Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный индустриальный университет»

Кафедра прикладных информационных технологий и программирования

УТВЕРЖДАЮ
Директор института
информационных технологий и
автоматизированных систем
_____ А.В. Зимин
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность компьютерных сетей

09.02.06 «Сетевое и системное администрирование»
(направленность (профиль): «Сетевое и системное администрирование»)

Квалификация выпускника
Системный администратор

Форма обучения
Очная форма

Срок обучения: 3 года 10 месяцев

Год начала подготовки 2025

Новокузнецк
2025

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: daba56d7b892efca3bf5c04ed0251c98b19b099c
Владелец: Директор ИИТиАС Зимин Алексей Валерьевич
Действителен: с 15 января 2025 г. по 10 апреля 2026 г.
Дата и время: 27-05-2025 13:14:47 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний и умений по защите компьютерных сетей с применением программно-аппаратных средств;
– понимание основных принципов, технологий и архитектур проектирования и реализации операционных систем.

Задачами учебной дисциплины являются:

– систематическое изложение лекционного материала по безопасности компьютерных сетей;
– формирование знаний о методах и средствах защиты информации в компьютерных сетях;
– формирование знаний о методах и средствах построения виртуальных частных сетей;
– формирование знаний о методах и средствах аудита уровня защищенности информационных систем.

2 Место учебной дисциплины в структуре ООП по специальности

Учебная дисциплина входит в состав профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» профессионального цикла ООП по специальности 09.02.06 «Сетевое и системное администрирование».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Компьютерные сети;
– Организация, принципы построения и функционирования компьютерных сетей;
– Информационные технологии.

Учебная дисциплина дополняет умения и знания, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Администрирование сетевых операционных систем.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

Общие компетенции

– 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

Профессиональные компетенции

– ПК 3.1.: Осуществлять проектирование сетевой инфраструктуры.

– ПК 3.2.: Обслуживать сетевые конфигурации программно-аппаратных средств.

– ПК 3.3.: Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

– ПК 3.4.: Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.

– ПК 3.5.: Модернизировать сетевые устройства информационно-коммуникационных систем.

Обучающийся должен быть готов к выполнению основных видов профессиональной деятельности:

– выполнение работы по проектированию сетевой инфраструктуры;

– организация сетевого администрирования;

– эксплуатация объектов сетевой инфраструктуры.

В результате освоения учебной дисциплины обучающийся должен уметь, знать, иметь практический опыт:

Код ОК, ПК	**Уметь**	**Знать**	**Иметь практический опыт**
ОК 04. ОК 05. ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5.	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; осуществлять диагностику и поиск неисправностей всех компонентов сети; выполнять действия по устранению неисправностей	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа локальных сетей; методы устранения неисправностей в технических средствах	в обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя; в удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры; в поддержке пользователей сети, в настройке аппаратного и программного обеспечения сетевой инфраструктуры

4 Объем и содержание учебной дисциплины

Учебная деятельность обучающихся предусматривает учебные занятия (лекция, практическое занятие, консультация), самостоятельную

работу, а также другие виды учебной деятельности, определенные учебным планом и календарным планом воспитательной работы.

Объем учебной дисциплины

Семестр / курс	***ИТОГО***	***6 семестр***	***7 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость, *академ. час.*	***168***	*48*	*120*
Лекции, *академ. час.*	***46***	*14*	*32*
в форме практической подготовки	***0***	*0*	*0*
Лабораторные работы, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Практические занятия, *академ. час.*	***64***	*16*	*48*
в форме практической подготовки	***0***	*0*	*0*
Курсовая работа / проект, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Консультации, *академ. час.*	***1***	*0*	*1*
в форме практической подготовки	***0***	*0*	*0*
Самостоятельная работа, *академ. час.*	***51***	*18*	*33*
в форме практической подготовки	***0***	*0*	*0*
Контроль, *академ. час.*	***6***	*0*	*6*
в форме практической подготовки	***0***	*0*	*0*

Содержание учебной дисциплины

Раздел 1 Фундаментальные принципы безопасной сети (Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.);

Раздел 2 Безопасность Сетевых устройств OSI (Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.);

Раздел 3 Авторизация, аутентификация и учет доступа (AAA) (Свойства AAA. Локальная AAA аутентификация. Server-based AAA.);

Раздел 4 Реализация технологий брандмауэра (ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах.);

Раздел 5 Реализация технологий предотвращения вторжения (IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS.);

Раздел 6 Безопасность локальной сети (Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей.);

Раздел 7 Криптографические системы (Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.);

Раздел 8 Реализация технологий VPN (VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN. Реализация Site-to-site IPSec VPN.);

Раздел 9 Управление безопасной сетью (Принципы безопасности. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Разработка регламентов компании и политик безопасности.);

