МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
КОЛЛЕДЖ СЕРВИСА И ДИЗАЙНА

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.01.03 Безопасность компьютерных сетей

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2026

Рабочая программа учебной дисциплины МДК.01.03 Безопасность компьютерных сетей профессионального модуля ПМ.01 Настройка сетевой инфраструктуры разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утверждённого приказом Минобрнауки РФ от 10.07.2023 г. № 619, примерной образовательной программой.

Разработчики:

Головин Д.И, преподаватель Колледжа сервиса и дизайна ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от «18» 05 2026 г.

Председатель ЦМК _____ Е.А. Стефанович
подпись

Согласована:

Начальник отдела информационных технологий, Филиал Российской телевизионной и радиовещательной сети «Приморский краевой радиотелевизионный передающий центр»

_____ *Д.М. Шумов*
(подпись, печать)

СОДЕРЖАНИЕ

1. Общая характеристика рабочей программы учебной дисциплины

1.1 Место дисциплины в структуре основной образовательной программы

Рабочая программа МДК.01.03 Безопасность компьютерных сетей является частью профессионального цикла основной образовательной программы (далее ООП) в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

1.2 Цель и планируемые результаты освоения дисциплины

По итогам освоения дисциплины, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице:

Код ОК, ПК	Код результата обучения	Наименование результата обучения
ПК1.1- ПК.1.7 ОК1- ОК9	У1	Проектировать локальную сеть, выбирать сетевые топологии
	У2	Использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети
	З1	Общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям
	З2	Архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры
	З3	Базовые протоколы и технологии локальных сетей
	З4	Принципы построения высокоскоростных локальных сетей
	З5	Стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	108
В том числе	
- теоретическое обучение	30
- практические занятия	46
- самостоятельная работа	32
- промежуточная аттестация – дифференцированный зачет 4 (6) семестр	-

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект		Объём в часах
1	2		3
Раздел 3. Безопасность компьютерных сетей			**108/46**
Раздел 3. Безопасность компьютерных сетей			**108/46**
Тема 1.3 Безопасность компьютерных сетей	**Содержание**		**30**
	1	**Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	
	2	**Безопасность Сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.	
	3	**Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA	
	4	**Списки контроля доступа (ACL)** Принцип работы ACL списков. Типы ACL-списков для IPv4. Рекомендации по созданию и размещению ACL-списков. Размещение стандартных и расширенных ACL-списков. Настройка стандартного ACL-списка. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков. Поиск и устранение неполадок ACL-списков.	
	5	**Реализация технологий брандмауэра** ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах.	
	6	**Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	
	7	**Безопасность локальной сети** Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN	
	8	**Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.	

	9	**Реализация технологий VPN** Сети VPN. Основы сетей VPN. Типы сетей VPN. Туннели GRE между объектами. Основы GRE. Настройка туннелей GRE. Общие сведения об IPsec. Защита протокола IP. Структура протокола IPsec. Удалённый доступ. Решения VPN для удалённого доступа. Сети VPN удалённого доступа с использованием IPsec.	
	10	**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.	
	Практические занятия и лабораторные работы		**46**
	3.1.1	Социальная инженерия	
	3.1.2	Исследование сетевых атак и инструментов проверки защиты сети	
	3.1.3	Настройка безопасного доступа к маршрутизатору	
	3.1.4	Обеспечение административного доступа AAA и сервера Radius	
	3.1.5	Настройка политики безопасности брандмауэров	
	3.1.6	Настройка системы предотвращения вторжений (IPS)	
	3.1.7	Настройка безопасности на втором уровне на коммутаторах	
	3.1.8	Исследование методов шифрования	
	3.1.9	Настройка Site-to-SiteVPN используя интерфейс командной строки	
	3.1.10	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	
	3.1.11	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	
	3.1.12	Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	
	3.1.13	НастройкаClientless Remote Access SSL VPNs используя ASDM	
	3.1.14	Настройка AnyConnect Remote Access SSL VPN используя ASDM	
	3.1.15	Финальная комплексная лабораторная работа по безопасности	
Самостоятельная работа при изучении раздела 3 ПМ.03 • Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). • Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа при самом широком использовании Интернета и других IT технологий.			**32**

• Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка • рефератов, докладов. • Выполнение чертежей, схем; выполнение расчётно-графических работ; модельный экономический анализ, • Опытно-экспериментальная работа. • Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** 1. Изучить характеристики, принципы работы, компоненты и конфигурирование коммутаторов Huawei. 2. Изучить характеристики, принципы работы, компоненты и конфигурирование маршрутизаторов Huawei. 3. Изучить характеристики, принципы работы, компоненты и конфигурирование брандмауэров Huawei. 4. Изучить характеристики, принципы работы, компоненты и конфигурирование брандмауэров Huawei. 5. Изучить характеристики, принципы работы, компоненты и конфигурирование беспроводных сетей Huawei.	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Кабинет информационных технологий:

количество посадочных мест – 25, стол для преподавателя 1 шт., стул для преподавателя 1 шт., компьютерный стол 20 шт., персональный компьютер ПК i3 2120/500Gb/4Gb 20 шт., мультимедийный комплект: проектор, интерактивная доска Elite Panaboard UBT-T880W 1 шт., звуковые колонки 1 шт., доска маркерная меловая комбинированная 1 шт., информационный стенд 2 шт., дидактические пособия.

ПО: 1. Windows 7(профессиональная лицензия, ООО "Битроникс Владивосток" Контракт№ 032010003081400018-45081 от 09.09.14 № 48609744, №62096196, № 48958910, № 45829305, бессрочно);

2. MS Office 2010 pro (лицензия № 48958910, № 47774898, бессрочно);

3. Autodesk AutoCAD 2019 Edu (свободное);

4. visual c++ 2008 express edition (свободное),

5. oracle vm virtualbox (свободное),

6. cisco packet tracer (свободное),

7. microsoft SQL server 2008 (свободное),

8. k-lite codec pack (свободное),

9. visual studio 2008 (свободное).

Лаборатория организации и принципов построения компьютерных систем:

количество посадочных мест – 15, стол для преподавателя 1 шт., стул для преподавателя 1 шт.,

мультимедийный проектор с экраном 1 шт., персональный компьютер "B-tronix professional 3872\2015" 13 шт, стартовый набор Arduino UNO R3 Starter Kit V2 6 компонентов,

myRIO 6 шт контроллер ILC 131 STARTEKIT 10 шт., коммутатор 6 шт., маршрутизатор 6 шт.,

доска маркерная 1 шт.

Программное обеспеспечение:

1. "Microsoft Windows 7 Professional Russian, ООО ""Битроникс Владивосток" "Контракт№ 032010003081400018-45081 от 09.09.14, лицензия №64099496, бесрочно"

2. Microsoft Office профессиональный плюс 2013

3. "AUTOMATIONWORX Software Suite 2016 v1.83, ООО ""Лидер Электро Поставки"", Договор ЛАП059177 от 12.08.14, лицензия №77190396 от 24.10.14"

4. Android Studio (свободное),

5. Microsoft Visual Studio (свободное)

6. Visual Studio Community 2019 (свободное)

Студия проектирования и дизайна сетевых архитектур и инженерной графики

автоматизированные рабочие места на 20 обучающихся (персональный компьютер Lenovo ThinkStation P330 Tiny (процессор I7 9700T, оперативная память 32gb, жесткий диск 1tb)

монитор Lenovo ThinkCentre TIO27 2560x1440 (веб камера, микрофон, динамики встроены в монитор), мышь, клавиатура;

автоматизированное рабочее место преподавателя (ноутбук Lenovo IdealPad L340, процессор i7 9750H, оперативная память 8gb, жесткий диск 1tb), мышь, клавиатура;

специальная эргономическая мебель для работы за компьютером: компьютерный стол 20шт., компьютерное кресло 20 шт., стол преподавателя 1 шт., компьютерное кресло для преподавателя 1шт., 1 роектор CASIO XJ-F210WN 1 шт., экран 1 шт., принтер МФУ Xerox VersaLink C7020, цветной 1 шт., графический планшет WACOM Cintiq 16-10 шт.

25

Программное обеспечение:

1. Windows 10 Pro, ИП Струлев О.Ю. Д№32008976244 от 06.04.2020, OEM
2. OfficeProfessional Plus 2019 AcademicEdition, ООО "Акцент", Договор №292 от 24.04.2020 лицензия №V6635206 от 07.05.2020, бессрочно;
3. Adobe Creative Cloud, ООО"ИНФОРМИКА", Договор №32008982727 от 16.04.2020, лицензия от 19.04.2020;
4. Corona Render for 3ds Max-Educational-1WS+NODE, ООО"ИНФОРМИКА", Договор №32008982727 от 16.04.2020, лицензия от 08.04.2020;
5. Autodesk 3ds Max (свободное);
6. Autodesk Maya (свободное);
7. Autodesk AutoCad 2020 (свободное);
8. Autodesk Fusion 360 (свободное)

Мастерская по компетенции «Сетевое и системное администрирование»

Ноутбук -9шт; монитор 9; маршрутизатор 15; модуль Serial 9; коммутатор L2 - 9; межсетевой экран 5; напольная рэковая стойка 5; сервер 9; источник бесперебойного питания 9; коммутатор 1; телекоммуникационный шкаф 1; коммутатор L3- 9in/

Программное обеспечение:

1. Microsoft Office 2019
2. Microsoft Windows 10
3. Desktop & Application Virtualization VMware Horizon Standard Price

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 464 с.

