МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
О.Н. Выборнова
«05» мая 2025 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой
информационной безопасности
В.А. Черкасова
«05» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность компьютерных сетей

наименование дисциплины (модуля)

Составитель(-и)	**Выборнова О.Н., доцент, к.т.н, доцент кафедры цифровых технологий** **Мартьянова А.Е., доцент, к.т.н., доцент кафедры информационной безопасности**
Согласовано с работодателям	**Давидюк Н.В., доцент, к.т.н., заведующий кафедрой «Информационная безопасность», ФГБОУ;** **Барсуков В.А., начальник отдела информационной безопасности Управления корпоративной защиты ООО «Газпром добыча Астрахань»**
Направление подготовки	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**«Организация и технология защиты информации (в сфере информационных и телекоммуникационных технологий)»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная, очно-заочная**
Год приема (курс)	**2024**
Курс	**4 (по очной форме)** **5 (по очно-заочной форме)**
Семестры	**8 (по очной форме)** **9 (по очно-заочной форме)**

Астрахань – 2025

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ(МОДУЛЯ)

1.1. Целью освоения дисциплины «Безопасность компьютерных сетей» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации в вычислительных сетях предприятий, изучение студентами программных средств защиты конфиденциальной информации в вычислительных сетях.

1.2. Задачи освоения дисциплины (модуля):

- определение места системы защиты информации в корпоративной информационной системе;
- определение и классификация методов защиты информации в распределенной вычислительной сети предприятия;
- раскрытие принципов, методов и технологии защиты информации в корпоративной вычислительной сети;
- изучение научных, прикладных и методологических аспектов организации технологии защиты и обработки конфиденциальных данных;
- изучение научных и прикладных аспектов организации защищенной инфраструктуры корпоративной информационной системы;
- закрепление полученных знаний с целью их применения на практике после окончания учебы.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Безопасность компьютерных сетей» относится к части плана элективных дисциплин и осваивается в 8 семестре очной и в 9 семестре очно-заочной форм обучения.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами*:*

- Информатика.
- Аппаратные средства вычислительной техники.
- Безопасность жизнедеятельности.
- Основы информационной безопасности.
- Организационное и правовое обеспечение информационной безопасности.

Знания: основных понятий информатики, основных сетевых протоколов и основных принципов построения локальных и распределенных корпоративных вычислительных сетей; основных понятий информационной безопасности; основных понятий охраны труда и техники безопасности; основных поражающих факторов электрического тока; основных понятий и определений в области информационной безопасности и защиты информации.
Умения: использовать программные и аппаратные средства персонального компьютера, классифицировать возможные угрозы информационной безопасности, пользоваться нормативными документами по защите информации.
Навыки: поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); проектирования локальных и распределенных корпоративных вычислительных сетей; техники

безопасности и охраны труда; методикой и техникой составления различных управленческих и документов учреждений, организаций и предприятий.

2.3. Последующие учебные дисциплины (модули), для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной (модулем):

- Производственная практика.
- Выпускная квалификационная работа.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) профессиональных (ПК):

ПК-1: Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем.

ПК-4: Способен администрировать средства защиты информации в компьютерных системах и сетях.

Таблица 1. Декомпозиция результатов обучения

Код компетенции	Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
ПК-1	ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем	нормативные правовые акты в области защиты информации, организационные меры по защите информации, программно-аппаратные средства обеспечения защиты информации автоматизированных систем, методы контроля эффективности защиты информации от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	определять источники и причины возникновения инцидентов, устранять нарушения правил разграничения доступа; применять программные средства обеспечения безопасности данных, осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, использовать криптографические методы и средства защиты информации в автоматизированных системах	методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа
ПК-4	ПК-4. Способен администрировать	источники угроз	анализировать	навыками управления

	средства защиты информации в компьютерных системах и сетях	информационной безопасности в компьютерных сетях и меры по их предотвращению; принципы функционирования программных средств криптографической защиты информации; виды политик управления доступом и информационными потоками в компьютерных сетях; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	угрозы безопасности информации в компьютерных системах и сетях; настраивать правила обработки пакетов в компьютерных сетях; настраивать политики безопасности операционных систем, оценивать угрозы безопасности информации в компьютерных системах и сетях, противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем, настраивать антивирусные средства защиты информации в операционных системах	средствами межсетевого экранирования в компьютерных сетях, методикой оценки оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 2 зачетные единицы (72 часа).

Трудоемкость отдельных видов учебной работы студентов очной формы обучения приведена в таблице 2.1.

Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения	для заочной формы обучения
Объем дисциплины в зачетных единицах	2	2	
Объем дисциплины в академических часах	72	72	
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):	45	27	
- занятия лекционного типа, в том числе:	18	9	

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения	для заочной формы обучения
- практическая подготовка (если предусмотрена)			
- занятия семинарского типа (семинары, практические, лабораторные), в том числе:	27	18	
- практическая подготовка (если предусмотрена)			
- консультация (предэкзаменационная)[1]			
- промежуточная аттестация по дисциплине[2]			
Самостоятельная работа обучающихся (час.)	27	45	
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	Зачет – 8 семестр	Зачет – 9 семестр	

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы представлены в таблице 2.2.

Таблица 2.2. Структура и содержание дисциплины (модуля)

для очной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия	2				3			3	8	Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к	2				3			3	8	Контрольная работа №1 Лабораторная работа №2 Промежуточ

1 Числовые данные в данной строке соответствуют трудоемкости, указанной в учебном плане в столбце «Конс. (для гр.)»

