема защиты вычислительных систем становится еще более серьезной и в связи с *развитием и распространением вычислительных сетей, территориально распределенных систем* и систем с удаленным доступом к совместно используемым ресурсам.

Доступность средств вычислительной техники и прежде всего персональных ЭВМ привела к *распространению компьютерной грамотности* в широких слоях населения, что закономерно, привело к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих автоматизированных систем как со злым умыслом, так и чисто "из спортивного интереса". К сожалению, многие из этих попыток имеют успех и наносят значительный урон всем заинтересованным субъектам информационных отношений.

Отставание в области создания стройной и непротиворечивой *системы законодательно-правового регулирования отношений* в сфере накопления, использования и защиты информации создает условия для возникновения и широкого распространения "компьютерного хулиганства" и "компьютерной преступности".

Еще одним весомым аргументом в пользу усиления внимания к вопросам безопасности вычислительных систем является *бурное развитие и широкое распространение так называемых*

компьютерных вирусов, способных скрытно существовать в системе и совершать потенциально любые несанкционированные действия.

Особую опасность для компьютерных систем представляют *злоумышленники, специалисты - профессионалы в области вычислительной техники и программирования,* досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией и самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты.

Трудности решения практических задач обеспечения безопасности конкретных АС связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Тема 7: Место и роль информационных систем в управлении бизнес-процессами.

Цели и задачи информационных систем

Предприятие - это единый организм, и улучшение чего-либо одного может привести к малейшему сдвигу в сторону успеха в лучшем случае, либо к снижению общих показателей в худшем. Руководителям, а в особенности руководителям финансовых отделов, необходимо принимать комплексные решения, касающиеся всего предприятия. А загруженность решением оперативных задач еще более усложняет процесс управления.

Для упрощения управления предприятием, прежде всего финансового, необходимо иметь эффективную информационную систему, включающую функции планирования, управления и анализа. Что может дать внедрение информационной системы:

· снижение общих затрат предприятия в цепи поставок (при закупках),

· повышение скорости товарооборота,

· сокращение излишков товарных запасов до минимума,

· увеличение и усложнение ассортимента продукции,

· улучшение качества продукции,

· выполнение заказов в срок и повышение общего качества обслуживания заказчиков.

КИС выполняет технологические функции по накоплению, хранению, передаче и обработке информации. Она складывается, формируется и функционирует в регламенте, определенном методами и структурой управленческой деятельности, принятой на конкретном экономическом объекте, реализует цели и задачи, стоящие перед ним.

Основными целями автоматизации деятельности предприятия являются:

· Сбор, обработка, анализ, хранение и представление данных о деятельности организации и внешней среде в виде, удобном для принятия управленческих решений;

· Автоматизация выполнения бизнес операций (технологических операций), составляющих целевую деятельность предприятия;

· Автоматизация процессов, обеспечивающих выполнение основной деятельности.

Тема 1: 1**2**34 || Тема 2 >

Вредоносное программное обеспечение

Вредоносное программное обеспечение и, прежде всего, компьютерные вирусы представляют очень серьезную опасность для информационных систем. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. В то же время чрезмерное преувеличение угрозы вирусов негативно влияет на использование всех возможностей компьютерной сети. Знание механизмов действия вредоносного программного обеспечения (ПО), методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и нанесения вреда машинам и информации.

О наличии вредоносного ПО в системе пользователь может судить по следующим признакам:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении, "самопроизвольное" отключение антивирусных программных средств;
- явные проявления присутствия вируса, такие как: сообщения, выдаваемые на монитор или принтер, звуковые эффекты, неожиданный запуск программ, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в системе;
- неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств компьютерной системы – увеличение времени обработки той или иной информации (т.н. "задумчивость" ПК), необоснованное уменьшение свободного объёма на дисковых носителях, отказ выполнять программы-сканеры вирусной активности, "зависания" системы и т.п.;
- рассылка писем, которые пользователем не отправлялись, по электронной почте.

Вредоносная программа (Malware, malicious software – злонамеренное программное обеспечение) – это любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа.

Во многом "вредность" или "полезность" программного обеспечения определяется самим пользователем или способом его применения. Общепризнанной классификации вредоносного ПО пока не существует. Первые попытки упорядочить процесс классификации были предприняты еще в начале 90-х годов прошлого века в рамках альянса антивирусных специалистов CARO (Computer AntiVirus Researcher's Organization). Альянсом был создан документ "CARO malware naming scheme", который на какой-то период стал стандартом для индустрии.

Но со временем стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться. Ещё более важной причиной отказа от неё стало то, что технологии детектирования систем антивирусных компаний отличаются друг от друга и, как следствие, невозможно унифицировать результаты проверки разными антивирусными программами. Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов. Последним значительным проектом подобного рода было создание стандарта CME

(Common Malware Enumeration), суть которого заключается в присвоении одинаковым детектируемым объектам единого уникального идентификатора.

Рассмотрим классификацию, предложенную компанией "Лаборатория Касперского" и размещенную в Вирусной энциклопедии Лаборатории Касперского. Специалисты этой компании предлагают разделять вредоносное ПО на вредоносные программы (Malware) и потенциально нежелательные программы (PUPs, Potentially Unwanted Programs). В свою очередь, вредоносные программы включают следующие категории: *компьютерные вирусы и черви; троянские программы; подозрительные упаковщики и вредоносные утилиты.*

Компьютерные вирусы и черви

Термином "компьютерный вирус" сегодня уже никого не удивишь. Данное определение появилось (в середине 80-х годов) благодаря тому, что вредительские программы обладают признаками, присущими биологическим вирусам – незаметное и быстрое распространение, размножение, внедрение в объекты и заражение их, и, кроме того, негативное воздействие на систему. Вместе с термином "вирус" при работе в информационных системах используются и другие термины: "заражение", "среда обитания", "профилактика" и др.

Компьютерные вирусы – это небольшие исполняемые или интерпретируемые программы, обладающие свойством несанкционированного пользователем распространения и самовоспроизведения в компьютерах или компьютерных сетях. Полученные копии также обладают этой возможностью. Вирус может быть запрограммирован на изменение или уничтожение программного обеспечения или данных, хранящихся на объектах и устройствах компьютерной сети. В процессе распространения вирусы могут себя модифицировать.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры. Червь – это отдельный файл, в то время как вирус – это код, который внедряется в существующие файлы.

К категории вредоносных программ "компьютерные вирусы и черви" относятся:

- ***Virus*** (вирус) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для своего распространения и проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если заражённый объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

  - при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
  - вирус скопировал себя на съёмный носитель или заразил файлы на нем;
  - пользователь отослал электронное письмо с зараженным вложением.

- ***Worm*** (червь) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях через сетевые ресурсы. Для активации Worm пользователю необходимо запустить его (в отличие от Net-Worm).

Черви этого типа ищут в сети удаленные компьютеры и копируют себя в каталоги, открытые на чтение и запись (если таковые обнаружены). При этом черви данного типа перебирают доступные сетевые каталоги, используя функции операционной системы, и случайным образом ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ. Также к данному типу червей относятся черви, которые по тем или иным причинам не обладают ни одним из других поведений (например, "мобильные" черви).

- ***Net-Worm*** (сетевой червь) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения (т.е. непосредственно для активации вредоносной программы).

Зачастую при распространении такой червь ищет в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально сформированный сетевой пакет (эксплойт), в результате чего код (или часть кода) червя проникает на компьютер-жертву и активируется. Если сетевой пакет содержит только часть кода червя, то после проникновения в уязвимый компьютер он скачивает основной файл червя и запускает его на исполнение. Можно встретить сетевых червей данного типа, использующих сразу несколько эксплойтов для своего распространения, что увеличивает скорость нахождения ими компьютера-жертвы.

- ***Email-Worm*** (почтовый червь) – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам электронной почты. В процессе размножения червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, указатель URL на зараженный файл, расположенный на взломанном или хакерском Web-сайте).

В первом случае код червя активизируется при открытии (запуске) заражённого вложения, во втором – при открытии ссылки на заражённый файл. В обоих случаях эффект одинаков – активизируется код червя.

- ***P2P-Worm*** – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам файлообменных пиринговых сетей (например, Kazaa, Grokster, eDonkey, FastTrack, Gnutella и др.).

Механизм работы большинства подобных червей достаточно прост – для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

- ***IM-Worm*** – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам систем мгновенного обмена сообщениями (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.).

Для этих целей черви, как правило, рассылают на обнаруженные контакты (из контакт-листа) сообщения, содержащие URL на файл с телом червя, расположенный на каком-либо сетевом ресурсе. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

- ***IRC-Worm*** – вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению через Интернет-чат (Internet Relay Chats).

У этого типа червей существует два способа распространения по IRC-каналам, напоминающие способы распространения почтовых червей. Первый способ заключается в отсылке URL на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю IRC-канала. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение).

Серьезную опасность представляют ***поддельные антивирусы***, размещенные на специально подготовленных сайтах и которые злоумышленники предлагают загрузить для "лечения" компьютера от вирусов. Как правило, сами эти сайты не опасны, но загружаемые оттуда программы, в том числе лже-антивирусы, содержат вредоносные коды сетевых червей или троянских программ.

Троянские программы

Эти вредоносные программы внешне выглядят как легальный программный продукт, но при запуске осуществляют несанкционированные пользователем действия, направленные на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

К данной категории вредоносных программ относятся:

- ***Backdoor*** (бэкдор) – вредоносная программа, предназначенная для скрытого удалённого управления злоумышленником пораженного компьютера. По своей функциональности бэкдоры во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. Эти вредоносные программы позволяют делать с компьютером всё, что в них заложил автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д.

Представители данного типа вредоносных программ очень часто используются для объединения компьютеров-жертв в так называемые ботнеты, централизованно управляемые злоумышленниками в злонамеренных целях. Botnet (ботнет) – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на компьютере жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде "хозяина", управляющего данной копией троянской программы.

- ***Exploit*** (эксплойт) – программы, в которых содержатся данные или исполняемый код, позволяющие использовать одну или несколько уязвимостей в программном обеспечении на локальном или удаленном компьютере с заведомо вредоносной целью.

Обычно эксплойты используются злоумышленниками для проникновения на компьютер-жертву с целью последующего внедрения туда вредоносного кода (например, заражение вредоносной программой всех посетителей взломанного Web-сайта). Также эксплойты интенсивно используются программами типа Net-Worm для проникновения на компьютер-жертву без участия пользователя.

- ***Rootkit*** – программа, предназначенная для сокрытия в системе определенных объектов либо активности. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, процессы в памяти зараженного компьютера, вредоносная сетевая активность. Сам по себе Rootkit ничего вредоносного не делает, но данный тип программ в подавляющем большинстве случаев используется вредоносными программами для увеличения собственного времени жизни в пораженных системах в силу затрудненного обнаружения.

- ***Trojan*** – вредоносная программа, предназначенная для осуществления несанкционированных пользователем действий, влекущих уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей, и при этом не попадающая ни под одно из других троянских поведений.

К Trojan также относятся "многоцелевые" троянские программы, т.е. программы, способные совершать сразу несколько несанкционированных пользователем действий, присущих одновременно нескольким другим поведениям троянских программ, что не позволяет однозначно отнести их к тому или иному поведению.

Существует большое разнообразие троянских программ выполняющих те или иные действия и отличающихся друг от друга целями и способами воздействия на "жертву". Рассмотрим некоторые типы троянских программ:

- Trojan-Banker – предназначена для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт.

- Trojan-Dropper – предназначена для несанкционированной пользователем скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в теле этого типа троянцев.

- Trojan-Proxy – предназначена для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным Интернет-ресурсам через компьютер-жертву.

- Trojan-Mailfinder – предназначена для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику.

- Trojan-Clicker – предназначена для несанкционированного пользователем обращения к Интернет-ресурсам (обычно, к Web-страницам).
- Trojan-GameThief – предназначена для кражи пользовательской информации, относящейся к сетевым играм. Найденная информация передается злоумышленнику.
- Trojan-Ransom – предназначена для несанкционированной пользователем модификации данных на компьютере-жертве таким образом, чтобы сделать невозможным работу с ними, либо блокировать нормальную работу компьютера. После того как данные взяты злоумышленником под контроль, пользователю выдвигается требование выкупа.
- Trojan-PSW – предназначена для кражи пользовательских аккаунтов (логин и пароль) с пораженных компьютеров. Название PSW произошло от Password-Stealing-Ware.
- Trojan-DDoS – предназначена для проведения несанкционированной пользователем DoS-атаки с пораженного компьютера на компьютер-жертву по заранее определенному адресу.
- Trojan-IM – предназначена для кражи пользовательских аккаунтов (логин и пароль) от Интернет-пейджеров (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.).
- Trojan-SMS – предназначена для несанкционированной пользователем отсылки SMS-сообщений с пораженных мобильных устройств на дорогостоящие платные номера, которые "жестко" записаны в теле вредоносной программы.
- Trojan-ArcBomb – эти троянцы представляют собой архивы, специально сформированные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера или заполнение диска большим количеством "пустых" данных. Особенно опасны "архивные бомбы" для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации – архивная бомба может просто остановить работу сервера.
- Trojan-Downloader – предназначена для несанкционированной пользователем загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки троянцев или рекламных систем. Загруженные из Интернета программы либо запускаются на выполнение, либо регистрируются троянцем на автозагрузку в соответствии с возможностями операционной системы.
- Trojan-Notifier – предназначена для несанкционированного пользователем сообщения своему "хозяину" о том, что заражённый компьютер сейчас находится "на связи". При этом на адрес злоумышленника отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т.п.
- Trojan-Spy – предназначена для ведения электронного шпионажа за пользователем (вводимая с клавиатуры информация, снимки экрана, список активных приложений и т.д.). Найденная информация передается злоумышленнику.

Подозрительные упаковщики

Вредоносные программы часто сжимаются специфичными способами упаковки, включая использование многократных упаковщиков и совмещая упаковку с шифрованием содержимого файла для того, чтобы при распаковке усложнить анализ файла эвристическими методами.

К данному подклассу вредоносных программ относятся:

- ***MultiPacked*** – файловые объекты, многократно упакованные различными программами упаковки. Антивирус при детектировании такого объекта обнаруживает исполняемый файл, упакованный одновременно тремя и более упаковщиками.
- ***SuspiciousPacker*** – файловые объекты, сжатые специальными программами-упаковщиками, которые созданы для защиты вредоносного кода от детектирования антивирусным ПО.
- ***RarePacker*** – файловые объекты, сжатые различными редко встречающимися упаковщиками, например, реализовывающими какую-либо конкретную идею.

Вредоносные утилиты

Вредоносные программы, разработанные для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома компьютеров и т.п. В отличие от вирусов, червей и троянских программ, представители данной категории не представляют угрозы непосредственно компьютеру, на котором исполняются. Основным признаком, по которому различают вредоносные утилиты, являются совершаемые ими действия.

К данной категории вредоносных программ относятся:

- ***Constructor*** – программы, предназначенные для изготовления новых компьютерных вирусов, червей и троянских программ.
- ***HackTool*** – программы, используемые злоумышленниками при организации атак на локальный или удаленный компьютер (например, несанкционированное пользователем внесение нелегального пользователя в список разрешенных посетителей системы; очистка системных журналов с целью сокрытия следов присутствия в системе; снифферы с выраженным вредоносным функционалом и т.д.).
- ***Spoofer*** – программы, позволяющие отправлять сообщения и сетевые запросы с поддельным адресом отправителя.
- ***DoS*** – программы, предназначенные для проведения DoS-атак на компьютер-жертву.
- ***Hoax*** – программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности.
- ***irTool***V – программы, позволяющие злоумышленнику модифицировать другие вредоносные программы таким образом, чтобы они не детектировались антивирусным программным обеспечением.
- ***Flooder*** – программы, функцией которых является "забивание" бесполезными сообщениями сетевых каналов, отличных от почтовых, Интернет-пейджеров и SMS (например, IRC).

- ***Email-Flooder, IM-Flooder, SMS-Flooder*** – программы, функцией которых является "забивание" бесполезными сообщениями каналов электронной почты, каналов Интернет-пейджеров (ICQ, MSN Messenger и др.) и каналов передачи SMS-сообщений.

Классификация детектируемых объектов "Лаборатории Касперского" выделяет в отдельную группу ***условно нежелательные программы***, которые невозможно однозначно отнести ни к опасным, ни к безопасным. Речь идёт о программах, которые разрабатываются и распространяются легально и могут использоваться в повседневной работе, например, системными администраторами. Вместе с тем, некоторые из таких программ обладают функциями, которые могут причинить вред пользователю, но только при выполнении ряда условий. Например, если программа удаленного администрирования установлена на компьютер пользователя системным администратором, то ничего страшного в этом нет, т.к. администратор всего лишь получает возможность удаленно решать возникающие у пользователя проблемы. Но если та же программа установлена на компьютер пользователя злоумышленником, то последний получает полный контроль над компьютером-жертвой и дальнейшем может использовать его по своему усмотрению. Таким образом, подобные программы могут быть реализованы как во благо, так и во вред – в зависимости от того, в чьих руках они находятся.

Вредоносное ПО создаётся для компьютерных систем определенного типа, работающих с конкретными операционными системами. Привлекательность ОС для создателей вирусов определяется следующими факторами:

- распространенность ОС;
- отсутствие встроенных антивирусных механизмов;
- относительная простота;
- продолжительность эксплуатации.

Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру.

Тема 1:

Основные понятия в области информационной безопасности

А

|

версия для печати

Тема 1: 12**3**4 || Тема 2 >

Угрозы безопасности сетевых информационных систем

Удаленные воздействия на сетевые информационные системы, их классификация

Основной особенностью любой сетевой информационной системы является то, что ее компоненты распределены в пространстве, и связь между ними осуществляется физически (при помощи сетевых соединений) и программно (при помощи механизма сообщений). При этом все управляющие

сообщения и данные передаются по сетевым соединениям в виде *пакетов обмена*. Пакет, передаваемый по сети, состоит из заголовка и поля данных, в заголовок пакета заносится служебная информация, определяемая используемым протоколом обмена и необходимая для адресации пакета, его идентификации, преобразования и т. п. Эта особенность и является основной для рассматриваемых в этой главе удаленных атак на инфраструктуру и протоколы IP-сетей.

Удалённые воздействия (атаки) на информационные системы характеризуются несколькими признаками. Для рассмотрения их сущности и условий осуществления предлагается следующая классификация.

По характеру воздействия

По характеру воздействия удаленные атаки делятся на:

- пассивное воздействие;
- активное воздействие.

Пассивным воздействием на информационную систему является воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать политику доступа к защищаемым данным. Именно отсутствие влияния на работу распределенной системы приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия на информационную систему служит прослушивание канала связи в сети и перехват передаваемой информации.

Активное воздействие на ресурсы системы – это воздействие, оказывающее непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности. Очевидной особенностью активного воздействия, по сравнению с пассивным, является возможность его обнаружения (с большей или меньшей степенью сложности). Примером результата такого воздействия является отказ в обслуживании системы.

По цели реализации воздействия

По данному признаку удаленные атаки могут быть направлены на:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение работоспособности (доступности) системы.

Основным результатом практически любого злонамеренного воздействия на информационную систему является получение несанкционированного доступа к информации. Такой доступ достигается путем *перехвата или искажения* информации. Возможность перехвата информации означает получение к ней доступа, но невозможность ее изменения (модификации). Следовательно, перехват информации ведет к *нарушению ее конфиденциальности* . Примером перехвата информации может служить *анализ сетевого трафика* (не следует путать с санкционированным проведением анализа сетевого трафика).

Искажение информации возможно в том случае, если злоумышленник располагает полным контролем над информационным потоком между объектами системы и/или имеет возможность передавать данные под именем доверенного пользователя.

В этом случае, искажение информации ведет к *нарушению ее целостности*. Данное информационное разрушающее воздействие относится к *активному воздействию*. Примером удаленной атаки, цель которой нарушение целостности информации, может служить удаленная атака **"Ложный объект сети"**.