Сергеев А.Н. Основы локальных компьютерных сетей: учебное пособие. СПО. – Москва: Лань, 2020. – 184 с.

3.2.2. Электронные издания (электронные ресурсы)

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2019. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437357 (дата обращения: 26.07.2021).
2. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189333 (дата обращения: 26.07.2021). – Режим доступа: по подписке.

3.2.3. Дополнительные источники *(при необходимости)*

Новожилов Е.О. Компьютерные сети. – М.: ОИЦ «Академия, 2013.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	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 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 расход-	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. Оценка «**хорошо**» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	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 обучающегося в процессе освоения образовательной программы. Экзамен квалификационный.

ных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.		

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным 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 грамотности в различных жизненных ситуациях.	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
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	Демонстрация навыков 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 тради-	Формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению; взаимного уважения, бе-	Участие в мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной

ционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	режного отношения к культурному наследию и традициям многонационального народа Российской Федерации; нетерпимости к коррупционным Проявлениям.	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

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

МДК.01.03 Безопасность компьютерных сетей

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2026

Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по МДК.01.03 Безопасность компьютерных сетей разработан в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утверждённого приказом Минобрнауки РФ от 10.07.2023 г. № 619, примерной образовательной программой.

Разработчик: Д.И. Головин, преподаватель КСД ВВГУ

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 9 от «18» 05 2026 г.

Председатель ЦМК _____ *Е.А. Стефанович*

1 Общие положения

Фонд оценочных средств (далее – ФОС) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины 09.02.06 Безопасность компьютерных сетей.

ФОС включают в себя контрольные материалы для проведения текущего контроля успеваемости в виде устного собеседования или теста и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачета (с использованием оценочного средства - опрос в форме ответов на тест).

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения
ПК1.1- ПК.1.7 ОК1- ОК9	У1	Проектировать локальную сеть, выбирать сетевые топологии
	У2	Использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети
	З1	Общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям
	З2	Архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры
	З3	Базовые протоколы и технологии локальных сетей
	З4	Принципы построения высокоскоростных локальных сетей
	З5	Стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

3 Соответствие оценочных средств контролируемым результатам обучения

3.1 Средства, применяемые для оценки уровня теоретической подготовки

Краткое наименование раздела (МДК), темы, параграфа дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Тема 1 Безопасность компьютерных сетей: - фундаментальные принципы безопасности сети; - безопасность сетевых устройств OSI; - авторизация, аутентификация и учет доступа (AAA); - списки контроля доступа (ACL); - реализация технологий брандмауэра ACL; - реализация технологий предотвращения вторжения; - безопасность локальной сети; - криптографические системы; - реализация технологий VPN; - управление безопасной сетью.	**З1**	Способность использовать знания общих принципов построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям при создании и эксплуатации компьютерных сетей	*Устный опрос (п. 5.1, вопросы 1 –50)* *Реферат (п. 5.2)*	*Тест* *Билеты на экзамен*
	З2	Способность использовать знания архитектуры протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры при создании и эксплуатации компьютерных сетей		
	З3	Способность использовать знания базовых протоколов и технологий локальных сетей при создании и эксплуатации компьютерных сетей		
	З4	Способность использовать знания принципов построения высокоскоростных локальных сетей при создании и эксплуатации компьютерных сетей		
	З5	Способность использовать знания стандартов кабелей, основных видов коммуникационных устройств, терминов, понятий, стандартов и типовых		

	У1	элементов структурированной кабельной системы при создании и эксплуатации компьютерных сетей Способность использовать умения проектирования локальной сети, выбора сетевой топологии		
	У2	Способность использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети при эксплуатации компьютерных сетей.		

3.2 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (МДК), темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	
Тема 1 Безопасность компьютерных сетей *Практическая работа 3.1.1* Социальная инженерия *Практическая работа 3.1.2* Исследование сетевых атак и инструментов про-	**З1**	Способность использовать знания общих принципов построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям при создании и эксплуатации компьютерных сетей	*Защита практических работ 3.1.1 – 3.1.15.*	*Тест 1* *Билеты на экзамен*

верки защиты сети *Практическая работа 3.1.3* Настройка безопасного доступа к маршрутизатору *Практическая работа 3.1.4* Обеспечение административного доступа AAA и сервера Radius *Практическая работа 3.1.5* Настройка политики безопасности брандмауэров *Практическая работа 3.1.6* Настройка системы предотвращения вторжений (IPS) *Практическая работа 3.1.7* Настройка безопасности на втором уровне на коммутаторах *Практическая работа 3.1.8* Исследование методов шифрования *Практическая работа 3.1.9* Настройка Site-to-SiteVPN используя интерфейс командной строки *Практическая работа 3.1.10* Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки *Практическая работа 3.1.11* Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM *Практическая работа 3.1.12* Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны	**З2**	Способность использовать знания архитектуры протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры при создании и эксплуатации компьютерных сетей		
	З3	Способность использовать знания базовых протоколов и технологий локальных сетей при создании и эксплуатации компьютерных сетей		
	З4	Способность использовать знания принципов построения высокоскоростных локальных сетей при создании и эксплуатации компьютерных сетей		
	З5	Способность использовать знания стандартов кабелей, основных видов коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы при создании и эксплуатации компьютерных сетей		
	У1	Способность использовать умения проектирования локальной сети, выбора сетевой топологии		

используя шлюз безопасности ASA посредством ASDM *Практическая работа 3.1.13* НастройкаClientless Remote Access SSL VPNs используя ASDM *Практическая работа 3.1.14* Настройка AnyConnect Remote Access SSL VPN используя ASDM *Практическая работа 3.1.15* Финальная комплексная лабораторная работа по безопасности	**У2**	Способность использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети при эксплуатации компьютерных сетей.		

4 Описание процедуры оценивания

Результаты обучения по учебной дисциплине, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по профессиональному модулю проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками при проведении практических работ, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой профессиональному модулю).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по учебной дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом. Оценка на зачете выставляется с учетом оценок, полученных при прохождении текущей аттестации.

Критерии оценивания устного ответа

Оценочные средства: собеседование, устное сообщение, семинар.

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

Оценочные средства: реферат, конспект, контрольная работа, письменный отчет по лабораторной работе, доклад (сообщение), в том числе выполненный в форме презентации.

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полно-

стью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	*Отлично*	*Хорошо*	*Удовлетворительно*	*Неудовлетворительно*
Количество правильных ответов	91 % и ≥	от 81% до 90,9 %	не менее 60%	менее 60%

Критерии выставления оценки студенту на зачете

Оценочные средства: устный опрос в форме ответов на контрольные вопросы, устный опрос в форме собеседования, выполнение реферата.

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и

	умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

Тема 1 Фундаментальные принципы безопасности сети
1 Перечислите и охарактеризуйте современные угрозы сетевой безопасности
2 Перечислите и охарактеризуйте вирусы, черви и троянские кони.
3 Перечислите и охарактеризуйте методы атак.

Тема 2 Безопасность Сетевых устройств OSI
4 Что такое безопасный доступ к устройствам?
5 Что означает назначение административных ролей?
6 Расскажите про безопасность при мониторинге и управлении устройствами.
7 Опишите использование функция автоматизированной настройки безопасности.

Тема 3 Авторизация, аутентификация и учет доступа (AAA)
8 Опишите свойства AAA.
9 Что такое локальная AAA аутентификация?
10 Опишите Server-based AAA.

Тема 4 Списки контроля доступа (ACL)
11 Опишите принцип работы ACL списков.
12 Перечислите и охарактеризуйте типы ACL-списков для IPv4.
13 Какие есть рекомендации по созданию и размещению ACL-списков.?
14 Как размещать стандартные и расширенные ACL-списки?
15 Как настроить стандартный ACL-список?
16 Опишите структуру и настройку расширенных ACL-списков для IPv4?
17 Как выполняется фильтрация трафика с использованием расширенных ACL-списков?
18 Объясните поиск и устранение неполадок ACL-списков.

Тема 5. Реализация технологий брандмауэра
19 Что такое технология брандмауэра?
20 Что такое контекстный контроль доступа (CBAC)?

21 Опишите политики брандмауэра, основанные на зонах.

Тема 6. Реализация технологий предотвращения вторжения
22 Что такое IPS технологии?
23 Что такое IPS сигнатуры?
24 Объясните реализацию IPS.
25 Как выполняются IPS?

Тема 7 Безопасность локальной сети
26 Как обеспечивается безопасность пользовательских компьютеров?
27 Предложите свои соображения по безопасности второго уровня (Layer-2).
28 Охарактеризуйте безопасность беспроводных сетей, VoIP и SAN.

Тема 8 Криптографические системы
29 Какие криптографические сервисы Вы можете назвать?
30 Что такое конфиденциальность с точки зрения криптографии?
31 Опишите криптографию открытых ключей.

Тема 9 Реализация технологий VPN
32 Что такое сети VPN?
33 Объясните основы сетей VPN.
34 Перечислите типы сетей VPN.
35 Что такое туннели GRE между объектами?
36 Объясните основы GRE.
37 Дайте общие сведения об IPsec.
38 Как выполняется защита протокола IP?
39 Опишите структуру протокола IPsec.
40 Как выполняется удалённый доступ?
41 Опишите решения VPN для удалённого доступа.
42 Опишите сети VPN удалённого доступа с использованием IPsec.

