МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет»
в г. Славянске-на-Кубани

УТВЕРЖДАЮ

Проректор по работе с филиалами
ФГБОУ ВО «Кубанский
государственный университет»

_____ А.А. Евдокимов

«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.01.03 БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

специальность 09.02.06 Сетевое и системное администрирование

Краснодар 2024

Рабочая программа учебной дисциплины МДК.01.03 БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.06 Сетевое и системное администрирование (технологический профиль), утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519, (зарегистрирован в Министерстве юстиции России 15.08.2023 г. рег. № 74796), и примерной основной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование.

Дисциплина	МДК.01.03 БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ
Форма обучения	очная
Учебный год	2024-2025
2 курс	4 семестр
всего 153 часов, в том числе:	
лекции	72 ч.
практические занятия	72 ч.
самостоятельные занятия	–
консультация	–
промежуточная аттестация	9 ч.
форма итогового контроля	экзамен

Составитель: преподаватель _____ Р.Р. Сабиров

Утверждена на заседании предметной (цикловой) комиссии физико-математических дисциплин и специальных дисциплин УГС 09.00.00 Информатика и вычислительная техника протокол № 10 от «30» мая 2024 г.

Председатель предметной (цикловой) комиссии:

_____ М.С. Бушуев

«30» мая 2024 г.

Рецензенты:

Технический директор
ООО «Техностарт» _____ И.Г. Колодезный

Технический директор
ООО «ПРАЙ» _____ Б.А. Шишкин

ЛИСТ
согласования рабочей программы по учебной дисциплине
МДК.01.03 «Безопасность компьютерных сетей»

Специальность среднего профессионального образования:
09.02.06 Сетевое и системное администрирование

СОГЛАСОВАНО:

Нач. УМО филиала _____ А.С. Демченко
«31» мая 2024 г.

Заведующая библиотекой филиала _____ М.В. Фуфалько
«31» мая 2024 г.

Нач. ИВЦ (программно-информационное обеспечение образовательной программы) _____ В.А. Ткаченко
«31» мая 2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ МДК 01.03 «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

1.1 Область применения рабочей программы

Рабочая программа учебной дисциплины «Безопасность компьютерных сетей» является частью основной профессиональной образовательной программы в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее ФГОС СПО) для специальности 09.02.06 Сетевое и системное администрирование.

1.2 Место дисциплины в структуре программы подготовки специалистов среднего звена

Учебная дисциплина МДК 01.03 «Безопасность компьютерных сетей» относится к профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры».

1.3 Цель и задачи учебной дисциплины – требования к результатам освоения дисциплины

Цели дисциплины: формирование у учащихся системы знаний, умений и навыков в области использования средств информационных технологий как базы для развития профессиональных компетенций.

В результате изучения профессионального модуля обучающийся должен

иметь практический опыт в:

– проектировании архитектуры локальной сети в соответствии с поставленной задачей;

– установке и настройке сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей;

– выборе технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры;

– обеспечении безопасного хранения и передачи информации в локальной сети;

– использование специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей.

уметь:

– проектировать локальную сеть, выбирать сетевые технологии;

– использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети.

знать:

– общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям;

– архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры;

– базовые протоколы и технологии локальных сетей;

– принципы построения высокоскоростных локальных сетей;

– стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

Максимальная учебная нагрузка обучающегося 152 часов, в том числе:

– обязательная аудиторная учебная нагрузка обучающегося 140 часов.

1.4. Перечень планируемых результатов обучения по дисциплине (Перечень формируемых компетенций)

Освоение дисциплины «Безопасность компьютерных сетей» способствует формированию у студентов следующих профессиональных компетенций:

ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.

ОК 04 Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 1.1. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем

ПК 1.3. Устранять неисправности в работе инфокоммуникационных систем.

ПК 1.4. Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности

ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.

ПК 1.6. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.

ПК 1.7. Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ МДК 01.03 «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры
		4
Обязательная учебная нагрузка (всего)	**144**	**144**
В том числе:		
занятия лекционного типа	72	72
практические занятия (практикумы)	72	72
Консультации		
Вид промежуточной аттестации – экзамен	9	9
Общая трудоемкость 152 часа	**153**	**153**

2.2 Структура дисциплины

Освоение учебной дисциплины МДК.01.03 «Безопасность компьютерных сетей» включает изучение следующих разделов:

Наименование разделов и тем	Всего	Количество аудиторных часов	
		Теоретическое обучение	Практические занятия
Раздел 1. Информационная безопасность	**16**	8	8
Раздел 2. Технологии защиты данных	**28**	14	14
Раздел 3. Базовые технологии сетевой безопасности	**36**	20	16
Раздел 4. Технологии обнаружения вторжений	**34**	18	16
Раздел 5. Управление сетевой безопасностью	**30**	12	18
Всего по дисциплине	**144**	**72**	**72**

2.3 Тематический план и содержание учебной дисциплины МДК.01.03 «Безопасность компьютерных сетей»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Информационная безопасность	***Содержание учебного материала***	**16**	ПК 1.1-ПК 1.7 ОК 01-09
	Лекции	**8**	
	1. Основные понятия информационной безопасности и защиты информации.	2	
	2. Угрозы информационной безопасности.	2	
	2. Основные понятия политики информационной безопасности.	2	
	3. Социальная инженерия.	2	
	Практические занятия	**8**	

	1. Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права.	2	
	2. Подготовка описания охраняемой информации, модели угроз, построение модели информационной безопасности.	4	
	3. Способы защиты от социальной инженерии.	2	
Раздел 2. Технологии защиты данных	***Содержание учебного материала***	**28**	ПК 1.1-ПК 1.7 ОК 01-09
	Лекции	**14**	
	1. Фундаментальные угрозы сетевой безопасности.	2	
	2. Стандарты информационной безопасности.	2	
	3. Безопасность сетевых устройств OSI.	2	
	4. Криптографическая защита данных. Криптографические системы.	4	
	5. Технологии аутентификации. Авторизация, аутентификация и учет доступа.	4	
	Практические занятия	**14**	
	1. Исследование сетевых атак и инструментов проверки защиты сети.	2	
	2. Исследование методов шифрования.	2	
	3. Изучение криптографической системы.	2	
	4. Изучение криптографии открытых ключей.	2	
	5. Организация безопасного доступа к устройствам.	2	
	6. Настройка безопасного доступа к маршрутизатору.	2	
	7. Обеспечение административного доступа AAA и сервера Radius.	2	
Раздел 3. Базовые технологии сетевой безопасности	***Содержание учебного материала***	**36**	ПК 1.1-ПК 1.7 ОК 01-09
	Лекции	**20**	
	1. Протоколы защиты на канальном и сеансовом уровнях. Защита на сетевом уровне.	4	
	2. Технологии межсетевого экранирования.	4	
	3. Реализация технологий брандмауэра. ACL.	4	
	4. Безопасность локальной сети.	4	
	5. Реализация технологий VPN.	4	
	Практические занятия	**16**	
	1. Настройка политики безопасности брандмауэров.	6	
	2. Настройка безопасности на втором уровне на коммутаторах.	6	
	3. Настройка Site-to-Site VPN, используя интерфейс командной строки.	4	
Раздел 4. Технологии обнаружения вторжений	***Содержание учебного материала***	**24**	ПК 1.1-ПК 1.7 ОК 01-09
	Лекции	**18**	
	1. Концепция адаптивного управления безопасностью.	4	
	2. Технология анализа защищенности.	4	
	3. Реализация технологий предотвращения вторжения.	2	
	4. Компьютерные вирусы и проблемы антивирусной защиты.	4	
	5. Антивирусные программы и комплексы.	4	
	Практические занятия	**16**	
	1. Исследование технологий предотвращения вторжения.	6	
	2. Настройка системы предотвращения вторжений (IPS).	6	
	3. Организация обеспечения безопасности пользовательских компьютеров.	4	