2 Числовые данные в данной строке соответствуют трудоемкости, указанной в учебном плане в столбце «КПА»

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации										ное тестирование Опрос на зачете
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)	2				3			3	8	Отчет по лабораторной работе №2 Контрольная работа №2 Опрос на зачете
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками	2				3			3	8	Отчет по лабораторной работе №3 Опрос на зачете
Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации	2				3			3	8	Контрольная работа №3 Отчет по лабораторной работе №4 Опрос на зачете
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров	2				3			3	8	Промежуточное тестирование Деловая игра Опрос на зачете
Тема 7. Проектирование базовой защиты периметра	2				3			3	8	Деловая игра. Опрос на зачете
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные	2				3			3	8	Лабораторная работа №5 Опрос на

Раздел, тема дисциплины (модуля)	Контактная работа, час.						КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР					
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
сети										зачете
Тема 9. Проектирование базовой защиты Web-сервера	2				3			3	8	Отчет по лабораторной работе №5 Опрос на зачете
Консультации										
Контроль промежуточной аттестации										**Зачет**
ИТОГО за семестр:	***18***				***27***			***27***	***72***	***72***

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; КПА – контроль промежуточной аттестации; КС – консультации; СР – самостоятельная работа

для очно-заочной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.						КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР					
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия	1				2			5	8	Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации	1				2			5	8	Контрольная работа №1 Лабораторная работа №2 Промежуточное тестирование Опрос на зачете
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с	1				2			5	8	Отчет по лабораторной работе №2 Контрольная работа №2

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)										Опрос на зачете
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками	1				2			5	8	Отчет по лабораторной работе №3 Опрос на зачете
Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации	1				2			5	8	Контрольная работа №3 Отчет по лабораторной работе №4 Опрос на зачете
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров	1				2			5	8	Промежуточное тестирование Деловая игра Опрос на зачете
Тема 7. Проектирование базовой защиты периметра	1				2			5	8	Деловая игра. Опрос на зачете
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети	1				2			5	8	Лабораторная работа №5 Опрос на зачете
Тема 9. Проектирование базовой защиты Web-сервера	1				2			5	8	Отчет по лабораторной работе №5 Опрос на зачете
Консультации										
Контроль промежуточной аттестации										**Зачет**
ИТОГО за семестр:	***9***				***18***			***45***	***72***	***72***

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; КПА – контроль промежуточной аттестации; КС – консультации; СР – самостоятельная работа

[При заполнении таблиц 2.2. необходимо учесть следующее:

- заполняются таблицы только по реализуемым формам обучения;

- общий объем часов на каждую тему (раздел) для разных форм обучения должен быть одинаковым;

- практическая подготовка по видам учебных занятий распределяется разработчиком РПД по темам самостоятельно в пределах часов, выделенных в учебном плане на данную дисциплину;

- самостоятельная работа по каждой теме вычисляется как разность между общим объемом часов, выделенных на тему, и количеством часов, выделенных на сумму всех видов контактной работы;

- при подсчете консультаций необходимо учесть, что в случае наличия экзамена по дисциплине проводится одночасовая консультация; разбивать часы на консультации по разделам не нужно;

- при написании курсовой работы на контактную работу с преподавателем отводится 2 часа, объем самостоятельной работы студента на курсовую работу определяется разработчиком; разбивать часы на подготовку курсовой работы по разделам и (или) темам не нужно;

- контроль промежуточной аттестации вносится в соответствующую графу и столбец, разбивать часы на КПА по разделам не нужно.

Далее в данном пункте программы размещается матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых в них компетенций]

Таблица 3. Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции		Общее количество компетенций
		ПК-1	ПК-4	
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия	8	+	+	2
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации	8	+	+	2
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)	8	+	+	2
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками	8	+	+	2

Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации	8	+	+	2
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров	8	+	+	2
Тема 7. Проектирование базовой защиты периметра	8	+	+	2
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети	8	+	+	2
Тема 9. Проектирование базовой защиты Web-сервера	8	+	+	2
ИТОГО	72			

Краткое содержание каждой темы дисциплины (модуля)

Тема 1

Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности

Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия

Тема 2

Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки

Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации

Тема 3

Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов

Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)

Тема 4

Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения

Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками

Тема 5

Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS

Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации

Тема 6

Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки

Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров

Тема 7

Проектирование базовой защиты периметра

Тема 8

Проблемы с безопасностью электронной почты. Виртуальные частные сети

Тема 9

Проектирование базовой защиты Web-сервера

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Лекционные занятия

Основной формой реализации теоретического обучения является лекция, которая представляет собой систематическое, последовательное изложение преподавателем-лектором учебного материала теоретического характера. Цель лекции — организация целенаправленной познавательной деятельности студентов по овладению программным материалом учебной дисциплины.

Порядок подготовки лекционного занятия включает в себя выполнение следующих этапов:

- изучение требований программы дисциплины,
- определение целей и задач лекции,
- разработка плана проведения лекции,
- подбор литературы (ознакомление с методической литературой, публикациями периодической печати по темам лекционного занятия),
- отбор необходимого и достаточного по содержанию учебного материала,
- определение методов, приемов и средств поддержания интереса, внимания, стимулирования творческого мышления студентов,
- написание конспекта лекции.

Лекция должна включать следующие разделы:

- формулировку темы лекции,
- указание основных изучаемых разделов или вопросов и предполагаемых затрат времени на их изложение,
- изложение вводной части,
- изложение основной части лекции,
- краткие выводы по каждому разделу,
- заключение,
- рекомендации литературных источников по излагаемым вопросам.

Лабораторные занятия

Лабораторное занятие — целенаправленная форма организации педагогического процесса, направленна на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Они развивают научное мышление и речь, позволяют проверить знания студентов и выступают как средства оперативной обратной связи.

Правильно организованные лабораторные занятия ориентированы на решение следующих задач:

- обобщение, систематизация, углубление, закрепление полученных в процесс самостоятельной работы теоретических знаний по дисциплине (предмету),
- формирование практических умений и навыков необходимых в будущей профессиональной деятельности, реализация единства интеллектуальной и практической деятельности,
- выработка при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Состав заданий для лабораторных занятий должен быть спланирован с расчетом, чтобы за отведенное время они могли быть качественно выполнены большинством учащихся.
Лабораторные занятия должны быть так организованы, чтобы студенты ощущали нарастание сложности выполнения заданий, испытывали бы положительные эмоции от переживания собственного успеха в обучении и овладевании навыками правильных и точных решений.

Самостоятельная работа

Самостоятельная работа — это вид учебной деятельности, которую студент совершает в установленное время и в установленном объеме индивидуально или в группе, без непосредственно помощи преподавателя (но при его контроле), руководствуясь сформулированными ранее представлениями о порядке и правильности выполнения действий.
В учебном процессе образовательного учреждения выделяются два вида самостоятельной работы:

1) аудиторная — выполняется на учебных занятиях, под непосредственным руководством преподавателя и по его заданию (выполнение самостоятельных работ; выполнение контрольных и лабораторных работ; решение задач),
2) внеаудиторная — выполняется по заданию преподавателя, но без его непосредственного участия (подготовка к аудиторным занятиям; изучение учебного материала, вынесенного на самостоятельную проработку; выполнение домашних заданий разнообразного характера; выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы; подготовка к контрольной работе). Внеаудиторные самостоятельные работы представляют собой логическое продолжение аудиторных занятий, проводятся по заданию преподавателя, который инструктирует студентов и устанавливает сроки выполнения задания.