Тема 10 Управление безопасной сетью
43 Перечислите принципы безопасности сетевого дизайна.
44 Что такое безопасная архитектура?
45 Опишите управление процессами и безопасность.
46 Как выполняется тестирование сети на уязвимости?
47 Объясните понятия непрерывность бизнеса, планирование восстановления аварийных ситуаций.
48 Объясните жизненный цикл сети.
49 Что такое планирование сети?
50 Что такое разработка регламентов компании и политик безопасности?

5.2 Темы рефератов

1.Методы борьбы с фишинговыми атаками.

2.Законодательство о персональных данных.

3. Защита авторских прав.

4. Назначение, функции и типы систем видеозащиты.

5. Как подписывать с помощью ЭЦП электронные документы различных форматов.

6. Обзор угроз и технологий защиты Wi-Fi-сетей.

7. Проблемы внедрения дискового шифрования.

8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

9.Особенности процессов аутентификации в корпоративной среде.

10. Квантовая криптография.

11. Утечки информации: как избежать. Безопасность смартфонов.

12.Безопасность применения пластиковых карт - законодательство и практика.

13. Защита CD- и DVD-дисков от копирования.

14. Современные угрозы и защита электронной почты.

15. Программные средства анализа локальных сетей на предмет уязвимостей.

16.Безопасность применения платежных систем - законодательство и практика.

17.Аудит программного кода по требованиям безопасности.

18.Антишпионское ПО (antispyware).

19.Обеспечение безопасности Web-сервисов.

20.Защита от внутренних угроз.

21. Технологии RFID.

22. Уничтожение информации на магнитных носителях.

23. Ботнеты - плацдарм современных кибератак.

24.Цифровые водяные знаки в изображениях.

25. Электронный документооборот. Модели нарушителя.

26. Идентификация по голосу. Скрытые возможности.

27. Безопасность океанских портов.

28. Безопасность связи.

29. Безопасность розничной торговли.

30. Банковская безопасность.

31. Информатизация управления транспортной безопасностью.

32. Биопаспорт.

33. Обзор современных платформ архивации данных.

34. Что такое консалтинг в области ИБ.

35. Бухгалтерская отчетность как источник рассекречивания информации.

36. Управление рисками: обзор употребительных подходов.

37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38. Распределенные атаки на распределенные системы.

39. Оценка безопасности автоматизированных систем.

40. Windows и Linux: что безопаснее?

41. Функциональная безопасность программных средств.

42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43. Информационная безопасность: экономические аспекты.

5.3 Примеры тестовых заданий

Тест 1 Маршрутизация м коммутация. Масштабирование сетей

Количество вопросов – 143. Преподаватель формирует нужное количество вариантов теста с любым количеством вопросов.

№ п/п	Вопрос с вариантами ответов	Правильный ответ
1.	Какой термин безопасности используется для описания чего-либо ценного для организации? Он включает людей, оборудование и данные. 1. Уязвимость 2. Эксплойт 3. Ресурс 4. Риски	3
2.	Какой термин безопасности используется для описания слабости системы или ее структур, которые могут быть использованы злоумышленниками? 1. Уязвимость 2. Ресурс 3. Риски 4. Устранение	1
3.	Какой термин безопасности используется для описания компании? 1. Уязвимость 2. Эксплойт 3. Обнаружение угроз 4. Риски	3
4.	Какой термин безопасности используется для описания механизма, который использует уязвимость? 1. Эксплойт 2. Обнаружение угроз 3. Риски 4. Устранение	1
5.	Какой термин безопасности используется для описания потенциальной угрозы или риска? 1. Уязвимость 2. Эксплойт 3. Ресурс 4. Устранение	4
6.	Какой термин безопасности используется для описания вероятности угроз? 1. Уязвимость 2. Эксплойт 3. Обнаружение угроз 4. Риски	4
7.	Какой тип описания в сценарии: удаленное проникновение в несколько банкоматов с помощью ноутбука, 1. «Белый» хакер	2

	2. «Серый» хакер 3. «Черный» хакер	
8.	Какой тип описания в сценарии: Моя работа заключается в выявлении уязвимостей сети моей компании. 1. «Белый» хакер 2. «Серый» хакер 3. «Черный» хакер	1
9.	Какой тип описания в сценарии: Я использовал вредоносное ПО для нескольких стандартных систем с целью хранения данных кредитных карт. Я продал эту информацию по самой высокой цене. 1. «Белый» хакер 2. «Серый» хакер 3. «Черный» хакер	3
10.	Какой тип описания в сценарии: Во время исследования слабых мест в корпоративной сети, у меня есть доступ к уязвимости. 1. «Белый» хакер 2. «Серый» хакер 3. «Черный» хакер	1
11.	Какой тип описания в сценарии: Моя работа - работа с технологическими организациями, чтобы исправить ошибку с DNS. 1. «Белый» хакер 2. «Серый» хакер 3. «Черный» хакер	1
12.	Какой инструмент тестирования на проникновение использует алгоритмические схемы для кодирования данных? 1. Анализаторы пакетов 2. Средства шифрования 3. Средства эксплуатации уязвимостей 4. Инструменты технической экспертизы 5. Отладчики	2
13.	Какие инструменты используются «черными» хакерами для декомпиляции двоичных файлов при программировании эксплойтов? Они также используют «белыми» хакерами при анализе вредоносного ПО. 1. Инструменты создания пакетов 2. Детекторы руткитов 3. Средства эксплуатации уязвимостей 4. Инструменты технической экспертизы 5. Отладчики	5
14.	Какой инструмент тестирования на проникновение используется для исследований и проверок надежности межсетевого экрана? 1. Инструменты создания пакетов 2. Средства шифрования 3. Детекторы руткитов 4. Инструменты технической экспертизы 5. Отладчики	1
15.	Какой инструмент тестирования на проникновение использует «белыми» хакерами для анализа трафика на выявленные следы улиц,	4

	имеющихся на компьютере? 1. Фаззеры для поиска уязвимостей 2. Средства шифрования 3. Анализаторы пакетов 4. Инструменты технической экспертизы 5. Отладчики	
16.	Какой инструмент тестирования на проникновение является уязвимым к атаке злоумышленников? 1. Анализаторы пакетов 2. Средства шифрования 3. Средства эксплуатации уязвимостей 4. Инструменты технической экспертизы 5. Отладчики	3
17.	В памяти зараженного компьютера? Главная задача этого вредоносного ПО - автоматически копировать свой код и распространять его по сети от системы к системе. 1. Рекламные программы 2. Руткит 3. Шпионское ПО 4. Вирус 5. Интернет-червь	5
18	Какая вредоносная программа не создает своих копий? Она часто содержит вредоносный программный код, который можно скачать под другим именем, например, без приложения или файла. Атакует устройство изнутри. 1. Рекламные программы 2. Руткит 3. Шпионское ПО 4. Трояны 5. Червь	4
19.	В качестве вредоносного ПО, которое используется для сбора информации 1. Рекламные программы 2. Руткит 3. Шпионское ПО 4. Вирус 5. Вирусы-вымогатели	3
20.	Какое вредоносное ПО обычно отображает раздражающие всплывающие окна и используется для получения прибыли от рекламы? 1. Рекламные программы 2. Руткит 3. Шпионское ПО 4. Вирус 5. Интернет-червь	1
21.	Конфиденциальная информация пытается склонить людей к разглашению? 1. Фишинг 2. Руткит	1

	3. Шпионское ПО 4. Вирус 5. Интернет-червь	
22.	Привилегированный доступ? 1. Рекламные программы 2. Вирусы 3. Шпионское ПО 4. Руткит 5. Интернет-червь	4
23.	Защита от заражения требует доступа к зараженной системе? 1. Рекламные программы 2. Руткит 3. Шпионское ПО 4. Вирус 5. Вирусы-вымогатели	5
24	К какому типу атаки относится несанкционированное проникновение? 1. Разведывательная атака 2. Атака доступа 3. DoS-атака 4. Социальная инженерия	4
25	К какому типу относится атака с подбором пароля? 1. Разведывательная атака 2. Атака доступа 3. DoS-атака 4. Социальная инженерия	2
26	К какому типу атаки относится сканирование портов? 1. Разведывательная атака 2. Атака доступа 3. DoS-атака 4. Социальная инженерия	1
27	К какому типу относится атака через посредника (человек посередине)? 1. Разведывательная атака 2. Атака доступа 3. DoS-атака 4. Социальная инженерия	2
28	К какому типу относится спуфинг-атака? 1. Разведывательная атака 2. Атака доступа 3. DoS-атака 4. Социальная инженерия	2
29	Используется, когда данные используются для прозрачного мониторинга, сбора данных и контроля обмена данными. 1. Атака с подменой адреса 2. Атаки по методу умножения и отражения	4