Раздел 5. Управление сетевой безопасностью	***Содержание учебного материала***	**30**	ПК 1.1-ПК 1.7 ОК 01-09
	Лекции	**12**	
	1. Задачи управления системой сетевой безопасности.	2	
	2. Архитектура управления безопасностью корпоративных информационных систем.	2	
	3. Управление безопасной сетью.	4	
	4. Cisco ASA.	4	
	Практические занятия	**18**	
	1. Изучение основных понятий глобальной и локальной политики безопасности.	2	
	2. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	4	
	3. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	2	
	4. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.	4	
	5. Настройка Clientless Remote Access SSL VPNs используя ASDM.	2	
	6. Настройка AnyConnect Remote Access SSL VPN используя ASDM.	2	
	7. Финальная комплексная практическая работа по безопасности.	2	

2.4 Содержание разделов дисциплины

2.4.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	**Информационная безопасность**	Основные понятия информационной безопасности и защиты информации. Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Государственная информационная политика. Проблемы информационной безопасности в сфере государственного и муниципального управления. Угрозы информационной безопасности. Анализ угроз информационной безопасности Методы и модели оценки уязвимости информации. Основные понятия политики информационной безопасности. Социальная инженерия. Техники социальной инженерии.	У, Т

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
2	**Технологии защиты данных**	Фундаментальные угрозы сетевой безопасности. Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак. Стандарты информационной безопасности. Безопасность сетевых устройств OSI. Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности. Криптографическая защита данных. Криптографические системы. Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей. Технологии аутентификации. Авторизация, аутентификация и учет доступа (AAA). Свойства AAA. Локальная AAA аутентификация. Server-based AAA.	У, Т
3	**Базовые технологии сетевой безопасности**	Протоколы защиты на канальном и сеансовом уровнях. Защита на сетевом уровне. Технологии межсетевого экранирования. Реализация технологий брандмауэра. ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах. Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN. Реализация технологий VPN. VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с использованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN.	Т, У
4	**Технологии обнаружения вторжений**	Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности ОС. Технологии обнаружения атак. Реализация технологий предотвращения вторжения. IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS. Компьютерные вирусы и проблемы антивирусной защиты. Классификация вирусов. Основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети.	У, Т
5	**Управление сетевой безопасностью**	Задачи управления системой сетевой безопасности. Архитектура управления безопасностью корпоративных информационных систем. Основные понятия. Концепция глобального управления безопасностью. Глобальная и локальная политики безопасности. Управление безопасной сетью. Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности. Cisco ASA. Введение в Адаптивное устройство безопасности ASA. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.	У, Т
Примечание: Т – тестирование, Р – написание реферата, У – устный опрос, КР – контрольная работа			

2.4.2 Занятия семинарского типа

- не предусмотрены

2.4.3 Практические занятия.

№	Наименование раздела	Наименование практических (лабораторных) работ	Форма текущего контроля
1	2	3	4
1.	**Информационная безопасность**	Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права. Подготовка описания охраняемой информации, модели угроз, построение модели информационной безопасности. Способы защиты от социальной инженерии.	ПР, У
2.	**Технологии защиты данных**	Исследование сетевых атак и инструментов проверки защиты сети. Исследование методов шифрования. Изучение криптографической системы. Изучение криптографии открытых ключей. Организация безопасного доступа к устройствам. Настройка безопасного доступа к маршрутизатору. Обеспечение административного доступа AAA и сервера Radius.	ПР, У
3.	**Базовые технологии сетевой безопасности**	Настройка политики безопасности брандмауэров. Настройка безопасности на втором уровне на коммутаторах. Настройка Site-to-Site VPN, используя интерфейс командной строки.	ПР, Т
4.	**Технологии обнаружения вторжений**	Исследование технологий предотвращения вторжения. Настройка системы предотвращения вторжений (IPS). Организация обеспечения безопасности пользовательских компьютеров.	ПР, У
5	**Управление сетевой безопасностью**	Изучение основных понятий глобальной и локальной политики безопасности. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM. Настройка Clientless Remote Access SSL VPNs используя ASDM. Финальная комплексная практическая работа по безопасности.	ПР, У

Примечание: ПР – практическая работа, ЛР – лабораторная работа; Т – тестирование, Р – написание реферата, У – устный опрос, КР – контрольная работа

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для преподавания лекционного материала дисциплины «Безопасность компьютерных сетей» применяются аудиовизуальные технологии, которые поднимают на качественно новый уровень роль преподавателя. Применение мультимедийного комплекса повышает наглядность, информативность, позволяет экономить время занятий.

Практические работы.

Технология, применяемая в процессе проведения практических занятий, сочетает возможности информационных технологий и практической работы для формирования понятийно-терминологической основы модуля, приобретения необходимых умений и навыков. Это позволяет работать в малых группах, коллективно обсуждать используемые технологии работы, возникающие проблемы, а также инициирует самостоятельную работу учащихся. При выполнении практических работ проявляется преемственность в профессиональном и творческом развитии учащихся.

№ раздела	Наименование раздела	Технологии, применяемые при проведении лекционных занятий	Технологии, применяемые при проведении практических занятий
1	2	3	4
1	Информационная безопасность	Технология развивающего обучения, аудиовизуальные технологии	Компьютерные симуляции, групповая дискуссия
2	Технологии защиты данных	Технология развивающего обучения, аудиовизуальные технологии	Компьютерные симуляции, групповая дискуссия
3	Базовые технологии сетевой безопасности	Технология развивающего обучения, аудиовизуальные технологии	Компьютерные симуляции, групповая дискуссия
4	Технологии обнаружения вторжений	Технология развивающего обучения, аудиовизуальные технологии	Компьютерные симуляции, групповая дискуссия
5	Управление сетевой безопасностью	Технология развивающего обучения, аудиовизуальные технологии	Компьютерные симуляции, групповая дискуссия

4 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРОГРАММЫ ДИСЦИПЛИНЫ МДК 01.03 «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

4.1 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Лаборатории «Организация и принципы построения компьютерных систем», оснащенные в соответствии с п. 6.1.2.1. Примерной программы по специальности 09.02.06 «Сетевое и системное администрирование».

Оснащенные базы практики, в соответствии с п 6.1.2.3 Примерной программы по специальности09.02.06 «Сетевое и системное администрирование».

4.2 Перечень необходимого программного обеспечения

1. 7-zip (лицензия на англ. http://www.7-zip.org/license.txt)
2. Adobe Acrobat Reader (лицензия – https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
3. Adobe Flash Player (лицензия – https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
4. Apache Open Office (лицензия – http://www.openoffice.org/license.html)
5. Free Commander (лицензия -https://freecommander.com/ru/%d0%bb%d0%b8%d1%86%d0%b5%d0%bd%d0%b7%d0%b8%d1%8f/)
6. Google Chrome (лицензия – https://www.google.ru/chrome/browser/privacy/eula_text.html)
7. Libre Office (в свободном доступе)
8. Mozilla Firefox (лицензия – https://www.mozilla.org/en-US/MPL/2.0/)
9. VirtualBox (в свободном доступе)

5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1 Основная литература

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А. В. Назаров, А. Н. Енгалычев, В. П. Мельников. - Москва : КУРС ; ИНФРА-М, 2020. – 360 с. – (Среднее профессиональное образование). – ISBN 978-5-906923-06-6. - URL: https://znanium.com/catalog/product/1071722.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ФОРУМ : ИНФРА-М, 2021. – 416 с. – (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. – Текст : электронный. – URL: https://znanium.com/catalog/product/1189327.– Режим доступа: по подписке.

5.2 Дополнительная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. – Москва : Издательство Юрайт, 2019. – 321 с. – (Профессиональное образование). – ISBN 978-5-534-07979-1. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://urait.ru/bcode/442312.

2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. – Москва : ФОРУМ : ИНФРА-М, 2020. – 368 с. – (Среднее профессиональное образование). – ISBN 978-5-91134-360-6. – Текст : электронный. – URL: https://znanium.com/catalog/product/1082470.– Режим доступа: по подписке.

3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2021. – 432 с. – (Среднее профессиональное образование). – ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189328.– Режим доступа: по подписке.

4. Баранова, Е. К. Основы информационней безопасности : учебник / Е. К. Баранова, А. В. Бабаш. - Москва : РИОР : ИНФРА-М, 2021. – 202 с. – (Среднее профессионааьное образование). - ISBN 978-5-369-01806-4. – Текст : электронный. - URL: https://znanium.com/catalog/product/1209579. – Режим доступа: по подписке.

5. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю. Н. Сычев. – Москва : ИНФРА-М, 2021. – 201 с. – (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. – Текст : электронный. - URL: https://znanium.com/catalog/product/1191479.– Режим доступа: по подписке.

6. Информационная безопасность : учебник / Мельников В. П. под ред., Куприянов А. И. – Москва : КноРус, 2020. – 267 с. – ISBN 978-5-406-07382-7. – URL: https://book.ru/book/932059. – Текст : электронный.

5.3 Периодические издания

1. Computerworld Россия. – URL: http://dlib.eastview.com/browse/publication/64081/udb/2071.
2. Windows IT Pro / Re. – URL: http://dlib.eastview.com/browse/publication/64079/udb/2071.
3. БИТ. Бизнес & информационные технологии – URL : http://dlib.eastview.com/browse/publication/66752/udb/2071.
4. Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. - URL: https://dlib.eastview.com/browse/publication/9166.
5. Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. URL: https://dlib.eastview.com/browse/publication/71227/udb/2630.
6. Виртуализация. Облачные структуры. Системы хранения данных. – URL : https://dlib.eastview.com/browse/publication/84826/udb/2071.
7. Журнал сетевых решений LAN. – URL: http://dlib.eastview.com/browse/publication/64078/udb/2071.
8. Защита персональных данных. – URL : https://dlib.eastview.com/browse/publication/90727/udb/2071.
9. Информатика и образование. – URL: http://dlib.eastview.com/browse/publication/18946/udb/1270.
10. Информатика, вычислительная техника и инженерное образование. - URL: https://www.elibrary.ru/title_about.asp?id=32586.
11. Информационно-управляющие системы. – URL: http://dlib.eastview.com/browse/publication/71235.
12. Мир больших данных. – URL : https://dlib.eastview.com/browse/publication/90728/udb/2071.
13. Мир ПК. – URL: http://dlib.eastview.com/browse/publication/64067/udb/2071.
14. Новые информационные технологии в автоматизированных системах https://elibrary.ru/title_about.asp?id=32949.
15. Открытые системы. СУБД. – URL: http://dlib.eastview.com/browse/publication/64072/udb/2071.
16. Прикладная информатика. – URL: https://e.lanbook.com/journal/2067#journal_name.
17. Проблемы передачи информации. – URL: http://www.mathnet.ru/php/archive.phtml?jrnid=ppi&wshow=contents&option_lang=rus.
18. Программные продукты и системы. – URL: https://dlib.eastview.com/browse/publication/64086/udb/2071.
19. Программные продукты и системы. – URL: http://dlib.eastview.com/browse/publication/64086/udb/2071.
20. САПР и графика. - URL: https://sapr.ru/list,
21. Системный администратор. – URL: https://dlib.eastview.com/browse/publication/66751/udb/2071.
22. Системный анализ и прикладная информатика. – URL: https://e.lanbook.com/journal/2420#journal_name.
23. Управление проектами и программами. – URL :

https://grebennikon.ru/journal-20.html#volume2019-3.

5.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ЭБС «BOOK.ru» [учебные издания – коллекция для СПО] : сайт. – URL: https://www.book.ru/cat/576.
2. ЭБС «Университетская библиотека ONLINE» [учебные, научные здания, первоисточники, художественные произведения различных издательств; журналы; мультимедийная коллекция, карты, онлайн-энциклопедии, словари] : сайт. – URL: http://biblioclub.ru/index.php?page=main_ub_red.
3. ЭБС издательства «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы] : сайт. – URL: http://e.lanbook.com.
4. ЭБС «Юрайт» [учебники и учебные пособия издательства «Юрайт»] : сайт. – URL: https://urait.ru/.
5. ЭБС «Znanium.com» [учебные, научные, научно-популярные материалы различных издательств, журналы] : сайт. – URL: http://znanium.com/.
6. Научная электронная библиотека. Монографии, изданные в издательстве Российской Академии Естествознания [полнотекстовый ресурс свободного доступа] : сайт. – URL: https://www.monographies.ru/.
7. Научная электронная библиотека статей и публикаций «eLibrary.ru» [российский информационно-аналитический портал в области науки, технологии, медицины, образования; большая часть изданий – свободного доступа] : сайт. – URL: http://elibrary.ru.
8. Базы данных компании «Ист Вью» [периодические издания (на русском языке)] : сайт. – URL: http://dlib.eastview.com.
9. КиберЛенинка : научная электронная библиотека [научные журналы в полнотекстовом формате свободного доступа] : сайт. – URL: http://cyberleninka.ru.
10. Российская электронная школа : государственная образовательная платформа [полный школьный курс уроков] : сайт. – URL: https://resh.edu.ru/.
11. Единое окно доступа к образовательным ресурсам : федеральная информационная система свободного доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для всех уровней образования: дошкольное, общее, среднее профессиональное, высшее, дополнительное : сайт. – URL: http://window.edu.ru.
12. Федеральный центр информационно-образовательных ресурсов [для общего, среднего профессионального, дополнительного образования; полнотекстовый ресурс свободного доступа] : сайт. – URL: http://fcior.edu.ru.
13. Единая коллекция цифровых образовательных ресурсов [для преподавания и изучения учебных дисциплин начального общего, основного общего и среднего (полного) общего образования; полнотекстовый ресурс свободного доступа] : сайт. – URL: http://school-collection.edu.ru.
14. Официальный интернет-портал правовой информации. Государственная система правовой информации [полнотекстовый ресурс свободного доступа] : сайт. – URL: http://publication.pravo.gov.ru.
15. Кодексы и законы РФ. Правовая справочно-консультационная система

[полнотекстовый ресурс свободного доступа] : сайт. – URL: http://kodeks.systecs.ru.
16. ГРАМОТА.РУ : справочно-информационный интернет-портал : сайт. – URL: http://www.gramota.ru.
17. Энциклопедиум [Энциклопедии. Словари. Справочники : полнотекстовый ресурс свободного доступа] // ЭБС «Университетская библиотека ONLINE» : сайт. – URL: http://enc.biblioclub.ru/.
18. СЛОВАРИ.РУ. Лингвистика в Интернете : лингвистический портал : сайт. – URL: http://slovari.ru/start.aspx?s=0&p=3050.hall.ru/magazines.html.
19. Электронный каталог Кубанского государственного университета и филиалов. – URL: http://212.192.134.46/MegaPro/Web/Home/About.

6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учащиеся для полноценного освоения учебного курса должны составлять конспекты как при прослушивании его теоретической (лекционной) части, так и при подготовке к практическим (семинарским) занятиям. Желательно, чтобы конспекты лекций и семинаров записывались в логической последовательности изучения курса и содержались в одной тетради. Это обеспечит более полную подготовку как к текущим учебным занятиям, так и сессионному контролю знаний.

Самостоятельная работа учащихся является важнейшей формой учебно-познавательного процесса. Цель заданий для самостоятельной работы – закрепить и расширить знания, умения, навыки, приобретенные в результате изучения дисциплины; овладеть умением использовать полученные знания в практической работе; получить первичные навыки профессиональной деятельности.

Обучение студентов осуществляется по традиционной технологии (лекции, практики) с включением инновационных элементов.

С точки зрения используемых методов лекции подразделяются следующим образом: информационно-объяснительная лекция, повествовательная, лекция-беседа, проблемная лекция и т. д.

Устное изложение учебного материала на лекции должно конспектироваться. Слушать лекцию нужно уметь – поддерживать своё внимание, понять и запомнить услышанное, уловить паузы. В процессе изложения преподавателем лекции студент должен выяснить все непонятные вопросы. Записывать содержание лекции нужно обязательно – записи помогают поддерживать внимание, способствуют пониманию и запоминанию услышанного, приводит знание в систему, служат опорой для перехода к более глубокому самостоятельному изучению предмета.