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой (основной) из п.8.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой (дополнительной) из п.8.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Лекционные занятия

Лекция — основной вид обучения в вузе. В лекции излагаются основные положения теории, ее понятия и законы, приводятся факты, показывающие связь теории с практикой.
Накануне лекции необходимо повторить содержание предыдущей лекции (а также теорию по изучаемой теме в учебниках), а затем посмотреть тему очередной лекции по программе (по плану лекций).
Полезно вести записи (конспекты) лекций: для непонятных вопросов оставлять место при работе над темой лекции с учебными пособиями.
Записи лекций следует вести в отдельной тетради, оставляя место для дополнений во время самостоятельной работы.
При конспектировании лекций выделяйте главы и разделы, параграфы, подчеркивайте основное.

Лабораторные занятия

Лабораторное занятие — наиболее активный вид учебных занятий в вузе. Он предполагает самостоятельную работу над учебными пособиями, основной литературой, открытыми источниками информации.
К каждому лабораторному занятию нужно готовиться. Подготовку следует начинать с повторения теории (по учебному пособию). После этого нужно решать задачи из предложенного домашнего задания.

Самостоятельная работа

Самостоятельность в учебной работе способствует развитию заинтересованности студента в изучаемом материале, вырабатывает у него умение и потребность самостоятельно получать знания, что весьма важно для специалиста с высшим образованием.

Самостоятельная работа студентов представлена в следующих формах:

- работа с учебной литературой и конспектом лекций с целью подготовки к лабораторным занятиям, составление конспектов тем, выносимых на самостоятельную проработку,
- систематическое выполнение домашних работ.

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-ресурсами.

Таблица 4. Содержание самостоятельной работы обучающихся

для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации Контрольная работа №1 Отчет по лабораторной работе №2 Промежуточное тестирование Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI) Отчет по лабораторной работе №2 Контрольная работа №2 Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками Отчет по лабораторной работе №3 Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации Контрольная работа №3	3	Внеаудиторная, изучение учебных пособий

Отчет по лабораторной работе №4 Опрос на зачете		
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров Промежуточное тестирование Деловая игра Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 7. Проектирование базовой защиты периметра Деловая игра. Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети Отчет по лабораторной работе №5 Опрос на зачете	3	Внеаудиторная, изучение учебных пособий
Тема 9. Проектирование базовой защиты Web-сервера Отчет по лабораторной работе №5 Опрос на зачете	3	Внеаудиторная, изучение учебных пособий

для очно-заочной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации Контрольная работа №1 Отчет по лабораторной работе №2 Промежуточное тестирование Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI) Отчет по лабораторной работе №2 Контрольная работа №2 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками Отчет по лабораторной работе №3 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий

Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации Контрольная работа №3 Отчет по лабораторной работе №4 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров Промежуточное тестирование Деловая игра Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 7. Проектирование базовой защиты периметра Деловая игра. Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети Отчет по лабораторной работе №5 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
Тема 9. Проектирование базовой защиты Web-сервера Отчет по лабораторной работе №5 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно

Отчет по лабораторной работе – оформляется и отчитывается в электронном виде: формат листа А4, книжная ориентация страницы. Отчеты по всем лабораторным работам имеют единый титульный лист, на котором указывается наименование дисциплины, ФИО и группа исполнителя, ФИО преподавателя, принимающего отчеты. В отчете по каждой лабораторной работе должно быть представлено наименование работы, цель, ход выполнения работы (скриншоты, краткое текстовое описание), выводы по результатам работы.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

Таблица 5. Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое	Лабораторная

		занятие, семинар	работа
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, выполнение теста
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации	Лекция - презентация	Не предусмотрено	выполнение контрольной работы, выполнение теста
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров	Лекция - презентация	Не предусмотрено	выполнение теста Подготовка к деловой игре
Тема 7. Проектирование базовой защиты периметра	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, Подготовка к деловой игре
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети	Лекция - презентация	Не предусмотрено	выполнение теста
Тема 9. Проектирование базовой защиты Web-сервера	Лекция - презентация	Не предусмотрено	Подготовка к деловой игре

6.2. Информационные технологии

Название информационной технологии	Темы, разделы дисциплины	Краткое описание применяемой технологии
Использование возможностей Интернета в учебном процессе	1 - 9	Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения)
Использование возможностей электронной почты преподавателя	1 - 9	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1 - 9	Использование мультимедийной презентации

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- - использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));
- - использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;
- - использование возможностей электронной почты преподавателя;
- - использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);
- - использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);
- - использование виртуальной обучающей среды (или системы управления обучением LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров.

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Google Chrome	Браузер
Microsoft Office 2013, Microsoft Office Project 2013,	Офисная программа

Microsoft Office Visio 2013	
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

- Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
- Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.

3) Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/

4) Электронно-библиотечная система elibrary. http://elibrary.ru

5) Справочная правовая система КонсультантПлюс: http://www.consultant.ru

6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Безопасность компьютерных сетей» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6.Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

Контролируемые раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Тема 1. Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия	ПК-1, ПК-4	Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете
Тема 2. Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии	ПК-1, ПК-4	Контрольная работа №1 Лабораторная работа №2 Промежуточное тестирование Опрос на зачете

разграничения доступа и аутентификации		
Тема 3. Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)	ПК-1, ПК-4	Отчет по лабораторной работе №2 Контрольная работа №2 Опрос на зачете
Тема 4. Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками	ПК-1, ПК-4	Отчет по лабораторной работе №3 Опрос на зачете
Тема 5. Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации	ПК-1, ПК-4	Контрольная работа №3 Отчет по лабораторной работе №4 Опрос на зачете
Тема 6. Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров	ПК-1, ПК-4	Промежуточное тестирование Деловая игра Опрос на зачете
Тема 7. Проектирование базовой защиты периметра	ПК-1, ПК-4	Деловая игра Опрос на зачете
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети	ПК-1, ПК-4	Лабораторная работа №5 Опрос на зачете
Тема 9. Проектирование базовой защиты Web-сервера	ПК-1, ПК-4	Отчет по лабораторной работе №5 Опрос на зачете

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

Таблица 7. Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов

Шкала оценивания	Критерии оценивания
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8. Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания

7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1. «Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для администрирования ИТ-инфраструктуры предприятия»

1. Входное тестирование

1. Несанкционированный доступ к информации
   a) Доступ к информации, нарушающий установленные правила ее получения.
   b) Преднамеренное обращение пользователя к данным, доступ к которым ему не разрешен, с целью их чтения, обновления или разрушения.
   c) Доступ субъектов к информации или действия с информацией с использованием штатных средств объекта информатизации (сети передачи данных), нарушающий установленные правила получения и работы с информацией.
   d) Получение информации без соответствующего разрешения на доступ.