	3. Атака на основе ICMP 4. Атаки через посредника (MITM) 5. Перехват сеанса	
30	Какая атака используется, когда пользователи получают доступ к физической сети, а затем используют доступ через посредника для перехвата и обработки трафика законного пользователя? 1. Атака с подменой адреса 2. Атаки по методу умножения и отражения 3. Атака на основе ICMP 4. Атаки через посредника (MITM) 5. Перехват сеанса	5
31	Какая атака используется, когда злоумышленники начинают одновременную скоординированную атаку из нескольких компьютеров-источников? 1. Атака с подменой адреса 2. Атаки по методу умножения и отражения 3. Атака на основе ICMP 4. Атака через посредника (MITM) 5. Перехват сеанса	2
32	Используется эхо-атака, при которой обнаруживаются подсети и хосты в защищенной сети, для создания лавинной атаки DoS, а также изменяются данные маршрутизации хоста? 1. Атака с подменой адреса 2. Атаки по методу умножения и отражения 3. Атака на основе ICMP 4. Атака через посредника (MITM) 5. Перехват сеанса	3
33	Какая атака используется, когда злоумышленник создает пакеты с ложной информацией об IP-доступе к источнику, позволяющему либо скрыть личность отправителя, либо выдать себя за другого легитимного пользователя? 1. Атака с подменой адреса 2. таки по методу умножения и отражения 3. Атака на основе ICMP 4. Атака через посредника 5. Перехват сеанса	1
34	Какая атака использует трехстороннее квитирование? 1. атака со сбросом TCP; 2. флуд-атака UDP; 3. лавинная атака SYN-flood TCP; 4. DoS-атака 5. перехват сеанса ПТС.	3
35	Какая атака использует четырехсторонний обмен для завершения соединений, используя пару сегментов FIN и ACK от каждого хоста? 1. атака со сбросом TCP; 2. флуд-атака UDP; 3. атака SYN-флуда TCP; 4. DoS-атака	1

	5. перехват сеанса TCP.	
36	В этом случае мне пришлось бы использовать IP-адрес одного хоста, спрогнозировать следующий порядковый номер и отправить подтверждение (ACK) на другом хосте. 1. атака со сбросом TCP; 2. флуд-атака UDP; 3. атака SYN-флуда TCP; 4. DoS-атака 5. перехват сеанса TCP.	5
37	Как только сервер просматривает все известные порты, он пытается найти закрытые порты. 1. атака со сбросом TCP; 2. флуд-атака UDP; 3. атака SYN-флуда TCP; 4. DoS-атака 5. перехват сеанса TCP	2
38	Сетевое устройство гарантирует, что внутренний трафик не может вызвать соединения с внутренними узлами? 1. Сеть VPN 2. Межсетевой экран ASA 3. IPS 4. ESA / WSA 5. Сервер AAA	2
39	Какой сервер содержит защищенную базу данных? 1. Сеть VPN 2. Межсетевой экран ASA 3. IPS 4. ESA / WSA 5. Сервер AAA	5
40	Безопасность и безопасность трафика. 1. Сеть VPN 2. Межсетевой экран ASA 3. IPS 4. ESA / WSA 5. Сервер AAA	4
41	Сетевое устройство безопасности используется для предоставления защищенных сервисов VPN с корпоративными сайтами и поддержки удаленного доступа для удаленных пользователей, использующих защищенные зашифрованные туннели? 1. Сеть VPN 2. Межсетевой экран ASA 3. IPS 4. ESA / WSA 5. Сервер AAA	1
42	Устройство сетевой безопасности отслеживает входящий и исходный трафик на предмет поиска вредоносного программного обеспечения.	3

	1. Сеть VPN 2. Межсетевой экран ASA 3. IPS 4. ESA / WSA 5. Сервер AAA	
43	Какой метод шифрования повторяет процесс алгоритма три раза и считается очень надежным при реализации очень коротких сроков службы ключа? 1. Шифр Rivest 2. Тройной DES 3. Шифрование блоками 4. Стандарт шифрования данных (DES) 5. Поточное шифрование	2
44	Какой метод шифрования шифрует каждый бит или открытый текст? Примеры включают в себя RC4 и A5? 1. Шифр Rivest 2. Шифрование блоками 3. Стандарт шифрования данных (DES) 4. Алгоритм программного шифрования 5. Поточное шифрование	5
45	Ключ шифрования применяется для шифрования и расшифровки данных? 1. Тройной DES 2. Симметричное 3. Шифрование блоками 4. Стандарт шифрования данных (DES) 5. Асимметричное	2
46	Какой метод шифрования является потоковым шифром и используется для защиты веб-трафика в SSL и TLS? 1. Шифр Rivest 2. Тройной DES 3. Симметричное 4. Шифрование блоками 5. Стандарт шифрования данных (DES)	1
47	ИТ-отдел сообщает, что веб-сервер одновременно получает слишком большое количество запросов веб-страниц из разных мест. Какой тип атаки безопасности происходит? 1. Рекламное ПО 2. DDoS-атака 3. Фишинг 4. Социальная инженерия 5. Шпионское ПО	2
48	Что вызывает переполнение буфера? 1. запуск контрмер безопасности для нейтрализации троянов 2. загрузка и установка слишком большого количества обновлений программного обеспечения одновременно 3. попытка записать больше данных в области памяти, чем эта область может содержать	3

	4. Это приводит к потере пакетов. 5. отправка повторных подключений, таких как Telnet, к определенному устройству.	
49	Какая цель безопасной связи - результат шифрования данных? 1. Аутентификация 2. Доступность 3. Конфиденциальность 4. Целостность	3
50	Какой тип вредоносных программ имеет основную цель распространения по сети? 1. интернет-червь 2. вирус 3. троян 4. Ботнет	1
51	Какой алгоритм может обеспечить конфиденциальность данных? 1. MD5 2. AES 3. Использование RSA 4. ИПК	2
52	Какие три элемента являются составляющими триады КЦД? (Выберите три варианта.) 1. Доступ 2. Целостность 3. Масштабируемость 4. Доступность 5. Конфиденциальность 6. Вмешательство	2, 4, 5
53	В рамках какого кибератаки происходит скоординированная атака из ботнета, состоящего из компьютеров-зомби? 1. DDoS-атака 2. MITM 3. Перенаправление ICMP 4. Подмена адреса (спуфинг)	1
54	Какое специализированное сетевое устройство отвечает за соблюдение политик управления доступом между сетями? 1. Коммутатор 2. IDS 3. Мост 4. Межсетевой экран	4
55	К какой категории атакует система безопасности? 1. DoS-атака 2. Атака доступа 3. Разведывательная атака 4. Социальная инженерия	2
56	В чем состоит роль IPS? 1. Обнаружение шаблонов вредоносного трафика с использованием файлов сигнатур	1

	2. Обеспечение соблюдения политик управления доступом на основе пакета 3. Фильтрация трафика на основе определенных правил и контекста соединения 4. Фильтрации трафика на основе информации 7-го уровня	
57	При каком типе атакует DNS, киберпреступник взламывает родительский домен и создает несколько поддонов для использования во время атаки? 1. Подделка записей кеша 2. Лавинообразное умножение и отражение 3. Туннелирование 4. Теневое копирование	4
58	Какие два типа хакеров обычно классифицируются как "серые"? (Выберите два варианта.) 1. Спонсируемые ограничения хакеры 2. Хактивисты 3. Хакеры-дилетанты 4. Киберпреступники 5. Брокер уязвимостей	2, 5
59	Что является опасной угрозой вирусного ПО? 1. Вирус запускается событием в хост-системе. 2. После установки на хост-систему вирус автоматически распространяется на другие системы. 3. Вирус может работать независимо от хост-системы. 4. Вирус - это вредоносное ПО, которое может распространяться только через Интернет.	1
60	Уборщик пытается войти в компьютерную лабораторию, но в этот день не будет плановая уборка. Атака какого типа была только что предотвращена? 1. Троян 2. Взгляд через плечо 3. Вардрайвинг 4. Социальная инженерия 5. Фишинг	4
61	Какие преимущества VPN позволяют предприятию легко приглашать пользователей в сеть? 1. Сокращение затрат 2. Информационная безопасность 3. Масштабируемость 4. Совместимость	3
62	Какие преимущества VPN позволяют предприятию увеличить пропускную способность для удаленных сайтов без необходимости добавления дополнительного оборудования или каналов глобальной сети? 1. Сокращение затрат 2. Информационная безопасность 3. Масштабируемость 4. Совместимость	1

63	Какие преимущества VPN используют усовершенствованные протоколы шифрования и аутентификации для защиты данных от несанкционированного доступа? 1. Сокращение затрат 2. Информационная безопасность 3. Масштабируемость 4. Совместимость	2
64	Какой тип VPN используется для подключения мобильного пользователя? 1. Site-to-site (межузловые или межфилиальные) 2. удалённый доступ 3. GRE 4. Протокол IPsec	2
65	Какие решения VPN обычно используются на предприятии? (Выберите три варианта.) 1. MPLS VPN уровня 2 2. MPLS VPN уровня 3 3. Протокол IPsec 4. SSL 5. Frame Relay. 6. DMVPN	3, 4, 6
66	Какой тип VPN можно установить с помощью веб-браузера, используя HTTPS? 1. Протокол IPsec 2. Клиентский VPN 3. VPN "сайт-сайт" 4. VPN без использования клиента	4
67	Какая характеристика соответствует SSL VPN? 1. Все IP-приложения поддерживаются. 2. Требуется только веб-браузер на хосте. 3. Конкретные устройства могут подключаться с помощью доступных конфигураций 4. Используется двусторонняя аутентификация с использованием открытого ключа или цифрового сертификата.	2
68	К какому типу относится протокол GRE? 1. Протокол безопасности 2. Протокол-пассажир 3. Несущий протокол 4. Транспортный протокол	3
69	Какой тип VPN позволяет предприятию быстро масштабироваться? 1. DMVPN 2. Сеть VPN удалённого доступа 3. VPN "сайт-сайт" 4. MPLS VPN	1
70	Какой тип VPN позволяет организовать локальную сеть Ethernet с множественным доступом с удаленной площадки? 1. DMVPN	4