И совершенно другой вид атаки, когда получение атакующим несанкционированного доступа к информации не предполагается – это *нарушение работоспособности (доступности) системы*. В данном случае основная цель злоумышленника – резкое снижение производительности системы атакуемого объекта (или вывод ее из строя), и, как следствие – невозможность доступа пользователей к ее ресурсам. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить удалённая атака "Отказ в обслуживании" (DoS-атака, Denial of Service). И наиболее популярная разновидность DoS-атаки – DDoS-атака (Distributed Denial of Service), распределённая атака типа **"отказ в обслуживании"**.

По условию начала осуществления воздействия

Для того чтобы осуществить удаленное воздействие на объект информационной системы, необходимо наступление определенных условий. В распределенных сетях выделяются три условия для начала осуществления воздействия:

- ***Атака по запросу от атакуемого объекта***. В данном случае атакующий ожидает от потенциального объекта атаки передачи запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов могут быть DNS- и ARP-запросы.

- ***Атака по наступлению ожидаемого события на атакуемом объекте***. Атакующий ведет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие.

- ***Безусловная атака.*** В данном случае начало осуществления атаки безусловно по отношению к цели атаки, то есть атака осуществляется немедленно и независимо от состояния системы и атакуемого объекта. Атакующий является инициатором начала осуществления атаки.

По наличию обратной связи с атакуемым объектом

По данному признаку процесс осуществления удаленного воздействия может быть *с обратной связью* и *без обратной связи* (однонаправленная атака).

Обратная связь формируется ответом атакуемого объекта на определенный запрос, отправленный к нему злоумышленником, и позволяет последнему реагировать на все изменения, происходящие на атакуемом объекте.

Целью удаленной атаки *без обратной связи* не является получение данных от атакуемого объекта. Атакующий отправляет запросы, не ожидая ответа от объекта атаки. Поэтому подобную удалённую атаку называют однонаправленной. В качестве примера однонаправленной атаки можно привести типовую удалённую атаку **"Отказ в обслуживании"**.

По расположению нарушителя относительно атакуемого объекта

В соответствии с этим признаком воздействие реализуется как *внутрисегментно*, так и *межсегментно*.

Рассмотрим ряд определений:

Хост (host) – сетевое устройство (чаще всего компьютер).

Маршрутизатор (router) – устройство, обеспечивающее маршрутизацию пакетов обмена из одной сети в другую.

Подсеть (subnetwork) – совокупность хостов, являющихся частью сети, для которых маршрутизатором выделен одинаковый номер подсети. Подсеть – логическое объединение хостов маршрутизатором. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, без использования функций маршрутизации.

Сегмент сети – физическое или логическое объединение хостов. Например, беспроводный сегмент сети образует совокупность хостов, подключенных к точке доступа по схеме "общая шина". При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте. Аналогичная картина будет наблюдаться, если сегмент сети создан не физически, а логически (с применением виртуальных сетей VLAN, о которых мы поговорим в следующих главах).

С точки зрения удаленной атаки важно расположение злоумышленника и объекта атаки по отношению друг к другу, то есть в одном или в разных сегментах они находятся. В случае ***внутрисегментной атаки***, как следует из названия, злоумышленник и объект атаки находятся в одном сегменте. При ***межсегментной атаке*** злоумышленник и объект атаки находятся в разных сегментах. Данный классификационный признак позволяет судить о так называемой "степени удаленности" атаки.

На практике межсегментную атаку осуществить значительно труднее, чем внутрисегментную. Но межсегментная удаленная атака представляет большую опасность, чем внутрисегментная, так как именно удаленность нарушителя от атакуемого объекта может существенно воспрепятствовать мерам по отражению атаки.

Вероятность удачной внутрисегментной и межсегментной атаки значительно увеличивается в случае наличия беспроводных решений. Одно из главных отличий между проводными и беспроводными сетями связано с тем, осуществлять полный контроль над областью между конечными точками беспроводной сети достаточно сложно. В довольно широком пространстве сетей беспроводная среда никак не контролируется. Наиболее распространенная проблема в открытых и неуправляемых средах, таких как беспроводные сети, – это возможность анонимных атак.

По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие

Распределенные системы являются открытыми системами. Сетевые протоколы обмена, также как и сетевые программы, работают на разных уровнях модели OSI (Open System Interconnection – Взаимодействие открытых систем):

- Прикладной

- Представительский
- Сеансовый
- Транспортный
- Сетевой
- Канальный
- Физический

Вследствие того, что удаленная атака реализуется какой-либо сетевой программой, ее можно соотнести с определенным уровнем модели OSI.

По соотношению количества нарушителей и атакуемых объектов

По данному признаку удаленная атака может быть отнесена к следующим классам воздействия:

- воздействие "один к одному" – атака осуществляется одним злоумышленником в отношении одной цели;
- воздействие "один ко многим" – атака осуществляется одним злоумышлен-ником в отношении нескольких объектов;
- воздействие "несколько к одному";
- воздействие "несколько ко многим".

В двух последних случаях атака осуществляется несколькими злоумышленниками с разных компьютеров в отношении одного или нескольких объектов (распределенное или комбинированное воздействие).

Типовые удалённые атаки

Компьютерные сети проектируются (и создаются) на основе одних и тех же принципов, правил (шаблонов) и, следовательно, имеют практически одинаковые проблемы безопасности в сетевых информационных системах и можно ввести понятие *типовой удаленной атаки*.

Типовая удаленная атака – это удаленное информационное воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной системы.

Рассмотрим типовые удаленные атаки и механизмы их реализации.

Анализ сетевого трафика

Как уже отмечалось, основной особенностью сетевой информационной системы является то, что ее объекты распределены в пространстве, подключены по физическим каналам и взаимодействие между ними осуществляется программно. Передача пакетов по сетевым соединениям дает возможность прослушивать канал связи с использованием специального программно-аппаратного устройства или программы-анализатора пакетов (sniffer, сниффер). Такое воздействие называется ***анализ сетевого трафика***.

В настоящее время снифферы работают в сетях на вполне законном основании. Однако, вследствие того, что некоторые сетевые приложения (например, Telnet, FTP, SMTP, POP3) передают данные в текстовом формате и не предусматривают шифрование, злоумышленник с помощью сниффера может перехватить поток передаваемых данных. Последующий их анализ позволит извлечь идентификационную информацию, такую как статические пароли пользователей к удаленным хостам, используемые протоколы, доступные порты сетевых служб, активные сетевые сервисы и т.п. В процессе проведения анализа сетевого трафика злоумышленник изучает логику работы сети и, в случае успеха, может получить доступ к конфиденциальной информации удаленного объекта.

По характеру воздействия анализ сетевого трафика является *пассивным воздействием* (возможность изменения трафика отсутствует), осуществляется внутри одного сегмента сети на *канальном уровне OSI*. Реализация данной атаки без обратной связи ведет к нарушению *конфиденциальности информации*. При этом начало осуществления атаки *безусловно* по отношению к цели атаки.

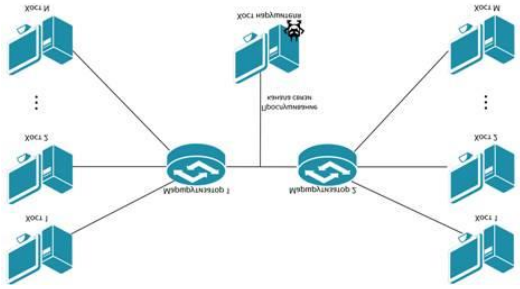


Рис. 1.3. Схема реализации воздействия «Анализ сетевого трафика»

Подмена доверенного объекта сети

Под доверенным объектом понимается элемент сети (компьютер, межсетевой экран, маршрутизатор и т.п.), имеющий легальное подключение, и которому присвоены права для доступа к сетевым ресурсам информационной системы.

Осуществление ***атаки "подмена доверенного объекта сети"*** и передача по каналам связи сообщений от его имени с присвоением его прав доступа возможна в системах, где используются нестойкие алгоритмы идентификации и аутентификации хостов. Типичным примером является перехват TCP-сессии.

Протокол TCP является одним из базовых протоколов транспортного уровня сети Интернет. Он позволяет исправлять ошибки, которые могут возникнуть в процессе передачи пакетов, устанавливая логическое соединение – виртуальный канал. По этому каналу передаются и принимаются пакеты с регистрацией их последовательности, осуществляется управление информационным потоком, организовывается повторная передача искаженных пакетов, а в конце сеанса канал разрывается. Для идентификации TCP-пакета в TCP-заголовке существуют два 32-разрядных идентификатора – Sequence Number (номер последовательности) и Acknowledgment Number (номер подтверждения), которые также играют роль счетчиков пакетов

Существуют две разновидности процесса осуществления удаленной атаки типа "подмена доверенного объекта сети":

- атака с установлением виртуального канала;

- атака без установления виртуального канала.

Процесс осуществления *атаки с установлением виртуального канала* состоит в присвоении прав доверенного пользователя, что позволяет злоумышленнику вести сеанс работы с объектами системы от имени доверенного пользователя. Для формирования ложного TCP-пакета атакующему достаточно подобрать соответствующие текущие значения идентификаторов TCP-пакета (ISSa и ISSb, см. рисунок 1.4) для данного TCP-соединения (например, FTP- или TELNET-подключение).

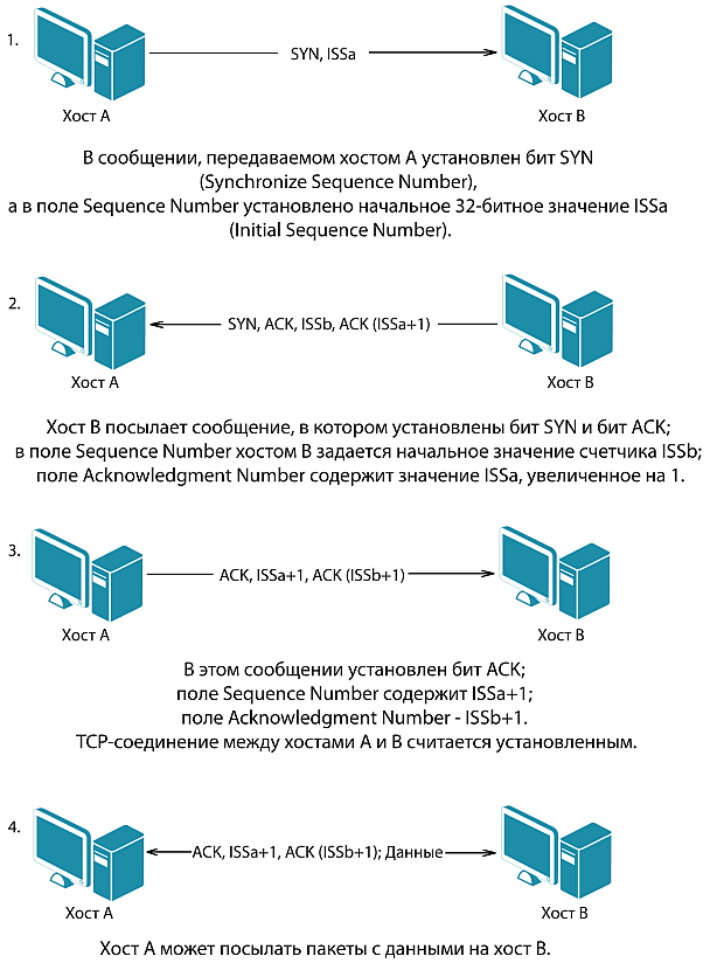


Рис. 1.4. Схема создания TCP-соединения

Так как для служебных сообщений в распределенных сетях часто используется передача одиночных сообщений, не требующих подтверждения, виртуальное соединение не создается. *Атака без установления виртуального канала* заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) о ложном изменении маршрутно-адресных данных. Идентификация передаваемых сообщений осуществляется только по сетевому адресу отправителя, который легко подделать. Типовая удаленная атака, использующая *навязывание ложного маршрута*, основана на описанной идее.

Подмена доверенного объекта сети является *активным воздействием*, совершаемым с целью нарушения *конфиденциальности и целостности информации*. Данная удаленная атака может являться как *внутрисегментной*, так и *межсегментной*, как с *обратной связью*, так и *без обратной связи* с атакуемым объектом и осуществляется *на сетевом и транспортном уровнях модели OSI*.

Ложный объект сети

Архитектура Интернета создавалась в условиях, когда внутри сети существовало доверие к действиям отдельных участников. В распределенных сетях механизмы идентификации сетевых управляющих устройств (маршрутизаторов) не обеспечивают безопасное использование протоколов управления сетью. Если участник сети (маршрутизатор) заявляет, что он владеет блоком адресного пространства, остальная часть IP-сети верит ему на слово и адресует ему весь соответствующий трафик. Значит, можно создать любой сетевой блок и запустить его в IP-сети, придав анонимность любой атаке, связанной с изменением маршрутизации и внедрением в систему ложного объекта. Такой тип воздействия на сетевую информационную систему ещё называют атакой типа MITM (man in the middle, "человек посередине").

Для перехвата трафика злоумышленники используют уязвимости, присущие протоколам различных уровней стека TCP/IP: сетевому, транспортному и прикладному. На сегодняшний день в подавляющем большинстве применяются стандартные протоколы семейства TCP/IP, среди которых к наиболее уязвимым относятся следующие: протокол управления передачей TCP, межсетевого взаимодействия IP, эмуляции терминала Telnet, передачи файлов FTP, разрешения адресов ARP, службы доменных имен DNS, управляющих сообщений сети Интернет ICMP и сетевого управления SNMP. Кроме того, для обеспечения эффективной и оптимальной маршрутизации в сетях применяются динамические протоколы RIP и OSPF, позволяющие маршрутизаторам обмениваться информацией друг с другом и обновлять таблицы маршрутизации.

Атакующий ставит целью внедрение ложного объекта в сеть путем изменения таблиц маршрутизации и навязывания ложного маршрута. Основная задача злоумышленника – не только прервать сообщение между сетями, а в первую очередь перевести трафик через свой хост, чтобы извлечь полезную информацию.

Реализация атаки основывается на уязвимостях или ошибках настройки протоколов маршрутизации (RIP, OSPF) и управления сетью (ICMP, SNMP). При этом злоумышленник посылает в сеть управляющее сообщение от имени сетевого управляющего устройства (например, маршрутизатора). Рисунок 1.5 иллюстрирует реализацию удаленной атаки "навязывание ложного маршрута" с использованием протокола ICMP. Пакеты с запросами в сеть 92.14.0.0/16 с хоста А проходят через маршрутизирующее устройство с IP-адресом 192.168.0.1 (рисунок 1.5а). Атакующий посылает управляющее сообщение ICMP Redirect о наилучшем маршруте в сеть 92.14.0.0/16 и получает возможность изменения таблиц маршрутизации хоста А. В результате весь трафик с хоста А, направляющийся в сеть 92.14.0.0/16, проходит через ложный объект хост В (рисунок 1.5б).

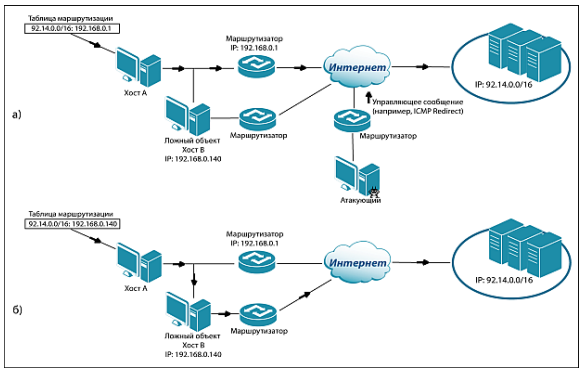


Рис. 1.5. Схема реализации атаки «навязывание ложного маршрута» с использованием протокола ICMP с целью перехвата трафика

Относительно недавно разработчиками израильского центра Electronic Warfare Research and Simulation Center была обнаружена брешь в сетевом протоколе OSPF. Как утверждают исследователи, уязвимость существует из-за того, что сам протокол допускает прием поддельных запросов новых таблиц маршрутизации. Например, при помощи ноутбука, можно отправить периодический запрос Link State Advertisement (LSA) на обновление таблиц маршрутизации. После чего маршрутизатор опознает запрос как легальный, поскольку в подтверждение он проверяет лишь порядковые номера запросов, которые также можно подделать. В результате подобной манипуляции, у злоумышленника будет полный доступ к сети в течение примерно 15-ти минут, пока маршрутизатор опять не обновит таблицы.

Также успешной может оказаться удаленная атака, использующая уязвимости сервисов, установленных на хостах (серверах). Для преобразования адресов из одного формата в другой в распределенных сетях используются протоколы удаленного поиска, заключающиеся в передаче по сети специальных запросов и получения на них ответов с искомой информацией. Так, в сетях Ethernet протокол ARP решает вопрос отображения MAC-адреса (6 байтов) в пространство сетевых IP-адресов (4 байта) и наоборот; протокол DNS используется при преобразовании текстового доменного имени в IP-адрес. При этом существует возможность перехвата злоумышленником поискового запроса и выдачи на него ложного ответа, использование которого приведет к изменению маршрутно-адресных данных. В результате весь сетевой трафик жертвы будет проходить через ложный объект.

На рисунке 1.6 представлена схема реализации атаки "внедрение ложного DNS-сервера" путем перехвата DNS-запроса. Атакующий (может находится либо на хосте B, либо на хосте C) ожидает DNS-запрос от хоста A (рисунок 1.6а). После перехвата поискового запроса от хоста A, атакующий посылает ему ложный DNS-ответ (рисунок 1.6б). Особенно стоит отметить возможность преднамеренного искажения информации: вместо ресурса http://security.dlink.com.tw хост A в результате запроса может получить ресурс с таким же Web-интерфейсом, как и у запрашиваемого, только с искаженной информацией (рисунок 1.6в).

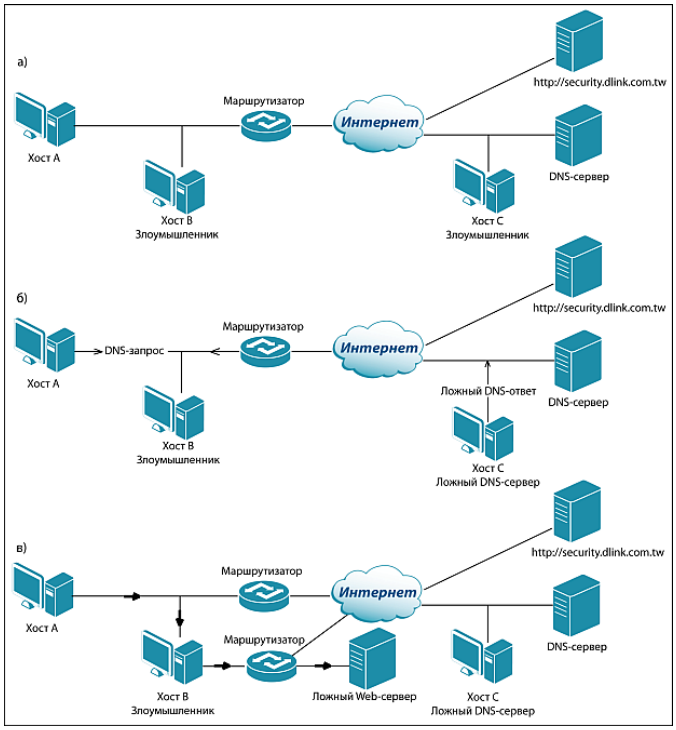


Рис. 1.6. Схема реализации атаки «внедрение ложного DNS-сервера» путем перехвата DNS-запроса

Перехват пользовательского сетевого трафика через ложный объект дает злоумышленнику возможность проведения анализа данных, передаваемых по сети, модификации информации, а также полной ее подмены.

Ниже приведены примеры некоторых наиболее распространенных атак, связанных с внедрением ложного объекта.