Раздел 10 Понятие о методах и средствах аудита уровня защищенности информационных систем (Введение в технический анализ всех элементов компьютерной сети. Выявление проблем функционирования сети и составление рекомендаций по их устранению. Оценка качества, инвентаризация и документирование.).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	в форме практической подготовки
Раздел 1.	Фундаментальные принципы безопасной сети	4	
Раздел 2.	Безопасность Сетевых устройств OSI	5	

Раздел 3.	Авторизация, аутентификация и учет доступа (AAA)	4	
Раздел 4.	Реализация технологий брандмауэра	4	
Раздел 5.	Реализация технологий предотвращения вторжения	4	
Раздел 6.	Безопасность локальной сети	5	
Раздел 7.	Криптографические системы	4	
Раздел 8.	Реализация технологий VPN	5	
Раздел 9.	Управление безопасной сетью	5	
Раздел 10.	Введение в аудит элементов компьютерной сети	6	
Итого:		**46**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	**Темы практических занятий (семинаров)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 2.	Настройка безопасного доступа к маршрутизатору	5	
Раздел 3.	Обеспечение административного доступа AAA и сервера	7	
Раздел 4.	Настройка политики безопасности брандмауэров	7	
Раздел 5.	Начальная настройка системы предотвращения вторжений (IPS)	3	
Раздел 6.	Исследование сетевых атак и инструментов проверки защиты сети.	7	
Раздел 7.	Криптографические системы	7	
Раздел 8.	Практическая настройка сервиса VPN	8	
Раздел 9.	Аудит безопасности. Получение информации из открытых источников	8	
Раздел 9.	Аудит безопасности. Получение информации от сетевых сервисов	8	
Раздел 10.	Базовая настройка шлюза	4	

	безопасности ASA и настройка брандмауэров используя интерфейс командной строки		
Итого:		**64**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	Темы лабораторных работ	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	Темы курсовых работ (проектов)	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	Виды самостоятельной работы	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	1. Изучение лекционного материала; 2. Прохождение тестирования.	3	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	
Раздел 3.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	
Раздел 4.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	

Раздел 5.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	
Раздел 6.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	
Раздел 7.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	
Раздел 8.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	5	
Раздел 9.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	6	
Раздел 10.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	7	
	Консультации	1	
Контроль	*Подготовка к экзамену*	6	
Итого:		**58**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые разделы (темы) дисциплины	Контролируемые компетенции	Оценочные средства
Раздел 1.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Оценка участия в работе на лекционном занятии; 3. Тестовые задания

Раздел 2.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 3.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 4.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 5.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 6.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 7.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 8.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 9.	ОК 04.; ОК 05.; ПК 3.1.;	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на

	ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Раздел 10.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии; 3. Оценка участия в работе на лекционном занятии; 4. Тестовые задания
Экзамен.	ОК 04.; ОК 05.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 3.5.	1. Вопросы к экзамену; 2. Задачи к экзамену

11 Входной контроль

11.1 Цель входного контроля − определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания обучающегося используются как начальные значения в индивидуальном профиле академической успешности обучающегося.

11.2 Описание оценочных средств

Форма проведения входного контроля – тестирование.

Длительность тестирования – 20 минут.

Тестирование проводится в течение первых двух недель изучения учебной дисциплины в СУО «Moodle».

Для проведения тестирования используются тестовые задания для входного контроля (для ответа на 1 вопрос, как правило, выделяется 1 минута).

Шкала оценивания результатов тестирования

За каждый правильный ответ выставляется 1 балл. Оценка выставляется в зависимости от процента правильных ответов:

Оценка формируется в соответствии с критериями таблицы:

Процент результативности (правильных ответов)	Оценка
86 до 100	«отлично»
от 67до 85	«хорошо»
от 50 до 66	«удовлетворительно»
менее 50	«неудовлетворительно»

Основываясь на результатах тестирования, формируется индивидуальная траектория обучающегося (группы обучающихся), исходя из следующих соображений:

– 86 – 100 % – обучающийся готов к изучению учебной дисциплины без дополнительного повторения изученного ранее материала;

– 50 – 67 % – обучающийся в целом готов к изучению учебной дисциплины, требуется повторение отдельных вопросов(тем) изученного ранее материала, необходимого для успешного освоения учебной дисциплины;

– 49% и менее – обучающийся имеет слабую подготовку к изучению учебной дисциплины, необходимы корректирующие занятия и консультации.

Тестовые задания для входного контроля знаний обучающихся приведены в приложении.

12 Текущий контроль

12.1 Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению учебной дисциплины и позволяет оценить степень освоения изученного материала.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы по индивидуальной инициативе педагогического работника, в том числе посредством использования СУО «Moodle».

Формы проведения текущего контроля – вопросы для устного обсуждения (опроса); наблюдение за работой на практическом занятии; оценка участия в работе на лекционном занятии; тестовые задания.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию устных ответов обучающихся

С целью контроля и подготовки обучающихся к изучению новой темы в начале лекции педагогическим работником проводится индивидуальный или фронтальный устный опрос по выполненным заданиям предыдущего раздела (темы).