Методические рекомендации по конспектированию лекций:

– запись должна быть системной, представлять собой сокращённый вариант лекции преподавателя. Необходимо слушать, обдумывать и записывать одновременно;

– запись ведётся очень быстро, чётко, по возможности короткими выражениями;

– не прекращая слушать преподавателя, нужно записывать то, что необходимо усвоить. Нельзя записывать сразу же высказанную мысль преподавателя, следует её понять и после этого кратко записать своими словами или словами преподавателя. Важно, чтобы в ней не был потерян основной смысл сказанного; имена, даты, названия, выводы, определения записываются точно. Следует обратить внимание на оформление записи лекции. Для каждого предмета заводится общая тетрадь. Отличным от остального цвета следует выделять отдельные мысли и заголовки, сокращать отдельные слова и предложения, использовать условные знаки, буквы латинского и греческого алфавитов, а также некоторые приёмы стенографического сокращения слов.

Практические занятия по дисциплине «Безопасность компьютерных сетей» проводятся в основном по схеме:

– устный опрос по теории в начале занятия (обсуждение теоретических проблемных вопросов по теме);

– индивидуальная работа при выполнении заданий с использованием

персонального компьютера;

– решение практических задач индивидуально;

– подведение итогов занятия (или рефлексия);

– индивидуальные задания для подготовки к следующим практическим занятиям.

Цель практического занятия – научить студентов применять теоретические знания при решении практических задач на основе реальных данных. На практических занятиях преобладают следующие методы:

– вербальные (преобладающим методом должно быть объяснение);

– практические (письменные здания, групповые задания и т. п.).

Важным для студента является умение рационально подбирать необходимую учебную литературу. Основными литературными источниками являются:

– библиотечные фонды филиала КубГУ в г. Славянске-на-Кубани;

– электронная библиотечная система «Университетская библиотека онлайн»;

– электронная библиотечная система Издательства «Лань».

Поиск книг в библиотеке необходимо начинать с изучения предметного каталога и создания списка книг, пособий, методических материалов по теме изучения.

Просмотр книги начинается с титульного листа, следующего после обложки. На нём обычно помещаются все основные данные, характеризующие книгу: название, автор, выходные данные, данные о переиздании и т.д. На обороте титульного листа даётся аннотация, в которой указывается тематика вопросов, освещённых в книге, определяется круг читателей, на который она рассчитана. Большое значение имеет предисловие книги, которое знакомит читателя с личностью автора, историей создания книги, раскрывает содержание.

Прочитав предисловие и получив общее представление о книге, следует обратиться к оглавлению. Оглавление книги знакомит обучаемого с содержанием и логической структурой книги, позволяет выбрать нужный материал для изучения. Год издания книги позволяет судить о новизне материала. В книге могут быть примечания, которые содержат различные дополнительные сведения. Они печатаются вне основного текста и разъясняют отдельные вопросы. Предметные и алфавитные указатели значительно облегчают повторение изложенного в книге материала. В конце книги может располагаться вспомогательный материал. К нему обычно относятся инструкции, приложения, схемы, ситуационные задачи, вопросы для самоконтроля и т.д.

Для лучшего представления и запоминания материала целесообразно вести записи и конспекты различного содержания, а именно:

– пометки, замечания, выделение главного;

– план, тезисы, выписки, цитаты;

– конспект, рабочая запись, реферат, доклад, лекция и т.д.

Читать учебник необходимо вдумчиво, внимательно, не пропуская текста, стараясь понять каждую фразу, одновременно разбирая примеры, схемы, таблицы, рисунки, приведённые в учебнике.

Одним из важнейших средств, способствующих закреплению знаний, является краткая запись прочитанного материала – составление конспекта. Конспект – это краткое связное изложение содержания темы, учебника или его части, без подробностей и второстепенных деталей. По своей структуре и последовательности

конспект должен соответствовать плану учебника. Поэтому важно сначала составить план, а потом писать конспект в виде ответа на вопросы плана. Если учебник разделён на небольшие озаглавленные части, то заголовки можно рассматривать как пункты плана, а из текста каждой части следует записать те мысли, которые раскрывают смысл заголовка.

Требования к конспекту:

– краткость, сжатость, целесообразность каждого записываемого слова;

– содержательность записи- записываемые мысли следует формулировать кратко, но без ущерба для смысла. Объём конспекта, как правило, меньше изучаемого текста в 7-15 раз;

–конспект может быть как простым, так и сложным по структуре – это зависит от содержания книги и цели её изучения.

Методические рекомендации по конспектированию:

– прежде чем начать составлять конспект, нужно ознакомиться с книгой, прочитать её сначала до конца, понять прочитанное;

– на обложке тетради записываются название конспектируемой книги и имя автора, составляется план конспектируемого теста;

– записи лучше делать при прочтении не одного-двух абзацев, а целого параграфа или главы;

– конспектирование ведётся не с целью иметь определённый записи, а для более полного овладения содержанием изучаемого текста, поэтому в записях отмечается и выделяется всё то новое, интересное и нужное, что особенно привлекло внимание;

– после того, как сделана запись содержания параграфа, главы, следует перечитать её, затем снова обращаться к тексту и проверить себя, правильно ли изложено содержание.

Техника конспектирования:

– конспектируя книгу большого объёма, запись следует вести в общей тетради;

– на каждой странице слева оставляют поля шириной 25-30 мм для записи коротких подзаголовков, кратких замечаний, вопросов;

– каждая станица тетради нумеруется;

– для повышения читаемости записи оставляют интервалы между строками, абзацами, новую мысль начинают с «красной» строки;

– при конспектировании широко используют различные сокращения и условные знаки, но не в ущерб смыслу записанного. Рекомендуется применять общеупотребительные сокращения, например: м.б. – может быть; гос. – государственный; д.б. – должно быть и т.д.

– не следует сокращать имена и названия, кроме очень часто повторяющихся;

– в конспекте не должно быть механического переписывания текста без продумывания его содержания и смыслового анализа.

7 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ МДК 01.03 «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

7.1 Паспорт фонда оценочных средств

№ раздела	Наименование раздела	Компетенции	Форма текущего контроля
1	2	3	4
1	Информационная безопасность	ПК 1.1-ПК 1.7 ОК 01-09	Тестирование, практическое занятие
2	Технологии защиты данных	ПК 1.1-ПК 1.7 ОК 01-09	Тестирование, практическое занятие
3	Базовые технологии сетевой безопасности	ПК 1.1-ПК 1.7 ОК 01-09	Тестирование, практическое занятие
4	Технологии обнаружения вторжений	ПК 1.1-ПК 1.7 ОК 01-09	Тестирование, практическое занятие
5	Управление сетевой безопасностью	ПК 1.1-ПК 1.7 ОК 01-09	Тестирование, практическое занятие

7.2 Критерии оценки результатов обучения

Код и наименование ПК и ОК, формируемых в рамках модуля[1]	Критерии оценки	Методы оценки
ПК 1.1. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем ПК 1.3. Устранять неисправности в работе инфокоммуникационных систем ПК 1.4. Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества	Определение профессиональной задачи и этапов ее выполнения Эффективный поиск информации для решения профессиональной задачи Определение ресурсов для решения профессиональной задачи Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью

[1] В ходе оценивания могут быть учтены личностные результаты.

сетевой топологии в рамках своей ответственности	Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	обучающегося в процессе освоения образовательной программы
ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.		
ПК 1.6. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта		
ПК 1.7. Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем		
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различными контекстам	Подбор вариантов решения конкретной профессиональной задачи или проблемы	Оценка полноты перечня подобранных вариантов
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы	Оценка полноты перечня подобранных вариантов
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой	Демонстрация интереса к выбранной специальности, к инновационным технологиям в области профессиональной деятельности	Участие в мероприятиях (олимпиады, конкурсы профессионального мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли

грамотности в различных жизненных ситуациях		
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	Демонстрировать навыки межличностного общения с соблюдением общепринятых правил со сверстниками в образовательной группе, с преподавателями во время обучения, с руководителями производственной практики	Экспертное наблюдение поведенческих навыков в ходе обучения
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Демонстрация навыков грамотной устной и письменной речи	Экспертное наблюдение навыков устного и письменного общения в ходе обучения
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	Формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению; взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации; нетерпимости к коррупционным проявлениям	Участие в мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной направленности
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	Формирование бережного отношения к природе и окружающей среде	Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Формирование бережного отношения к здоровью	Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Демонстрация умения составлять тексты документов, относящихся к профессиональной деятельности, на государственном и иностранном языках	Экспертная оценка соблюдения правил составления документов

7.3 Оценочные средства для проведения текущей аттестации

Текущий контроль может проводиться в форме:
– фронтальный опрос – индивидуальный устный опрос
– письменный контроль
– тестирование по теоретическому материалу
– практическая работа – подготовка отчета,
– защита выполненного задания,
– разработка проблемы курса (сообщение).