2. Информационная безопасность -- это
   a) Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба субъекту информационных отношений
   b) Состояние защищенности физических и юридических лиц, государства в информационной сфере.
   c) Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

d) Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.
e) Скрытость информационных ресурсов

3. Политика информационной безопасности, прежде всего необходима для:
   a) успешного прохождения компанией регулярного аудита по ИБ
   b) обеспечения реального уровня защищенности информационной системы компании
   c) понимания персоналом важности требований по ИБ
   d) обеспечения адекватной защиты наиболее важных ресурсов компании

4. Политика информационной безопасности в общем случае является
   a) руководящим документом для администраторов безопасности и системных администраторов
   b) руководящим документом для ограниченного использования
   c) руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов
   d) руководящим документом для всех сотрудников компании

5. Какой метод обычно используется профессиональными взломщиками при информационной атаке?
   a) атака на наиболее защищенную цель
   b) атака на промежуточную цель
   c) атака на наименее защищенную цель
   d) атака осуществляется без целенаправленного выбора цели

1. ***Лабораторная работа №1 «***Использование виртуальных машин для изучения операционных систем на примере VirtualBox***»***

1. Ознакомиться с основными понятиями VirtualBox, изучить теоретически процедуру настройки системы виртуализации Microsoft.
2. Изучить практически технологию установки и настройки гостевых операционных систем на примере Microsoft Windows 7 и Microsoft Windows Server 2008.
3. Изучить средства настройки виртуальной машины и установку дополнений к виртуальной машине.
4. Изучить средства управления виртуальными жесткими дисками и методы настройки сетевого взаимодействия в виртуальной сети.
5. Произвести проверку прохождение сетевых пакетов между созданными виртуальными машинами.
6. Произвести добавление серверных ролей в созданных виртуальных машинах.
7. Подготовить отчет о выполнении лабораторной работы.

Тема 2. «Проектирование безопасного управления сетью. Общие уязвимости в управлении сетью. Границы безопасности. Снижение к минимуму возможности атаки. Администрирование пользователей и компьютеров. Определение уровня административных полномочий. Планирование и реализация стратегии разграничения доступа и аутентификации»

1. Контрольная работа №1 «Основные принципы защиты сетевой инфраструктуры»

Вопросы:

1. Предмет, содержание и задачи курса, методы его изучения
2. Правовые требования к информационной безопасности предприятия
3. Основные методы защиты сетевой инфраструктуры предприятия
4. Анализ существующих политик и мер безопасности
5. Понятие информационных активов предприятия
6. Понятие угроз и уязвимостей вычислительной сети предприятия
7. Анализ рисков для администрирования ИТ-инфраструктуры предприятия
8. Структура и функции органов защиты информации на предприятии

1. Лабораторная работа №2 «Средства безопасности операционной системы Microsoft Windows Server***»***

А) Задание:

1. Создать домен Active Directory с именем zios.com. Произвести добавление серверной роли контроллера домена.
2. Произвести установку DNS-сервера.
3. Произвести установку DHCP-сервера (если требуется в данном варианте).
4. Выполнить создание и настройку консоли управления MMC.
5. Включить в домен zios.com клиентский компьютер под управлением Windows 7.
6. Произвести настройку на сервере подключения через Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

Б) Контрольные вопросы:

1. Раскройте понятия «домен», «дерево» и «лес» в Active Directory.
2. Раскройте понятие консоли MMC. В каком режиме по умолчанию создаются консоли MMC?
3. Может ли оснастка одновременно отображать информацию о локальном и удаленном компьютерах?
4. Если требуется ограничить доступ к оснастке, как сконфигурировать содержащую ее консоль MMC.
5. Какие реквизиты необходимы для администрирования удаленного компьютера из консоли MMC.

2. Промежуточное тестирование

1. Какая команда поможет найти учетные записи, не использовавшиеся в течение двух месяцев?
   a. DSADD.
   b. DSGET.
   c. DSMOD.
   d. DSRM.
   e. DSQUERY.
2. Какую переменную можно использовать в командах DSMOD и DSADD для создания домашних папок и папок профилей для определенных пользователей?
   a. %Username%.
   b. $Usemame$.
   c. CN=Username.
   d. <Username>.
3. При помощи какой команды можно вывести номера телефонов всех пользователей в ОП?
   a. DSADD.
   b. DSGET.
   c. DSMOD.

d. DSRM.
e. DSQUERY.

4. Какое из следующих разрешений NTFS позволяет удалять папку:
   a. чтение
   b. чтение и выполнение
   c. изменение
   d. администрирование
5. Характеристики TLS/SSL:
   А. Шифрование трафика.
   Б. Двухсторонняя аутентификация.
   В. Периодическая смена ключей.
   Г. Односторонняя аутентификация.
6. Какое средство используется на сервере для включения удаленного подключения к рабочему столу?
   А. Диспетчер служб терминалов (Terminal Services Manager).
   Б. Настройка служб терминалов (Terminal Services Configuration).
   В. Система (System Properties) из Панели управления.
   Г. Лицензирование служб терминалов (Terminal Services Licensing).
7. Обязательные компоненты TLS/SSL:
   А. Аутентификация сервера.
   Б. Сертификат X.509.
   В. Аутентификация пользователя.
   Г. Статический симметричный ключ.
   Д. Все ответы неверны.
8. Где в интерфейсе можно изменить членство компьютера под управлением Windows Server в домене?
   А. Окно свойств Мой компьютер (My Computer)
   Б. Приложение Система (System) из Панели управления
   В. Консоль Active Directory - пользователи и компьютеры (Active Directory Users And Computers)
   Г. Папка Сетевые подключения (Network Connections)
   Д. Приложение Пользователи (Users) из Панели управления
   Е. Все ответы неверны.