Критерии оценки:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– сознательность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели);

– своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается умение грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);

– использование дополнительного материала (обязательное условие);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени).

Оценка «отлично» ставится, если обучающийся:

– полно и аргументировано отвечает по содержанию задания;

– обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, в том числе самостоятельно составленные;

– излагает материал последовательно и правильно.

Оценка «хорошо» ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1 – 2 ошибки, которые сам же исправляет.

Оценка «удовлетворительно» ставится, если обучающийся обнаруживает знание и понимание основных положений данного задания, но:

– излагает материал неполно и допускает неточности в определении понятий или формулировке правил;

– не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;

– излагает материал непоследовательно и допускает ошибки.

Оценка «неудовлетворительно» ставится, если обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному освоению последующего материала.

12.2.2 Рекомендации по оцениванию результатов тестирования обучающихся

Тестирование проводится по изученным разделам (темам) учебной дисциплины для выявления уровня умений и знаний обучающегося, мотивирования обучающегося к активизации самостоятельной работы по усвоению учебного материала, выявления и устранения пробелов в знаниях, повышения дисциплины и организации учебной деятельности обучающегося.

Тестирование проводится в СУО «Moodle» в рамках часов, отведенных на самостоятельную работу обучающихся. Для тестирования используется не менее 20 вопросов из базы типовых тестовых заданий по изученным разделам (темам) учебной дисциплины. В случае выбора неправильного ответа обучающийся получает за данный вопрос 0 баллов; в случае правильного ответа – 1 балл; в заданиях на соответствие за каждый правильный ответ – 0,5 баллов.

Оценка формируется в соответствии с критериями таблицы:

Максимальный балл	Проходной балл	Оценка
20	не менее 18	отлично
17	не менее 14	хорошо
13	не менее 10	удовлетворительно
9	–	неудовлетворительно

12.2.3 Рекомендации по оцениванию участия обучающихся в работе на лекционных занятиях

Формирование у обучающихся добросовестного и ответственного отношения к собственному профессиональному образованию проявляется в обязательном его присутствии на лекционном занятии.

На лекционных занятиях происходит формирование информационной компетентности обучающихся, в том числе способности фиксировать информацию с помощью конспектирования учебного материала. Преподаватель на лекционных занятиях акцентирует внимание обучающихся на том, как необходимо оформлять конспект лекций в тетради. По окончании лекционных занятий преподаватель осуществляет проверку тетрадей обучающихся и оценивает их.

Критерии оценки участия обучающихся в работе на лекционных занятиях

Наименование параметра оценки	Максимальное количество баллов за одно лекционное занятие

Наличие у обучающихся добросовестного и ответственного отношения к собственному профессиональному образованию, выраженное в посещении лекций	0,5
Умение конспектировать учебный материал в тетради, в том числе: - материал изложен последовательно, четко и аккуратно - в конспекте имеются изученные темы, основные термины, схемы	0,5
Всего	1

Если по результатам оценки участия обучающийся в лекционных занятиях в среднем за семестр обучающийся набрал не менее 0,5 баллов, то ему выставляется оценка «зачтено», менее 0,5 баллов – «не зачтено».

12.2.4 Рекомендации по оцениванию в процессе наблюдения за работой на практическом занятии

Наблюдение за работой на практическом занятии – важнейший компонент контроля деятельности обучающихся и качества их обучения.

Критерии оценки в процессе наблюдения за работой на практическом занятии:

– самостоятельность выполнения задания и работы с методическими указаниями (учитывается работа в течение занятия, быстрота и способность нахождения в методических указаниях нужной информации);

– правильность выполнения работы (учитывается последовательность выполняемых действий, умение работать с инструментами и/или средствами вычислительной техники);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения работы с учетом индивидуальных особенностей обучающихся);

– активность обучающегося при выполнении практической работы (учитывается индивидуальная работа и работа в группе).

Критерии оценки по результатам наблюдения за работой на практическом занятии

Наименование параметра оценки	Максимальное количество баллов
Самостоятельно выполняет задания; умеет работать с методическими указаниями.	2,5
Указанные в методических указаниях действия выполняет в правильной последовательности; умеет работать с инструментами и/или средствами вычислительной техники.	1,25

Наименование параметра оценки	Максимальное количество баллов
Рационально использует время, отведенное на задание; проявляет активность при выполнении практической работы.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины приведены в приложении.

13 Промежуточная аттестация

13.1 Оценочные материалы для промежуточной аттестации обучающихся по учебной дисциплине предназначены для оценки степени достижения запланированных результатов обучения по завершению изучения учебной дисциплины в установленной учебным планом форме и позволяют определить качество усвоения изученного материала.

Итоговой формой контроля сформированности компетенций у обучающихся по учебной дисциплине является: экзамен.

Оценочные материалы для промежуточной аттестации обучающихся включают: вопросы к экзамену; задачи к экзамену.