Форма аттестации	**Знания**	**Умения**	**Владения (навыки)**	**Личные качества студента**	**Примеры оценочных средств**
Устный (письменный) опрос по темам	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков работы с литературными источниками	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Контрольные вопросы по темам прилагаются
Практические (лабораторные) работы	Контроль знания теоретических основ информатики и информационных технологий, возможностей и принципов использования современной компьютерной техники.	Оценка умения работать с современной компьютерной техникой, использовать возможности вычислительной техники и программного обеспечения при решении практических задач.	Оценка навыков работы с техническими средствами информатизации, специальными программными средствами	Оценка способности оперативно и качественно решать поставленные на практических работах задачи и аргументировать результаты	Темы работ прилагаются

Тестирование	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков логического анализа и синтеза при сопоставлении конкретных понятий	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Вопросы прилагаются

Примеры задач и вопросов для текущего контроля:

1. Терминология в области безопасности информационных сетей.

2. Методология построения безопасных информационных сетей.

3. Типовые модели атак, направленные на преодоление защиты информационных систем, условия их осуществимости, возможные последствия, способы предотвращения.

4. Описать роль человеческого фактора в обеспечении безопасности сетей.

5 Сформировать и произвести назначение ролей пользователям информационной системы.

6. Описать классификацию компьютерных вирусов.

7. Перечислить основные законодательные документы в области обеспечения безопасности хранения и обработки информации.

Примеры тестовых заданий:

1. Информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем, называется

А) конфиденциальной

Б) доступной

В) целостной

Г) все варианты верны

2. Набор правил, которые регламентируют функционирование механизма информационной безопасности называются

А) политикой

Б) идентификацией

В) конфиденциальностью

Г) все варианты верны

3. Формирование профиля прав для конкретного участника процесса информационного обмена, называется

А) авторизацией

Б) идентификацией

В) аутентификацией

Г) все варианты верны

4. Устройства контроля доступа из одной информационной среды в другую предоставляют

А) межсетевые экраны

Б) антивирусное обеспечение

В) сканеры безопасности

Г) все варианты верны

5. Устройства проверки качества функционирования модели безопасности для конкретной информационной системы обеспечивают

А) сканеры безопасности

Б) антивирусные программы

В) межсетевые экраны

Г) все варианты верны

6. Обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети – это

А) модель межсетевого взаимодействия OSI

Б) виртуальная частная сеть VPN

В) протокол IPSEC

Г) межсетевые экраны

7. Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними – это

А) протокол Kerberos

Б) протокол ARP

В) протокол ICMP

Г) протокол POP3

7.4. Оценочные средства для проведения промежуточной аттестации

Форма аттестации	Знания	Умения	Владение (навыки)	Личные качества студента	Примеры оценочных средств
Итоговая аттестация					
Экзамен	Контроль знания базовых положений в области администрирования компьютерных систем	Оценка умения понимать специальную терминологию. Оценка умения решать типовые задачи в области эксплуатации объектов сетевой инфра-	Оценка навыков логического сопоставления и характеристики объектов Оценка навыков логического мышления при решении задач в области эксплуатации объектов сетевой инфраструктуры	Оценка способности грамотно и четко излагать материал Оценка способности грамотно и четко излагать ход решения задач в области эксплуатации объектов сетевой инфраструктуры	Вопросы прилагаются Задачи прилагаются

7.4.1 Примерные вопросы для проведения промежуточной аттестации

1. Понятие национальной безопасности.
2. Национальные интересы в информационной сфере.
3. Источники и содержание угроз в информационной сфере.
4. Современные угрозы сетевой безопасности.

5. Безопасность сетевых устройств OSI.

6. Обеспечение безопасности пользовательских компьютеров.

7. IPS технологии.

8. Технология брандмауэра.

9. Основные понятия криптографической защиты информации.

10. Симметричные криптосистемы шифрования.

11. Асимметричные криптосистемы шифрования.

12. Электронная цифровая подпись и функция хэширования.

13. Аутентификация, авторизация и администрирование действий пользователей.

14. Концепция построения виртуальных защищенных сетей VPN.

15. Протоколы формирования защищенных каналов на канальном и сеансовом уровнях.

16. Технологии защиты в беспроводных сетях.

17. Протокол Kerberos.

18. Технологии обнаружения атак.

19. Компьютерные вирусы и проблемы антивирусной защиты.

20. Антивирусные программы и комплексы.

21. Управление безопасной сетью.

7.4.2 Примерные задачи для проведения промежуточной аттестации

1. Продемонстрировать использование встроенных средств ОС для обеспечения безопасности.

2. Продемонстрировать процесс установки и настройки программных средств защиты (программные прокси-серверы, диагностические программы и т.п.).

4. Продемонстрировать управление пользователями и их правами доступа в ОС Windows.

5. Продемонстрировать использование программы Ethereal для анализа сетевого трафика.

6. Провести анализ уровня безопасности защиты данных в ОС Windows.

8 ДОПОЛНИТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Криптографическая защита данных. Криптографические системы.

Наука, занимающаяся вопросами безопасной связи (т.е. посредством зашифрованных сообщений называется *Криптологией* (kryptos – тайный, logos – наука). Она в свою очередь разделяется на два направления *криптографию* и *криптоанализ.*

Криптография – наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

Криптоанализ – данный раздел посвящен исследованию возможности чтения сообщений без знания ключей, т. е. связана непосредственно со взломом шифров. Люди, занимающиеся криптоанализом и исследованием шифров называются *криптоаналитиками*.

Шифр – совокупность обратимых преобразований множества открытых текстов (т.е. исходного сообщения) на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

Криптографическая система – семейство преобразований шифра и совокупность ключей (т.е. алгоритм + ключи). Само по себе описание алгоритма не является криптосистемой. Только дополненное схемами распределения и управления ключами оно становится системой. Примеры алгоритмов – описания DES, ГОСТ28.147-89. Дополненные алгоритмами выработки ключей превращаются в криптосиситемы. Как правило, описание алгоритма шифрования уже включает в себя все необходимые части. Криптосистемы могут обеспечивать не только секретность передаваемых сообщений, но и их аутентичность (подлинность), а также подтверждение подлинности пользователя.

Современные криптосистемы делятся на симметричные и асимметричные.

Симметричные криптосистемы (с секретным ключом) – данные криптосистемы построены на основе сохранения в тайне ключа шифрования. Процессы зашифровывания и расшифровывания используют один и тот же ключ. Секретность ключа является постулатом. Основная проблема при применении симметричных криптосистем для связи заключается в сложности передачи обоим сторонам секретного ключа. Однако данные системы обладают высоким быстродействием. Раскрытие ключа злоумышленником грозит раскрытием только той информации, что была зашифрована на этом ключе. Американский и Российский стандарты шифрования DES и ГОСТ28.147-89, кандидаты на AES – все эти алгоритмы являются представителями симметричных криптосистем.

Асимметричные криптосистемы (*системы открытого шифрования*) – смысл данных криптосистем состоит в том, что для зашифрования и расшифрования используются разные преобразования. Одно из них – зашифрование – является абсолютно открытым для всех. Другое же – расшифрование – остается секретным. Таким образом, любой, кто хочет что-либо зашифровать, пользуется открытым преобразованием.