	2. Сеть VPN удалённого доступа 3. VPN "сайт-сайт" 4. MPLS VPN	
71	В каких слоях OSI IPsec может защитить трафик? (Выберите четыре варианта.) 1. Уровень 1 2. Уровень 2 3. Уровень 3 4. Уровень 4 5. Уровень 5 6. Уровень 6 7. Уровень 7	4, 5, 6, 7
72	Какая функция IPsec использует предварительные пароли, цифровые сертификаты или сертификаты RSA? 1. IPSec протокол 2. Конфиденциальность 3. Целостность 4. Аутентификация 5. Алгоритм Диффи – Хеллмана	4
73	Истина или ложь: Платформа IPsec должна обновляться каждый раз при разработке нового стандарта. 1. Истина 2. Ложь	2
74	IPsec в стандартной фреймворке IPsec? (Выберите два варианта.) 1. AES 2. AH 3. DH24 4. ESP 5. PSK 6. Использование RSA 7. ША	2, 4
75	IPsec? (Выберите три варианта.) 1. 3DES 2. AES 3. AH 4. DH24 5. PSK 6. SEAL 7. SHA	1, 2, 6
76	IPsec? (Выберите два варианта.) 1. AES 2. AH 3. DH24 4. MD5 5. PSK 6. SEAL 7. SHA	4, 7

77	IPsec? (Выберите два варианта.) 1. AES 2. AH 3. DH24 4. PSK 5. Использование RSA 6. SEAL 7. SHA	4, 5
78	Выбор какой группы Диффи-Хеллмана больше не рекомендуется? 1. DH групп 1, 2 и 5 2. DH групп 14, 15 и 16 3. DH групп 19, 20, 21 и 24	1
79	Какие два утверждения описывают VPN для удалённого доступа? (Выберите два варианта.) 1. Она связывает друг с другом целые сети. 2. TCP / IP через шлюз VPN. 3. Она используется для подключения отдельных узлов к корпоративной сети через Интернет. 4. Для нее может требоваться наличие клиентского ПО VPN на узлах. 5. Для неё требуется статическая настройка туннеля VPN.	3, 4
80	IPsec является использование 3DES в IPsec? 1. Аутентификация 2. Конфиденциальность 3. Алгоритм Диффи - Хеллмана 4. Целостность 5. Невозможность отклонения	2
81	Для какого типа VPN может потребоваться программное обеспечение Cisco VPN клиент? 1. VPN для удаленного доступа 2. SSL VPN 3. VPN "сайт-сайт" 4. MPLS VPN	1
82	Какой метод необходим для частной передачи данных с использованием VPN? 1. Авторизация 2. Шифрование 3. Масштабируемость **4.** Виртуализация	2
83	VPN в VPN? (Выберите два варианта.) 1. Spoke-to-spoke (луч-луч) 2. Site-to-site (узел-узел) 3. Hub-to-spoke (концентратор-луч) 4. Client-to-site (клиент-узел) 5. Server-to-client (сервер-клиент)	1, 3
84	Компания может использовать технологию VPN. (Выберите два варианта.)	2, 4

	1. для увеличения пропускной способности сети 2. для подключения удалённых пользователей к сети 3. для проверки сетевых соединений с удалёнными пользователями 4. для предоставления поставщикам возможности доступа к сети **5.** для исключения необходимости использовать шлюз	
85	Верно или нет утверждение? Все VPN безопасно передают чистый текст через Интернет. 1. Верно 2. Неверно	2
86	Какое решение позволяет работникам эффективно и безопасно осуществлять дистанционную связь? 1. VPN "сайт-сайт" 2. Удаленный доступ к сети VPN 3. Коммутируемое подключение. 4. Подключение по DSL	2
87	Какой тип VPN является VPN, управляемой провайдером? 1. VPN "сайт-сайт" 2. Уровень 3 MPLS VPN 3. VPN для удаленного доступа 4. GRE через IPSec VPN	2
88	Какой протокол инфраструктуры IPsec обеспечивает полную целостность данных и аутентификацию данных? 1. AH 2. IP протокол 50 3. ESP 4. DH	1
89	Какой алгоритм используется для обеспечения целостности данных? 1. HMAC 2. DH 3. RSA 4. AES	1
90	Какое утверждение имеет отношение к длине ключа шифрования? 1. Длина ключа не зависит от алгоритма шифрования. 2. Длина ключа не влияет на степень безопасности. 3. Чем короче ключ, тем сложнее его сломать. 4. Чем длиннее ключ, тем сложнее его сломать.	4
91	Какой тип сети VPN, как правило, является прозрачным для конечного пользователя? 1. Сайт-сайт (межузловые или межфилиальные) 2. Удаленный доступ 3. Публичная 4. Закрытая	1
92	Атака шифрует данные на хостах в попытке получить денежные средства от жертвы?	4

	1. DDoS-атака 2. Утечка данных 3. Вредоносное ПО **4.** Вирусы-вымогатели	
93	Какие устройства специально предназначены для сетевой безопасности? (Выберите три варианта.) 1. маршрутизатор с поддержкой VPN 2. NGFW 3. Коммутатор 4. ВЗК 5. NAC	1, 2, 5
94	Какое устройство отслеживает SMTP-трафик, чтобы блокировать угрозы и шифровать исходные сообщения. 1. NGFW 2. ESA 3. NAC 4. WSA	2
95	Какое устройство отслеживает HTTP-трафик, чтобы блокировать доступ к опасным сайтам и шифровать исходные сообщения? 1. NGFW 2. ESA 3. NAC 4. WSA	4
96	Какой компонент AAA отвечает за сбор и представление данных? 1. Аутентификация 2. Авторизация 3. Учет	3
97	Какой компонент AAA отвечает за контроль того, кому разрешен доступ к сети? 1. Аутентификация 2. Авторизация 3. Учет	1
98	Какой компонент AAA отвечает за определение того, что пользователь может получить доступ? 1. Аутентификация 2. Авторизация 3. Учет	2
99	В реализации 802.1X, какое устройство отвечает за ретрансляцию ответов? 1. Запрашивающее устройство 2. Аутентификатор 3. Маршрутизатор 4. Сервер аутентификации 5. Клиент	2
100	Модели OSI? (Выберите три варианта.) 1. Анализ DHCP-трафика 2. Сеть VPN	2, 3, 5

	3. Межсетевые экраны 4. IPSG 5. IPS устройства	
101	Протокол MAC-адресов и атака с истощением DHCP? 1. IPSG 2. Анализ DHCP-трафика 3. DAI 4. Безопасность портов	4
102	MAC-адреса и IP-адреса? 1. IPSG 2. Анализ DHCP-трафика 3. DAI 4. Безопасность портов 5. ARP-адреса и «отравление» ARP-кэша?	1
103	ARP-адреса и «отравление» ARP-кэша? 1. IPSG 2. Анализ DHCP-трафика 3. DAI 4. Безопасность портов 5. DHCP и атака спуфинга DHCP?	3
104	DHCP и атака спуфинга DHCP? 1. IPSG 2. Анализ DHCP-трафика 3. DAI 4. Безопасность портов	2
105	Как будет вести себя коммутатор в результате успешной атаки на таблицу CAM? 1. Коммутатор отключится. 2. Интерфейсы коммутатора перейдут в состояние отключения из-за ошибок. 3. Коммутатор будет пересылать все возможные кадры на все другие порты в пределах VLAN. 4. Коммутатор будет удалять все измеренные кадры.	3
106	Какую главную цель мог бы преследовать злоумышленник, запуская атаку переполнением таблицы MAC-адресов? 1. Таким образом, исполнитель угрозы может видеть кадры, предназначенные для других устройств. 2. Чтобы получить этот код на коммутаторе. 3. Чтобы коммутатор прекратил пересылку трафика. 4. Чтобы легитимные хосты не могли получить MAC-адрес.	1
107	MAC-адреса? 1. IPSG 2. DAI 3. Безопасность портов 4. Анализ DHCP-трафика	3

108	Злоумышленник меняет MAC-адрес своего устройства на MAC-адрес шлюза по умолчанию. К какому типу относится такая атака? 1. Подмена адреса 2. ARP-спуфинг 3. Разведывательная атака CDP 4. Атака истощения ресурсов DHCP 5. Атака СТП 6. VLAN прыжки	1
109	Злоумышленник отправляет сообщение BPDU с приоритетами 0. К какому типу относится такая атака? 1. Подмена адреса 2. ARP-спуфинг 3. Разведывательная атака CDP 4. Атака истощения ресурсов DHCP 5. Атака СТП 6. VLAN прыжки	5
110	Злоумышленник арендовал все доступные IP-адреса в подсети. К какому типу относится такая атака? 1. Подмена адреса 2. ARP-спуфинг 3. Разведывательная атака CDP 4. Атака истощения ресурсов DHCP 5. Атака СТП 6. VLAN прыжки	4
111	По умолчанию это MAC-адрес, который он должен использовать по умолчанию. К какому типу относится такая атака? 1. Подмена адреса 2. ARP-спуфинг 3. Разведывательная атака CDP 4. Атака истощения ресурсов DHCP 5. Атака СТП 6. VLAN прыжки	2
112	Злоумышленник настраивает хост с протоколом 802.1Q и формирует магистральный канал с подключенным коммутатором. К какому типу относится такая атака? 1. Подмена адреса 2. ARP-спуфинг 3. Разведывательная атака CDP 4. Атака истощения ресурсов DHCP 5. Атака СТП 6. VLAN прыжки	6
113	Злоумышленник узнает версию IOS и IP-адреса локального коммутатора. К какому типу относится такая атака? 1. Подмена адреса 2. ARP-спуфинг 3. Разведывательная атака CDP 4. Атака истощения ресурсов DHCP 5. Атака СТП	3