- Одним из способов внедрения ложного объекта может быть ***SQL-инъекция*** – это один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.

Атакующий использует индексы поисковых систем для идентификации уязвимых сайтов. Злоумышленники ищут сайты, использующие распространенные системы управления контентом и другое ПО, содержащее уязвимости процессов обработки входных данных, применяемых в SQL-запросах. Результатом одной из последних атак такого рода стало то, что пользователи, посещающие зараженные страницы переводятся на другие сайты и на сервер Lilupophilupop.com, где им предлагается загрузить вредоносное ПО под видом Adobe Flash Player или несуществующего антивируса.

С использованием SQL-инъекций злоумышленник может не только получить закрытую информацию из базы данных, но и, при определенных условиях, внести туда изменения.

В целом, атаки, связанные с различного рода инъекциями, возможны ввиду недостаточной проверки входных данных и подразумевают внедрение сторонних команд или данных в работающую систему (чаще всего это связано с Web-сайтами) с целью изменения хода её работы, а в результате – получение доступа к закрытым ресурсам и информации, либо дестабилизации работы системы в целом.

- Техника ***Clickjacking*** заключается в создании специального тега iFrame, который создает кнопку-подделку. При нажатии (или автоматически, без действия пользователя) на эту кнопку в невидимый iFrame загрузится специальная страница с вредоносным кодом. Спрятанная страница может быть подделкой текущей, где будет предложено вновь ввести идентификационные данные пользователя, которые при повторном вводе сохраняться на хосте злоумышленника.

- Как рассматривалось выше, существует множество вредоносных программ, которые инфицировав сетевой компьютер, обеспечивают злоумышленникам удаленный доступ и полное управление этим компьютером, а также возможность использовать его в качестве ложного объекта сети, выдавая себя за легального пользователя. ***Люки (Backdoors)*** – программы, обеспечивающие вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий. Часто используются для обхода системы безопасности. Люки не инфицируют файлы, но прописывают себя в реестр, модифицируя, таким образом, ключи реестра. BackDoor.Bitsex – троянская программа, представляющая собой полноценный сервер для удаленного управления инфицированным компьютером.

- ***Атака ARP-spoofing*** – применяется преимущественно в сетях Ethernet, но возможна и в других сетях, использующих протокол ARP. Данная атака основана на использовании такой уязвимости протокола ARP, как отсутствие системы аутентификации пользователей. Она

состоит в том, что злоумышленник посылает ложные ARP-пакеты с целью убедить компьютер жертвы в том, что ложный объект и есть легальный конечный адресат. Далее пакеты пересылаются реальному получателю, MAC-адрес отправителя в них подменяется, чтобы ответные пакеты тоже шли через ложный объект. Злоумышленник получает возможность прослушивать трафик, например, общение по ICQ, почту жертвы и др. При этом в случае прохождения через ложный объект трафика многих пользователей может возникнуть переполнение ARP-таблиц и сетевой отказ в обслуживании.

Достаточно часто злоумышленник проводит атаку на систему с целью ее отказа в работе.

Отказ в обслуживании (DoS, DDoS-атаки)

Одной из возможностей сетевой операционной системы (ОС), установленной на каждом объекте распределенной сети, является наличие сетевых служб, позволяющих удалённым пользователям использовать ресурсы данного объекта. Программа-сервер (например, FTP-сервер или Web-сервер), запущенная в сетевой ОС компьютера, обеспечивает удаленный доступ к FTP- или Web-ресурсам этого компьютера. Пользователь отправляет запросы на предоставление услуги, ОС обрабатывает приходящие извне запросы, пересылает их на соответствующий сервер (FTP или Web), а сервер отвечает на них по созданному виртуальному каналу.

Любая операционная система имеет ограничения по количеству открытых виртуальных соединений и существует предел ответов на поступающие запросы. Данные ограничения зависят от системных ресурсов, основными из которых являются вычислительные мощности, оперативная память, дисковое пространство или пропускная способность каналов связи. Если какой-то из ресурсов достигнет максимальной загрузки, приложение будет недоступно.

Как правило, атаки типа **DoS (Denial of service)** направлены на исчерпание критичных системных ресурсов, что приводит к прекращению функционирования системы, т.е. к **отказу в обслуживании** и невозможности доступа к серверу удаленных пользователей.

Выделяется два типа отказа в обслуживании: первый, основанный на ошибке в приложении, и второй, основанный на плохой реализации или уязвимости протокола.

Отказ в обслуживании приложения становится возможен, если уязвимости приложения ведут к получению контроля над машиной (например, с помощью переполнения буфера обмена). Приложение станет недоступным либо из-за нехватки ресурсов, либо из-за аварийного завершения. Уязвимость приложения может быть использована и для нарушения работоспособности других компонентов системы, таких как сервер СУБД или сервер аутентификации.

Сетевой отказ в обслуживании основывается на особенностях стека протоколов TCP/IP.

Если атака выполняется одновременно с большого числа хостов, говорят о ***распределённой атаке типа "отказ в обслуживании"*** – DDoS-атаке (Distributed Denial of Service). В некоторых случаях к DDoS-атаке приводит легальное действие, например, на популярном Интернет-ресурсе указана ссылка на сайт, размещённый на не очень производительном сервере (так называемый слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер, и он очень быстро становится недоступным или доступ к нему затрудняется в результате перегруженности.

Ниже представлены некоторые типы подобных атак, однако, это всего лишь малая часть от существующих на сегодняшний день вариантов DoS-атак, информация о которых постоянно обновляется на специализированных Web-сайтах.

- ***SYN-flood***. Выше был рассмотрен механизм установления TCP-соединения (рисунок 1.4). Атака типа SYN-flood использует именно этот механизм. TCP-соединение включает три состояния: отправка SYN-пакета, получение пакета SYN-ACK и посылка ACK-пакета.

Идея атаки состоит в создании большого количества не до конца установленных TCP-соединений. Для реализации этого злоумышленник отправляет на сервер-жертву множество запросов на установление соединения (пакеты, с выставленным флагом SYN), машина-жертва отвечает пакетами SYN-ACK. Злоумышленник же игнорирует эти пакеты, не высылая ответные, либо подделывает заголовок пакета таким образом, что ответный SYN-ACK отправляется на несуществующий адрес. Процесс установки соединения не завершается, а остается в полуоткрытом состоянии, ожидая подтверждения от клиента. А так как под каждый полученный SYN-пакет сервер резервирует место в своем буфере, то при огромном количестве запросов, буфер достаточно быстро переполняется. В результате, вновь поступающие SYN-запросы, в том числе от легальных пользователей, не обрабатываются, и новые соединения не устанавливаются.

- ***UDP-flood***. Данный метод основан на применении UDP-протокола и обычно используется для того, чтобы максимально загрузить канал связи сервера-жертвы бесполезными данными.

Злоумышленник генерирует большое количество UDP-датаграмм (UDP-шторм), направленных на определенную машину. В результате происходит перегрузка сети и недоступность сервера-жертвы. В протоколе TCP есть механизмы предотвращения перегрузок: если подтверждения приема пакетов приходят со значительной задержкой, передающая сторона замедляет скорость передачи TCP-пакетов. Так как в протоколе UDP такой механизм отсутствует, то после начала атаки UDP-трафик "захватывает" практически всю доступную полосу пропускания.

Вредоносное ПО **LOIC** (Low Orbit Ion Cannon) выполняет распределённую атаку на отказ в обслуживании путём постоянной отправки TCP и UDP пакетов на целевой сайт или сервер. Это ПО создано для организации DDoS-атак на Web-сайты с участием тысяч анонимных пользователей, пользующихся программой. Атаки производятся на такие сайты, как Visa.com или Mastercard.com.

- ***ICMP-flood*** (ICPM-smurfing). Принцип работы такой DDoS-атаки довольно прост. Злоумышленник, изменяя адрес источника, посылает пакет ICMP Echo Request (больше известный как ping) к конкретным хостам.

Эти хосты отвечают пакетом *ICMP Echo Reply*, отправляя его на тот IP-адрес, который злоумышленник указал как источник. Часто для усиления атаки используются локальные сети (LAN) с включенной опцией направленной широковещательной рассылки (directed broadcast) в ответ на команду "ping" с каждого хоста в составе сети. Например, на один запрос будет отправлено 100 ответов. В результате вся сеть подвергается отказу из-за перегрузки.

- ***Mailbombing***. Суть атаки сводится к тому, чтобы генерировать большое количество сообщений с разных источников для почтового сервера (почтового ящика) с тем, чтобы реализовать ограничение доступа (или полный отказ) к этому почтовому серверу (ящику).

- Атаки, основанные на уязвимостях протоколов управления. Например, утилита **THC-SSL-DOS**, которую некоторые злоумышленники применяют в качестве инструмента для проведения DoS-атак на SSL-серверы, использует уязвимость в функции повторного подтверждения SSL (SSL renegotiation).

Функция, предназначенная для обеспечения большей безопасности SSL, на самом деле делает его более уязвимым перед атакой.

- ***Программы Backdoors*** способны производить DDoS атаку.

Например, троян **Backdoor.IRCBot.ADEQ** представляет собой вредоносное ПО, которое распространяется как регулярное обновление для Java платформы, и являет собой чрезвычайно опасный инструмент для инициации распределенной атаки "отказ в обслуживании". Данная программа имеет возможность установки ссылки целевого ресурса, назначения времени атаки, интервала и частоты запросов.

Удаленная атака типа "отказ в обслуживании" является *активным воздействием*, осуществляемым *с целью нарушения работоспособности системы, безусловно* относительно цели атаки. Данная удалённая атака является однонаправленным воздействием, как *межсегментным*, так и *внутрисегментным*, осуществляемым на *транспортном и прикладном уровнях модели OSI*.

Социальная инженерия

Говоря об информационной безопасности, нельзя не упомянуть о появившемся не так давно, но ставшим уже типичным, явлении – *социальная инженерия*.

Социальная инженерия (Social Engineering) – использование некомпетентности, непрофессионализма или небрежности персонала для получения доступа к информации. Суть этого метода сводится к тому, что злоумышленник старается получить интересующие его сведения путем установления контакта с человеком, владеющим необходимой информацией, тем или иным способом (при ведении телефонного разговора, почтовой переписки, доверительной беседы в кафе и т.п.)

С бурным развитием социальных сетей такой метод доступа к конфиденциальной информации стал очень популярным.

Phishing (фишинг) – одна из разновидностей социальной инженерии. Цель такого мошенничества – получить идентификационные данные пользователей. Это и кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. Фишинг осуществляется с помощью пришедших на почту поддельных уведомлений от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и пр. Фишинговые сайты, как правило, живут недолго (в среднем – 5 дней). Так как анти-фишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники. Наиболее часто жертвами фишинга становятся пользователи электронных платежных систем, аукционов, электронной почты и, помимо этого – пользователи "социальных сетей" (vkontakte, odnoklassniki, twitter, facebook и др.).

Spear Phishing (направленный фишинг). Это комбинация обыкновенного фишинга и методов социальной инженерии, направленная против одного человека или целевой группы. Чтобы атака была успешной, она должна быть очень хорошо подготовлена, чтобы не вызвать подозрений. Злоумышленник собирает максимум сведений о конкретном человеке (группе лиц). Очень часто такие атаки направлены против финансовых организаций. Атакующий использует собранную персональную информацию и так подготавливает электронное (а бывает, и бумажное) письмо, чтобы оно выглядело достоверно и заставило человека ответить и выдать свои конфиденциальные данные (логины и пароли). Например, используя найденную в прессе информацию о назначении господина X на новую должность, ему присылают официальное с виду письмо от службы технической поддержки, и в результате господин X позволяет "службе поддержки" установить у себя троянскую программу или просит завести себе логин и пароль, схожий с логином и паролем в другой системе.

В последнее время механизм социальной инженерии очень часто используется для организации и реализации DDoS-атаки на сетевой ресурс, когда злоумышленники провоцируют пользователей ресурса на определённые действия, связанные с рассылкой сообщений (т.н. "письма счастья" или "магические письма", мнимые предупреждения о вредоносных программах, или событиях и необходимости оповещения об этом других пользователей и т.п.). В этом случае добропорядочные пользователи, если они играют по правилам злоумышленников (т.е. рассылают полученные злоумышленниками сообщения), невольно становятся соучастниками DDoS-атаки на сетевой ресурс.

Тема :**Формирование системы информационной безопасности**

Наибольший эффект при обеспечении защиты информации достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм – ***систему информационной безопасности***. Функционирование механизма защиты должно постоянно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

С позиции системного подхода, к системе информационной безопасности предъявляются определенные требования, включающие:

- **Адекватность угрозам**. Предполагается тщательный анализ угроз как реальных, так и потенциальных. По результатам такого анализа формируются требования к системе информационной безопасности конкретного объекта в конкретной обстановке (завышение требований приводит к неоправданным расходам, занижение – к резкому возрастанию вероятности реализации угроз).
- **Непрерывность**. Обеспечение защиты информации конкретного объекта – это непрерывный процесс, заключающийся в развитии системы информационной безопасности, постоянном контроле, выявлении её узких и слабых мест и потенциально возможных каналов утечки информации.
- **Плановость**. Данное требование подразумевает разработку детального плана защиты информации для каждой службы в сфере ее компетенции с учетом общей цели предприятия.
- **Централизованность**. В рамках определенной структуры должен быть организован процесс единого (централизованного) управления по обеспечению защиты информации.

- **Целенаправленность**. При реализации защитных мер, направленных на обеспечение безопасности информации, действия должны быть сосредоточены на защите конкретного объекта и обеспечивать достижение поставленной цели.
- **Надежность**. Методы защиты должны гарантировано блокировать возможные каналы утечки информации, независимо от формы ее представления, языка выражения и вида физического носителя, на котором она хранится.
- **Универсальность**. Методы защиты должны обеспечивать возможность перекрытия канала утечки информации, независимо от его вида и места появления.
- **Комплексность**. Система информационной безопасности включает в себя все виды, формы и средства защиты информации в полном объеме. Недопустимо применять отдельные формы или технические средства. Необходимо использовать все имеющиеся средства защиты на всех этапах технологического цикла обработки информации и передачи ее по каналам связи.

Построение системы информационной безопасности подразумевает выполнение ряда мероприятий правового и организационно-технического характера. Каждое предприятие (компания) определяет свою **политику информационной безопасности**, включающую цели и принципы по защите информации компании. Согласно данной политике разрабатываются документы по вопросам обеспечения информационной безопасности с учетом требований нормативных правовых актов, разрабатываются и внедряются технические решения и*средства защиты информации* от утечки защищаемой информации и от несанкционированного или случайного воздействия на нее.

Тема: Мероприятия системы защиты информации технического характера

Инженерно-технический элемент системы защиты информации предназначен для активного и пассивного противодействия средствам технической разведки и формирования контролируемой зоны с помощью комплексов технических средств. При защите информационных систем этот элемент имеет большое *значение* и включает в себя:

- организацию физической защиты от проникновения посторонних лиц на территорию, в здания и помещения, а так же к линиям связи;
- средства защиты технических каналов утечки информации, возникающих при работе компьютерного оборудования, средств связи, модемов, факсов и других устройств, участвующих в передаче сообщений по каналам связи;
- средства защиты помещений от визуальных способов технической разведки;
- средства наблюдения (в т.ч. видеонаблюдения), оповещения, сигнализации, информирования, идентификации нарушений работы технических средств и изменений параметров сетей связи;
- средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств и т.п.);
- технические средства контроля, предотвращающие вынос персоналом с места работы специально маркированных предметов, дискет, любых внешних носителей информации и т.п.;
- резервирование технических средств, дублирование носителей информации.

Один из важных элементов системы защиты информации – это обеспечение бесперебойного питания всех электронных устройств системы. Многие ошибочно полагают, что только полное прекращение подачи электроэнергии на носители может негативно повлиять на рабочее состояние компьютера и другого электронного оборудования. Наибольший же вред оборудованию наносят невидимые невооруженным глазом помехи и перепады напряжения в электросети. Высокочувствительное электронное оборудование, к которому относятся компьютеры, коммутаторы и маршрутизаторы, моментально реагирует на малейшее изменение напряжения в электросети.

Кроме того, необходимо помнить, что *злоумышленник* может организовать съём информации, обрабатываемой в информационной среде объекта (предприятия, организации), посредством силовой электрической сети 127/220/380 В. Для уменьшения уровня побочных электромагнитных излучений применяют специальные *средства защиты информации*:

- экранирование помещений;
- дополнительное заземление объектов защиты;
- развязку цепей электропитания с помощью сетевых помехоподавляющих фильтров;
- электромагнитную развязку между информационными цепями контролируемой зоны и внешними линиями связи.

Некоторые аспекты безопасности структурированных кабельных систем

Под структурированной кабельной системой (*СКС*) обычно подразумевают специально спроектированную систему кабельной проводки внутри здания для организации коммуникационной сети, обеспечивающей передачу речи и данных.

Кабельные системы – неотъемлемая часть всего комплекса средств, обеспечивающих *деятельность* любого предприятия. Поэтому и решение проблем безопасности неизбежно затрагивает процесс функционирования *СКС*. Важным аспектом безопасности всей *СКС* является, так называемый, *человеческий фактор*.

Зачастую именно неквалифицированные или ошибочные действия персонала становятся причиной возникновения неполадок в кабельной системе, что может привести к сбою в сети и потере ее работоспособности. Как правило, подобное происходит в следующих случаях:

- Неправильное ведение технической документации в процессе эксплуатации СКС или полное её отсутствие.

За время службы СКС ее конфигурация претерпевает множество изменений. Если каждое такое действие не документировать, впоследствии информация о соединениях будет утеряна и устранение неполадок в случае их возникновения займет много времени и приведет к неоправданным затратам.

- Неправильная организация кабельной проводки.

Ошибки, допускаемые техническим персоналом при проведении коммутаций, могут вызвать критический сбой в работе сети или нарушить режим безопасности доступа к конфиденциальной информации. При применении двухрядных панелей в кроссовых (серверных) комнатах коммутация осуществляется с помощью коммутационных шнуров, подключаемых к портам на лицевой

поверхности панелей. Если не нанести специальную маркировку на кроссовые панели, существует опасность ошибки при коммутации, и поиск неисправностей в данном случае отнимет много времени.

При формировании системы безопасности необходимо помнить, что кроссовая комната с точки зрения доступа к информации – одно из самых незащищенных мест *СКС*. В случае использования системы коммутационных шнуров для коммутации линий связи на коммутационных панелях *злоумышленник* может мгновенно изменить порядок соединений либо подключить в разрыв устройство съема/записи информации, т. е. легко разорвать соединение любого пользователя с сетью передачи данных и речи или перехватить и записать весь информационный обмен, оставаясь при этом незамеченным.

Тема : **Механизмы защиты информации**

Одним из условий безопасной работы в информационной системе является соблюдение пользователем ряда правил, которые проверены на практике и показали свою высокую эффективность. Их несколько:

1. Использование программных продуктов, полученных законным официальным путем. Вероятность наличия вируса в пиратской копии во много раз выше, чем в официально полученном программном обеспечении.

2. Дублирование информации. Прежде всего, необходимо сохранять дистрибутивные носители программного обеспечения. При этом запись на носители, допускающие выполнение этой операции, должна быть, по возможности, заблокирована. Следует особо позаботиться о сохранении рабочей информации. Предпочтительнее регулярно создавать копии рабочих файлов на съемных машинных носителях информации с защитой от записи. Копируется либо весь файл, либо только вносимые изменения. Последний вариант применим, например, при работе с базами данных.

3. Регулярное обновление системного ПО. Операционную систему необходимо регулярно обновлять и устанавливать все исправления безопасности от Microsoft и других производителей, чтобы устранить существующие уязвимости программного обеспечения.

4. Ограничение доступа пользователей к настройкам операционной системы и системным данным. Для обеспечения стабильной работы системы довольно часто требуется ограничивать возможности пользователей, что можно сделать либо с помощью встроенных средств Windows, либо с помощью специализированных программ, предназначенных для управления доступом к компьютеру.