Но расшифровать и прочитать это сможет лишь тот, кто владее секретным преобразованием. В настоящий момент во многих асимметричных криптосистемах вид преобразования определяется ключом. Т.е у пользователя есть два ключа – секретный и открытый. Открытый ключ публикуется в общедоступном месте, и каждый, кто захочет послать сообщение этому пользователю – зашифровывает текст открытым ключом. Расшифровать сможет только упомянутый пользователь с секретным ключом. Таким образом, пропадает проблема передачи секретного ключа (как у симметричных систем). Однако, несмотря на все свои преимущества, эти криптосистемы достаточно трудоемки и медлительны. Стойкость асимметричных криптосистем базируется, в основном, на алгоритмической трудности решить за приемлемое время какую-либо задачу. Если злоумышленнику удастся построить такой алгоритм, то дискредитирована будет вся система и все сообщения, зашифрованные с помощью этой системы. В этом состоит главная опасность асимметричных криптосистем в отличие от симметричных. Одно из основных правил криптографии (если рассматривать ее коммерческое применение, т.к. на государственном уровне все несколько иначе) можно выразить следующим образом: *взлом шифра с целью прочесть закрытую информацию должен обойтись злоумышленнику гораздо дороже, чем эта информация стоит на самом деле*.

Тайнопись.

Тайнописью называются приемы, с помощью которых содержание написанного скрывалось от тех, кто не должен был прочитать текст.

Начиная с самых древних времен, человечество обменивалось информацией, отсылая друг другу бумажные письма. В Древнем Великом Новгороде необходимо был сворачивать свои берестяные грамоты словами наружу – только таким образом они могли перевозиться и храниться, в противном случае они разворачивались самопроизвольно из-за изменения уровня влажности. Это было похоже на современные почтовые карточки, в которых текст, как известно, также открыт для чужих взоров.

Точных дат и абсолютно бесспорных данных о тайнописи в древности сохранилось очень и очень мало, поэтому на нашем сайте многие факты представлены путем художественного анализа. Однако, вместе с изобретением шифров существовали, разумеется, и способы сокрытия текста от посторонних глаз. В древней Греции, к примеру, для этого как-то раз обрили раба, нанесли надпись на его голове, и, после того как волосы отросли, отправили с поручением к адресату.

Шифрова́ние – способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи. Согласно ГОСТ 28147-89, шифрование подразделяется на процесс зашифровывания и расшифровывания.

Стеганогра́фия (от греч. скрытый и греч. пишу, буквально «тайнопись») – это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Основные принципы компьютерной стеганографии и области её применения

К. Шеннон дал нам общую теорию тайнописи, которая является базисом стеганографии как науки. В современной компьютерной стеганографии существует два основных типа файлов: сообщение– файл, который предназначен для скрытия, и контейнер–файл, который может быть использован для скрытия в нем сообщения. При этом контейнеры бывают двух типов. Контейнер–оригинал (или “Пустой” контейнер) – это контейнер, который не содержит скрытой информации. Контейнер–результат (или “Заполненный” контейнер) – это контейнер, который содержит скрытую информацию. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер.

Основными положениями современной компьютерной стеганографии являются следующие:

1. Методы скрытия должны обеспечивать аутентичность и целостность файла.
2. Предполагается, что противнику полностью известны возможные стеганографические методы.
3. Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации – ключа.
4. Даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

В связи с возрастанием роли глобальных компьютерных сетей становится все более важным значение стеганографии. Анализ информационных источников компьютерной сети Internet позволяет вделать вывод, что в настоящее время стеганографические системы активно используются для решения следующих основных задач:

1. Защита конфиденциальной информации от несанкционированного доступа;
2. Преодоление систем мониторинга и управления сетевыми ресурсами;
3. Камуфлирования программного обеспечения;
4. Защита авторского права на некоторые виды интеллектуальной собственности.

Криптографическая стойкость (или криптостойкость) – способность криптографического алгоритма противостоять возможным атакам на него. Атакующие криптографический алгоритм используют методы криптоанализа. Стойким считается алгоритм, который для успешной атаки требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна, и т. Д

Типы криптостойких систем шифрования.

Абсолютно стойкие системы. Доказательство существования абсолютно стойких алгоритмов шифрования было выполнено Клодом Шенноном и опубликовано в работе «Теория связи в секретных системах». Там же определены требования к такого рода системам:

- ключ генерируется для каждого сообщения (каждый ключ используется один раз)
- ключ статистически надёжен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны)

- длина ключа равна или больше длины сообщения
- исходный (открытый) текст обладает некоторой избыточностью (является критерием оценки правильности расшифровки)

Стойкость этих систем не зависит от того, какими вычислительными возможностями обладает криптоаналитик. Практическое применение систем, удовлетворяющих требованиям абсолютной стойкости, ограничено соображениями стоимости и удобства пользования.

Некоторыми аналитиками утверждается, что Шифр Вернама является одновременно абсолютно криптографически стойким и к тому же единственным шифром, который удовлетворяет этому условию.

Достаточно стойкие системы. В основном применяются практически стойкие или вычислительно стойкие системы. Стойкость этих систем зависит от того, какими вычислительными возможностями обладает криптоаналитик. Практическая стойкость таких систем базируется на теории сложности и оценивается исключительно на какой-то определенный момент времени и последовательно с двух позиций:

- вычислительная сложность полного перебора
- известные на данный момент слабости (уязвимости) и их влияние на вычислительную сложность.

В каждом конкретном случае могут существовать дополнительные критерии оценки стойкости.

Сложность алгоритма позволяет оценить, насколько быстро растет его трудоёмкость с увеличением объема входных данных. Под трудоемкостью понимается количество элементарных операций, которые необходимо выполнить для решения задачи с помощью данного алгоритма. Обычно оценка сложности алгоритма представляется в виде O(f(N)), где O – функция сложности, а N – число обрабатываемых наблюдений или примеров. Наименее затратными являются алгоритмы, для которых функция сложности имеет вид f(N) = C и f(N) = C*N, где C – константа. В первом случае вычислительные затраты не зависят от количества обрабатываемых данных, а во втором – линейно возрастают. Самыми затратными являются алгоритмы, сложность которых имеет степенную и факториальную зависимости от числа обрабатываемых наблюдений.

Длина ключа.

Количество информации в ключе, как правило, измеряется в битах.

Для современных симметричных алгоритмов (AES, CAST5, IDEA, Blowfish, Twofish) основной характеристикой криптостойкости является длина ключа. Шифрование с ключами длиной 128 бит и выше считается сильным, так как для расшифровки информации без ключа требуются годы работы мощных суперкомпьютеров. Для асимметричных алгоритмов, основанных на проблемах теории чисел (проблема факторизации – RSA, проблема дискретного логарифма – Elgamal) в силу их особенностей минимальная надёжная длина ключа в настоящее время – 1024 бит. Для асимметричных алгоритмов, основанных на использовании теории эллиптических кривых (ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002), минимальной надёжной длиной ключа считается 163 бит, но рекомендуются длины от 191 бит и выше.

В этой методологии и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия.

Если ключ не был скомпрометирован, то при расшифровке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию.

Так как отправитель и получатель – единственные люди, которые знают этот симметричный ключ, при компрометации ключа будет скомпрометировано только взаимодействие этих двух пользователей. Проблемой, которая будет актуальна и для других криптосистем, является вопрос о том, как безопасно распространять симметричные (секретные) ключи.

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Порядок использования систем с симметричными ключами:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.
2. Отправитель создает электронную подпись с помощью расчета хэш-функции для текста и присоединения полученной строки к тексту
3. Отправитель использует быстрый симметричный алгоритм шифрования-расшифровки вместе с секретным симметричным ключом к полученному пакету (тексту вместе с присоединенной электронной подписью) для получения зашифрованного текста. Неявно таким образом производится аутентификация, так как только отправитель знает симметричный секретный ключ и может зашифровать этот пакет. Только получатель знает симметричный секретный ключ и может расшифровать этот пакет.
4. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.
5. Получатель использует тот же самый симметричный алгоритм шифрования-расшифровки вместе с тем же самым симметричным ключом (который уже есть у получателя) к зашифрованному тексту для восстановления исходного текста и электронной подписи. Его успешное восстановление аутентифицирует кого-то, кто знает секретный ключ.
6. Получатель отделяет электронную подпись от текста.
7. Получатель создает другую электронную подпись с помощью расчета хэш-функции для полученного текста.
8. Получатель сравнивает две этих электронных подписи для проверки целостности сообщения (отсутствия его искажения)

Доступными сегодня средствами, в которых используется симметричная методология, являются:

- Kerberos, который был разработан для аутентификации доступа к ресурсам в сети, а не для верификации данных. Он использует центральную базу данных, в которой хранятся копии секретных ключей всех пользователей.
- Сети банкоматов (ATM Banking Networks). Эти системы являются оригинальными разработками владеющих ими банков и не продаются. В них также используются симметричные методологии.