	6. VLAN прыжки	
114	Пользователи не получают действительные IP-адреса? 1. ARP-спуфинг 2. Атака истощения ресурсов DHCP 3. Спуфинг IP-адресов 4. Переполнение таблицы MAC-адресов.	2
115	Опасность переполнения таблиц коммутации? 1. Отключить протокол DTP. 2. Отключение STP. 3. Включение открытого порта безопасности. 4. Перевод неиспользуемых портов в неиспользуемую сеть VLAN.	3
116	Какие три продукта Cisco ориентированы на решения для обеспечения безопасности оконных устройств? (Выберите три варианта.) 1. Устройство IPS Sensor 2. Устройство обеспечения безопасности веб-трафика 3. Устройство защиты электронной почты 4. Устройство SSL / IPsec VPN 5. Многофункциональное устройство обеспечения безопасности 6. NAC Appliance	2, 3, 6
117	Верно или нет утверждение? В стандарте 802.1X клиент пытается получить доступ к сети. 1. Верно 2. Неверно	1
118	Почему аутентификация с использованием AAA предпочтительнее 1. Он использует меньшую пропускную способность сети. 2. Требуется сочетание логины и пароля на консоли, линиях VTY и Aux-портах. 3. Он является резервным методом аутентификации, если администратор забывает логин или пароль. 4. Он определяет разные пароли для каждой линии или порта.	
119	Что включает в себя атаку спуфинга IP-адреса? 1. Легитимный сетевой IP-адрес захвачен подставным узлом. 2. Подставной узел отвечает на запрос ARP своим собственным MAC-адресом, указанным для целевого IP-адреса. 3. Подставной DHCP-сервер предоставляет ложные параметры настройки IP легитимным DHCP-клиентам. 4. Поддельные сообщения DHCPDISCOVER отправляются для использования всеми имеющимися IP-адресами на DHCP-сервере.	1
120	В серверной реализации AAA, какой протокол позволит успешно обмениваться данными с сервером AAA? 1. SSH 2. РАДИУС 3. TACACS 4. 802.1x	2
121	Какие три сервиса предоставляет архитектуру аутентификации?	1, 3, 4

	(Выберите три варианта.) 1. Учет 2. Автоматизация 3. Авторизация 4. Аутентификация 5. Автобалансировка 6. Автоматическая конфигурация	
122	Cisco для коммуникаций AAA? (Выберите два варианта.) 1. VTP 2. LLDP 3. HSRP 4. РАДИУС 5. TACACS +	4, 5
123	Какую службу по умолчанию можно использовать в маршрутизаторе Cisco, может ли она предоставить более уязвимую информацию для атаки? 1. HTTP 2. CDP 3. FTP 4. LLDP	2
124	Какова цель учета AAA? 1. для сбора и отчета об использовании приложений 2. определить, к какому ресурсу пользователь может получить доступ 3. чтобы определить пользователей, кем они являются 4. определить, какая операция может выполнить пользователь	1
125	OSI считается самым слабым звеном в сетевой системе? 1. Уровень 4 2. Уровень 2 3. Уровень 3 4. Уровень 7	2
126	Уровень коммутации 2-го уровня. 1. Атаки путем подделки ARP 2. Спуфинг IP-адресов 3. Переполнение таблицы MAC-адресов. 4. Манипуляции протокола STP	3
127	Благодаря реализованному мерам безопасности пользователь может получить доступ только к серверу с FTP. Какой компонент AAA выполняет это? 1. доступность 2. Учет 3. Проверка 4. Аутентификация 5. Авторизация	5
128	Какое решение Cisco помогает противодействовать атаке по подмене MAC и IP-адресов? 1. Безопасность портов	3

	2. Отслеживание DHCP-сообщений 3. Защита источника IP 4. Динамический анализ ARP	
129	Что рекомендуется сделать при использовании сети VLAN? 1. Отключить динамический протокол транкинга (DTP). 2. Использовать информационную безопасность портов. 3. Назначить ее неиспользуемой сети VLAN. 4. VLAN для управления сетью VLAN.	3
130	PortFast для повышения стабильности STP? 1. Применимо ко всем портам конечного пользователя. 2. только на портах, которые подключены к соседнему коммутатору 3. на всех магистральных портах. 4. только на портах, которые выбраны в качестве назначенных портов	1
131	Коммутатор Cisco должен выполнять практические рекомендации Cisco? **1. shutdown** **2. ip dhcp snooping** **3. switchport port-security mac-address закреплён** **4. switchport порт-нарушение безопасности отключение** 5. **switchport port-security mac-address закрепленный** mac-адрес	1
132	Cisco Catalyst можно использовать для нейтрализации атакующего истощения DHCP и атакующего спуфинга DHCP? (Выберите два варианта.) 1. Port security 2. расширенный ACL-список 3. Анализ DHCP-трафика 4. отказоустойчивый сервер DHCP 5. надежный пароль на DHCP-сервере	1, 3
133	Как проложить VLAN? 1. Отключите STP на всех нетранковых портах. 2. Используйте инкапсуляцию ISL на всех магистральных каналах. 3. Используйте VLAN 1 в качестве собственной VLAN на магистральных портах. 4. Отключение согласование внешних линий для внешних портов и статически установите нетранковые порты в качестве портов доступа.	4
134	Какая процедура рекомендуется для выявления вероятности подмены ARP? 1. Включение безопасности портов глобально. 2. Включение отслеживания DHCP на выбранных VLAN. 3. Включение DAI в управляющей VLAN. 4. Включение IP Source Guard на доверенных портах.	2
135	Коммутаторы Cisco для защиты от атак DHCP-спуфинга? (Выберите	2, 4

	два варианта.) 1. Неизвестный порт. 2. Недоверенный порт. 3. Неавторизованный порт. 4. Доверенный порт DHCP. 5. Авторизованный порт DHCP. 6. Порт DHCP с установленным соединением.	
136	Какие две команды можно использовать для включения PortFast на коммутаторе? (Выберите два варианта.) **1.** S1 (config-if) # **spanning-tree portfast** 2. S1 (config-line) # **spanning-tree portfast** **3.** S1 (config) # **spanning-tree portfast default** 4. S1 (config-if) # **enable spanning-tree portfast** 5. S1 (config) # **enable spanning-tree portfast default**	1, 3
137	При поиске и устранении неполадок на коммутаторе администратор заметил, что на коммутаторе порт безопасности находится в состоянии ошибки-отключен. Как следует повторять порт после проверки причин нарушения, не нарушена работа сети? 1. Перезагрузить коммутатор. 2. Использовать для интерфейса команде shutdown, а затем команде no shutdown. 3. Использовать команду no switchport port-security, а затем снова включить безопасность портов. 4. Использовать команду no switchport port-security violation shutdown для этого интерфейса.	2
138	Сетевой администратор настраивает отслеживание DHCP на коммутаторе. Какую команду конфигурации следует использовать в первую очередь? **1. ip dhcp snooping** **2. ip dhcp snooping vlan** **3. ip dhcp snooping trust** 4. **ip dhcp snooping limit rate**	1
139	Сетевой администратор настраивает DAI на коммутаторе с помощью команды **Проверка ip arp подтверждает dst-mac**. Зачем нужна эта команда? 1. Проверяет MAC-адрес назначения в заголовке Ethernet по отношению к целевому MAC-адресу в таблице MAC-адресов. 2. Проверяет MAC-адрес назначения в заголовке Ethernet по настроенным пользователям спискам ARP 3. Проверяет MAC-адрес назначения в заголовке Ethernet по отношению к целевому MAC-адресу в теле ARP. 4. Проверяет MAC-адрес назначения в заголовке Ethernet по сравнению с исходным MAC-адресом в теле ARP	3
140	Функция MAC-адресов коммутатора MAC-адресов должна быть включена для предотвращения переполнения. 1. BPDU filter 2. Port security 3. Storm control	2

	4. Root guard	
141	Какая атака 2-го уровня нейтрализуется отключенным протоколом динамического транкинга? 1. VLAN hopping 2. DHCP-спуфинг (несанкционированный доступ к протоколу DHCP) 3. Атаки путем подделки ARP 4. ARP-спуфинг	1
142	Сетевой администратор настраивает DAI на коммутаторе. Команда подключена к маршрутизатору? **1. ip arp inspection vlan** **2. ip arp inspection trust** **3. ip dhcp snooping** 4. **Snapping-tree portfast**	2
143	Где хранятся динамически определяемые MAC-адреса, когда включена функция липкого обучения (команда **switchport безопасность порта mac-address sticky**)? 1. ПЗУ 2. ОЗУ 3. Энергонезависимая память (NVRAM) 4. флеш-память	2

Ключи к ФОС по дисциплине «Компьютерные сети»

5.1 Ответы на вопросы для собеседования (устного опроса):

Тема 1 Фундаментальные принципы безопасности сети

1 Современные угрозы сетевой безопасности включают фишинг, программы-вымогатели, DDoS-атаки, APT-атаки (сложные целевые атаки), эксплуатацию уязвимостей нулевого дня и социальную инженерию. Они направлены на кражу данных, остановку бизнес-процессов и получение выкупа, характеризуясь использованием ИИ, высокой маскировкой и нацеленностью на цепочки поставок.