13.2 Оценивание обучающегося на экзамене

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, обладает приемами выполнения практических задач по формированию компетенций.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, обладает необходимыми умениями и приемами их выполнения.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает сложности при

Оценка	Требования к знаниям
	выполнении практических работ и затрудняется связать теорию вопроса с практикой.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по данной учебной дисциплине.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) основная литература:

1 Новожилов, О. П. Информатика : учебник для среднего профессионального образования. В 2 ч. Часть 1 / О. П. Новожилов. – 3-е изд., пер. и доп. – Москва : Юрайт, 2022. – 320 с. – ISBN 978-5-534-06372-1. – URL: https://urait.ru/bcode/493964 (дата обращения: 15.05.2025);

2 Новожилов, О. П. Информатика : учебник для среднего профессионального образования. В 2 ч. Часть 2 / О. П. Новожилов. – 3-е изд., пер. и доп. – Москва : Юрайт, 2022. – 302 с. – ISBN 978-5-534-06374-5. – URL: https://urait.ru/bcode/493965 (дата обращения: 15.05.2025);

3 Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., пер. и доп. – Москва : Издательство Юрайт, 2022. – 161 с. – ISBN 978-5-534-13948-8. – URL: https://urait.ru/bcode/495525 (дата обращения: 15.05.2025).

б) дополнительная литература:

1 Новожилов, О. П. Архитектура компьютерных систем : учебное пособие для среднего профессионального образования. В 2 ч. Часть 1 / О. П. Новожилов. – Москва : Издательство Юрайт, 2022. – 276 с. – ISBN 978-5-534-10299-4. – URL: https://urait.ru/bcode/495226 (дата обращения: 15.05.2025);

2 Новожилов, О. П. Архитектура компьютерных систем : учебное пособие для среднего профессионального образования. В 2 ч. Часть 2 / О. П. Новожилов. – Москва : Издательство Юрайт, 2022. – 246 с. – ISBN 978-5-534-10301-4. – URL: https://urait.ru/bcode/495227 (дата обращения: 15.05.2025);

в) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru. – URL: https://libr.sibsiu.ru;

2 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для авторизир. пользователей. – URL: https://library.sibsiu.ru/LibrELibraryFullText.asp;

3 Электронная библиотека Издательского центра «Академия» / ИП Бурцева Антонина Петровна. – Москва, [200 ?]. – URL: https://academia-library.ru. – Режим доступа: для авторизир. пользователей;

4 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, [200 –]. – URL: http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

5 ЛАНЬ : электронно-библиотечная система : [Единая профессиональная база знаний издательства Лань для СПО - Издательство Лань (СПО)] / ООО «Издательство ЛАНЬ». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

6 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

7 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: https://biblioclub.ru. – Режим доступа: для авторизир. пользователей;

8 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

9 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: http://eivis.ru. – Режим доступа: по подписке.

г) лицензионное и свободно распространяемое программное обеспечение:

– 7-Zip;
– Adobe Acrobat Reader;
– Astra Linux Special Edition;
– Kaspersky Endpoint Security;
– Microsoft Office;
– Microsoft Windows;
– OnlyOffice;
– VirtualBox;

– Р7-Офис.

д) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

15 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории для проведения занятий всех видов, предусмотренных учебным планом, в том числе для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, кабинеты, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов.

Для проведения занятий лекционного типа (лекций) предусмотрена аудитория, оборудованная компьютерной техникой, экраном и мультимедийным проектором, учебной доской? для проведения практических занятий предусмотрены лаборатории «Организация и принципы построения компьютерных систем», оснащенные 12-15 компьютерами обучающихся и 1 компьютером преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ, пакет САПР), сервером в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение: Windows Server 2012 или более новая версия, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионный программы по виртуализации.), компьютерами с лицензионным программным обеспечением, интерактивной доской, 6 маршрутизаторами, 6 коммутаторами, телекоммуникационной стойкой, 2 беспроводными маршрутизаторами Linksys, IP телефонами 3 шт., программно-аппаратными шлюзами безопасности 2 шт., 1 компьютером для лабораторных занятий с ОС Microsoft Windows Server, Linux и системами виртуализации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС СПО по направлению подготовки (специальности) 09.02.06 «Сетевое и системное администрирование».

Составитель(и):

преподаватель Грачев Александр Викторович (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.
Согласован:

Генеральный директор
ООО «Агит-плюс» А.Ю. Рыжих

Приложение

Тестовые задания для входного контроля знаний обучающихся

Выберите один правильный ответ.