Сравнение с асимметричными криптосистемами.

Достоинства:

- скорость (по данным Applied Cryptography – на 3 порядка выше)
- простота реализации (за счёт более простых операций)

- меньшая требуемая длина ключа для сопоставимой стойкости
- изученность (за счёт большего возраста)

Недостатки:

- сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 – 499500 и т. д.
- сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.

Для компенсации недостатков симметричного шифрования в настоящее время широко применяется комбинированная (гибридная) криптографическая схема, где с помощью асимметричного шифрования передаётся сеансовый ключ, используемый сторонами для обмена данными с помощью симметричного шифрования.

Важным свойством симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне.

В этой методологии ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится в тайне. Хотя можно шифровать и расшифровывать обоими ключами, данные, зашифрованные одним ключом, могут быть расшифрованы только другим ключом.

Все асимметричные криптосистемы являются объектом атак путем прямого перебора ключей, и поэтому в них должны использоваться гораздо более длинные ключи, чем те, которые используются в симметричных криптосистемах, для обеспечения эквивалентного уровня защиты. Брюс Шнейер в книге «Прикладная криптография: протоколы, алгоритмы и исходный текст на С» приводит следующие данные об эквивалентных длинах ключей.

Длина симметричного ключа	Длина открытого ключа
56 бит	384 бит
64 бита	512 бит
80 бит	768 бит
112 бит	1792 бита
128 бит	2304 бита

Для того чтобы избежать низкой скорости алгоритмов асимметричного шифрования, генерируется временный симметричный ключ для каждого сообщения и только он шифруется асимметричными алгоритмами. Само сообщение шифруется с использованием этого временного сеансового ключа и алгоритма шифрования/расшифровки, описанного в пункте 2.1.1.1. Затем этот сеансовый ключ шифруется с помощью открытого асимметричного ключа получателя и асимметричного алгоритма шифрования. После этого этот зашифрованный сеансовый ключ вместе с зашифрованным сообщением передается получателю. Получатель использует тот же самый асимметричный алгоритм шифрования и свой секретный ключ для расшифровки

сеансового ключа, а полученный сеансовый ключ используется для расшифровки самого сообщения.

В асимметричных криптосистемах важно, чтобы сеансовые и асимметричные ключи были сопоставимы в отношении уровня безопасности, который они обеспечивают. Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Хакеры будут атаковать не их, а сеансовые ключи. Асимметричные открытые ключи уязвимы к атакам прямым перебором отчасти из-за того, что их тяжело заменить. Если атакующий узнает секретный асимметричный ключ, то будет скомпрометирован не только текущее, но и все последующие взаимодействия между отправителем и получателем.

Порядок использования систем с асимметричными ключами:

1. Безопасно создаются и распространяются асимметричные открытые и секретные ключи (см. раздел 2.2 ниже). Секретный асимметричный ключ передается его владельцу. Открытый асимметричный ключ хранится в базе данных X.500 и администрируется центром выдачи сертификатов (по-английски – Certification Authority или CA). Подразумевается, что пользователи должны верить, что в такой системе производится безопасное создание, распределение и администрирование ключами. Более того, если создатель ключей и лицо или система, администрирующие их, не одно и то же, то конечный пользователь должен верить, что создатель ключей на самом деле уничтожил их копию.

2. Создается электронная подпись текста с помощью вычисления его хэш-функции. Полученное значение шифруется с использованием асимметричного секретного ключа отправителя, а затем полученная строка символов добавляется к передаваемому тексту (только отправитель может создать электронную подпись).

3. Создается секретный симметричный ключ, который будет использоваться для шифрования только этого сообщения или сеанса взаимодействия (сеансовый ключ), затем при помощи симметричного алгоритма шифрования/расшифровки и этого ключа шифруется исходный текст вместе с добавленной к нему электронной подписью – получается зашифрованный текст (шифр-текст).

4. Теперь нужно решить проблему с передачей сеансового ключа получателю сообщения.

5. Отправитель должен иметь асимметричный открытый ключ центра выдачи сертификатов (CA). Перехват незашифрованных запросов на получение этого открытого ключа является распространенной формой атаки. Может существовать целая система сертификатов, подтверждающих подлинность открытого ключа CA. Стандарт X.509 описывает ряд методов для получения пользователями открытых ключей CA, но ни один из них не может полностью защитить от подмены открытого ключа CA, что наглядно доказывает, что нет такой системы, в которой можно было бы гарантировать подлинность открытого ключа CA.

6. Отправитель запрашивает у CA асимметричный открытый ключ получателя сообщения. Этот процесс уязвим к атаке, в ходе которой атакующий вмешивается во взаимодействие между отправителем и получателем и может модифицировать трафик, передаваемый между ними. Поэтому открытый асимметричный ключ получателя «подписывается» CA. Это означает, что CA использовал свой асимметричный секретный ключ для шифрования асимметричного отрытого ключа получателя. Только CA знает асимметричный секретный ключ CA, поэтому есть гарантии того, что

открытый асимметричный ключ получателя получен именно от CA.

7. После получения асимметричный открытый ключ получателя расшифровывается с помощью асимметричного открытого ключа CA и алгоритма асимметричного шифрования/расшифровки. Естественно, предполагается, что CA не был скомпрометирован. Если же он оказывается скомпрометированным, то это выводит из строя всю сеть его пользователей. Поэтому можно и самому зашифровать открытые ключи других пользователей, но где уверенность в том, что они не скомпрометированы?

8. Теперь шифруется сеансовый ключ с использованием асимметричного алгоритма шифрования-расшифровки и асимметричного ключа получателя (полученного от CA и расшифрованного).

9. Зашифрованный сеансовый ключ присоединяется к зашифрованному тексту (который включает в себя также добавленную ранее электронную подпись).

10. Весь полученный пакет данных (зашифрованный текст, в который входит помимо исходного текста его электронная подпись, и зашифрованный сеансовый ключ) передается получателю. Так как зашифрованный сеансовый ключ передается по незащищенной сети, он является очевидным объектом различных атак.

11. Получатель выделяет зашифрованный сеансовый ключ из полученного пакета.

12. Теперь получателю нужно решить проблему с расшифровкой сеансового ключа.

13. Получатель должен иметь асимметричный открытый ключ центра выдачи сертификатов (CA).

14. Используя свой секретный асимметричный ключ и тот же самый асимметричный алгоритм шифрования получатель расшифровывает сеансовый ключ.

15. Получатель применяет тот же самый симметричный алгоритм шифрования-расшифровки и расшифрованный симметричный (сеансовый) ключ к зашифрованному тексту и получает исходный текст вместе с электронной подписью.

16. Получатель отделяет электронную подпись от исходного текста.

17. Получатель запрашивает у CA асимметричный открытый ключ отправителя.

18. Как только этот ключ получен, получатель расшифровывает его с помощью открытого ключа CA и соответствующего асимметричного алгоритма шифрования-расшифровки.

19. Затем расшифровывается хэш-функция текста с использованием открытого ключа отправителя и асимметричного алгоритма шифрования-расшифровки.

20. Повторно вычисляется хэш-функция полученного исходного текста.

21. Две эти хэш-функции сравниваются для проверки того, что текст не был изменен.

Алгоритмы криптосистемы с открытым ключом можно использовать:

– как самостоятельные средства для защиты передаваемой и хранимой информации;

– как средства распределения ключей. Обычно с помощью алгоритмов криптосистем с открытым ключом распределяют ключи, малые по объёму. А саму передачу больших информационных потоков осуществляют с помощью других алгоритмов;

– как средства аутентификации пользователей.

Преимущества:

1. Преимущество асимметричных шифров перед симметричными шифрами состоит в отсутствии необходимости предварительной передачи секретного ключа по надёжному каналу.

2. В симметричной криптографии ключ держится в секрете для обеих сторон, а в асимметричной криптосистеме только один секретный.

3. При симметричном шифровании необходимо обновлять ключ после каждого факта передачи, тогда как в асимметричных криптосистемах пару (*E,D*) можно не менять значительное время.