В корпоративных сетях возможно применение групповых политик в сети домена Windows.

5. Для максимально эффективного использования сетевых ресурсов необходимо вводить ограничения доступа авторизованных пользователей к внутренним и внешним сетевым ресурсам и блокировать доступ неавторизованных пользователей.

6. Регулярное использование антивирусных средств. Перед началом работы целесообразно выполнять программы-сканеры и программы-ревизоры. Антивирусные базы должны

регулярно обновляться. Кроме того, необходимо проводить антивирусный контроль сетевого трафика.

7. Защита от сетевых вторжений обеспечивается применением программно-аппаратных средств, в том числе: использованием межсетевых экранов, систем обнаружения/предотвращения вторжений IDS/IPS (Intrusion Detection/Prevention System), реализацией технологий VPN (Virtual Private Network).

8. Применение средств аутентификации и криптографии – использование паролей (простых/сложных/неповторяющихся) и методов шифрования. Не рекомендуется использовать один и тот же пароль на разных ресурсах и разглашать сведения о паролях. При написании пароля на сайтах следует быть особенно внимательным, чтобы не допустить ввода своего пароля на мошенническом сайте-двойнике.

9. Особую осторожность следует проявлять при использовании новых (не известных) съемных носителей информации и новых файлов. Новые съёмные носители обязательно должны быть проверены на отсутствие загрузочных и файловых вирусов, а полученные файлы – на наличие файловых вирусов. При работе в распределенных системах или в системах коллективного пользования новые сменные носители информации и вводимые в систему файлы целесообразно проверять на специально выделенных для этой цели компьютерах, не подключенных к локальной сети. Только после всесторонней антивирусной проверки дисков и файлов они могут передаваться пользователям системы.

10. При работе с полученными (например, посредством электронной почты) документами и таблицами целесообразно запретить выполнение макрокоманд средствами, встроенными в текстовые и табличные редакторы (MS Word, MS Excel), до завершения полной проверки этих файлов.

11. Если не предполагается осуществлять запись информации на внешние носители, то необходимо заблокировать выполнение этой операции, например, программно отключив USB-порты.

12. При работе с общими ресурсами в открытых сетях (например, Интернет) использовать только проверенные сетевые ресурсы, не имеющие вредоносного контента. Не следует доверять всей поступающей на компьютер информации – электронным письмам, ссылкам на Web-сайты, сообщениям на Интернет-пейджеры. Категорически не рекомендуется открывать файлы и ссылки, приходящие из неизвестного источника.

Постоянное следование приведенным рекомендациям позволяет значительно уменьшить вероятность заражения программными вирусами и защищает пользователя от безвозвратных потерь информации. Однако даже при скрупулезном выполнении всех правил профилактики возможность заражения ПК компьютерными вирусами полностью исключить нельзя, поэтому методы и средства противодействия вредоносному ПО необходимо постоянно совершенствовать и поддерживать в работоспособном состоянии.

Тема : Антивирусные средства защиты информации

Массовое распространение вредоносного программного обеспечения, серьезность последствий его воздействия на информационные системы и сети вызвали необходимость разработки и использования специальных ***антивирусных средств*** и методов их применения.

Нужно отметить, что не существует антивирусных средств, гарантирующих обнаружение всех возможных программ-вирусов.

Антивирусные средства применяются для решения следующих задач:

- обнаружение вредоносного ПО в информационных системах;
- блокирование работы вредоносного ПО;
- устранение последствий воздействия вредоносного ПО.

Обнаружение вредоносного ПО желательно осуществлять на стадии его внедрения в систему или, по крайней мере, до начала осуществления им деструктивных действий. При обнаружении такого программного обеспечения или его деятельности необходимо сразу же прекратить работу программы-вируса в целях минимизации ущерба от ее воздействия на систему.

Устранение последствий воздействия вирусов ведется в двух направлениях:

- удаление вирусов;
- восстановление (при необходимости) файлов, областей памяти.

Процедуру удаления обнаруженного вредоносного кода из зараженной системы необходимо выполнять крайне аккуратно. Часто вирусы и троянские программы предпринимают специальные действия, чтобы скрыть факт своего присутствия в системе, или встраиваются в нее так глубоко, что задача его уничтожения становится достаточно нетривиальной.

Восстановление системы зависит от типа вируса, а также от времени его обнаружения по отношению к началу деструктивных действий. В том случае, когда программа-вирус уже запущена в системе и ее деятельность предусматривает изменение или удаление данных, восстановление информации (особенно, если она не продублирована) может быть невыполнимо.Для борьбы с вирусами используются программные и программно-аппаратные средства, которые применяются в определенной последовательности и комбинации, образуя методы защиты от вредоносного ПО.

Известны следующие методы обнаружения вирусов, активно применяемые современными антивирусными средствами:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- использование резидентных сторожей;
- использование программно-аппаратной защиты от вирусов.

Сканирование – один из самых простых методов обнаружения вирусов, осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса – ***сигнатуры***. Под сигнатурой понимается уникальная последовательность байтов, принадлежащая конкретному вирусу и не встречающаяся в других программах.

Программа фиксирует наличие уже известных вирусов, для которых сигнатура определена. Для эффективного применения антивирусных программ, использующих метод сканирования, необходимо регулярное обновление сведений о новых вирусах.

Метод ***обнаружения изменений*** базируется на использовании программ-ревизоров, которые следят за изменениями файлов и дисковых секторов на компьютере. Любой вирус каким-либо образом изменяет систему данных на диске. Например, может измениться загрузочный сектор, появиться новый исполняемый файл или измениться уже существующий, и т.п.

Как правило, антивирусные программы-ревизоры определяют и запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров диска. Периодически ревизор проверяет текущее состояние областей дисков и файловой системы, сравнивает с предыдущим состоянием и немедленно выдает сообщения обо всех подозрительных изменениях.

Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов.

Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе.

Эвристический анализ, как и метод обнаружения изменений, позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе.

Эвристический анализ в антивирусных программах основан на сигнатурах и эвристическом алгоритме, призван улучшить способность программ-сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда код неизвестной программы совпадает с сигнатурой не полностью, но в подозрительной программе явно выражены более общие признаки вируса либо его поведенческая модель. При обнаружении подобных кодов, выдается сообщение о возможном заражении. После получения таких сообщений необходимо тщательно проверить предположительно зараженные файлы и загрузочные сектора всеми имеющимися антивирусными средствами.

Недостатком данного метода является большое количество ложных срабатываний антивирусных средств в тех случаях, когда в легальной программе присутствуют фрагменты кода, выполняющего действия и/или последовательности, свойственные некоторым вирусам.

Метод ***использования резидентных сторожей*** основан на применении программ, которые постоянно находятся в оперативной памяти устройства (компьютера) и отслеживают все действия, выполняемые остальными программами. В случае выполнения какой-либо программой подозрительных действий, свойственных вирусам (обращение для записи в загрузочные сектора,

помещение в оперативную память резидентных модулей, попытки перехвата прерываний и т.п.), резидентный сторож выдает сообщение пользователю.

Применение антивирусных программ с резидентным сторожем снижает вероятность запуска вирусов на компьютере, но следует учитывать, что постоянное использование ресурсов оперативной памяти под резидентные программы уменьшает объем памяти, доступной для других программ.

На сегодняшний день одним из самых надежных механизмов защиты информационных систем и сетей являются *программно-аппаратные средства*, как правило, включающие в себя не только антивирусные системы, но и обеспечивающие дополнительный сервис. Эта тема подробно рассмотрена в разделе "Программно-аппаратные средства обеспечения безопасности информационных сетей".

Тема: Криптографические методы защиты информации

Криптографические методы защиты информации – это мощное оружие в борьбе за информационную безопасность.

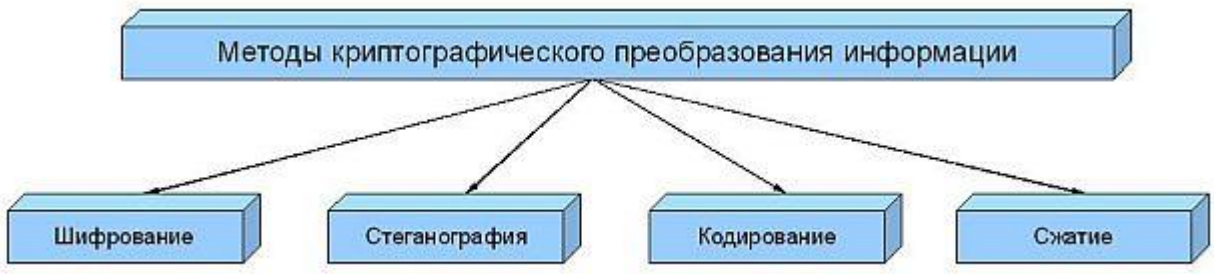
Криптография (от древне-греч. κρυπτος – скрытый и γραφω – пишу) – наука о методах обеспечения конфиденциальности и аутентичности информации.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы:



увеличить изображение

Рис. 2.1. Классификация методов криптографического преобразования информации

Процесс ***шифрования*** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых

зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются **алгоритм преобразования** и **ключ**. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Операнд – это константа, переменная, функция, выражение и другой объект языка программирования, над которым производятся операции.

В отличие от других методов криптографического преобразования информации, методы ***стеганографии*** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих. Обработка мультимедийных файлов в информационных системах открыла практически неограниченные возможности перед стеганографией.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение.

Скрытый файл также может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса ***кодирование*** информации является замена исходного смысла сообщения (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков. При кодировании и обратном преобразовании используются специальные таблицы или словари. В информационных сетях кодирование исходного сообщения (или сигнала) программно-аппаратными средствами применяется для повышения достоверности передаваемой информации.

Часто кодирование и шифрование ошибочно принимают за одно и тоже, забыв о том, что для восстановления закодированного сообщения, достаточно знать правило замены, в то время как для расшифровки сообщения помимо знания правил шифрования, требуется ключ к шифру.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации.

Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени передачи данных целесообразно совмещать процесс сжатия и шифрования информации.

Основным видом криптографического преобразования информации в компьютерных сетях является ***шифрование***. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. ***Методом шифрования (шифром)*** называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление компьютеров и компьютерных сетей инициировало процесс разработки новых шифров, учитывающих возможности использования компьютерной техники как для зашифрования/расшифрования информации, так и для атак на шифр. ***Атака на шифр (криптоанализ, криптоатака)*** – это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

Работа простой криптосистемы проиллюстрирована на рис. 2.2.

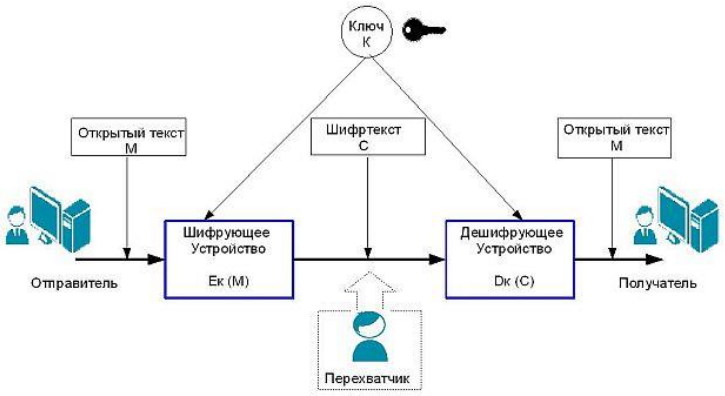


Рис. 2.2. Обобщённая схема криптографической системы

Отправитель генерирует открытый текст исходного сообщения **М**, которое должно быть передано законному получателю по незащищённому каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения **М**, отправитель шифрует его с помощью обратимого преобразования **Ек** и получает шифртекст (или криптограмму) **С=Ек(М)** , который отправляет получателю.

Законный получатель, приняв шифртекст **С**, расшифровывает его с помощью обратного преобразования **Дк(С)** и получает исходное сообщение в виде открытого текста **М**.

Преобразование **Ек** выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное преобразование, называется криптографическим ключом **К**.

Криптосистема имеет разные варианты реализации: набор инструкций, аппаратные средства, комплекс программ, которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа **К**.

Преобразование шифрования может быть **симметричным** и **асимметричным** относительно преобразования расшифрования. Это важное свойство определяет два класса криптосистем:

- симметричные (одноключевые) криптосистемы;
- асимметричные (двухключевые) криптосистемы (с открытым ключом).

Симметричное шифрование

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных. Для того чтобы обеспечить конфиденциальность данных, пользователи должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий (секретный) ключ, который будет использоваться с принятым ими алгоритмом шифрования/дешифрования, т.е. один и тот же ключ используется и для зашифрования, и для расшифрования (слово "симметричный" означает одинаковый для обеих сторон).

Пример симметричного шифрования показан на рис. 2.2.

Сегодня широко используются такие алгоритмы шифрования, как Data Encryption Standard (DES), 3DES (или "тройной DES") и International Data Encryption Algorithm (IDEA). Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов:

- электронной кодовой книги (Electronic Code Book, ECB);
- цепочки зашифрованных блоков (Cipher Block Changing, CBC);
- x-битовой зашифрованной обратной связи (Cipher FeedBack, CFB-x);
- выходной обратной связи (Output FeedBack, OFB).

Triple DES (3DES) – симметричный блочный шифр, созданный на основе алгоритма DES, с целью устранения главного недостатка последнего – малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше. Время, требуемое для криптоанализа 3DES, может быть намного больше, чем время, нужное для вскрытия DES.

Алгоритм ***AES*** (Advanced Encryption Standard), также известный как Rijndael – симметричный алгоритм блочного шифрования – шифрует сообщения блоками по 128 бит, использует ключ 128/192/256 бит.

Шифрование с помощью секретного ключа часто используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых "вшитых" программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных.

С методом симметричного шифрования связаны следующие проблемы:

- необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия (компрометации);
- достаточно сложно обеспечить безопасность секретных ключей при их генерировании, распространении и хранении.

Тема : Механизмы защиты информации

- **Асимметричное шифрование**
- Асимметричное шифрование часто называют шифрованием с помощью **открытого ключа**, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Отношение между ключами является математическим – один ключ зашифровывает информацию, а другой ее расшифровывает.
- Асимметричное шифрование – система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации цифровой подписи и для расшифрования сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в защищенных протоколах

передачи данных **TLS** и его предшественнике **SSL** (лежащих в основе протокола **HTTPS**), в протоколе безопасного удаленного управления **SSH**. Также используется в протоколах шифрования электронной почты **PGP** и **S/MIME**.

- Для того чтобы установить связь с использованием шифрования через открытый ключ, обеим сторонам нужно получить два ключа: открытый K_1 и частный (секретный) K_2 (рис. 2.3). Для шифрования и расшифровки данных обе стороны будут пользоваться разными ключами.

- В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищённому схеме распространения ключей (например из рук в руки или с помощью поверенного курьера). В асимметричной криптосистеме по подобной схеме передается только открытый ключ, а частный (секретный) ключ хранится на месте его генерации (у владельца).

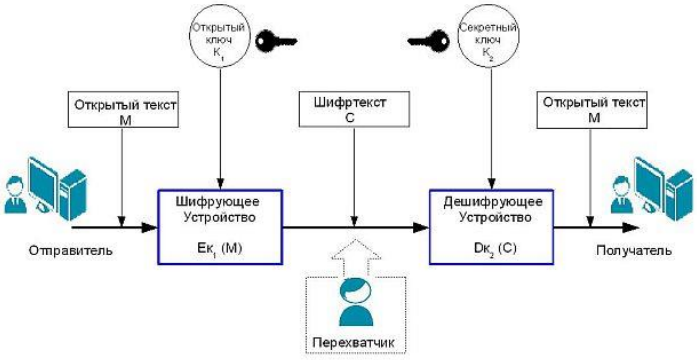
- 

Рис. 2.3. Обобщенная схема асимметричной криптосистемы

- Механизмы генерирования пар открытых/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится открытым ключом, а другое – секретным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары открытых/частных ключей. Алгоритмы шифрования с использованием открытых ключей часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

- Среди наиболее известных алгоритмов открытых ключей можно назвать **RSA** (Rivest-Shamir-Adleman) и **DSA** (Digital Signature Algorithm). Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм DSA применяется для создания цифровой подписи, но не для шифрования

- При использовании алгоритма RSA можно не только использовать открытый ключ для зашифрования, а секретный для расшифрования, но и наоборот: данные можно зашифровать с помощью секретного ключа, а открытый ключ применять при расшифровывании данных. Конечно, такой способ не дает возможность сохранять секреты, поскольку открытый ключ свободно доступен и любой может расшифровать информацию, но это дает способ поручиться за целостность содержимого сообщения: если открытый ключ правильно расшифровывает данные, значит, они были зашифрованы с помощью секретного ключа. Такой метод

называется ***электронной цифровой подписью***. Идея применения цифровой подписи строится на двух основных предположениях: во-первых, что секретный ключ уникален и защищен (только владелец ключа имеет к нему доступ), и, во-вторых, единственным способом поставить цифровую подпись является применение этого секретного ключа.

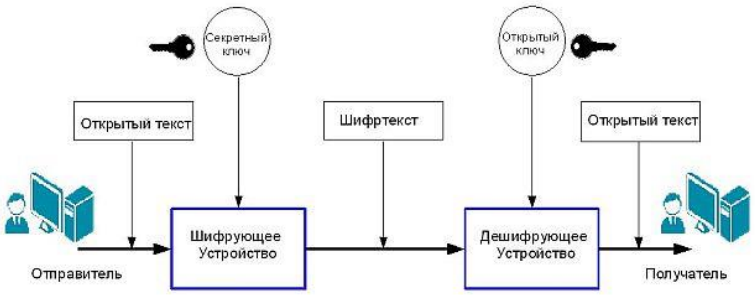


Рис. 2.4. Применение цифровой подписи

- Если данные зашифрованы с помощью не секретного ключа отправителя, а, например, открытого ключа или какого-либо другого, то получатель, расшифровав данные с использованием открытого ключа, получит не открытый текст сообщения, а бессмыслицу.

- Как правило, при создании цифровой подписи шифруется не весь открытый текст, а определенный фрагмент, так называемый ***дайджест сообщения*** (message digest), который генерируется (на основе вычислений) из исходного текста сообщения. К нему добавляется информация о том, кто подписывает документ. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись.

- Отправитель посылает дайджест сообщения вместе с этим сообщением. При приеме получателем производятся такие же вычисления дайджеста. Если в сообщение были внесены изменения, результат вычисления будет отличаться от полученного, что свидетельствует о том, что целостность сообщения нарушена.

- Алгоритм вычисления дайджеста принимает входные данные любой длины и преобразует их, чтобы получить псевдослучайный результат фиксированной длины. Другой термин, часто использующийся для дайджеста сообщений, – это хэш.

- ***Хэш (hash)*** – это результат преобразования входных данных произвольной длины в данные фиксированной длины. Функция, с помощью которой реализуется это преобразование, называется *функция хэширования* или *хэш-функция*.

- В криптографии принято выделять *криптографически стойкие* хэш-функции, удовлетворяющие следующим условиям: во-первых, необратимость (т.е. невозможность восстановления исходного текста по результатам вычислений) и, во-вторых, стойкость к коллизиям. Коллизия – это ситуация, когда двум сообщениям соответствует один и тот же хэш. Наиболее часто в качестве алгоритма хэширования используется алгоритм **MD5** (генерируется 128-битное значение) или **SHA-1** (генерируется 160-битное значение).

- Хэш-функции широко применяются при создании пользовательских паролей, когда строка произвольной длины (пароль) преобразуется в указанный ключ заранее заданной длины, и для проверки целостности данных, когда данные отправляются вместе с контрольным значением.