Тема 3. «Проектирование проверки подлинности в гетерогенной сети. Понятие Kerberos. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI)»

1. Лабораторная работа №2 «Средства безопасности операционной системы Microsoft Windows Server» (продолжение)

А) Задание:

7. Выполнить настройку удаленного подключения к рабочему столу, при этом активировать удаленное подключение к рабочему столу, изменить число разрешенных одновременных подключений на сервере и настроить параметры завершения подключения. Для этого на вкладке «Сетевой адаптер» (Network Adapter) установить значение параметра Максимальное число подключений (Maximum Connections) равным 1.
8. На вкладке Сеансы (Sessions) установить оба флажка «Заменить параметры пользователя» (Override User Settings) и изменить настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей

закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.

- Завершение отключенного сеанса (End a disconnected session): 15 минут.
- Ограничение активного сеанса (Active session limit): никогда (never).
- Ограничение активного сеанса (Active session limit): 15 минут.
- При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

9. Произвести подключение к серверу с помощью клиента удаленного подключения к рабочему столу.
10. Подготовить отчет о выполнении лабораторной работы.

Б) Контрольные вопросы:

6. Все ли функции оснастки, применяемые на локальном компьютере, можно использовать при удаленном подключении.
7. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования?
8. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу.
9. В чем сходство и различие программ Удаленный помощник и Удаленный рабочий стол для администрирования.
10. Какие выгоды приносит использование программы Удаленный помощник?

2. Контрольная работа №2 «Проектирование защиты управления и поддержки сети»

Вопросы:

1. Проектирование безопасного управления сетью.
2. Общие уязвимости в управлении сетью.
3. Границы безопасности. Снижение к минимуму возможности атаки.
4. Администрирование пользователей и компьютеров.
5. Определение уровня административных полномочий.
6. Программно-техническая реализация средств защиты управления и поддержки сети.

Тема 4. «Политики паролей в сетях. Инструменты для реализации политик паролей и их ограничения. Требования к учетным записям пользователей. Параметры безопасности и ограничения средств управления политиками»

1. Лабораторная работа №3 «Учетные записи пользователей»

А) Задание:

1. Создание групп:

- Создайте 2 группы безопасности с локальной доменной областью действия
- Создайте 2 группы безопасности с глобальной областью действия

2. Создание учебных записей пользователей и помещение в группы

- Создайте по 1 учетной записи для каждой из групп, задавая в качестве параметра человеческие имена
- Создайте 1 учетную запись и поместите ее в каждую из групп

3. Включение групп в другие группы

- Поместите по 1 глобальной группе в каждую локальную группы

4. Создайте учетную запись для нового компьютера, который предполагается подключить к домену
5. Проверьте результат выполнения лабораторной работы
6. Оформите отчет

Б) Контрольные вопросы

1) Создание и управление учетными записями пользователей.
2) Создание и модификация учетных записей пользователей при помощи консоли Active Directory – пользователи и компьютеры (Active Directory Users And Computers).
3) Создание и модификация учетных записей пользователей средствами автоматизации.
4) Импорт учетных записей пользователей.
5) Управление локальными, перемещаемыми и обязательными профилями пользователей.
6) Устранение проблем с учетными записями пользователей.
7) Обнаружение заблокированных учетных записей и их разблокирование.
8) Диагностирование и устранение проблем со свойствами учетных записей пользователей.
9) Устранение ошибок, связанных с проверкой подлинности пользователей.

1. Лабораторная работа №3 «Учетные записи пользователей»

А) Задание

1. Создайте папку, поместите в нее текстовый файл и файл-приложение с расширением .exe (например, notepad.exe)

2. Установите для этой папки разрешения полного доступа для одного из пользователей группы «Администраторы» и ограниченные разрешения для пользователей с ограниченной учетной записью

3. Выполните различные действия с папкой и файлами для обеих учетных записей, чтобы проверить, как действуют ограничения

4. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера

5. Установите ограничения на доступ к папке с правами, аналогичными п.2, и подключитесь к ней через сеть с другого виртуального компьютера

6. Составьте отчет о проведенных экспериментах

Б) Контрольные вопросы

1. Какие объекты по умолчанию наследуют ограничения, установленные для родительской папки?

2. Кто может устанавливать разрешения для отдельных пользователей и групп

3. Особенности настройки общего доступа к папке в NTFS

Тема 5. «Проектирование защиты файлов шифрованием (EFS). Основные понятия EFS. Планирование и внедрение EFS в среде домена с PKI. Проектирование восстановления файлов с использованием центров сертификации»

1. ***Контрольная работа №3 «Основы защиты базовых сетевых функций»***

Вопросы

1. Планирование и реализация стратегии разграничения доступа и аутентификации.
2. Понятие протокола Kerberos.
3. Сертификаты. Основные понятия инфраструктуры открытых ключей (PKI).
4. Требования к учетным записям пользователей.
5. Проектирование проверки подлинности в гетерогенной сети.
6. Проверка подлинности с использованием Kerberos. Получение сеансовых билетов.
7. Политики паролей в сетях Windows Server 2003. Инструменты для реализации политик паролей и их ограничения.
8. Параметры безопасности и ограничения средств управления политиками.

1. ***Лабораторная работа №4*** «Проектирование инфраструктуры открытых ключей. Управление цифровыми сертификатами»

Задание:

1. Создать сертификат для шифрования файлов
2. Просмотреть созданные сертификаты
3. Зашифровать файл
4. Выполнить экспорт сертификата
5. Удалить сертификат. Проверить доступность файла
6. Импортировать сертификат. Проверить доступность файла

Тема 6. «Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и реализация защищенной базовой конфигурации для клиентских компьютеров»

1. Промежуточное тестирование

1. Для каких целей может выдавать сертификаты только **ЦС** предприятия?

a. Защиты **IPsec**.
b. Входа со смарт-картой.
c. Подписания кода.
d. Проверки подлинности в беспроводных сетях.