1. Значение понятия «Хост» – это
   а) конечный пользовательский узел,
   б) сервер сетевых ресурсов;
   в) коммутатор сетевых ресурсов.
2. В связке «клиент-сервер», *клиент* – это
   а) любой ресурс сети;
   б) рабочая станция или пользователь;
   в) любое устройство ввода-вывода, например принтер.
3. Состояние «Коллизия» – это
   а) очередность передачи данных;
   б) метод внеочередной передачи данных;
   в) столкновение, попытка одновременной передачи данных.
4. Соединение непересекающихся сегментов локальной сети осуществляется через?
   а) маршрутизатор;
   б) мост;
   в) концентратор.
5. Задача каждого уровня сетевой модели OSI
   а) перенаправление задачи на вышележащий уровень;
   б) перенаправление задачи на нижележащий уровень;
   в) перенаправление задачи на любой уровень.
6. TFTP (Trivial File Transfer Protocol) – это
   а) протокол обслуживания электронной почты;
   б) простейший протокол пересылки файлов;
   в) протокол обмена гипертекстовой информацией.
7. Отображение текущей настройки TCP/IP выполняет утилита
   а) ping;
   б) ipconfig;
   в) route.
8. По области использования сети делятся на:
   а) Локальные и INTERNET
   б) Сети с одноранговыми пользователями и сети с разными категориями пользователей
   в) Локальные, региональные и глобальные
9. Компьютер, подключенный к сети Internet, обязательно имеет.
   а) IP-адрес
   б) Web-страницу
   в) URL-адрес
10. Глобальная компьютерная сеть - это.

а) Сеть в пределах одной или нескольких стран
б) Сеть в пределах одного города
в) INTERNET
г) Сеть, в пределах от одного города до трансконтинентальных

11. Конфликтом называется:
а) ситуация, при которой две или более станции «одновременно» бездействуют;
б) ситуация, при которой две или более станции «одновременно» пытаются захватить линию;
в) ситуация, при которой два или более сервера «одновременно» пытаются захватить линию;
г) ситуация, при которой сервер и рабочая станция «одновременно» пытаются захватить линию.

12. Коммуникационный протокол, описывающий формат дейтаграммы данных называется:
а) TCP|IP
б) TCP
в) UPD
г) IP

13. Маршрутизация это…
а) это правило назначения выходной линии связи данного узла связи ТКС для передачи пакета, базирующегося на информации, содержащейся в заголовке пакета (адреса отправителя и получателя), и информации о загрузке этого узла (длина очередей пакетов) и, возможно, ТКС в целом;
б) это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;
в) это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;
г) специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

14. Сервер - это?
а) сетевая программа, которая ведёт диалог одного пользователя с другим;
б) мощный компьютер, к которому подключаются остальные компьютеры;
в) компьютер отдельного пользователя, подключённый в общую сеть;
г) стандарт, определяющий форму представления и способ пересылки сообщения.

15. Компьютер, подключённый к Интернету, обязательно должен иметь:

а) Web - сайт;
б) установленный Web - сервер;
в) IP - адрес;
г) брандмауэр

16. Как по-другому называют корпоративную сеть:

а) глобальная;
б) региональная;
в) локальная;
г) отраслевая;

17. Провайдер – это:

а) владелец узла сети, с которым заключается договор на подключение к его узлу;
б) специальная программа для подключения к узлу сети;
в) владелец компьютера с которым заключается договор на подключение его компьютера к узлу сети;
г) аппаратное устройство для подключения к узлу сети.

18. Программа, взаимодействующая с сетевым адаптером называется:

а) сетевой драйвер;
б) передающая среда;
в) мультиплексор;
г) сетевой адаптер;

19. Сервер, служащий для хранения файлов, которые используются всеми рабочими станциями называется:

а) сервер телекоммуникаций;
б) дисковый сервер;
в) файловый сервер;
г) почтовый сервер.

20. Информация в компьютерных сетях передается по каналам связи в виде отдельных:

а) сообщений;
б) данных;
в) посланий;
г) пакетов.

Задания и вопросы для текущего контроля знаний обучающихся учебной дисциплины

1 Устный опрос на лекции

Перечень вопросов для устного опроса

Раздел 1 Фундаментальные принципы безопасной сети. Раздел 2 Безопасность Сетевых устройств OSI

1. Основные понятия информационной безопасности.
2. Комплекс мер по созданию атмосферы информационной безопасности.
3. Специальные мероприятия по обеспечению информационной безопасности.
4. Средства защиты информации.
5. Информационная безопасность в сети Интернет.
6. Сетевые протоколы и модели взаимодействия открытых систем.
7. Дайте определение понятию угроза?
8. В чем состоит суть атаки на отказ в обслуживании?
10. В чем состоит суть физической безопасности сети?

Раздел 3 Авторизация, аутентификация и учет доступа (AAA) Раздел 4 Реализация технологий брандмауэра Раздел 5 Реализация технологий предотвращения вторжения

1. Что такое аутентификация?
2. Какие протоколы аутентификации существуют?
3. Что такое шифрование?
4. Дайте определение понятию авторизация?
5. Дайте определение понятию аутентификация?
6. Для чего предназначен учет доступа?
7. Какие протоколы применяют авторизацию, аутентификацию и учет доступа?
8. Перечислите основные цели сетевой безопасности?
9. Что такое целостность данных?
10. Что такое межсетевые экраны? Виды межсетевых экранов.
11. Организационные меры и физическая безопасность.
12. Физическая и логическая схемы компьютерной сети.
13. Когда стали появляться стандартные технологии локальных сетей?
14. Вычислительная сеть - это…?
15. Основная цель сети - это…?
16. Значение слова «Интерфейс» - это…?
17. Поясните значение термина "топология"?