- **Сертификаты открытых ключей**

- Криптография с открытым ключом предоставляет не только мощный механизм для шифрования, но и средства идентификации и аутентификации пользователей и устройств. Однако, если между отправителем и получателем нет конфиденциальной схемы передачи асимметричных ключей, то возникает серьезная опасность появления злоумышленника-посредника. Ручное распространение ключей становится непрактичным и создает бреши в системе безопасности. По этим причинам было разработано другое решение – применение ***сертификатов открытых ключей***.

- В своей основной форме сертификатом называется информационный пакет, содержащий открытый ключ, электронную подпись, подтверждающую этот ключ, и имя доверенной третьей стороны, удостоверяющей достоверность этих фактов. Третья сторона, которой доверяют пользователи и которая подтверждает идентичность пользователя и его права, называется ***удостоверяющим центром CA (Certificate Authority)*** или ***центром сертификации*** . CA создает сертификаты пользователей, включающие следующую информацию: имя пользователя (сюда же относится пароль и другие дополнительные сведения, однозначно идентифицирующие этого пользователя), открытый ключ пользователя, время действия сертификата, конкретные операции, в которых этот ключ может быть использован (идентификация, шифрование). Удостоверяющий центр полностью ответственен за аутентичность своих конечных пользователей.

- Удостоверяющие центры можно разделить на 2 категории: открытые и частные. Открытые CA действуют через Интернет, предоставляя услуги сертификации всем желающим. Частные CA, как правило, принадлежат организациям или закрытым сетям и выдают сертификаты только пользователям локальных сетей.

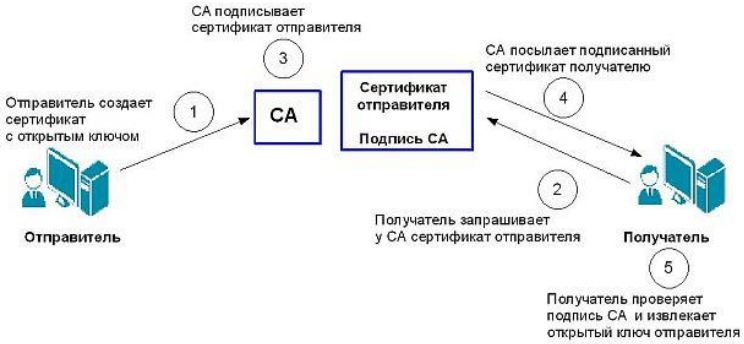


Рис. 2.5. Выдача сертификатов удостоверяющим центром CA

- Наиболее широко распространенным форматом сертификатов, принятым для технологии открытых ключей, является *стандарт X.509 v.3*, описанный в документах RFC 2459 и RFC 5280.

- Надежной системой распространения открытого ключа СА является *инфраструктура открытых ключей PKI (Public Key Infrastructure)*, которая определяет взаимодействие между конечными пользователями и доверяющими сторонами, предоставляя возможность безопасно выпускать и работать с сертификатами.

- Криптографические средства широко применяются в различных программно-аппаратных элементах системы защиты информации, таких как межсетевые экраны, Интернет-маршрутизаторы, концентраторы доступа. Один из примеров реализации программно-аппаратной криптографической системы представлен комплексом "КРИПТОН" фирмы "Анкад". Программный комплекс *Crypton IPMobile* предназначен для организации виртуальной частной сети (VPN).

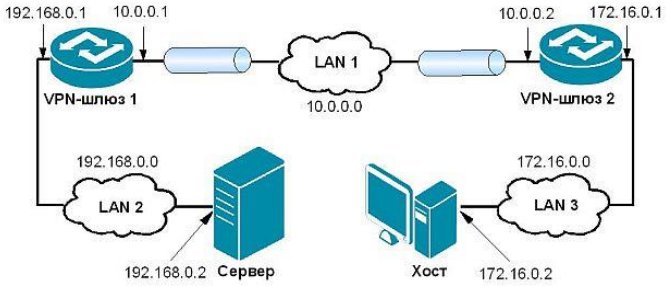


Рис. 2.6. Типичная схема организации частной виртуальной сети с использованием VPN-шлюзов

- Crypton IPMobile может работать на основе концентратора доступа **D-Link DSA-3110**.

- 

- **Рис. 2.7.** Crypton-VPN на базе концентратора доступа D-Link DSA-3110

- Программно-аппаратный комплекс **Crypton-VPN DSA-3110** обладает функциональностью криптографического маршрутизатора с применением шифрования. Концентратор доступа DSA-3110 представляет собой систему обеспечения доступа к сети с использованием технологии VPN, которая интеллектуально управляет аутентификацией, авторизацией и учетом подключающихся пользователей. Это устройство обеспечивает сеть полным набором функций, включая управление учетными записями и выдачу статистики по трафику с использованием технологии NetFlow.

- **Безопасность сетевого доступа**

- Концентратор доступа DSA-3110 обеспечивает клиентским компьютерам удобный и безопасный способ предоставления доступа к сети оператора/глобальной сети. Система гарантирует, что только зарегистрированные пользователи смогут использовать ресурсы сети. Используемые технологии доступа VPN (PPTP или PPPoE) позволяют надежно авторизовать пользователей и обеспечить защищенное и безопасное подключение. Активирование режима криптографического маршрутизатора и инициализация ключей и политики осуществляется с помощью информации, записанной на сменный носитель Touch Memory (TM).

- **Выполнение функций AAA**
- DSA-3110 выполняет 3 основные функции – аутентификацию, авторизацию и учет (Authentication, Authorization and Accounting (AAA)), которые часто встречаются во многих сетевых сервисах. Примером этих сервисов является доступ в Интернет через телефонную линию, электронная коммерция, печать через Интернет. Аутентификация выполняет проверку идентичности для авторизации доступа к сетевому ресурсу. Для учета использования ресурсов выдаются данные статистики подключений и соответствующая информация о трафике с целью анализа тенденций, планирования пропускной способности, биллинга, аудита и распределения затрат.
- **Использование в сетях операторов**
- DSA-3110 также может использоваться в коммерческих сетях, предоставляя сервисы клиентам (рис. 2.8). Для того чтобы удостовериться, что пользователь является именно тем, кем он себя заявил, необходима аутентификация. После того, как пользователь будет аутентифицирован, необходимо удостовериться, что он авторизован на выполнение тех операций, которые запрашивает. Авторизация обычно обеспечивается путем использования списков доступа или политик безопасности.
- **Использование в компаниях**
- Зачастую при предоставлении сотрудникам доступа в глобальную сеть предприятию необходимо разграничить доступ своих сотрудников к различным службам (рис. 2.9). DSA-3110 позволяет инициировать и использовать различные гибкие правила доступа к сети оператора/глобальной сети на основании множества критериев, таких как: адрес/служба/протокол/порт. Использование режима криптомаршрутизатора базируется на статических IP-адресах клиентов. При этом DSA-3110 является аппаратным межсетевым экраном (Firewall), что позволяет организовать защиту сети предприятия от внешних атак. Так же устройство позволяет сотрудникам, находящимся за пределами компании, получить защищенный доступ в локальную сеть предприятия.
- 

- **Рис. 2.8.** Схема применения DSA-3110 в сети оператора

Рис. 2.9. Схема применения DSA-3110 в сети компании

Тема: Способы предотвращения удаленных атак на информационные системы

Удаленные атаки были бы не осуществимы, если бы на каждое сетевое соединение была выделена отдельная линия связи, но инфраструктура сетей общего пользования не предусматривает соединения по принципу выделенного канала для каждого сетевого объекта. Альтернативой выделенному каналу связи стало использование защищенных виртуальных соединений по технологиям VPN (Virtual Private Network – виртуальные частные сети). Данному механизму посвящен отдельный раздел "Виртуальные частные сети (VPN)".

Задача идентификации и аутентификации пользователей в распределенной сети имеет чрезвычайно важное значение. От успеха ее решения зависит безопасность информационной системы в целом. Как выше было рассмотрено, стандартными способами компрометации пользователей злоумышленником являются:

- выдача себя за легального пользователя с присвоением его прав и полномочий для доступа в систему (например, типовая удалённая атака "MITM");
- внедрение в систему ложного объекта, выдающего себя за доверенный объект системы (например, типовая удалённая атака "Ложный объект сети").

Исходя из того, что стандартные методы идентификации и аутентификации (имя/ пароль) в информационных системах не достаточны для защиты от удалённых атак на неё, необходимо введение дополнительных средств идентификации объектов в информационной сети и *криптозащиты* передаваемой в ней информации.

При создании виртуального канала могут использоваться криптоалгоритмы с открытым ключом (например, SSL – Secret Socket Layer). Как упоминалось ранее, основная идея заключается в способе шифрования с двумя ключами, при котором *ключ шифрования* и *ключ для дешифровки* отличаются друг от друга, причем последний нельзя определить по первому. Суть криптографии с открытым ключом (или двухключевой криптографии) заключается в том, что ключи, имеющиеся в криптосистеме, входят в нее парами и каждая пара удовлетворяет следующим двум свойствам:

- информация, зашифрованная на одном ключе, может быть дешифрована на другом;
- знание одного ключа не позволяет вычислить другой.

Поэтому один из ключей может быть опубликован. При опубликованном (открытом) ключе шифрования и секретном ключе дешифрования получается ***система шифрования с открытым ключом***. Каждый пользователь сети связи может зашифровать сообщение при помощи открытого ключа, а расшифровать его сможет только владелец секретного ключа. При опубликовании ключа дешифрования получается система цифровой подписи. Здесь только владелец секретного ключа

создания подписи может правильно зашифровать текст (т.е. подписать его), а проверить подпись (дешифровать текст) может любой на основании опубликованного ключа проверки подписи.

В 1976 г. У. Диффи и М. Хеллман предложили следующий метод открытого распределения ключей. Пусть два объекта А и В условились о выборе в качестве общей начальной информации большого простого числа **P** и большого простого числа **a**. Тогда эти пользователи действуют в соответствии с алгоритмом:

- А вырабатывает случайное число x, вычисляет число a^x (mod P) и посылает его В;
- В вырабатывает случайное число y, вычисляет число a^y (mod P) и посылает его А;
- затем А и В возводят полученное число в степень со своим показателем и получают число a^{xy} (mod P).

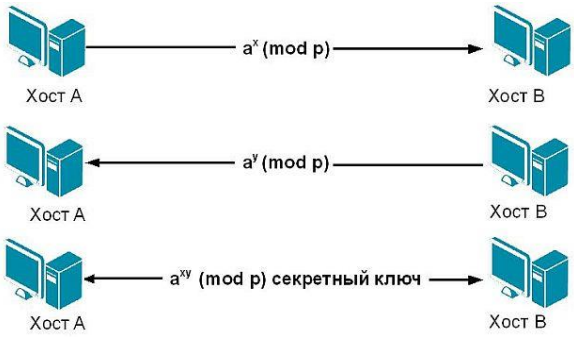


Рис. 2.10. Алгоритм В.Диффи и М.Хеллмана открытого распределения ключей

Следует отметить, что объекты А и В обменялись не своими секретными кодами, а только результатами mod-функций, что делает достаточно трудным провести обратную операцию для получения секретного ключа.

Это число и является сеансовым ключом для одноключевого алгоритма, например, DES. Для раскрытия этого ключа криптоаналитику необходимо по известным a^x (mod P), a^y (mod P) найти a^{xy} (mod P), т.е. найти x или y. Нахождение числа x по его экспоненте a^x (mod P) называется задачей дискретного логарифмирования в простом поле. Эта задача является труднорешаемой, и поэтому полученный ключ, в принципе, может быть стойким.

Особенность данного криптоалгоритма состоит в том, что перехват по каналу связи пересылаемых в процессе создания виртуального канала сообщений a^x (mod P) и a^y (mod P) не позволит атакующему получить конечный ключ шифрования a^{xy} (mod P). Этот ключ далее должен использоваться, во-первых, для цифровой подписи сообщений и, во-вторых, для их криптозащиты. Цифровая подпись сообщений позволяет надежно идентифицировать объект распределенной сети, который запрашивает доступ к ресурсам информационной системы по виртуальному каналу.

Защита от атаки "анализ сетевого трафика"

Анализ сетевого трафика относится к постоянно ожидаемой угрозе, которую невозможно устранить, но можно сделать бессмысленной для атакующего, если применять стойкие криптоалгоритмы в передаваемом потоке данных.

Для предоставления удаленного авторизованного доступа к ресурсам информационных систем не рекомендуется использовать протоколы удаленного доступа TELNET, HTTP и FTP, так как они не предусматривают элементарную криптозащиту передаваемых по сети идентификаторов (имен) и аутентификаторов (паролей). Использование защищенных протоколов обмена (таких как SSL, TLS, SSH, HTTPS) обеспечит защищенный удаленный доступ к ресурсам своих систем.

Для передачи конфиденциальной информации рекомендуется применять виртуальные каналы связи (VPN), подключения в которых обеспечиваются с использованием средств криптографии.

Защита от DoS-атак

Сегодня ряд компаний предлагает как программные средства защиты от DoS-атак, так и программно-аппаратные. Однако стопроцентной защиты от отказа в обслуживании для стандарта IPv4 в распределенной сети не существует. Это связано с тем, что в IPv4 невозможен контроль за маршрутом сообщений. Поэтому нельзя обеспечить надежный контроль за сетевыми соединениями, так как одним пользователем может быть занято неограниченное число каналов связи с удаленным объектом, и при этом сохраняется анонимность пользователя.

Тем не менее, выполняя определенные правила, можно значительно ослабить DoS-атаку и снизить ее воздействие на атакуемую систему. Ниже приведены рекомендации, применение которых позволит в определенной степени защититься от DoS-атак.

1. Для повышения надежности работы системы использовать как можно более мощные компьютеры. Чем больше число и частота работы процессоров, чем больше объем оперативной памяти, тем более надежной будет работа сетевой ОС, когда на нее обрушится направленный шторм ложных запросов на создание соединения. Кроме того, необходимо использование соответствующих вычислительным мощностям операционных систем с внутренней очередью, способной вместить большое число запросов на подключение.

2. Применение функций анти-DoS и анти-spoofing на межсетевых экранах и маршрутизаторах защищает систему от перегрузки за счет ограничения полуоткрытых каналов.

3. Регулярное обновление операционной системы и программного обеспечения.

4. Использование кластера серверов позволяет увеличить надежность и производительность работы в несколько раз по сравнению с обычным сервером.

5. При обнаружении атаки маскирование IP-адреса сервера.

Программно-аппаратные средства обеспечения безопасности информационных сетей

Как указывалось выше, система защиты информации – это комплекс мер, а также соответствующих им мероприятий, сил, средств и методов. Программно-аппаратный компонент системы защиты информации предназначен для защиты данных, обрабатываемых и хранящихся в компьютерах и серверах локальных сетей в различных информационных системах. Как правило, он реализует тесно взаимосвязанные процессы:

- управление доступом и управление политикой безопасности,
- идентификацию и аутентификацию пользователей,

- регистрацию событий и аудит,
- криптографическую защиту,
- сетевую защиту,
- антивирусную защиту,
- обнаружение атак программными средствами (IDS – Intrusion Detection Systems).

Средства управления доступом позволяют разграничивать и контролировать выполняемые над информацией действия, которые совершаются пользователями (ограничение доступа на вход в систему, разграничение доступа авторизованных пользователей, запрет доступа неавторизованных пользователей и т.п.). То есть речь идет о логическом управлении доступом, который реализуется программными средствами. Контроль прав доступа осуществляется посредством различных компонентов программной среды – ядром сетевой операционной системы, системой управления базами данных, дополнительным программным обеспечением и т.д.

Идентификация предназначена для того, чтобы пользователь мог идентифицировать себя путем сообщения своего имени. С помощью аутентификации вторая сторона убеждается, что пользователь, пытающийся войти в систему, действительно тот, за кого себя выдает.

Регистрация событий (протоколирование, журналирование) – это процесс сбора и накопления информации о событиях, происходящих в информационной системе. Возможные события принято делить на две группы:

1. внешние события, вызванные действиями как авторизованных, так и неавторизованных пользователей;
2. внутренние события, вызванные действиями пользователей и администраторов. Аудитом называется процедура анализа накопленной в результате журналирования информации. Этот анализ может осуществляться оперативно, почти в реальном времени, или периодически.

Методы криптографии – одно из наиболее мощных средств обеспечения конфиденциальности и целостности информации. Как уже упоминалось, основной элемент криптографии – шифрование.

Сетевая защита, как правило, обеспечивается установкой на границе сетей так называемых экранов. Экран – это средство разграничения доступа пользователей из одного сетевого множества к ресурсам, принадлежащим другому сетевому множеству. Функция экрана заключается в контроле всех информационных потоков между двумя множествами систем. Примерами экранов являются межсетевые экраны, устанавливаемые для защиты локальной сети организации, имеющей выход в публичную сеть (такую как Интернет).

Помимо прочего, сегодня практически все производители программно-аппаратных средств обеспечения безопасности информации включают поддержку антивирусной защиты и систем обнаружения вторжений, обеспечивающих защиту от вредоносного ПО и атак.

Для примера приведем аппаратные межсетевые экраны **D-Link** серии **DFL**, обладающие функцией проверки трафика на наличие вредоносных программ. В частности, даже "младшая" модель **DFL-260/260E** позволяет сканировать на наличие вредоносного ПО файлы любого размера, используя

технологию потокового сканирования. Данный метод сканирования увеличивает производительность проверки, сокращая так называемые "узкие места" в сети. Межсетевые экраны серии DFL используют сигнатуры вирусов от антивирусной компании "Лаборатории Касперского" (Kaspersky Labs). При этом существует возможность обновления сигнатур. В результате вирусы и вредоносные программы могут быть эффективно заблокированы до того, как они достигнут устройств локальной сети.

Кроме того, для эффективной борьбы с вредоносным трафиком и для того, чтобы минимизировать влияние аварийной ситуации на всю сеть, межсетевые экраны компании D-Link (**DFL-800/860/860E/1600/1660/2500/2560**) поддерживают специальную функцию – **ZoneDefense**, представляющую собой механизм, позволяющий им работать с коммутаторами локальных сетей D-Link и обеспечивающий активную сетевую безопасность. Функция **ZoneDefense** автоматически изолирует инфицированные компьютеры локальной сети и предотвращает распространение ими вредоносного трафика. Более подробно аппаратные межсетевые экраны компании D-Link и о технологии **ZoneDefense** мы рассмотрим в следующих главах.

Рис. 2.11. DFL-260E – межсетевой экран NetDefend для сетей SOHO

Тема 2: Политика Безопасности.

Политика *безопасности*. Политика сетевой безопасности каждой организации должна включать (кроме всего прочего) две составляющие: политика доступа к сетевым сервисам и политика реализации межсетевых экранов.

Однако недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений – главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений).

Таким образом, управляющие решения требуют, чтобы межсетевой экран имел доступ, возможность анализа и использования следующих факторов:

- информации о соединениях – информация от всех семи уровней (модели OSI) в пакете;
- истории соединений – информация, полученная от предыдущих соединений;
- состоянии уровня приложения – информация о состоянии соединения, полученная из других приложений;
- манипулировании информацией – вычисление разнообразных выражений, основанных на всех вышеперечисленных факторах.

Типы межсетевых экранов

Различают несколько типов межсетевых экранов в зависимости от следующих характеристик:

- обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;
- происходит ли контроль потока данных на сетевом уровне или более высоких уровнях модели OSI;
- отслеживаются ли состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных межсетевые экраны подразделяются на:

- ***традиционный сетевой (или межсетевой) экран*** – программа (или неотъемлемая часть операционной системы) на шлюзе (устройстве, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями (объектами распределённой сети);
- ***персональный межсетевой экран*** – программа, установленная на пользова-тельском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

В зависимости от уровня OSI, на котором происходит контроль доступа, сетевые экраны могут работать на:

- *сетевом уровне*, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;
- *сеансовом уровне* (также известные, как **stateful**), когда отслеживаются сеансы между приложениями и не пропускаются пакеты, нарушающие спецификации TCP/IP, часто используемые в злонамеренных операциях – сканирование ресурсов, взломы через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных;
- *прикладном уровне* (или уровне приложений), когда фильтрация производится на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Фильтрация на сетевом уровне

Фильтрация входящих и исходящих пакетов осуществляется на основе информации, содержащейся в следующих полях TCP- и IP-заголовков пакетов: IP-адрес отправителя; IP-адрес получателя; порт отправителя; порт получателя.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются ненадежными.