2. Какое изменение параметров сертификата не увеличит нагрузку на процессор **ЦС**?

a. Увеличение длины ключа.
b. Увеличение срока действия сертификата.
c. Выдача новых ключей при каждом обновлении сертификата.
d. Изменение типа сертификата.

3. Кто выдает сертификат корневому **ЦС**?

a. Сторонний **ЦС**.
b. Подчиненный **ЦС**.
c. Другой корневой **ЦС**.
d. Он сам.

4. Какие из перечисленных средств администраторы применяют для ручной выдачи сертификатов клиентам изолированного ЦС?

a. Оснастка ***Сертификаты***.

b. Консоль ***Центр сертификации***.
c. Интерфейс ***Служба подачи заявок на сертификат через Интернет***.
d. Оснастка ***Шаблоны сертификатов***.

5. В чем преимущество использования разностных CRL вместо полных?

6. Выберите из перечисленного ниже все, что потребуется пользователю для получения сертификатов от **ЦС** предприятия, использующего автоматическую подачу заявок?
a. Разрешение на использование шаблонов сертификатов.
b. Членство в подразделении, к которому администратор применил соответствующий **GPO**.
c. Доступ к **Active Directory**.
d. Доступ к оснастке ***Сертификаты***.

7. Укажите все **ЦС**, которые после развертывания следует отключить от сети по соображениям безопасности.
a. Корневой **ЦС**.
b. Промежуточные **ЦС**.
c. Один из выдающих **ЦС** в каждом офисе с промежуточным **ЦС**.
d. Все выдающие **ЦС**.

8. Позволит ли спроектированная **PKI** достичь всех поставленных целей?
a. Да.
b. Нет, так как удастся защитить только внутренних пользователей сети.
c. Нет, так как не обеспечена поддержка входа с использованием смарт-карт.

9. Как гарантировать, что только работники отдела разработки смогут получить сертификаты для входа со смарт-картой, **EFS** и **IPSec**?
a. Предоставить пользователям из научно-исследовательского отдела разрешения на доступ к консоли ***Сертификаты***, через которую они смогут запрашивать соответствующие сертификаты.
b. При помощи **GPO** отменить автоматическую подачу заявок для домена и активизировать автоматическую подачу заявок для подразделения, содержащего пользователей из научно-исследовательского отдела.
c. Предоставить пользователям из научно-исследовательского отдела право на использование шаблонов сертификатов ***Вход со смарт-картой*** (**Smartcard Logon**), ***Базовое шифрование EFS*** (**Basic EFS**) и ***IPSec***.
d. Установить модуль ***Служба подачи заявок на сертификат через Интернет*** и предоставить доступ к его Web-интерфейсу только пользователям из научно-исследовательского отдела.

10. Основа безопасного взаимодействия протокола Kerberos:
А. Статический симметричный ключ.
Б. Открытый и закрытый ключи.
В. Общий секрет.
Г. Все ответы неверны.

1. ***Деловая игра «Составление организационно-распорядительных документов по обеспечению политик сетевой безопасности на предприятиях различных форм собственности»***

Задание:

1. Разработать макет организационной структуры предприятия.
2. Разработать проект Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратно-программных средств автоматизированных систем предприятия.
3. Разработать проект Инструкции по организации резервного копирования информационных ресурсов вычислительной сети предприятия.
4. Разработать проект Регламента доступа сотрудников предприятия к сети Интернет для организаций и предприятий различных форм собственности.
5. Быть в готовности в роли руководителя предприятия, руководителя подразделения информационной безопасности решать управленческие задачи, связанные с обеспечением сетевой информационной безопасности на предприятии (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
6. Студентам письменно выполнить задание (объем 10-12 страниц) и быть в готовности к его защите на практическом занятии.

Порядок проведения практического занятия

1. Организация занятия (проверка присутствующих и готовности к занятиям, объявление темы и цели занятия, доведение порядка проведения занятия).
2. Распределение на подгруппы и озвучивается ситуация. Студентами выбирается одно из предприятий (например, коммерческий банк, предприятие сферы торговли, телекоммуникационная компания, предприятие топливно-энергетического комплнекса и т.д.), на котором создается вычислительная сеть.
3. Присвоение подгруппам первоначальных ролей (руководители службы информационной безопасности, руководители предприятия, системные администраторы).
4. Обсуждение студентами каждой подгруппы вопросов, решаемых руководством и сотрудниками предприятия по обеспечению информационной безопасности вычислительных сетей предприятия, вынесенных на практическое занятие с целью выработки общих позиций.
4.1. Вопросы со стороны подгруппы выступающих в роли руководителей предприятия.
4.2. Вопросы со стороны подгруппы выступающих в роли руководителей службы информационной безопасности.
4.3. Вопросы со стороны подгруппы выступающих в роли системных администраторов.
4.4. Ответы и дискуссии.
4.5. Выработка общей позиции и общего подхода к вопросам обеспечения информационной безопасности вычислительных сетей предприятия.
5. Обсуждение преподавателем и старшими групп оценок участников занятия.
6. Подведение итогов занятия с объявлением окончательных оценок участников практического занятия.

Роли:

Студенты распределены на 3 подгруппы:

1-я подгруппа - руководители предприятия;

2-я подгруппа – руководители службы информационной безопасности предприятия;

3-я подгруппа – системные администраторы.

Тема 7. «Проектирование базовой защиты периметра»

1. Деловая игра «Составление организационно-распорядительных документов по обеспечению политик сетевой безопасности на предприятиях различных форм собственности»

a.