Раздел 6 Безопасность локальной сети Раздел 7 Криптографические системы Раздел 8 Реализация технологий VPN Раздел 9 Управление безопасной сетью Раздел 10 Понятие

о методах и средствах аудита уровня защищенности информационных систем

1. Что понимается под «Информационной безопасностью»? Назовите основные методы обеспечения информационной безопасности и дайте их краткую характеристику
2. Эшелонированная модель системы защиты.
3. Какие алгоритмы шифрования существуют? В каких протоколах они применяются?
4. Технология VPN. Пример использования в организации с несколькими филиалами.
5. Технология VPN.
6. Понятие угрозы информационной безопасности.
7. Информационная безопасность в условиях функционирования в России глобальных сетей.
8. Виды противников или «нарушителей» информационной безопасности.
9. Краткая характеристика компьютерных вирусов – источники и категории атак.
10. Угрозы информационной безопасности.
11. Просмотр сертификатов на компьютере – расположение сертификатов.
12. Просмотр сертификатов на компьютере – основные поля сертификата.
13. Технология создания электронной цифровой подписи.
14. Генерация ЭЦП и проверка ЭЦП.
15. Характеристики качества ЭЦП.

2 Примеры тестовых заданий

Раздел 1 Фундаментальные принципы безопасной сети.
Раздел 2 Безопасность Сетевых устройств OSI

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

а) Разработка аппаратных средств обеспечения правовых данных

б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий

в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

а) Хищение жестких дисков, подключение к сети, инсайдерство

б) Перехват данных, хищение данных, изменение архитектуры системы

в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

а) Персональная, корпоративная, государственная

б) Клиентская, серверная, сетевая

в) Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

а) несанкционированного доступа, воздействия в сети

б) инсайдерства в организации

в) чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

а) Компьютерные сети, базы данных

б) Информационные системы, психологическое состояние пользователей

в) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

а) Искажение, уменьшение объема, перекодировка информации

б) Техническое вмешательство, выведение из строя оборудования сети

в) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

а) Экономической эффективности системы безопасности

б) Многоплатформенной реализации системы

в) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

а) руководители, менеджеры, администраторы компаний

б) органы права, государства, бизнеса

в) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

а) Установление регламента, аудит системы, выявление рисков

б) Установка новых офисных приложений, смена хостинг-компании

в) Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

а) Неоправданных ограничений при работе в сети (системе)

б) Рисков безопасности сети, системы

в) Презумпции секретности

Раздел 3 Авторизация, аутентификация и учет доступа (AAA) Раздел 4 Реализация технологий брандмауэра Раздел 5 Реализация технологий предотвращения вторжения

1) Что такое авторизация?

а) назначение и контроль доступа легальных пользователей к ресурсам с теми правами, которые определены этим пользователям администратором

б) назначение и контроль доступа нелегальных пользователей к ресурсам с теми правами, которые определены этим пользователям администратором

в) назначение и контроль доступа неизвестных пользователей к ресурсам с теми правами, которые определены этим пользователям администратором

2) Что такое аутентификация?

а) проверка и предотвращение доступа нежелательных лиц, разрешение доступа только легальным пользователям

б) отсутствие проверки и назначение доступа нежелательных лиц

в) свободный доступ любых пользователей и нежелательных лиц

3) Какое название носит некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении к компьютерной системе:

а) аутентификатор

б) пароль

в) идентификатор

4) Какое название носят полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом:

а) аудит

б) аутентификация

в) авторизация

5) Программная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации называется:

а) брандмауэром;

б) NAT-сервером;

в) антивирусом.

6) Основная задача брандмауэра:

а) защита сети от удаленных атак;

б) выполняет функцию внешнего маршрутизатора;

в) защита от вирусов;

г) запрещает доступ к любым другим компьютерам.

7) На каком минимум уровне модели OSI должен работать брандмауэр, чтобы обеспечивать фильтрацию трафика:

а) на сетевом;

б) на физическом;

в) на сеансовом;

г) на прикладном?

8) Составляющей политики сетевой безопасности не является:

а) политика доступа к сетевым сервисам;

б) политика реализации межсетевых экранов;

в) политика прав учетных записей пользователей.

9) Программное или аппаратное средство предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления или в основном через Интернет это -…

а) Система обнаружения несанкционированного доступа

б) Система обнаружения вторжений

в) Система обнаружения коллизий

10) Протокольные СОВ используются для….