К преимуществам такой фильтрации относится:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки:

- не собирает фрагментированные пакеты;
- нет возможности отслеживать взаимосвязи (соединения) между пакетами.?

Фильтрация на сеансовом уровне

В зависимости от отслеживания активных соединений межсетевые экраны могут быть:

- *stateless* (простая фильтрация), которые не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил;
- *stateful, stateful packet inspection (SPI)* (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений.

Межсетевые экраны с SPI позволяют эффективнее бороться с различными видами DoS-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как H.323, SIP, FTP и т. п., которые используют сложные схемы передачи данных между адресатами, плохо поддающиеся описанию статическими правилами, и зачастую несовместимых со стандартными, stateless сетевыми экранами.

К преимуществам такой фильтрации относится:

- анализ содержимого пакетов;
- не требуется информации о работе протоколов 7 уровня.

Недостатки:

- сложно анализировать данные уровня приложений (возможно с использованием ALG – Application level gateway).

Application level gateway, ALG (шлюз прикладного уровня) – компонент NAT-маршрутизатора, который понимает какой-либо прикладной протокол, и при прохождении через него пакетов этого протокола модифицирует их таким образом, что находящиеся за NAT’ом пользователи могут пользоваться протоколом.

Служба ALG обеспечивает поддержку протоколов на уровне приложений (таких как SIP, H.323, FTP и др.), для которых подмена адресов/портов (Network Address Translation) недопустима. Данная служба определяет тип приложения в пакетах, приходящих со стороны интерфейса внутренней сети и соответствующим образом выполняя для них трансляцию адресов/портов через внешний интерфейс.

Технология SPI (Stateful Packet Inspection) или технология инспекции пакетов с учетом состояния протокола на сегодня является передовым методом контроля трафика. Эта технология позволяет контролировать данные вплоть до уровня приложения, не требуя при этом отдельного приложения посредника или proxy для каждого защищаемого протокола или сетевой службы.

Исторически эволюция межсетевых экранов происходила от пакетных фильтров общего назначения, затем стали появляться программы-посредники для отдельных протоколов, и, наконец, была разработана технология stateful inspection. Предшествующие технологии только дополняли друг друга, но всеобъемлющего контроля за соединениями не обеспечивали. Пакетным фильтрам недоступна информация о состоянии соединения и приложения, которая необходима для принятия заключительного решения системой безопасности. Программы-посредники обрабатывают только данные уровня приложения, что зачастую порождает различные возможности для взлома системы. Архитектура stateful inspection уникальна потому, что она позволяет оперировать всей возможной информацией, проходящей через машину-шлюз: данными из пакета, данными о состоянии соединения, данными, необходимыми для приложения.

Пример работы механизма Stateful Inspection. Межсетевой экран отслеживает сессию FTP, проверяя данные на уровне приложения. Когда клиент запрашивает сервер об открытии обратного соединения (команда FTP PORT), межсетевой экран извлекает номер порта из этого запроса. В списке запоминаются адреса клиента и сервера, номера портов. При фиксировании попытки установить соединение FTP-data, межсетевой экран просматривает список и проверяет, действительно ли данное соединение является ответом на допустимый запрос клиента. Список соединений поддерживается динамически, так что открыты только необходимые порты FTP. Как только сессия закрывается, порты блокируются, обеспечивая высокий уровень защищенности.

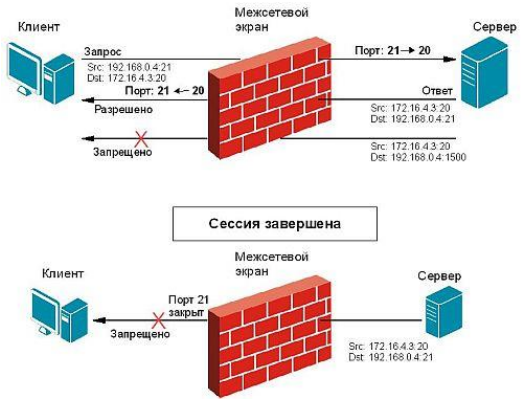


Рис. 2.12. Пример работы механизма Stateful Inspection с FTP-протоколом

Фильтрация на прикладном уровне

С целью защиты ряда уязвимых мест, присущих фильтрации пакетов, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как, например, Telnet, HTTP, FTP. Подобное приложение называется ***proxy-службой*** , а хост, на котором работает proxy-служба – шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне (уровне приложений – верхний уровень сетевой модели) и может анализировать содержимое данных, например, адрес URL, содержащийся в HTTP-сообщении, или команду, содержащуюся в FTP-сообщении. Иногда эффективнее бывает фильтрация пакетов, основанная на информации, содержащейся в самих данных. Фильтры пакетов и фильтры

уровня канала не используют содержимое информационного потока при принятии решений о фильтрации, но это можно сделать с помощью фильтрации уровня приложений. Фильтры уровня прил ожений могут использовать информацию из заголовка пакета, а также содержимого данных и информации о пользователе. Администраторы могут использовать фильтрацию уровня приложений для контроля доступа на основе идентичности пользователя и/или на основе конкретной задачи, которую пытается осуществить пользователь. В фильтрах уровня приложений можно установить правила на основе отдаваемых приложением команд. Например, администратор может запретить конкретному пользователю скачивать файлы на конкретный компьютер с помощью FTP или разрешить пользователю размещать файлы через FTP на том же самом компьютере.

К преимуществам такой фильтрации относится:

- простые правила фильтрации;
- возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием "дыр" в программном обеспечении;
- способность анализировать данные приложений.

Недостатки:

- относительно низкая производительность по сравнению с фильтрацией пакетов;
- proxy должен понимать свой протокол (невозможность использования с неизвестными протоколами)?;
- как правило, работает под управлением сложных ОС.

Сравнение аппаратных и программных межсетевых экранов

Для сравнения межсетевых экранов разделим их на два типа: 1-й – аппаратные и программно-аппаратные и 2-й – программные.

К аппаратным и программно-аппаратным межсетевым экранам относятся устройства, установленные на границе сети. Программные межсетевые экраны – это те, которые установлены на конечных хостах.

Основные направления, присущие и первому, и второму типам:

- обеспечение безопасности входящего и исходящего трафика;
- значительное увеличение безопасности сети и уменьшение риска для хостов подсети при фильтрации заведомо незащищенных служб;
- возможность контроля доступа к системам сети;
- уведомление о событиях с помощью соответствующих сигналов тревоги, которые срабатывают при возникновении какой-либо подозрительной деятельности (попытки зондирования или атаки);
- обеспечение недорогого, простого в реализации и управлении решения безопасности.

Аппаратные и программно-аппаратные межсетевые экраны дополнительно поддерживают функционал, который позволяет:

- препятствовать получению из защищенной подсети или внедрению в защищенную подсеть информации с помощью любых уязвимых служб;
- регистрировать попытки доступа и предоставлять необходимую статистику об использовании Интернет;
- предоставлять средства регламентирования порядка доступа к сети;
- обеспечивать централизованное управление трафиком.

Программные межсетевые экраны, кроме основных направлений, позволяют:

- контролировать запуск приложений на том хосте, где установлены;
- защищать объект от проникновения через "люки" (back doors);
- обеспечивать защиту от внутренних угроз.

Межсетевой экран не является симметричным устройством. Он различает понятия: "снаружи" и "внутри". Межсетевой экран обеспечивает защиту внутренней области от неконтролируемой и потенциально враждебной внешней среды. В то же время межсетевой экран позволяет разграничить доступ к объектам общедоступной сети со стороны субъектов защищенной сети. При нарушении полномочий работа субъекта доступа блокируется, и вся необходимая информация записывается в журнал.

Межсетевые экраны могут использоваться и внутри защищенных корпоративных сетей. Если в локальной сети имеются подсети с различной степенью конфиденциальности информации, то такие фрагменты целесообразно отделять межсетевыми экранами. В этом случае экраны называют внутренними.

Тема: Механизмы защиты информации

Прокси-сервер

Прокси-сервер (proxy – представитель, уполномоченный) – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (cache) (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Proxy являются попыткой реализовать межсетевой экран на уровне приложения. Их основное преимущество – поддержка полной информации о приложениях. Proxy обеспечивают частичную информацию об истории соединений, полную информацию о приложении и частичную информацию о текущем соединении и имеют возможность обработки и действий над информацией.

Однако имеются очевидные трудности в использовании proxy на уровне приложения в качестве межсетевого экрана:

- Ограничения на соединения – каждый сервис требует наличия своего собственного прокси, поэтому число доступных сервисов и их масштабируемость ограничены.
- Ограничения технологии – шлюз прикладного уровня (ALG) не может обеспечить прокси для протокола UDP.
- Производительность – реализация на уровне приложения имеет значительные потери в производительности.

В добавление, proxy беззащитны к ошибкам в приложениях и ОС, неверной информации в нижних уровнях протоколов и в случае традиционных прокси-серверы очень редко являются прозрачными.

Исторически proxy уровня приложений удовлетворяли общему их применению и нуждам сети Интернет. Однако, по мере превращения Интернета в постоянно меняющуюся динамичную среду, предлагающую новые протоколы, сервисы и приложения, proxy более не способны обработать различные типы взаимодействий в сети Интернет или отвечать новым нуждам бизнеса, высоким требованиям к пропускной способности и безопасности сетей.

Интернет-маршрутизатор

Так называемые *классические маршрутизаторы* действуют на сетевом уровне, и их очевидным недостатком является неспособность обеспечивать безопасность даже для наиболее известных сервисов и протоколов. Маршрутизаторы не являются устройствами обеспечения безопасности, так как они не имеют основных возможностей межсетевого экрана:

- информации о соединении – маршрутизаторы имеют доступ лишь к ограниченной части заголовка пакетов;
- наследуемой информации о соединении и приложении – маршрутизаторы не поддерживают хранение информации об истории соединения или приложения;
- манипулирований информацией – маршрутизаторы имеют очень ограниченные возможности по действиям над информацией.

К тому же, маршрутизаторы достаточно сложно конфигурировать, следить за их состоянием и управлять. Они не обеспечивают должного уровня журналирования событий и механизмов оповещения.

В последнее время получили распространение устройства класса SOHO (Small Office/Home Office), значительно упрощающие задачу подключения локальной вычислительной сети к сети Интернет и условно называемые ***Интернет-маршрутизаторами*** . Как правило, Интернет-маршрутизатор – это аппаратное решение с одним (или несколькими) портом WAN для подключения к сети общего пользования (Интернет) и несколькими (чаще четыре) портами LAN для подключения рабочих станций локальной сети. Иногда Интернет-маршрутизатор оборудован беспроводной точкой доступа

для организации связи в локальной сети с беспроводными клиентами. Может оснащаться USB-портом для подключения принтера и/или других устройств (например, 3G-модема).

Интернет-маршрутизатор разработан для совместного доступа группы пользователей к широкополосному Интернет-соединению через выделенную линию, DSL или кабельный модем. Кроме того, в качестве дополнительного канала возможно применение Wimax / 3G-модемов, обеспечивающих доступ в Интернет через Wimax / 3G-сети.

Интернет-маршрутизатор оснащен встроенным межсетевым экраном для защиты компьютеров в сети от вирусных и DoS-атак. Управление доступом осуществляется с помощью фильтрации пакетов на основе MAC-адресов источника и приемника.

Маршрутизатор может быть настроен таким образом, что отдельные FTP, Web- и игровые серверы смогут совместно использовать один, видимый извне IP-адрес, и в тоже время останутся защищенными от атак хакеров. Пользователи через Web-интерфейс маршрутизатора могут настроить любой (или конкретно выделенный производителем для этой цели) из LAN-портов как DMZ-порт (см. раздел "Механизмы PAT и NAT"). В последнее время всё чаще стала присутствовать функция "родительского" контроля (Parental control), которая позволяет фильтровать нежелательные URL-адреса Web-сайтов, блокировать домены и управлять использованием Интернет по расписанию.

Поддержка Интернет-маршрутизаторами технологии QoS (см. раздел "Качество обслуживания (QoS) и управление полосой пропускания трафика (Traffic Shaping)") обеспечивает более эффективную передачу приложений, чувствительных к задержкам, таких как Интернет-телефония (VoIP), мультимедиа и игры по Интернет.

Таблица 2.1. Стандартный набор возможностей Интернет-маршрутизаторов и используемых в работе технологий

Типы подключения WAN:

- Static IP
- Dynamic IP
- PPPoE
- L2TP
- PPTP
- DualAccess PPPoE
- DualAccess PPTP

Поддержка VPN:

- PPTP pass-through
- IPSec pass-through
- L2TP pass-through

Функции Интернет-шлюза:

- Преобразование сетевых адресов (NAT)
- DHCP-сервер (для автоматического назначения параметров IP)

Управление доступом пользователей:

- Фильтрация MAC-адресов
- Фильтрация по расписанию

Межсетевой экран:

- NAT (преобразование сетевых адресов) с VPN pass-through
- SPI (Stateful Packet Inspection)

Фильтрация Web-сайтов с помощью фильтрации URL-адресов.

Приоритизация VoIP-трафика и потоковых медиафайлов при приеме/передаче.

Широковещательный поток IGMP (Internet Group Management Protocol)

Рис. 2.13. DIR-857 – Высокопроизводительный двухдиапазонный беспроводной Интернет-маршрутизатор D-Link, оснащенный 4 портами Gigabit Ethernet, портом USB 3.0 и слотом для SD-карты

Тема : Технологии безопасности беспроводных сетей и унифицированные решения

Технологии безопасности беспроводных сетей

Говоря о сетевой безопасности как части информационной безопасности объекта, нельзя обойти стороной тему о методах защиты беспроводных сегментов компьютерной сети.

Как уже упоминалось ранее, существует множество технологий, призванных повысить сетевую *безопасность*, и все они предлагают решения для важнейших компонентов политики в области защиты данных: *аутентификации*, поддержания *целостности данных* и *активной проверки*. Под ***аутентификацией*** подразумевается *аутентификация* пользователя или конечного устройства (*хост* клиента, *сервер*, *коммутатор*, *маршрутизатор*, *межсетевой экран* и т.д.) и его местоположения с последующей авторизацией пользователей и конечных устройств. ***Целостность данных*** включает такие области, как *безопасность* сетевой инфраструктуры, *безопасность* периметра и *конфиденциальность* данных. ***Активная проверка*** помогает удостовериться в том, что установленная политика в области безопасности выдерживается на практике, и отследить все аномальные случаи и попытки несанкционированного доступа.

Стандарт *IEEE* 802.11 с традиционной безопасностью (Tradition *Security Network*, TSN) предусматривает два механизма аутентификации беспроводных клиентов: **открытую аутентификацию** (*Open Authentication*) и **аутентификацию с общим ключом** (Shared Key *Authentication*). Для аутентификации в беспроводных сетях также широко используются два других механизма, которые не являются частью стандарта 802.11, а именно –

назначение **идентификатора беспроводной локальной сети** (*Service Set Identifier, SSID*) и **аутентификация клиента по его MAC-адресу** (*MAC Address Authentication*).

Идентификатор беспроводной локальной сети (SSID) представляет собой *атрибут* беспроводной сети (так называемое имя сети), позволяющий логически отличать сети друг от друга. Когда *пользователь* пытается войти в *сеть*, беспроводной *адаптер* с помощью программы, прежде всего, сканирует *пространство* на предмет наличия в ней беспроводных сетей. При применении режима скрытого идентификатора *сеть* не отображается в списке доступных и подключиться к ней можно только в том случае, если, во-первых, точно известен ее *SSID*, а во-вторых, заранее создан профиль подключения к этой сети.

Аутентификация в стандарте *IEEE* 802.11 ориентирована на аутентификацию клиентского устройства радиодоступа, а не конкретного клиента как пользователя сетевых ресурсов (несмотря на то, что в литературе распространено *выражение* "*аутентификация* клиента"). Процесс аутентификации клиента беспроводной локальной сети *IEEE* 802.11 проиллюстрирован на рисунке 2.14 и состоит из следующих этапов:

1. Клиент посылает кадр (фрейм) запроса *Probe Request* во все радиоканалы.
2. Каждая точка радиодоступа (Access Point, AP), в зоне радиуса действия которой находится клиент, посылает в ответ фрейм *Probe Response*.
3. Клиент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию *Authentication Request*.
4. Точка радиодоступа посылает подтверждение аутентификации *Authentication Reply*.
5. В случае успешной аутентификации клиент посылает точке доступа запрос на соединение (ассоциирование) *Association Request*.
6. Точка доступа посылает в ответ фрейм подтверждения ассоциации *Association Response*.
7. Клиент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

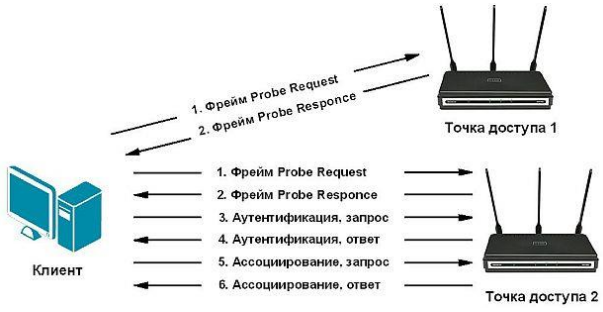


Рис. 3.1. Аутентификация по стандарту 802.11

Аутентификация с общим ключом является вторым методом аутентификации стандарта *IEEE* 802.11. Процесс аутентификации с общим ключом аналогичен процессу открытой аутентификации, отличаясь тем, что данный метод требует настройки статического ключа шифрования *WEP*, идентичного на клиентском устройстве (беспроводной *адаптер*) и на беспроводной точке доступа.

Аутентификация клиента по его MAC-адресу поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. При аутентификации *по MAC*-адресу происходит сравнение *MAC*-адреса клиента либо со списком разрешенных (или запрещенных) адресов клиентов, внесенным в MAC-таблицу точки доступа, либо с помощью внешнего сервера аутентификации (рисунок 3.2). *Аутентификация по MAC*-адресу используется в *дополнение* к открытой аутентификации и аутентификации с общим ключом стандарта *IEEE* 802.11 для уменьшения вероятности доступа посторонних пользователей.

увеличить изображение

Рис. 3.2. Аутентификация с помощью внешнего сервера

Но перечисленные *механизмы* аутентификации не обеспечат неуязвимость и полную *безопасность* беспроводной сети.

Идентификатор SSID регулярно передается точками радиодоступа в специальных фреймах Beacon. Любая приемо-передающая станция, расположенная в радиусе действия и поддерживающая стандарт 802.11, может определить *SSID* с помощью анализатора трафика протокола 802.11. Некоторые точки радиодоступа, в том числе D-Link, позволяют административно запретить широковещательную передачу *SSID* внутри фреймов Beacon. Однако и в этом случае *SSID* можно легко определить путем захвата фреймов Probe *Response*, посылаемых точками радиодоступа. *SSID* не обеспечивает *конфиденциальность* данных, данный *идентификатор* не разрабатывался для использования в качестве механизма обеспечения безопасности. Кроме этого, отключение широковещательной передачи *SSID* точками радиодоступа может серьёзно отразиться на совместимости оборудования беспроводных сетей различных производителей при использовании в одной беспроводной сети.

Открытая *аутентификация* не позволяет точке доступа определить, разрешен ли клиенту *доступ* к сети или нет. Это становится уязвимым местом в системе безопасности в том случае, если в беспроводной локальной сети не используется так называемое *WEP-шифрование*. В случаях, когда использование *WEP*-шифрования не требуется или невозможно (например, в беспроводных локальных сетях публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством *Интернет*-шлюзов.