2 Вирусы, черви и троянские кони — основные виды вредоносного ПО (ВПО). Вирусы саморазмножаются, заражая файлы. Черви самостоятельно распространяются по сетям, засоряя систему. Трояны маскируются под легитимные программы для кражи данных или удаленного управления, не размножаясь самостоятельно. Основная цель всех — кража данных, повреждение системы или майнинг.

3 Методы атак в компьютерных сетях — это действия, направленные на нарушение конфиденциальности, целостности или доступности данных. К основным относятся DDoS (перегрузка ресурсов), MITM (перехват трафика), фишинг (кража учетных данных), сканирование портов, брутфорс (подбор паролей) и использование вредоносного ПО.

Тема 2 Безопасность Сетевых устройств OSI

4 Безопасный доступ к устройствам в компьютерных сетях — это комплекс методов, технологий и политик, направленных на защиту сетевых ресурсов (серверов, рабочих станций, сетевого оборудования, IoT-устройств) от несанкционированного доступа, кибератак, модификации или уничтожения данных. Это критическая часть общей сетевой безопасности, обеспечивающая, чтобы только доверенные пользователи и проверенные устройства могли подключаться к сети и работать с необходимыми данными.

5 Назначение административных ролей в компьютерных сетях — это процесс предоставления определенным пользователям (сотрудникам ИТ-отдела) специфических прав и привилегий для управления сетевой инфраструктурой, сервисами или безопасностью.
Это позволяет распределить ответственность между несколькими специалистами, избегая ситуации, когда один человек имеет неограниченный доступ ко всем системам, что повышает безопасность и эффективность работы.

6 Безопасность при мониторинге и управлении сетевыми устройствами (маршрутизаторами, коммутаторами, серверами) — это критически важный аспект, так как эти системы имеют высокий уровень привилегий. Незащищенные протоколы управления (например, Telnet) или слабые пароли могут позволить злоумышленнику получить полный контроль над сетью.

7 Автоматизированная настройка безопасности в компьютерных сетях — это использование технологий (SIEM, SOAR, IDS/IPS) для оперативного управления защитой без участия человека. Она обеспечивает быстрое реагирование на угрозы (блокировка IP, изоляция

узлов), автоматическое развертывание политик безопасности (VPN, межсетевые экраны) и адаптацию системы к новым рискам.

Тема 3 Авторизация, аутентификация и учет доступа (AAA)

8 AAA (Authentication, Authorization, Accounting — Аутентификация, Авторизация и Учет) — это концептуальная модель безопасности, используемая для контроля доступа к компьютерным сетям, управления политиками и аудита использования ресурсов. Она обеспечивает надежную проверку пользователей, определение их прав и мониторинг их действий.

9 Локальная AAA-аутентификация — это метод обеспечения безопасности, при котором проверка подлинности пользователя (аутентификация), определение его прав (авторизация) и учет действий (аккаунтинг) осуществляются непосредственно самим сетевым устройством (маршрутизатором, коммутатором, межсетевым экраном), а не внешним сервером.

10 Server-based AAA (Authentication, Authorization, and Accounting) — это централизованная система управления безопасностью в компьютерных сетях, которая использует выделенный сервер для проверки личности пользователей, определения их прав доступа и ведения учета сетевой активности.
В отличие от локальной аутентификации (где каждый сетевой элемент, например, маршрутизатор, хранит свою базу пользователей), AAA-сервер позволяет управлять доступом ко всей инфраструктуре из единого центра.

Тема 4 Списки контроля доступа (ACL)

11 ACL (Access Control List) — это набор упорядоченных правил, используемых маршрутизаторами и коммутаторами для фильтрации сетевого трафика. ACL проверяет заголовки пакетов (IP-адреса, порты, протоколы) и на основе разрешающих (permit) или запрещающих (deny) условий пропускает их или блокирует, обеспечивая безопасность сети.

12 Для IPv4-сетей (в частности, в Cisco IOS) существуют два основных типа списков контроля доступа (ACL): стандартные и расширенные. Они фильтруют трафик, разрешая или запрещая пакеты на основе IP-адресов источника/назначения, протоколов и портов, обеспечивая базовую безопасность.

13 Создание и размещение ACL-списков (Access Control Lists) требует соблюдения принципа наименьших привилегий: размещайте расширенные ACL ближе к источнику трафика, а стандартные — ближе к цели. Используйте именные ACL для удобства редактирования, нумеруйте правила с шагом (10, 20, 30) для вставки новых условий и всегда завершайте список неявным запретом всего остального (deny any).

14 Размещение ACL (Access Control Lists) зависит от их типа: расширенные ACL размещают ближе к источнику трафика для эффективной фильтрации, а стандартные — ближе к получателю, чтобы не блокировать лишний трафик. Именованные списки предпочтительнее нумерованных для гибкости управления.

15 Настройка стандартного ACL (Access Control List) в Cisco IOS включает создание правил (номер 1-99) для фильтрации трафика по IP-адресу источника и применение их к интерфейсу. Используются команды access-list [номер] {permit|deny} [источник] и ip access-group [номер] {in|out}. Рекомендуется применять ACL ближе к получателю трафика.

16 Расширенные IPv4 ACL (диапазон 100–199 и 2000–2699) фильтруют трафик на основе источника, назначения, протокола (IP, TCP, UDP) и портов, обеспечивая высокую гибкость. Они создаются последовательностью правил permit/deny, применяются к интерфейсу (in/out) и завершаются неявным запретом всего трафика.

17 Фильтрация трафика расширенными (Extended) ACL-списками выполняется путем анализа заголовков пакетов по совокупности критериев: IP-адресам источника/назначения, протоколу (IP, TCP, UDP, ICMP) и номерам портов. Списки создаются (обычно с номерами 100-199) и применяются к интерфейсам в определенном направлении (in/out) для детального разрешения или запрета.

18 Поиск и устранение неполадок ACL (Access Control Lists) — это процесс проверки правильности применения, порядка следования правил (ACE) и совпадений трафика для устранения блокировок легитимного трафика. Ключевые этапы включают использование команд show access-lists для анализа счетчиков, проверку направления (IN/OUT) и убежденность в том, что более конкретные правила стоят выше обобщающих.

Тема 5. Реализация технологий брандмауэра

19 Брандмауэр (межсетевой экран, фаервол) — это технология защиты сети, выступающая барьером между доверенной локальной сетью (или компьютером) и небезопасным интернетом. Он фильтрует входящий и исходящий трафик на основе заранее заданных правил безопасности, пропуская безопасные данные и блокируя вирусы, хакерские атаки и несанкционированный доступ.

20 Контекстный контроль доступа (CBAC) — это метод динамической защиты сети (преимущественно в маршрутизаторах Cisco IOS), который анализирует состояние сетевых соединений (stateful inspection) и их контекст, а не просто фильтрует трафик по IP/портам. CBAC проверяет запросы до 7-го уровня OSI, создает временные правила для обратного трафика и блокирует подозрительные сессии, значительно повышая безопасность по сравнению с обычными ACL.

21 Политики брандмауэра, основанные на зонах (Zone-Based Policy Firewall, ZBF), — это подход к сетевой безопасности, где интерфейсы маршрутизатора или межсетевого экрана объединяются в логические группы (зоны) с разным уровнем доверия. Политики применяются не к конкретным портам, а к трафику, переходящему между зонами (например, из LAN в WAN).

Тема 6. Реализация технологий предотвращения вторжения

22 IPS (Intrusion Prevention System — система предотвращения вторжений) в компьютерных сетях — это программное или аппаратное средство безопасности, которое в реальном времени анализирует сетевой трафик, обнаруживает подозрительную активность и автоматически блокирует атаки.
В отличие от систем обнаружения вторжений (IDS), которые только сигнализируют об угрозе, IPS действует проактивно, прерывая вредоносную сессию.

23 IPS-сигнатуры — это уникальные цифровые «отпечатки» или шаблоны известных кибератак, вредоносного трафика и аномалий, используемые системами предотвращения

вторжений (IPS) для их мгновенного обнаружения и блокировки. Они работают как антивирус: сверяют проходящие сетевые пакеты с базой данных, пресекая подозрительную активность в реальном времени.

24 IPS (Intrusion Prevention System — Система предотвращения вторжений) — это активное средство сетевой безопасности, предназначенное для обнаружения, анализа и автоматической блокировки потенциальных угроз в режиме реального времени. В отличие от IDS (систем обнаружения), которые только оповещают об угрозе, IPS действует превентивно, разрывая соединения или блокируя вредоносный трафик.

25 IPS (Intrusion Prevention System) в компьютерных сетях функционирует как активный «телохранитель», работающий в режиме реального времени. Она анализирует весь проходящий трафик, сравнивая его с базой сигнатур известных атак или выявляя аномалии, и при обнаружении угроз моментально блокирует вредоносные действия, разрывает соединения или изолирует узлы.

Тема 7 Безопасность локальной сети

26 Безопасность пользовательских компьютеров в компьютерных сетях обеспечивается комплексным подходом, сочетающим технические средства, программные решения и организационные меры. Защита направлена на предотвращение несанкционированного доступа, кражи данных, заражения вирусами и атак на инфраструктуру.

27 Безопасность второго уровня (Layer-2, Data Link Layer) модели OSI является критически важной, так как именно на этом уровне происходят атаки, направленные на обход сетевых экранов, перехват трафика и нарушение работы локальной сети (LAN). Злоумышленник, находящийся в том же широковещательном домене, может скомпрометировать сеть, даже если верхние уровни защищены.