4. В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки:

1. Преимущество алгоритма симметричного шифрования над несимметричным заключается в том, что в первый относительно легко внести изменения.

2. Хотя сообщения надежно шифруются, но «засвечиваются» получатель и отправитель самим фактом пересылки шифрованного сообщения.

3. Несимметричные алгоритмы используют более длинные ключи, чем симметричные. Ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа несимметричного алгоритма с аналогичной криптостойкостью:

Длина симметричного ключа, бит	Длина несимметричного ключа, бит
56	384
64	512
80	768
112	1792
128	2304

Процесс шифрования-расшифрования с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом.

В чистом виде асимметричные криптосистемы требуют существенно больших вычислительных ресурсов, потому на практике используются в сочетании с другими алгоритмами.

Для ЭЦП сообщение предварительно подвергается хешированию, а с помощью асимметричного ключа подписывается лишь относительно небольшой результат хеш-функции.

Для шифрования они используются в форме гибридных криптосистем, где большие объёмы данных шифруются симметричным шифром на сеансовом ключе, а с помощью асимметричного шифра передаётся только сам сеансовый ключ.

В криптографии линейным криптоанализом называется метод криптоаналитического вскрытия, использующий линейные приближения для описания работы шифра.

Линейный криптоанализ был изобретён японским криптологом Мицуру Мацуи (Mitsuru Matsui).

Предложенный им в 1993 г. (на Еврокрипте-93) алгоритм был изначально направлен на вскрытие DES и FEAL. Впоследствии линейный криптоанализ был распространён и на другие алгоритмы. На сегодняшний день наряду с дифференциальным криптоанализом является одним из наиболее распространённых методов вскрытия блочных шифров. Разработаны атаки на блочные и потоковые шифры.

Открытие линейного криптоанализа послужило толчком к построению новых криптографических схем.

Принцип работы.

Криптоанализ происходит в два шага. Первый – построение соотношений между открытым текстом, шифротекстом и ключом, которые справедливы с высокой вероятностью. Второй – использование этих соотношений вместе с известными парами открытый текст – шифротекст для получения битов ключа.

Защита от линейного криптоанализа

Для атаки на блочный шифр с помощью линейного криптоанализа достаточно, как было описано выше, получить линейное соотношение, существенно смещённое по вероятности от 1/2. Соответственно, первая цель при проектировании шифра, стойкого к атаке, – минимизировать вероятностные смещения, убедиться, что подобное соотношение не будет существовать. Другими словами, необходимо сделать так, чтобы при *любом* изменении текста или ключа в получающемся шифротексте ровно половина бит меняла своё значение на противоположное, причём каждый бит изменялся с вероятностью 1/2. Обычно это достигается путём выбора высоко нелинейных S-боксов и усилением *диффузии*.

Данный подход обеспечивает хорошее обоснование стойкости шифра, но чтобы строго доказать защищённость от линейного криптоанализа, разработчикам шифров необходимо учитывать более сложное явление – *эффект линейных оболочек* (linear hull effect).

Несколько более общая теория доказательства защищённости от класса атак, основанных на линейном криптоанализе, базируется на понятии *декорреляции*. Теория предполагает, чтобы устройство являлось так называемым декорреляционным модулем, эффективно блокирующим распространение традиционных линейных и дифференциальных характеристик. Следует заметить, что шифры, которые оптимальны против некоторого узкого класса атак, обычно слабы против других типов атак.

Управление ключами (УК) является настолько важной и развитой областью криптографии, что требует отдельного и детального рассмотрения. На системы УК возлагается огромный набор различных функций, обеспечение самых разных базовых и вновь приобретенных свойств криптосистем, которые ими укомплектованы. Подобные схемы могут выполнять хранение, пересылку, шифрование (то есть обеспечение конфиденциальности), аутентификацию, «сдачу на хранение» (депонирование) и разделение ключей. Единственным общим свойством систем УК является то, что как результат разнообразных трансформаций они должны снабдить криптосистему ключом (симметричным или асимметричным), на котором и будет произведен основной процесс шифрования документа.

В зависимости от того, какой тип ключа генерирует в итоге система УК, производится их деление на системы управления, симметричными ключами и системы управления асимметричными ключами.

Системы управления симметричными ключами делятся в свою очередь на системы с наличием начальных мастер-ключей и системы с нулевой начальной информацией. Как отдельный материал рассмотрены системы депонирования ключей и системы разделения секрета. К сожалению, данный раздел не может охватить даже половины различных схем УК и криптографических протоколов на их основе – на сегодняшний день исследователями разработано более сотни различных схем. Все чаще и чаще встречающееся сейчас введение третьего субъекта криптоопераций – доверенных лиц с различными функциями и полномочиями – породило целую волну протоколов, обеспечивающих новые свойства криптосистем (апеллируемость, подтверждение даты/времени подписания, депонирование ключей и т. п.).

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины
МДК.01.03 Безопасность компьютерных сетей
для специальности 09.02.06 Сетевое и системное администрирование

Рабочая программа учебной дисциплины МДК.01.03 Безопасность компьютерных сетей соответствует ФГОС по специальности среднего профессионального образования 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519, зарегистрирован в Министерстве юстиции 15.08.2023 г. (рег. № 74796), и примерной основной образовательной программе по специальности 09.02.06 Сетевое и системное администрирование.

В рабочую программу учебной дисциплины включены разделы «Паспорт рабочей программы учебной дисциплины», «Структура и содержание учебной дисциплины», «Образовательные технологии», «Условия реализации программы учебной дисциплины», «Перечень основных и дополнительных информационных источников, необходимых для освоения дисциплины», «Методические рекомендации обучающимся по освоению дисциплины», «Оценочные средства для контроля успеваемости» и «Дополнительное обеспечение дисциплины».

Структура и содержание рабочей программы соответствуют целям образовательной программы СПО по специальности 09.02.06 «Сетевое и системное администрирование» и будущей профессиональной деятельности студента.

Объем рабочей программы учебной дисциплины полностью соответствует учебному плану подготовки по данной специальности. В программе четко сформулированы цели обучения, а также прогнозируемые результаты обучения по дисциплине.

На основании проведенной экспертиза можно сделать заключение, что рабочая программа учебной дисциплины МДК.01.03 Безопасность компьютерных сетей по специальности 09.02.06 «Сетевое и системное администрирование» соответствует требованиям стандарта, профессиональным требованиям, а также современным требованиям рынка труда.

Технический директор ООО «ПРАЙ»
« » 20 г.

Б.А. Шишкин

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины
МДК.01.03 Безопасность компьютерных сетей
для специальности 09.02.06 Сетевое и системное администрирование

Рабочая программа учебной МДК.01.03 Безопасность компьютерных сетей соответствует ФГОС по специальности среднего профессионального образования 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519, зарегистрирован в Министерстве юстиции 15.08.2023 г. (рег. № 74796), и примерной основной образовательной программе по специальности 09.02.06 Сетевое и системное администрирование.

В рабочую программу учебной дисциплины включены разделы «Паспорт рабочей программы учебной дисциплины», «Структура и содержание учебной дисциплины», «Образовательные технологии», «Условия реализации программы учебной дисциплины», «Перечень основных и дополнительных информационных источников, необходимых для освоения дисциплины», «Методические рекомендации обучающимся по освоению дисциплины», «Оценочные средства для контроля успеваемости» и «Дополнительное обеспечение дисциплины».

Структура и содержание рабочей программы соответствуют целям образовательной программы СПО по специальности 09.02.06 «Сетевое и системное администрирование» и будущей профессиональной деятельности студента.

Объем рабочей программы учебной дисциплины полностью соответствует учебному плану подготовки по данной специальности. В программе четко сформулированы цели обучения, а также прогнозируемые результаты обучения по дисциплине.

На основании проведенной экспертиза можно сделать заключение, что рабочая программа учебной дисциплины МДК.01.03 Безопасность компьютерных сетей по специальности 09.02.06 «Сетевое и системное администрирование» соответствует требованиям стандарта, профессиональным требованиям, а также современным требованиям рынка труда.

Технический директор
ООО «ТехноСтарт» И.Г. Колодезный

« » 20 г.