Стандарт *IEEE* 802.11 требует передачи *MAC*-адресов клиента и точки радиодоступа в открытом виде. В результате этого в беспроводной сети, использующей аутентификацию *по MAC*-адресу, *злоумышленник* может обмануть метод аутентификации путём подмены своего *MAC*-адреса на разрешенный.

Первым *стандартом шифрования данных* в беспроводных сетях стал протокол **WEP** (Wired Equivalent *Privacy*). *Шифрование* осуществляется с помощью 40 или 104-битного ключа (поточное *шифрование* с использованием алгоритма *RC4* на статическом ключе) и дополнительной

динамической составляющей размером 24 бита, называемой вектором инициализации (*Initialization Vector*, IV).

Процедура *WEP*-шифрования выглядит следующим образом. Первоначально передаваемые в пакете данные проверяются на *целостность* (*алгоритм* CRC-32) для получения значения контроля целостности (*Integrity Check* Value, ICV), добавляемого в конец исходного сообщения. Далее генерируется 24-битный *вектор* инициализации (IV), а к нему добавляется статический (40- или 104-битный) *секретный ключ*. Полученный таким образом 64- или 128-битный *ключ* и является исходным ключом для генерации псевдослучайного числа, которое используется для шифрования данных. Далее данные смешиваются (шифруются) с помощью логической *операции XOR* с псевдослучайной ключевой последовательностью, а *вектор* инициализации добавляется в служебное *поле* кадра.

Рис. 3.3. Формат WEP-кадра

Как и любая другая система безопасности на основе паролей, *надежность WEP* зависит от длины и состава ключа, а также частоты его смены. Первый серьезный недостаток – применение статического ключа – за относительно небольшое время *ключ* можно подобрать перебором. И второй недостаток *WEP*-шифрования – самосинхронизация для каждого сообщения, поскольку *вектор* инициализации передается незашифрованным текстом с каждым пакетом и через небольшой промежуток времени он повторяется. В результате протокол шифрования *WEP* на основе алгоритма *RC4* в настоящее время не является стойким.

Тема : Комплексная система обеспечения безопасности беспроводных сетей

На смену *WEP* пришёл стандарт *IEEE* 802.11i, представляющий из себя комплексную систему обеспечения безопасности. Эта система включает в себя *системы аутентификации*, создания новых ключей для каждой сессии, управления ключами (на базе технологии *Remote* Access Dial-In *User Service*, *RADIUS*), проверки подлинности пакетов и т.д.

Разработанный стандарт *IEEE* 802.11i призван расширить возможности протокола *IEEE* 802.11, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные организации, участвующие в разработке и продвижении стандартов Wi-Fi, в лице ассоциаций Wi-Fi Alliance и *IEEE*, не дожидаясь ратификации стандарта *IEEE* 802.11i, в ноябре 2002г. анонсировали спецификацию Wi-Fi *Protected* Access (*WPA*), соответствие которой обеспечивает совместимость оборудования различных производителей. В последующем *WPA* стал составной частью стандарта *IEEE* 802.11i.

Новый стандарт безопасности *WPA* обеспечил уровень безопасности куда больший, чем может предложить *WEP*, и имеет то преимущество, что микропрограммное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

А позже был разработан и утвержден стандарт *WPA2*, обеспечивающий еще более высокий уровень безопасности, чем первая версия *WPA*.

WPA/WPA2 (Wi-Fi Protected Access, защищенный доступ Wi-Fi) представляет собой обновленную программу сертификации устройств беспроводной связи. Преимуществами *WPA* являются усиленная *безопасность* данных и ужесточенный *контроль доступа* к беспроводным сетям. Изначально *WPA* основывался на протоколе *TKIP* (*Temporal* Key *Integrity Protocol*), использующий метод шифрования *RC4*. Между тем *WPA2* задействует новый метод шифрования CCMP (*Counter-Mode with CBC-MAC Protocol*), основанный на более мощном, чем *RC4*, алгоритме шифрования *AES* (*Advanced Encryption Standard*). CCMP является обязательной частью стандарта *WPA2* и необязательной частью стандарта *WPA*. Кроме того, в *WPA*/*WPA2* обеспечена *поддержка* стандартов *IEEE* 802.1x, протокола *EAP* (*Extensible Authentication Protocol* – расширяемый протокол аутентификации) и проверка целостности сообщений *MIC* (Message *Integrity Check*).

Wi-Fi Alliance дает следующую формулу для определения сути *WPA*:

WPA = IEEE 802.1X + TKIP + EAP + MIC

Из этой формулы видно, что *WPA, по* сути, является суммой нескольких технологий.

Стандарт **IEEE 802.1x** не требует обязательной смены ключей шифрования одноадресной рассылки. Кроме того, в стандартах *IEEE* 802.11 и *IEEE* 802.1x не определены *механизмы* изменения открытого ключа шифрования, который используется для многоадресного и широковещательного трафика. В *WPA* требуется смена обоих ключей. В случае использования ключа одноадресной рассылки протокол *TKIP* (*Temporal* Key *Integrity Protocol*) изменяет *ключ* для каждого кадра, а изменение синхронизируется между беспроводным клиентом и точкой беспроводного доступа. Для общего ключа шифрования в *WPA* включены средства передачи измененного ключа от точки беспроводного подключения к клиентам.

TKIP отвечает за увеличение размера ключа с 40 до 128 *бит*, а также за замену одного статического ключа *WEP*-ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Кроме того, в *TKIP* используется специальная *иерархия* ключей и методология управления ключами, которая убирает излишнюю *предсказуемость*, которая использовалась для несанкционированного снятия защиты *WEP*-ключей.

Сервер аутентификации после получения сертификата от пользователя использует 802.1x для генерации уникального базового ключа для сеанса связи. *TKIP* осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний *ключ* для динамической генерации ключей шифрования данных, которые в свою *очередь* используются для шифрования каждого пакета данных. Подобная *иерархия* ключей *TKIP* заменяет один *ключ WEP* (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

Как упомянуто выше, в стандарте *WPA* используется расширяемый протокол аутентификации **EAP** как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства, подтверждающего его право на *доступ* в *сеть*. Для этого *права пользователь* проходит проверку *по* специальной базе зарегистрированных пользователей. Без аутентификации работа в сети для пользователя будет запрещена.

WPA может работать в двух режимах: **Enterprise** (корпоративный) и **Pre-Shared Key** (персональный).

В первом случае, хранение *базы данных* и проверка аутентичности *по* стандарту *IEEE* 802.1x в больших сетях обычно осуществляются специальным сервером, чаще всего *RADIUS*.

Во втором случае подразумевается применение *WPA* всеми категориями пользователей беспроводных сетей, т.е. имеет упрощенный режим, не требующий сложных механизмов. Этот режим называется *WPA*-PSK (Pre-Shared Key) и предполагает введение одного пароля на каждый узел беспроводной сети (точку доступа, беспроводной *маршрутизатор*, клиентский *адаптер, мост*). До тех пор пока пароли совпадают, клиенту будет разрешен *доступ* в *сеть*. Можно заметить, что подход с использованием пароля делает *WPA*-PSK уязвимым для атаки методом подбора, однако этот режим избавляет от путаницы с ключами *WEP*, заменяя их целостной и четкой системой на основе цифробуквенного пароля.

Другим важным механизмом аутентификации является проверка целостности сообщений **MIC** (Message *Integrity Check*). Ее используют для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан *по* сети. *MIC* построена на основе мощной математической функции, которая применяется на стороне отправителя и получателя, после чего сравнивается результат. Если проверка показывает на несовпадение результатов вычислений, данные считаются ложными и пакет отбрасывается. Благодаря такому механизму могут быть ликвидированы слабые места защиты, способствующие проведению атак с использованием поддельных фреймов и манипуляцией битами.

Даже не принимая во внимания тот факт, что *WEP* не обладает какими-либо механизмами аутентификации пользователей как таковой, его ненадёжность состоит, прежде всего, в криптографической слабости алгоритма шифрования. Стандарт *WPA*/*WPA2* позволяет использовать *алгоритм* **AES** – симметричный *алгоритм* блочного шифрования (размер блока 128 *бит, ключ* 128/192/256 *бит*).

CCMP (*Counter Mode with* Cipher *Block Chaining* Message *Authentication* Code *Protocol* – протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счётчика) – протокол шифрования *IEEE* 802.11i, созданный для замены *TKIP* – обязательного протокола шифрования в *WPA* и *WEP* – как более надёжный вариант. CCMP, являясь частью стандарта 802.11i, использует *алгоритм AES*. В отличие от *TKIP*, управление ключами и целостностью сообщений осуществляется одним компонентом, построенным вокруг *AES* с использованием 128-битного ключа, 128-битного блока, в соответствии со стандартом шифрования FIPS-197.

Стандарт *IEEE* 802.11i использует концепцию повышенной безопасности (*Robust Security Network, RSN*), и это потребует изменений в аппаратной части и программном обеспечении, т.е. *сеть*, полностью соответствующая *RSN*, станет несовместимой с существующим оборудованием *WEP*. Сейчас пока еще поддерживается как оборудование *RSN*, так и *WEP* (на самом деле *WPA*/*TKIP* было решением, направленным на сохранение инвестиций в оборудование), но в дальнейшем устройства *WEP* перестанут использоваться.

IEEE 802.11i применим к различным сетевым реализациям и может задействовать *TKIP*, но *по* умолчанию *RSN* использует *AES* (*AdvancedEncryption Standard*) и CCMP

(*Counter Mode CBC MAC Protocol*) и, таким образом, является более мощным расширяемым решением (*AES – блочный шифр*, оперирующий блоками данных *по* 128 *бит*).

802.11i (*WPA2*) – это наиболее устойчивое и безопасное решение, предназначенное в первую *очередь* для больших предприятий, где управление ключами и *администрирование* были главной головной болью. С 13 марта 2006 года *поддержка WPA2* является обязательным условием для всех сертифицированных Wi-Fi устройств.

Производительность канала связи, как свидетельствуют результаты тестирования оборудования различных производителей, падает на 5-20% при включении как *WEP*-шифрования, так и *WPA*. Однако испытания того оборудования, в котором включено *шифрование AES* вместо *TKIP*, не показали сколько-нибудь заметного падения скорости.

WPA2, так же как и *WPA*, может работать в двух режимах: **Enterprise** (корпоративный) и **Pre-Shared Key** (персональный).

Тема : **Технологии безопасности беспроводных сетей и унифицированные решения**

Стандарт IEEE 802.1x/EAP

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта *IEEE* 802.11, вынудили искать новые решения защиты беспроводных сетей. Были выявлены компоненты, влияющие на системы безопасности беспроводной локальной сети:

- архитектура аутентификации;
- механизм аутентификации;
- механизм обеспечения конфиденциальности и целостности данных.

Стандарт *IEEE* 802.1x описывает единую архитектуру контроля доступа к портам с использованием разнообразных методов аутентификации клиентов и обеспечивает аутентификацию пользователей на канальном уровне любой топологии (как проводной, так и беспроводной) семейства стандартов *IEEE* 802.

Алгоритм аутентификации *EAP* поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и её пользователей с возможностью динамической генерации ключей шифрования.

Аутентификация по стандарту *IEEE* 802.1x – это процесс, независимый от аутентификации *по* стандарту *IEEE* 802.11. При аутентификации *по* стандарту *IEEE* 802.1x используется метод установления подлинности между клиентом и сервером (например, удаленная *аутентификация RADIUS*), к которому подключена *точка доступа*. Процесс аутентификации использует идентификационную информацию, например, *пароль* пользователя, который не передается через беспроводную *сеть*. Большинство видов аутентификации *IEEE* 802.1x поддерживают динамические ключи для пользователя, сеанса и для усиления защиты ключа.

Аутентификация стандарта *IEEE* 802.1x для беспроводных сетей имеет три главных компонента:

- Беспроводной клиент (программное обеспечение клиентского устройства)

- Аутентификатор (точка доступа)
- Сервер аутентификации (RADIUS)

Защита аутентификации стандарта 802.1x инициирует *запрос* на аутентификацию от клиента беспроводной сети в точку доступа, которая устанавливает его подлинность через протокол *EAP* в соответствующем сервере *RADIUS*. Этот *сервер RADIUS* может выполнить аутентификацию пользователя (с помощью пароля или сертификата) или компьютера (с помощью адреса *MAC*). Теоретически, клиент беспроводной сети не может войти в *сеть* до завершения транзакции. (Не все методы аутентификации используют *сервер RADIUS*. Режимы *WPA*-PSK и *WPA2*-PSK используют общий *пароль*, который вводится в точке доступа и в устройствах, запрашивающих *доступ* к сети).

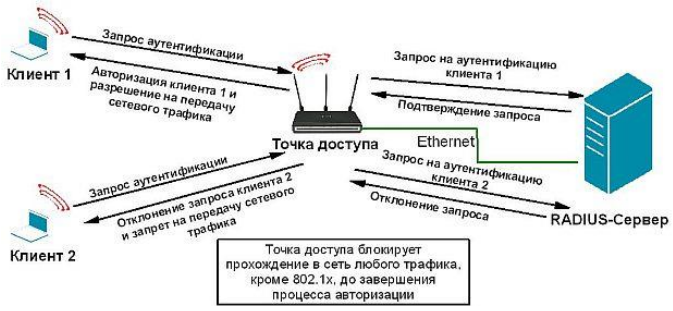


Рис. 3.4. Процесс аутентификации в 802.1x/EAP

IEEE 802.1x предоставляет клиенту беспроводной локальной сети лишь средства передачи атрибутов серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является *поддержка* требуемых политикой сетевой безопасности методов аутентификации.

Аутентификатор (*точка доступа*) создаёт *логический порт* для каждого клиента на основе его идентификатора ассоциирования. *Логическийпорт* имеет два канала для обмена данными. Неконтролируемый канал беспрепятственно пропускает трафик из беспроводного сегмента в проводной и обратно, в то время как контролируемый канал требует успешной аутентификации для беспрепятственного прохождения сетевого трафика.

Таким образом, в терминологии стандарта *IEEE* 802.1x *точка доступа* играет роль коммутатора в проводных сетях *Ethernet*. Очевидно, что в проводном сегменте сети, к которому подсоединена *точка доступа*, должен быть подключен *сервер* аутентификации. Его функции, как уже отмечалось ранее, обычно выполняет *RADIUS-сервер*, интегрированный с той или иной базой данных пользователей, в качестве которой может выступать стандартный *RADIUS, LDAP* или *Windows Active Directory*. Беспроводные шлюзы высокого класса могут реализовывать как функции аутентификатора, так и сервера аутентификации.

Клиент активизируется и ассоциируется с точкой доступа (или физически подключается к сегменту в случае проводной локальной сети). *Аутентификатор* распознаёт факт подключения и активизирует *логический порт* для клиента, сразу переводя его в состояние "неавторизован". В результате этого через клиентский *порт* возможен обмен лишь трафиком протокола *IEEE* 802.1x, для всего остального трафика *порт* заблокирован. Поскольку в локальных сетях *IEEE* 802.11 нет физических портов, то *ассоциация* между беспроводным клиентским устройством и точкой доступа считается сетевым портом доступа. Клиент также может (но не обязан) отправить сообщение *EAP* Start (начало аутентификации *EAP*) для запуска процесса аутентификации.

После завершения аутентификации *сервер* отправляет сообщение *RADIUS*-ACCEPT (принять) или *RADIUS*-REJECT (отклонить) аутентификатору. При получении сообщения RADI¬US-ACCEPT *аутентификатор* переводит *порт* клиента в состояние "авторизован", и начинается передача всего трафика пользователя.

В стандарте *IEEE* 802.1x *аутентификация* пользователей на канальном уровне выполняется *по* протоколу *EAP*. Протокол *EAP* подобен протоколу *CHAP* (*Challenge* Handshake *Authentication Protocol* – протокол взаимной аутентификации), который применяется в PPP (*Point* to *Point Protocol* – протокол соединения "*точка-точка*"), он предназначен для использования в локальных сетях. *EAP* является "обобщённым" протоколом в системе аутентификации, авторизации и учёта (*authentication, authorization, and accounting, AAA*), обеспечивающим работу разнообразных методов аутентификаци. *AAA*-клиент (*сервер* доступа *по* терминологии *AAA* в беспроводной сети представлен точкой доступа), поддерживающий *EAP*, может не понимать конкретных методов, используемых клиентом и сетью в процессе аутентификации. *Сервер* доступа туннелирует сообщения протокола аутентификации, которыми обмениваются клиент и *сервер* аутентификации. *Сервер* доступа интересует лишь факт начала и окончания процесса аутентификации.

Есть несколько вариантов EAP, спроектированных с участием различных компаний-производителей. Такое разнообразие вносит дополнительные проблемы совместимости, так что выбор подходящего оборудование и программного обеспечения для беспроводной сети становится непростой задачей. Возможные варианты *EAP* при конфигурировании способа аутентификации пользователей в беспроводной сети:

EAP-MD5 – это обязательный уровень EAP, который должен присутствовать во всех реализациях стандарта 802.1x, именно он был разработан первым. С точки зрения работы он дублирует протокол *CHAP*. Протокол *EAP*-MD5 не поддерживает динамическое *распределение ключей*. Кроме того, он уязвим для атаки "человек посередине" с применением фальшивой точки доступа и для атаки на *сервер* аутентификации, так как аутентифицируются только клиенты. И наконец, в ходе аутентификации *злоумышленник* может подслушать *запрос* и зашифрованный ответ, после чего провести атаку с известным открытым или шифрованным текстом.

EAP-TLS (*EAP-Transport Layer Security* – протокол защиты транспортного уровня) поддерживает взаимную аутентификацию на базе сертификатов. *EAP-TLS* основан на протоколе SSLv3 и требует наличия удостоверяющего центра. Протоколы *TLS* и *SSL* используют ряд элементов инфраструктуры *PKI* (*Public Key Infrastructure*). Клиент должен иметь действующий сертификат для аутентификации *по* отношению к сети. *AAA-сервер* должен иметь действующий сертификат для аутентификации *по* отношению к клиенту. *Центр сертификации* с сопутствующей инфраструктурой управляет сертификатами субъектов *PKI*. Клиент и *RADIUS-сервер* должны поддерживать метод аутентификации *EAP-TLS*. *Точка доступа* должна поддерживать процесс аутентификации в рамках 802.1x/*EAP*, хотя может и не знать деталей конкретного метода аутентификации.

EAP-LEAP (Lightweight EAP – облегчённый *EAP*) был первой (и на протяжении длительного времени единственной) схемой аутентификации в стандарте *IEEE* 802.1x, основанной на паролях. *Сервер* аутентификации посылает клиенту *запрос*, а тот должен вернуть *пароль*, предварительно выполнив его свертку со строкой запроса. Будучи основан на применении паролей, *EAP*-LEAP аутентифицирует пользователя, а не устройство. В то же время

очевидна *уязвимость* этого варианта для атак методом полного перебора и *по* словарю, не характерная для методов аутентификации с применением сертификатов.