а) Отслеживания трафика

б) Отслеживание вирусов

в) Отслеживание неисправностей

11) Что используют протокольные системы обнаружения вторжений для отслеживания трафика нарушающего правила?

а) Программный язык

б) Систему управления

в) Синтаксис языка

Раздел 6 Безопасность локальной сети Раздел 7 Криптографические системы Раздел 8 Реализация технологий VPN Раздел 9 Управление безопасной сетью Раздел 10 Понятие о методах и средствах аудита уровня защищенности информационных систем

1) Наиболее распространены угрозы информационной безопасности корпоративной системы:

а) Покупка нелицензионного ПО

б) Ошибки эксплуатации и неумышленного изменения режима работы системы

в) Сознательного внедрения сетевых вирусов

2) Наиболее распространены угрозы информационной безопасности сети:

а) Распределенный доступ клиент, отказ оборудования

б) Моральный износ сети, инсайдерство

в) Сбой (отказ) оборудования, нелегальное копирование данных

3) Принципом политики информационной безопасности является принцип:

а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

б) Одноуровневой защиты сети, системы

в) Совместимых, однотипных программно-технических средств сети, системы

4) Что такое шифрование?

а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

в) удобная среда для вычисления конечного пользователя

5) Что такое кодирование?

а) преобразование обычного, понятного текста в код

б) преобразование

в) написание программы

6) Для восстановления защитного текста требуется:

а) ключ

б) матрица

в) вектор

7) Из представленного ниже, подсистема управления криптографическими ключами структурно состоит из:

а) подсистемы защиты ключей
б) подсистемы генерации ключей
в) центра распределения ключей

8) Каковы альтернативы VPN

а) аренда каналов у операторов связи
б) ведение общения в бумажной форме
в) построение собственной сети связи

9) К недостаткам VPN можно отнести:

а) необходимость использования коммутируемого соединения;
б) необходимость использовать выделенные линии;
в) сложность в настройке подключения.

10) Туннелирование позволяет:

а) организовать передачу пакетов одного протокола в логической среде, использующей другой протокол;
б) организовать передачу пакетов одного протокола в логической среде, использующей тот же протокол;
в) организовать передачу пакетов одного протокола в физической среде, использующей тот же протокол;

г) организовать передачу пакетов одного протокола в физической среде, не использующей протокол.

11) Логический путь передвижения инкапсулированных пакетов в транзитной сети называется:

а) туннель;
б) шлюз;
в) магистраль; путь.

12) Информационная безопасность зависит от:

а) компьютеров, поддерживающей инфраструктуры +

б) пользователей

в) информации

13) Таргетированная атака – это:

а) атака на сетевое оборудование

б) атака на компьютерную систему крупного предприятия

в) атака на конкретный компьютер пользователя

14) Какие угрозы безопасности информации являются преднамеренными:

а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ

15) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

а) Регламентированной

б) Правовой

в) Защищаемой

16) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

а) Программные, технические, организационные, технологические

б) Серверные, клиентские, спутниковые, наземные

в) Личные, корпоративные, социальные, национальные

17) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

а) Владелец сети

б) Администратор сети

в) Пользователь сети

18) Политика безопасности в системе (сети) – это комплекс:

а) Руководств, требований обеспечения необходимого уровня безопасности

б) Инструкций, алгоритмов поведения пользователя в сети

в) Нормы информационного права, соблюдаемые в сети

19) Наиболее важным при реализации защитных мер политики безопасности является:

а) Аудит, анализ затрат на проведение защитных мер

б) Аудит, анализ безопасности

в) Аудит, анализ уязвимостей, риск-ситуаций

3 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения и вопросы для собеседования представлены в методических указаниях к практическим занятиям.

4 Вопросы к экзамену для промежуточной аттестации

1. Основные понятия информационной безопасности.
2. Комплекс мер по созданию атмосферы информационной безопасности.
3. Специальные мероприятия по обеспечению информационной безопасности.
4. Международные стандарты информационного обмена.
5. Понятие угрозы информационной безопасности.
6. Информационная безопасность в условиях функционирования в России глобальных сетей.
7. Виды противников или «нарушителей» информационной безопасности.