Продолжение. Задания приведены выше

Тема 8. «Проблемы с безопасностью электронной почты. Виртуальные частные сети»

1. ***Лабораторная работа №5*** «Фильтрация трафика»

Задание:

1. Опишите текущие настройки межсетевого экрана
2. Создайте новое разрешающее правило
3. Найдите правило, разрешающее отправку ICMP пакетов, запретите отправку на конкретный адрес
4. Проверьте функционирование правил

Тема 9 «Проектирование базовой защиты Web-сервера»

1) ***Лабораторная работа №5*** «Фильтрация трафика» (продолжение)

Задание:

1. Запретите web-трафик
2. Разрешите соединение по протоколу telnet с определенного адреса
3. Активируйте ведение журнала (регистрация событий блокировки доступа)
4. Проверьте функционирование правил, регистрацию событий

Вопросы к зачету

1. Предмет и основные задачи курса.
2. Принципы проектирования информационной безопасности.
3. Использование многоуровневой системы защиты.
4. Классификация нарушителей и модель нарушителя.
5. Причины и источники появления угроз.
6. Классификация атак.
7. Виды обеспечения автоматизированных систем.
8. Основные задачи администрирования компьютерных сетей.
9. Основные средства управления Windows Server.
10. Службы каталогов Active Directory.
11. Логическая структура Active Directory.
12. Физическая структура Active Directory.
13. Учетные записи и группы учетных записей.
14. Модель безопасности рабочей группы и доменная модель безопасности.
15. Концепция и основные возможности Active Directory.
16. Основные правила именования объектов Active Directory.
17. Локальные и доменные учетные записи.
18. Понятия дерева, леса и сайта в Active Directory.
19. Структура и основные свойства учетной записи.
20. Управление группами. Локальные и доменные группы.
21. Концепция групп в Active Directory. Область действия групп и типы групп.
22. Утилиты командной строки для управление Active Directory.
23. Назначение и состав групповых политик AD.
24. Структура объекта групповых политик.

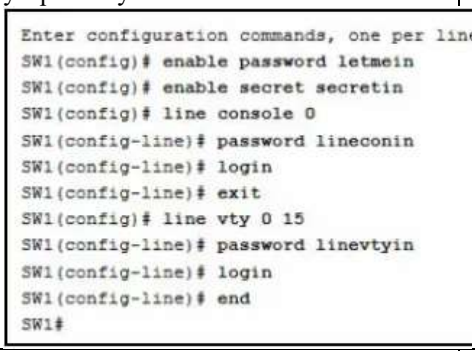
25. Порядок применения групповых политик.
26. Делегирование полномочий и операций в AD.
27. Роль и задачи аутентификации в AD.
28. Общие сведения о протоколе Kerberos.
29. Этапы регистрации клиента с использование протокола Kerberos.
30. Назначение и структура сеансового билета.
31. Протокол TLS/SSL.
32. Протокол SSH.
33. Концепция системы управления обновлениями Windows.
34. Windows Update. MBSA. WSUS. Интеграция MBSA и WSUS.
35. Назначение и структура WSUS.
36. Файловая система NTFS.
37. Файловая система EFS.
38. Протокол BitLocker Drive Encryption.
39. Технологии безопасности Windows.
40. Служба контроля учетных записей (UAC).
41. Windows BitLocker To Go и AppLocker.
42. Резервное копирование и восстановление данных. Уровни резервного копирования.
43. Полное, добавочное и дифференциальное резервирование.
44. Схемы ротации носителей при резервировании данных.
45. Структура PKI.
46. Понятие сертификата. Роль PKI в современных информационных системах.
47. Понятие стандарта X.509. Структура цифрового сертификата.
48. Использование цифровых сертификатов для обеспечения безопасности вычислительных сетей.
49. Жизненный цикл цифровых сертификатов и ключевой пары.
50. Общие сведения о службе сертификации Windows Server. Назначение центров сертификации.

Таблица 9. Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем.				
1	Задание закрытого типа	Какие два устройства являются промежуточными устройствами? 1. Хост 2. Роутер 3. Коммутатор 4. Сервер	2,3	2
2		Сопоставьте команду и режим, в котором она должна быть введена 1) Login 2) Service password-encription 3) Ip address 192.168.4.4 255.255.255.0 4) Copy running-config startup-config 5) Enable А) R1(config)# Б) R1> В) R1# Г) R1(config-line)#	1) Г 2) А 3) Д 4) В 5) Б	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		Д) R1(config-if)#		
3		Клиент создает пакет для отправки на сервер. Клиент запрашивает службу HTTPS. Какой номер будет использоваться в качестве номера порта назначения в отправляемом пакете? 1) 443 2) 161 3) 110 4) 80	1	3
4		Какой из перечисленных протоколов является протоколом маршрутизации по состоянию канала? 1) RIP 2) EIGRP 3) OSPF 4) BGP	3	3
5		Какую последовательность шагов должен содержать структурированный подход к устранению неполадок в сети?	Определите проблему. Создайте теорию возможных причин. Проверьте теорию, чтобы определить причину. Составьте план действий по решению проблемы. Проверьте полную функциональность системы и примите превентивные меры. Документируйте выводы, действия и результаты	6
6	Задание открытого типа	Три сотрудника банка пользуются корпоративной сетью. Первый сотрудник использует веб-браузер для просмотра веб-страницы компании, чтобы прочитать некоторые объявления. Второй сотрудник обращается к корпоративной базе данных для выполнения некоторых финансовых операций. Третий сотрудник участвует в важной аудиоконференции в прямом эфире с другими корпоративными менеджерами в филиалах. Если QoS будет реализовано в этой сети, каковы будут приоритеты различных типов данных (от самого высокого до самого низкого)?	Аудио-конференция (3й сотрудник), финансовая транзакция (2й сотрудник), веб-страница (1й сотрудник)	5
7		Каково назначение протокола SMTP	Позволяет клиентам отправлять электронные письма на сервер и пересылать сообщения между серверами электронной почты	3
8		В чем преимущество для небольших организаций использования IMAP вместо POP?	Сообщения хранятся на почтовых серверах до тех пор, пока не будут вручную удалены из почтового клиента.	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
9		В чем преимущество использования облачных вычислений в сети?	Возможности сети расширяются, не требуя инвестиций в новую инфраструктуру, персонал или программное обеспечение.	3
10	Задание комбинированного типа	Сетевой администратор устраняет проблемы с подключением на сервере. Используя тестер, администратор замечает, что сигналы, генерируемые сетевой картой сервера, искажены и непригодны для использования. На каком уровне модели OSI классифицируется ошибка? Опишите его назначение 1) физический, 2) канальный, 3) сетевой, 4) транспортный, 5) сеансовый, 6) представлений, 7) прикладной	Физический уровень OSI предоставляет средства для передачи битов, составляющих кадр, по сетевой среде. Этот уровень принимает полный кадр от уровня канала передачи данных и кодирует его как серию сигналов, которые передаются в локальную среду.	5
ПК-4: Способен администрировать средства защиты информации в компьютерных системах и сетях.				
11	Задание закрытого типа	Какой диапазон адресов зарезервирован для многоадресной рассылки IPv4? • 240.0.0.0 – 254.255.255.255 • 224.0.0.0 – 239.255.255.255 • 169.254.0.0 – 169.254.255.255 • 127.0.0.0 – 127.255.255.255	2	3
12		Какое из определений описывает вирус? 1) сетевое устройство, которое фильтрует доступ и трафик, поступающий в сеть 2) использование украденных учетных данных для доступа к личным данным 3) атака, которая замедляет или приводит к сбою устройства или сетевой службы 4) вредоносное программное обеспечение или код, работающий на конечном устройстве	4	2
13		В компании есть файловый сервер, который использует общую папку Public. Политика сетевой безопасности указывает, что общедоступной папке назначаются права только на чтение всем, кто может войти на сервер, а права на редактирование назначаются только группе сетевых администраторов. Какой компонент рассматривается в структуре сетевых услуг AAA? 1) Автоматизация 2) Учет 3) Аутентификация	4	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		4) Авторизация		
14		Сетевому администратору необходимо сохранять в тайне идентификатор пользователя, пароль и содержимое сеанса при установлении удаленного соединения CLI с коммутатором для управления им. Какой способ доступа выбрать? 1) Telnet 2) AUX 3) SSH 4) Console	3	3
15		Каковы два наиболее эффективных способа защиты от вредоносных программ? 1) Реализовать VPN. 2) Внедрить сетевые брандмауэры. 3) Реализовать RAID. 4) Использовать надежные пароли. 5) Обновить операционную систему и другое прикладное программное обеспечение. 6) Установить и обновить антивирусное программное обеспечение.	5,6	4
16	Задание открытого типа	Какая команда по созданию ACL позволит всем пользователям сети 192.168.10.0/24 получить доступ к веб-серверу, расположенному по адресу 172.17.80.1?	access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80	5
17		Какая команда по созданию ACL запретит всем пользователям сети 192.168.10.0/24 доступ к серверу, расположенному по адресу 172.17.80.1, по протоколу Telnet?	access-list 103 deny tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 23	5
18		На коммутаторе выполнены настройки, представленные на картинке. Какой пароль должен ввести администратор при консольном подключении к устройству  Enter configuration commands, one per lin SW1(config)# enable password letmein SW1(config)# enable secret secretin SW1(config)# line console 0 SW1(config-line)# password lineconin SW1(config-line)# login SW1(config-line)# exit SW1(config)# line vty 0 15 SW1(config-line)# password linevtyin SW1(config-line)# login SW1(config-line)# end SW1#	lineconin	8
19		Пользователь получает телефонный звонок от человека, который утверждает, что представляет ИТ-услуги, а затем запрашивает у этого пользователя подтверждение имени	Социальная инженерия	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		пользователя и пароля для целей аудита. Какую угрозу безопасности представляет этот телефонный звонок?		
20	Задание комбинированного типа	Определите адрес сети, адрес широковещательной рассылки и диапазон доступных адресов устройств для сети, которой принадлежит IP адрес 192.168.1.68/27	Адрес сети – 192.168.1.64/27 Адрес широковещательной рассылки – 192.168.1.95 Диапазон адресов устройств – 192.168.1.65-192.168.1.94	8