PEAP (*Protected* EAP – защищённый *EAP*) и **EAP-TTLS** (Tunneled *Transport Layer Security* EAP – протокол защиты транспортного уровня *EAP*) достаточно популярны и поддерживаются производителями сетевого оборудования, в том числе D-link. Для работы *EAP*-TTLS требуется, чтобы был сертифицирован только *сервер* аутентификации, а у претендента сертификата может и не быть, так что процедура развертывания упрощается. *EAP*-TTLS поддерживает также ряд ранних методов аутентификации, в том числе *PAP*, *CHAP*, MS-*CHAP*, MS-CHAPv2 и даже *EAP*-MD5. Чтобы обеспечить *безопасность* при использовании этих методов, *EAP*-TTLS создает зашифрованный *по* протоколу *TLS туннель*, внутри которого эти протоколы и работают. Протокол PEAP очень похож на *EAP*-TTLS, только он не поддерживает методы аутентификации типа PAP и *CHAP*. Вместо них поддерживаются протоколы PEAP-MS-CHAPv2 и PEAP-*EAP-TLS*, работающие внутри безопасного туннеля. *Поддержка* PEAP реализована в пакете программ точек доступа D-link и хорошо реализована в наиболее популярных операционных системах персональных компьютеров. В общем виде схема обмена PEAP выглядит следующим образом:

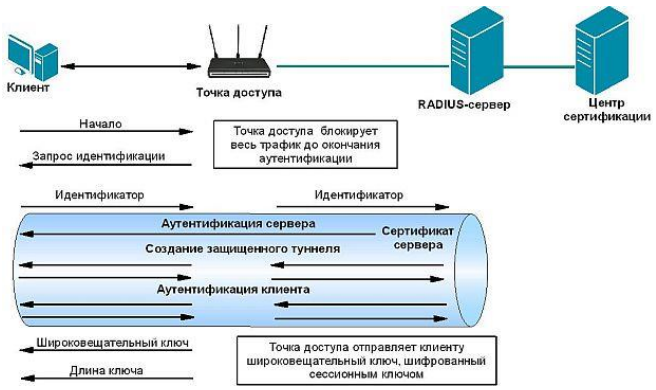


Рис. 3.5. Процесс аутентификации PEAP

Еще два варианта EAP – это *EAP-SIM* и EAP-AKA для аутентификации на базе *SIM* и USIM (Universal Subscriber *Identity* Modules). В основном они предназначены для аутентификации в сетях *GSM*, а не в беспроводных сетях *IEEE* 802.11. Тем не менее, протокол *EAP-SIM* поддерживается точками доступа и клиентскими устройствами некоторых производителей.

Развертывание беспроводных виртуальных сетей

Подробнее технология *VPN* рассмотрена в разделе "*Виртуальные частные сети* (*VPN*)". Здесь мы рассмотрим ситуации, возможные в беспроводных сетях.

Виртуальная частная *сеть* (*VPN*) – это метод, позволяющий воспользоваться сетевой инфраструктурой общего пользования, например сетью *Интернет*, для предоставления удаленным офисам или отдельным пользователям безопасного доступа к локальной сети организации. Поскольку беспроводные сети 802.11 работают в нелицензируемом диапазоне частот и легкодоступны для случайного или злонамеренного прослушивания, то именно в них *развертывание* и обслуживание *VPN* приобретает особую важность, если необходимо обеспечить высокий уровень защиты информации.

Защищать нужно как соединения между хостами в беспроводной локальной сети, так и двухточечные каналы между беспроводными мостами. Для обеспечения безопасности особо секретных данных

нельзя полагаться на какой-то один механизм или на защиту лишь одного уровня сети. В случае двухточечных каналов проще и экономичнее развернуть *VPN*, покрывающую две сети, чем реализовывать защиту на базе стандарта *IEEE* 802.11i включающую *RADIUS-сервер* и базу данных о пользователях.

VPN и технологии безопасности беспроводных сетей не конкурируют, а дополняют друг друга. *VPN* работает поверх разделяемых сетей общего пользования, обеспечивая в то же время *конфиденциальность* за счет специальных мер безопасности и применения туннельных протоколов, таких как туннельный протокол на канальном уровне (*Layer* Two *Tunneling Protocol*, *L2TP*). Смысл их в том, что, осуществляя *шифрование данных* на отправляющем конце и дешифрирование на принимающем, протокол организует *туннель*, в который не могут проникнуть данные, незашифрованные должным образом.
Дополнительную *безопасность* может обеспечить *шифрование* не только самих данных, но и сетевых адресов отправителя и получателя. Беспроводную локальную *сеть* можно сравнить с разделяемой сетью общего пользования, а в некоторых случаях она таковой и является (например, хот-споты).

VPN-сеть не является устойчивой к DoS- или DDoS-атакам и не может гарантировать доступность на физическом уровне просто в силу своей виртуальной природы и зависимости от нижележащих протоколов.

Две наиболее важные особенности *VPN*, особенно в беспроводных средах, где имеется лишь ограниченный *контроль* над распространением сигнала – это *целостность* и, что еще более существенно, *конфиденциальность* данных. Предположим ситуацию, когда злоумышленнику удалось преодолеть *шифрование по* протоколу *WEP* и подключиться к беспроводной локальной сети. Если *VPN* отсутствует, то он сможет прослушивать данные и вмешиваться в работу сети. Но если пакеты аутентифицированы, то *атака* "человек посередине" становится практически бесполезной, хотя перехватить данные *по*-прежнему легко. Включение в *VPN* элемента шифрования уменьшает негативные последствия перехвата данных. *VPN* обеспечивает не столько полную изоляцию всех сетевых взаимодействий, сколько осуществление таких взаимодействий в более контролируемых условиях с четко определенными группами допущенных участников.

Системы обнаружения вторжения в беспроводных сетях

Системы обнаружения вторжения (*Intrusion Detection System*, *IDS*) – это устройства, с помощью которых можно выявлять и своевременно предотвращать вторжения в вычислительные сети. Они делятся на два вида: на базе сети и на базе узла.

Сетевые системы (*Network Intrusion Detection* Systems, *NIDS*) анализируют трафик с целью обнаружения известных атак на основании имеющихся у них наборов правил (экспертные системы). Подмножеством сетевых систем обнаружения вторжений являются системы для наблюдения только за одним узлом сети (*Network Node IDS*).

Другой вид систем обнаружения вторжений представляют системы на базе узла (*Host Intrusion Detection* Systems, *HIDS*). Они устанавливаются непосредственно на узлах и осуществляют наблюдение за целостностью файловой системы, системных журналов и т.д.

NIDS делятся в свою *очередь* на две большие категории: на основе сигнатур и на основе базы знаний. Сигнатурные *IDS* наиболее распространены. В таких системах события, происходящие в сети,

сравниваются с признаками известных атак, которые и называются сигнатурами. *Базы данных*, содержащие сигнатуры, необходимо надежно защищать и часто обновлять. *IDS* на основе базы знаний следят за сетью, собирают статистику о её поведении в нормальных условиях, обнаруживают различные отклонения и помечают их как подозрительные. Поэтому такие *IDS* еще называют основанными на поведении или статистическими.

Для эффективной работы статистической *IDS* необходимо иметь надежную информацию о том, как ведет себя *сеть* в нормальных условиях, так называемую точку отсчета. Хотя такую *IDS* обмануть сложнее, но и у нее есть свои проблемы: ложные срабатывания и трудности при обнаружении некоторых видов коммуникаций *по* скрытому каналу. Ложные срабатывания особенно вероятны в беспроводных сетях из-за нестабильности передающей среды. Кроме того, атаки, проведенные на ранних стадиях периода фиксации точки отсчета, могут исказить процедуру обучения статистической *IDS*.

Хорошая *IDS* для беспроводной сети должна быть одновременно сигнатурной и статистической. Некоторые инструменты для проведения атак на беспроводные сети имеют четко выраженные сигнатуры. Если они обнаруживаются в базе данных, то можно поднимать тревогу. С другой стороны, у многих атак очевидных сигнатур нет, зато они вызывают отклонения от нормальной работы сети на нижних уровнях стека протоколов. Отклонение может быть неощутимым (например, несколько пришедших не *по* порядку фреймов) или сразу заметным (выросшая в несколько раз нагрузка). Обнаружение таких аномалий – это непростая задача, поскольку не существует двух одинаковых беспроводных сетей. То же относится и к проводным локальным сетям, но там хотя бы нет радиопомех, отражения, рефракции и рассеивания сигнала. Поэтому эффективное применение *IDS* в беспроводных сетях возможно только после длительного периода детального исследования сети. При разворачивании системы необходимо четко понимать, что, как и зачем нужно анализировать и постараться ответить на эти вопросы, чтобы сконструировать необходимую систему *IDS*.

Рис. 3.6. Характеристики систем обнаружения вторжений

Только собрав значительный объем статистических данных о работе конкретной сети, можно решить, что является аномальным поведением, а что – нет, и идентифицировать проблемы со связью, ошибки пользователей и атаки. Многократные запросы на аутентификацию *по* протоколу *IEEE* 802.1x/LEAP могут свидетельствовать о попытке атаки методом полного перебора. Но это может объясняться и тем, что *пользователь* забыл свой *пароль* или работой плохо написанного клиентского приложения, которое продолжает попытки войти в *сеть*, пока не будет введен правильный *пароль*. Увеличение числа фреймов-маяков может быть признаком DoS-атаки или присутствия в сети фальшивой точки доступа, но не исключено, что все дело в неисправной или неправильно сконфигурированной законной точке доступа. События, фиксируемые *IDS* на верхних уровнях стека протоколов, например большое число

фрагментированных пакетов или запросов *TCP SYN*, может указывать на сканирование портов или DoS-атаку, но, возможно, это просто результат плохой связи на физическом уровне.

Таким образом, любое событие требует тщательного исследования и анализа.

Тема : Технологии безопасности беспроводных сетей и унифицированные решения

Унифицированные решения

В данном разделе познакомимся с одним любопытным решением компании D-Link, связанным с созданием унифицированных коммутируемых локальных сетей (проводных и беспроводных), которые обеспечивают высокую *производительность* при безопасной передаче информации и *масштабируемость* с возможностью управления и контроля.

Система Унифицированного Доступа (**Unified Access System**) – комплексное решение от компании D-Link. Позволяет развёртывать безопасные беспроводные сети *WLAN* (*Wireless LAN*), обеспечивая внедрение современных беспроводных сетевых возможностей, в том числе бесшовный роуминг уровней L2 и L3 для конечных пользователей.

В приведенном на рис. 3.7 примере организации локальной сети точки доступа отделов 1 и 2 управляются коммутатором *Unified* Access.

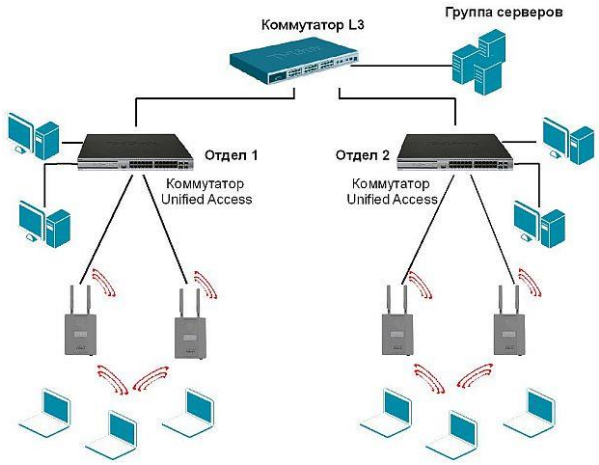


Рис. 3.7. Организация локальной сети с использованием Unified Access System

Компоненты D-Link Unified Access System:

1. Унифицированные проводные/беспроводные коммутаторы Gigabit Ethernet, серии D-Link DWS-3024/3024L/3026/4026:

2. Коммутируемые беспроводные точки доступа типа DWL-8500/8600AP – унифицированные беспроводные точки доступа, управление которыми осуществляется при подключении к беспроводному коммутатору DWS-3024/3024L/3026/4026.

Гигабитные беспроводные коммутаторы DWS-3024/3024L/3026/4026 являются корневыми устройствами, позволяющими управлять безопасностью, полосой пропускания и поддерживать функционирование всей беспроводной сети. Помимо этого, выполняя *мониторинг* пользователей и управляя их аутентификацией во время роуминга, коммутаторы могут задавать и управлять всеми параметрами беспроводных точек доступа, включая радиочастотные каналы, управление питанием,

сегментацией беспроводного трафика, роумингом, балансировкой нагрузки, обнаружением несанкционированных точек доступа и параметрами безопасности.

Разработанные для легкого развертывания сети, коммутаторы поддерживают от 24 до 64 (в зависимости от модели) беспроводных точек доступа, которые могут быть подключены к портам беспроводного коммутатора непосредственно или опосредованно через *коммутатор* локальной сети. В сетях малого и среднего бизнеса (сектор *SMB* – Small *and Medium* Business) для управления несколькими точками доступа или для использования в смешанной проводной/беспроводной локальной сети потребуется только один беспроводной *коммутатор*. При увеличении количества точек доступа в систему централизованного управления можно объединить до 4 коммутаторов. Благодаря простоте расширения, поддержке гигабитных скоростей для подключения высокоскоростных точек доступа и маршрутизации уровня 3 для организации межсетевого роуминга, DWS-3024/3024L/3026/4026 обеспечивают архитектуру, которая унифицирует и упрощает сложную конфигурацию беспроводной сети, подготавливая простой переход к будущим технологиям.

Коммутируемые беспроводные точки доступа DWL-8500/8600 являются высокопроизводительными устройствами, предоставляя беспроводным клиентам мобильность и возможность работы в двух частотных диапазонах (2,4 Ггц и 5 ГГц). При подключении к этим коммутаторам каждая *точка доступа* (AP, *Access Point*) автоматически настраивается на оптимальный радиочастотный канал и выходную *мощность* передатчика, обеспечивая беспроводных клиентов сигналом наилучшего качества.

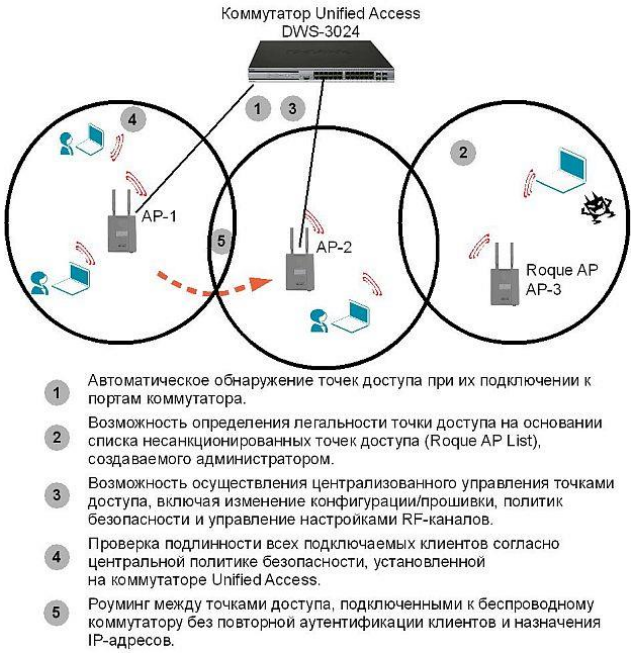


Рис. 3.8. Организация беспроводной сети с использованием коммутатора и точек доступа Unified Access System

Каждый клиент, подключаемый к беспроводной сети, проходит через процесс строгой аутентификации, что гарантирует максимальную *безопасность*. Неважно, является ли клиент постоянным пользователем, гостем или просто имеет *доступ* к сети отдела, коммутаторы DWS-3024/3024L/3026/4026 защищают сетевую инфраструктуру с помощью большого набора функций безопасности, включая: *WEP-шифрование данных, WPA/WPA2*, аутентификацию пользователей 802.1x и стандарт безопасности 802.11i, адаптивный портал и аутентификацию *MAC*-адресов.

Коммутаторы обеспечивают *определение* и обнаружение несанкционированных точек доступа для предотвращения нелегального вторжения во внутреннюю *сеть*, а также предоставляют такие сервисы, как членство в виртуальной частной группе (*SSID*), аутентификацию, *определение* местонахождения и выдачу статистики о сетях. Во время роуминга *пользователь* сохраняет авторизацию, т.к. все коммутаторы DWS-3024/3024L/3026/4026 имеют общую базу данных, гарантируя безопасный *доступ* к соответствующим ресурсам сети. Наряду с проверкой учетных данных подключаемых пользователей в локальной базе данных, также может быть осуществлена *аутентификация* пользователей на внешнем сервере *RADIUS*.

Кроме того, DWS-4026 поддерживает новейшую функцию *Wireless Intrusion Detection System* (WIDS), предназначенную для обнаружения несанкционированных точек доступа и несанкционированных клиентов, а также различных угроз безопасности беспроводной сети. С помощью функции WIDS администраторы могут обнаружить различные угрозы и использовать сканирование радиочастотных каналов для обзора беспроводной сети в целях предотвращения любых потенциальных угроз безопасности. Для проводных клиентов DWS-4026 использует функцию *Dynamic ARP Inspection* (*DAI*) и *DHCP Snooping* для обеспечения максимальной безопасности. Совместное использование функций *Dynamic ARP Inspection* (*DAI*) и *DHCP Snooping* предотвращает угрозы самого высокого уровня, например, "man-in-the-middle" и *ARP* poisoning.

Благодаря централизованным радиочастотным политикам, автоматическому выбору наименее используемого канала и балансировке нагрузки точек доступа, коммутаторы DWS-3024/3024L/3026/4026 могут эффективно управлять беспроводной полосой пропускания для оптимизации трафика *WLAN*.

Коммутаторы поддерживают централизованную базу данных с информацией *по* доступу беспроводных пользователей к ресурсам, например, *MAC*-адреса и ключи аутентификации. В сети с несколькими коммутаторами эта *информация* обеспечивается обменом данными между ними. *По* мере перемещения пользователей *по* офису с использованием беспроводного оборудования, может меняться используемая для подключения *точка доступа*.

Источники информации:

Шаньгин В. Ф. Ш20 Информационная безопасность компьютерных систем и сетей: учеб. пособие. - М.: ИД «ФОРУМ»: ИНФРА-М, 2011. - 416 е.: ил. — (Профессиональное образование).

Завгородний В.И. 3-13 Комплексная зашита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А Егоров, 2001. - 264 с: ил.

на рабочую программу
учебной дисциплины « ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.»

На рецензию представлена рабочая программа профессионального модуля «ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.», разработчиком которой является преподаватель Багаутдинова Зарема Магомедзапировна преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева» и Джамалутдинова М.Д преподаватель дисциплин общего и профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева»

Рабочая программа профессионального модуля «ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.» разработана на основе требований ФГОС СПО по специальности 11.02.11 Сети связи и системы коммутации, в соответствии с рабочим учебным планом образовательной организации на 2021/2022 учебный год, с учетом Методических рекомендаций по разработке рабочей программы профессионального модуля при реализации основной профессиональной образовательной программы среднего профессионального образования (ППКРС И ППССЗ) разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан.

Профессиональный модуль ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. является обязательной частью модульного цикла ППССЗ.

Рабочая программы профессионального модуля включает: титульный лист, содержание, раздел 1 «Паспорт рабочей программы учебной дисциплины», раздел 2 «Результаты освоения профессионального модуля», раздел 3 «Структура и примерное содержание профессионального модуля», раздел 4 «Условия реализации профессионального модуля», раздел 5 «Контроль и оценка результатов освоения профессионального модуля», Все разделы программы представлены и выполнены в соответствии с рекомендованной формой.

В паспорте программы указываются область применения программы, место профессионального модуля в структуре программы подготовки специалистов среднего звена, Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля, количество часов на освоение программы профессионального модуля.

В тематическом плане программы профессионального модуля. содержится почасовое распределение видов учебной работы студентов, обеспечивается логическая последовательность и четкость в наименовании разделов и тем. Содержание теоретического материала, практических занятий и самостоятельной работы студентов соответствует целям и задачам освоения профессионального модуля, уровни освоения обозначаются дидактически целесообразно.

Перечисленное оборудование лаборатории и рабочих мест лаборатории, в том числе персональные компьютеры с необходимым комплектом лицензионного программного обеспечения, технические средства обучения, печатные и электронные издания основной и дополнительной литературы, обеспечивают материально-технические и информационные условия реализации программы профессионального модуля.

В качестве рекомендаций составителю рабочей программы профессионального модуля предлагается ежегодно корректировать содержание теоретических и практических занятий с учётом новых тенденций в области информационных технологий, обновлять перечень информационных источников.

Представленная на рецензию рабочая программа профессиональный модуль ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. рекомендуется к практическому применению в образовательном процессе в профессиональных образовательных организациях, реализующих программу подготовки специалистов среднего звена по специальности 11.02.11 Сети связи и системы коммутации.

Рецензент _____ Гуляев Е.Е зам генерального директора ООО «Квант-Телеком»