28 Безопасность беспроводных сетей (Wi-Fi), VoIP и SAN (сетей хранения данных) требует комплексного подхода, сочетающего шифрование, аутентификацию и сетевую изоляцию. Основные угрозы включают перехват данных, несанкционированный доступ и DoS-атаки, требующие применения стандартов WPA3, TLS/SRTP и зональной структуры SAN для защиты инфраструктуры.

Тема 8 Криптографические системы

29 Криптографические сервисы и средства защиты информации (СКЗИ) делятся на программные, аппаратные и программно-аппаратные решения. Они обеспечивают конфиденциальность, целостность и подлинность данных.

30 С точки зрения криптографии, конфиденциальность — это обеспечение доступа к информации (данным, сообщениям) только авторизованным пользователям, процессам или устройствам, предотвращая её чтение или интерпретацию посторонними лицами.
Amazon Web Services

31 Криптография с открытым ключом (асимметричная криптография) — это метод шифрования, использующий пару математически связанных ключей: открытый (публичный) для шифрования и закрытый (приватный) для дешифрования. Открытый ключ доступен всем, а закрытый хранится в тайне, что обеспечивает безопасный обмен данными без предварительной передачи секретного ключа.

Тема 9 Реализация технологий VPN

32 VPN (Virtual Private Network — виртуальная частная сеть) — это технология, создающая защищенное, зашифрованное соединение («туннель») поверх общедоступной сети Интернет. Она скрывает реальный IP-адрес, маскирует местоположение и защищает передаваемые данные от перехвата, обеспечивая конфиденциальность.

33 VPN (Virtual Private Network — виртуальная частная сеть) — это технология, создающая защищенное, зашифрованное соединение (логическую сеть) поверх другой, обычно открытой или незащищенной, сети (например, Интернет). VPN позволяет пользователям отправлять и получать данные через публичные сети так, будто их устройства подключены напрямую к частной (корпоративной или домашней) сети.

34 VPN (виртуальные частные сети) делятся по архитектуре и протоколам, обеспечивая безопасное соединение через публичные сети. Основные типы: удаленный доступ (Client-to-Site) для пользователей, «сайт-сайт» (Site-to-Site) для объединения офисов, и персональные/мобильные VPN. Используемые протоколы: WireGuard, OpenVPN, IKEv2/IPSec, L2TP/IPSec, SSTP и устаревший PPTP.

35 Туннели GRE (Generic Routing Encapsulation) — это протокол туннелирования, разработанный Cisco, который позволяет инкапсулировать (заворачивать) пакеты одного сетевого протокола в IP-пакеты, создавая виртуальное соединение «точка-точка» между удаленными объектами через общедоступную сеть (например, интернет).
Простыми словами, GRE создает виртуальный «тоннель» внутри обычного интернета, по которому можно передавать специфический трафик, который иначе не прошел бы через публичные маршрутизаторы (например, частные IP-адреса или многоадресный трафик).

36 GRE (Generic Routing Encapsulation) — это протокол туннелирования, разработанный Cisco, который позволяет упаковывать (инкапсулировать) пакеты одного сетевого протокола в IP-пакеты другого, создавая виртуальный туннель «точка-точка» между двумя маршрутизаторами через публичную сеть (например, интернет).

37 IPsec (Internet Protocol Security) — это набор протоколов и правил, предназначенных для обеспечения защиты данных, передаваемых по IP-сетям (в частности, через интернет). Он обеспечивает конфиденциальность, целостность и аутентичность информации, превращая незащищенные сети в безопасные каналы связи.

38 Защита протокола IP в компьютерных сетях реализуется преимущественно через набор протоколов IPsec (Internet Protocol Security), который обеспечивает аутентификацию, целостность и конфиденциальность передаваемых данных на сетевом уровне.

39 IPsec (IP Security) — это набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, функционирующий на сетевом уровне (уровень 3 модели OSI). Он обеспечивает конфиденциальность, целостность и аутентификацию данных. Структура IPsec состоит из трех основных компонентов: протоколов защиты (AH, ESP), протоколов управления ключами (IKE) и механизмов ассоциации безопасности (SA).

40 Удалённый доступ выполняется через передачу данных между клиентским и хост-устройством (сервером) с использованием специализированного ПО или протоколов (RDP, VNC, SSH). Технология позволяет отображать экран удаленного ПК, управлять им

с помощью мыши и клавиатуры, передавать файлы, используя IP-адрес или уникальный ID для идентификации.?

41 VPN-решения для удаленного доступа (Remote Access VPN) представляют собой критически важный инструмент обеспечения безопасного подключения сотрудников к корпоративной сети через публичный интернет. Они создают зашифрованные «туннели» между устройством удаленного пользователя и внутренней сетью компании, защищая данные от перехвата и обеспечивая конфиденциальность.

42 VPN удалённого доступа (Remote Access VPN) с использованием IPsec — это технология, обеспечивающая безопасное подключение отдельных пользователей (удаленных сотрудников) к корпоративной сети через публичный интернет. IPsec (Internet Protocol Security) настраивает шифрованный туннель между устройством пользователя (клиентом) и шлюзом безопасности (VPN-сервером/файрволом) компании.

Тема 10 Управление безопасной сетью

43 Безопасный дизайн компьютерной сети базируется на нескольких фундаментальных принципах, направленных на защиту данных, ограничение доступа и предотвращение угроз. Ключевые принципы включают:

- Глубокая защита (Defense in Depth): Использование нескольких уровней защиты (межсетевые экраны, IPS, антивирусы, шифрование) для защиты активов, чтобы сбой одной системы не нарушил безопасность всей сети.
- Сегментация сети: Разделение сети на более мелкие, изолированные зоны (VLAN, DMZ) для ограничения распространения угроз. Это позволяет локализовать атаку и защитить критически важные ресурсы.
- Принцип наименьших привилегий (Least Privilege): Предоставление пользователям, устройствам и процессам только того уровня доступа, который необходим для выполнения их задач.
- Минимизация поверхности атаки: Уменьшение количества точек доступа, отключение ненужных сервисов, протоколов и портов для снижения вероятности взлома.
- Zero Trust (Нулевое доверие): Принцип «никому не доверяй, всегда проверяй». Требуется аутентификация и авторизация для каждого запроса доступа, даже если он исходит из внутренней сети.
- Безопасность по умолчанию (Security by Default): Сеть должна быть спроектирована так, что начальные настройки являются максимально безопасными (например, закрыты все порты, кроме явно разрешенных).
- Непрерывный мониторинг и аудит: Систематический анализ сетевого трафика и инфраструктуры для обнаружения уязвимостей и признаков вторжения.
- Физическая безопасность: Защита сетевого оборудования (серверов, коммутаторов, кабелей) от несанкционированного физического доступа.
- Отказоустойчивость и доступность: Обеспечение резервирования критических компонентов для защиты от сбоев, а также гарантированный доступ пользователей к необходимым ресурсам.

Эти принципы помогают создать надежную архитектуру, способную противостоять современным киберугрозам.

44 Безопасная архитектура компьютерной сети — это стратегическая модель проектирования ИТ-инфраструктуры, объединяющая технические средства (файрволы, шифрование) и организационные меры для защиты данных от атак, несанкционированного доступа и сбоев. Она встраивает защиту на всех уровнях (Secure by Design), минимизируя риски и обеспечивая конфиденциальность, целостность и доступность информации.

45 Управление процессами и безопасность в компьютерной сети — это комплекс взаимосвязанных мер, направленных на обеспечение стабильной, производительной и защищенной работы сетевой инфраструктуры. Управление обеспечивает работоспособность, а безопасность защищает данные и ресурсы от угроз.

46 Тестирование сети на уязвимости (анализ защищенности) — это систематический процесс поиска слабых мест в ИТ-инфраструктуре с использованием автоматизированных сканеров (Nessus, MaxPatrol) и ручных методов (пентест). Оно включает этапы планирования, сбора информации, сканирования портов/сервисов, активной эксплуатации уязвимостей и формирования отчета с рекомендациями. Цель — выявить точки входа до того, как ими воспользуются хакеры.

47 Непрерывность бизнеса (BCP) — это комплекс стратегий, гарантирующих работу критических процессов компании во время сбоев сети. Планирование аварийного восстановления (DRP) — часть BCP, фокусирующаяся на быстром восстановлении ИТ-инфраструктуры, данных и серверов после катастроф. Оба процесса минимизируют простои и потерю данных.

48 Жизненный цикл компьютерной сети — это непрерывный, циклический процесс, охватывающий все стадии существования сетевой инфраструктуры: от возникновения идеи и проектирования до эксплуатации, модернизации и вывода из эксплуатации.
Обычно этот цикл описывается моделью PPDIOO (Plan, Design, Implement, Operate, Optimize — Планирование, Проектирование, Внедрение, Эксплуатация, Оптимизация), которая обеспечивает эффективное функционирование и развитие сети.

49 Планирование сети — это процесс проектирования логической и физической структуры компьютерной сети для достижения целей организации. Оно включает определение размеров, скорости, выбор оборудования, IP-адресацию, меры безопасности и схему размещения устройств. Это непрерывный процесс моделирования будущей сети для обеспечения эффективности, масштабируемости и надежности.

50 Разработка регламентов и политик безопасности — это создание комплекса документированных правил, процедур и норм, определяющих защиту информационных активов и работу компьютерной сети компании. Это документальное обеспечение безопасности, направленное на защиту конфиденциальности данных, соблюдение законодательства и снижение рисков киберугроз.