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Методические рекомендации по выполнению практических и контрольных работ, проведению зачета

Критерии оценки обсуждения вопросов по теме:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки.

Отчет по практической работе

Отчет по практической работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

a. тема лабораторной работы,

b. пакет документов в соответствии с темой лабораторной работы,
c. использованная литература.

Критерии оценки:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам дисциплины.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;

- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.

- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.

- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;

- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Критерии оценки деловой игры:

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине отводится 100 баллов (90 баллов на текущие формы контроля и до 10 баллов отводится на бонусы), которые накапливаются студентом в течение всего семестра изучения дисциплины.

Оценивание студентов на **зачете** осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения лабораторных и контрольной работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Критерии оценки зачета:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна

негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам дисциплины.

Таблица 10.Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	5/10	50	По расписанию
2.	*Выполнение контрольной работы*	3/8	24	
3.	*Тест*	3/2	6	
4.	*Деловая игра*	2/5	10	
Всего			**90**	-
Блок бонусов				
5.	*Посещение занятий без пропусков*	1	3	
6.	*Своевременное выполнение всех заданий*	1	3	
7.	*Активность студента на занятии*	1	4	
Всего			**10**	-
ИТОГО, зачет			**100**	-

Таблица 11. Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	незачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Защита от хакеров корпоративных сетей / Ахмад Д.М. и др. ; Пер. с англ. А.А. Петренко. - Второе издание. - М. : ДМК Пресс, 2016. - (Серия "Информационная безопасность"). - URL: http://www.studentlibrary.ru/book/ISBN5984530155.html (ЭБС «Консультант студента»).
2. Информационная безопасность открытых систем / Мельников Д.А. - М. : ФЛИНТА, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785976516137.html (ЭБС «Консультант студента»).
3. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М. : Горячая линия - Телеком, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785991203234.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература:

1. "Компьютерные сети и службы удаленного доступа / Ибе О. ; Пер. с англ. - М. : ДМК Пресс, 2007." - URL: http://www.studentlibrary.ru/book/ISBN5940740804.html (ЭБС «Консультант студента»).
2. Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. - М. : Компания АйТи; ДМК Пресс. – 2004. -288 с.: ил. - (Информационные технологии для инженеров). URL: http://www.studentlibrary.ru (ЭБС «Консультант студента»).
3. Олифер, В.Г. Сетевые операционные системы : учебник для вузов / В. Г. Олифер, Олифер, Наталья Алексеевна. - 2-е изд. - СПб. : Питер, 2009. - 669 с. - (Учеб. для вузов). - ISBN 978-5-91180-528-9 : 219-30. (10 экз.)
4. Олифер, В.Г. Сетевые операционные системы : учебник для вузов / В. Г. Олифер, Олифер, Наталья Алексеевна. - 2-е изд. - СПб. : Питер, 2006. - 539 с. - (Учеб. для вузов). (35 экз.)
5. Олифер, В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы6 учебник. – 2 изд. – СПб.:Пите5р, 2006. –958 с. (53 экз.)

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований.www.studentlibrary.ru.

2. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

Для проведения публичной защиты проектов, необходима мультимедийная аудитория с проектором.

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет и установлено программное обеспечение:

10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).