8. Краткая характеристика компьютерных вирусов – источники и категории атак.
9. Угрозы информационной безопасности.
10. Средства защиты информации.
11. Информационная безопасность в сети Интернет.
12. Сетевые протоколы и модели взаимодействия открытых систем.
13. Пакеты физического, канального, сетевого, транспортного уровней.
14. Концепция виртуальной цепи.
15. Дайте определение понятию угроза?
16. В чем состоит суть атаки на отказ в обслуживании?
17. В чем состоит суть физической безопасности сети?
18. Что такое межсетевые экраны? Виды межсетевых экранов.
20. Что такое аутентификация?
21. Какие протоколы аутентификации существуют?
22. Дайте определение понятию авторизация?
23. Дайте определение понятию аутентификация?
24. Для чего предназначен учет доступа?
25. Какие протоколы применяют авторизацию, аутентификацию и учет доступа?
26. Что такое сетевой брандмауэр?
27. Зачем нужен брандмауэр?
28. От чего может защитить брандмауэр?
29. От чего не может защитить брандмауэр?
30. Системы обнаружения вторжений. Принцип работы.
31. Перечислить основные причины невозможности обеспечения 32. адекватной защиты только средствами межсетевых экранов.
33. Дайте определение понятию «система обнаружения вторжений»
34. Какие подходы для обнаружения атак и вторжений Вы знаете?
35. Дайте определение понятия data mining.
36. Перечислите основные цели сетевой безопасности?
37. Что такое целостность данных?
38. Дайте определение понятию конфиденциальность данных.
39. Дайте определение понятию доступность данных.
40. Какие технические угрозы существуют в локальной сети?
41. Дайте определение понятиям: вирус, троянский конь.
42. Для чего предназначены «снифферы»?
43. Как влияет человеческий фактор на безопасность локальной сети?
44. Что такое шифрование?
45. Какие алгоритмы шифрования существуют? В каких протоколах они применяются?
46. Криптографическая защита информации в Интернете.
47. Симметричное и асимметричное шифрование.
48. Алгоритмы хэширования. Сертификаты.
49. Симметричные блочные шифры. Принципы их построения и режимы работы.

50. Системы шифрования с открытыми ключами, принципы их построения и области применения.
51. Электронная подпись, схемы ее построения.
52. Дайте определение VPN?
53. В чем преимущества использования VPN-технологий по сравнению с технологиями глобальных сетей (WAN)?
54. Можно ли описать требования безопасности для VPN при использовании общедоступных и частных сетей?
55. Расскажите, пожалуйста, подробнее о VPN, связывающих две ЛВС.
56. Приведите классификацию угроз ИБ с примерами.
57. Эшелонированная модель системы защиты. Назовите ее компоненты. Почему они расположены именно в таком порядке, поясните каждый компонент.
58. Аудит информационной безопасности.
59. Протоколирование и аудит.
60. Принципы обеспечения целостности

5 Задачи к экзамену для промежуточной аттестации

1. Сохранить резервную копию документов не на физическом носителе. Создать резервную копию 2 документов из папки в «облачном пространстве» на «Яндекс диск».
2. Сохранить резервную копию документов не на физическом носителе. Создать резервную копию 2 документов из папки в «облачном пространстве» на «mega.co».
3. Сохранить резервную копию документов не на физическом носителе. Создать резервную копию 2 документов из папки в «облачном пространстве» на «Mail.ru».
4. Запустите антивирусную программу и выполните проверку оперативной памяти компьютера на наличие вирусов. Выполните тестирование дисков Д: и С: на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.
5. Запустите антивирусную программу и выполните проверку диска С на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.
6. Настройте параметры локальной политики безопасности операционной системы Windows 10.
7. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.
8. После успешного выполнения предыдущего задания измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

7. .Произвести настройку Брандмауэра на виртуальной машине. Произвести настройку механизма Windows «Удаленные сеансы» на виртуальной машине ПК.
8. Произвести настройку Брандмауэра на виртуальной машине. Произвести настройку механизма правил брандмауэра для разрешения ping-запросов;
9. В рамках работы с виртуальными машинами реализовать стенд, описывающий Рабочие места, входящие в состав сети, которым требуется включить сетевые адаптеры в режиме NAT, что позволит использовать внешнее интернет соединение на каждой машине.
10. Придумайте и описать новую концепцию обеспечения информационной безопасности предприятия с заданными условиями:
    а. На ПК допускается хранение секретной информации
    б. Предприятие использует финансовую информацию в виде вложений в переписке с контрагентами.
11. Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников. Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.
12. Используя выбранный способ криптографической защиты зашифровать системой шифрования Цезаря свою фамилию, имя, отчество.
13. Используя выбранный способ криптографической защиты зашифровать алгоритмом двойных перестановок свою фамилию, имя, отчество.
14. Используя выбранный способ криптографической защиты зашифровать используя шифр перестановки название своей специальности и название предмета.
15. Используя выбранный способ криптографической защиты зашифровать системой шифрования Цезаря название своей специальности и название предмета.
16. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок название своей специальности и название изучаемого модуля.
17. Используя средства криптографической защиты используя шифр перестановки зашифровать название своей специальности и название предмета.
18. На виртуальной машине с Windows Server 2016 реализовать поддержку роли VPN.
19 В среде графического сетевого симулятора GNS3 реализовать пример работы технологии VPN для трех виртуальных машин.
20. Провести **моделирование объектов сетевой инфраструктуры локальной сети в среде в среде GNS3.**

21. Произвести первичный сбор информации для пяти любых сайтов.
22. Промести проверку и идентификацию доступности ресурсов.
23. Произвести проверку отслеживание маршрутов.
24. Провести сканирование портов нескольких ресурсов.
25. Провести проверку установленных ОС.

.....