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

Р.Ю. Демина

«23» мая 2023 г.

УТВЕРЖДАЮ

И.о .заведующего кафедрой
информационной безопасности

Р.Ю. Демина

«23» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность компьютерных сетей

наименование

Составитель(-и)	**Выборнова О.Н., к.т.н, доцент кафедры информационной безопасности** **Мартьянова А.Е., к.т.н., доцент кафедры информационной безопасности**
Направление подготовки / специальность	**10.03.01 Информационная безопасность**
Направленность (профиль) ОПОП	**«Организация и технология защиты информации»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очно-заочная**
Год приема	**2023**
Курс	**5**
Семестр	**9**

Астрахань – 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели освоения дисциплины «Безопасность компьютерных сетей»: 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 «Безопасность компьютерных сетей» относится к вариативной части (элективные дисциплины) учебного плана направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации» 2023 года набора, изучается в девятом семестре пятого курса, обучение длится один семестр.

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

- Информатика;
- Безопасность информационных технологий и систем;
- Техническая защита информации.
- 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 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; методикой и техникой составления различных управленческих и документов учреждений, организаций и предприятий

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

Дисциплина «Безопасность компьютерных сетей» поможет студентам при реализации задач преддипломной практики и написании бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

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

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 и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	**Уметь (2)**	**Владеть (3)**
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-1.1. Знать: 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	ПК-1.2. Уметь: 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	ПК-1.3. Владеть: методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа
ПК-4. Способен администрировать средства защиты информации в компьютерных	ПК-4.1. Знать: источники угроз информационной безопасности в компьютерных сетях и меры по их	ПК-4.2. Уметь: анализировать угрозы безопасности информации в компьютерных системах и сетях;	ПК-4.3. Владеть: навыками управления средствами межсетевого экранирования в

системах и сетях	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	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	компьютерных сетях методикой оценки оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) в зачетных единицах 2 **зачетные единицы**. Всего 72 часа: 27 часов выделено на контактную работу обучающихся с преподавателем (лекции – 9, лабораторные работы – 18), 45 часов – на самостоятельную работу обучающихся:

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	**Тема 1.** Правовые требования к информационной безопасности предприятия. Анализ существующих политик и мер безопасности. Построение модели нарушителя и анализ угроз и рисков для	6	1-2	1		2		5	Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете

	администрирования ИТ-инфраструктуры предприятия								
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		3-4	1		2		5	Контрольная работа №1 Лабораторная работа №2 Промежуточное тестирование Опрос на зачете
3	**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)		5-6	1		2		5	Отчет по лабораторной работе №2 Контрольная работа №2 Опрос на зачете
4	**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		7-8	1		2		5	Отчет по лабораторной работе №3 Опрос на зачете
5	**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		9-10	1		2		5	Контрольная работа №3 Отчет по лабораторной работе №4 Опрос на зачете
6	**Тема 6.** Проектирование защиты для серверных ролей. Внедрение защиты серверных ролей при помощи оснастки. Планирование и		11-12	1		2		5	Промежуточное тестирование Деловая игра Опрос на зачете

	реализация защищенной базовой конфигурации для клиентских компьютеров								
7	**Тема 7.** Проектирование базовой защиты периметра		13-14	1		2		5	Деловая игра. Опрос на зачете
8	**Тема 8.** Проблемы с безопасностью электронной почты. Виртуальные частные сети		15-16	1		2		5	Лабораторная работа №5 Опрос на зачете
9	**Тема 9.** Проектирование базовой защиты Web-сервера		17	1		2		5	Отчет по лабораторной работе №5 Опрос на зачете
	ИТОГО			**9**		**18**		**45**	зачет

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых в них компетенций

Темы, разделы дисциплины	Кол-во часов	Компетенции		Общее кол-во 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.	8	+	+	2

Темы, разделы дисциплины	Кол-во часов	Компетенции		Общее кол-во компетенций
		ПК 1	ПК 4	
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	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 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)

При подготовке к лекционным и лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8 Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPoint.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	Входное тестирование Отчет по лабораторной работе №1 Опрос на зачете	5	Внеаудиторная, участие студентов в составлении тестов
2	Контрольная работа №1 Лабораторная работа №2 Промежуточное тестирование Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
3	Отчет по лабораторной работе №2 Контрольная работа №2 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
4	Лабораторная работа №3 Отчет по лабораторной работе №3 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
5	Контрольная работа №3 Лабораторная работа №4 Отчет по лабораторной работе №4 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
6	Промежуточное тестирование Деловая игра Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
7	Деловая игра. Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
8	Лабораторная работа №5 Опрос на зачете	5	Внеаудиторная, изучение учебных пособий
9	Отчет по лабораторной работе №5 Опрос на экзамене	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

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная 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 лабораторной 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	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, выполнение контрольной работы

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	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	Подготовка к деловой игре
Тема 8. Проблемы с безопасностью электронной почты. Виртуальные частные сети	Лекция - презентация	Не предусмотрено	Выполнение лабораторной работы
Тема 9. Проектирование базовой защиты Web-сервера	Лекция - презентация	Не предусмотрено	Выполнение лабораторной работы

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.

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

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 электронных учебников и различных сайтов как источник информации	1 - 9	Подготовка к защите отчетов по лабораторным работам
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 сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов 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 (LMS Moodle «Цифровое обучение») 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
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional, Microsoft Windows Server	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
VirtualBox	Программный продукт виртуализации операционных систем

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. 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

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1.	**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
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	ПК-1, ПК-4	Контрольная работа №1 Лабораторная работа №2 Промежуточное тестирование Опрос на зачете
3.	**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

4.	**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
5.	**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
6.	**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
7.	**Тема 7.** Проектирование базовой защиты периметра	ПК-1, ПК-4	Деловая игра Опрос на зачете
8.	**Тема 8.** Проблемы с безопасностью электронной почты. Виртуальные частные сети	ПК-1, ПК-4	Лабораторная работа №5 Опрос на зачете
9.	**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

Для оценки результатов обучения применяются следующие критерии:

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
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, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

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

Тема 1 «Правовые требования к информационной безопасности предприятия. 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. Администрирование пользователей и компьютеров.»

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. 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?

1. ***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 Windows Server 2003. Требования к учетным записям пользователей.»

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.»

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. 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. Основные возможности программного брандмауэра ISA Server»

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

Продолжение. Задания приведены выше

Тема 8 «Проблемы с безопасностью электронной почты. Настройка ISA Server для защиты передачи данных по протоколу SMTP»

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»***

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 экзамену

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 и Windows 8.
40. Служба контроля учетных записей (UAC). Реализация UAC в Windows 7.
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 типа трафика используют Real-Time Transport Protocol (RTP)? 1) Видео 2) Веб 3) Передача файлов 4) Голос 5) Peer to peer	2, 4	2
2.		Какая беспроводная технология требует малой мощности и скорости передачи данных, что делает ее популярной в приложениях «умного дома»? 1) ZigBee 2) LoRaWAN 3) 5G 4) Wi-Fi	1	2
3.		Клиент получает пакет от сервера. В пакете указан порт назначения 110. Какому сервису предназначен пакет? 1) DNS 2) DHCP 3) SMTP 4) POP3	4	3
4.		Проводной лазерный принтер подключен к домашнему компьютеру. Этот принтер является общим, поэтому другие компьютеры в домашней сети также могут использовать этот принтер. Какая сетевая модель используется? 1) Client-based 2) Master-slave 3) Point-to-point 4) Peer-to-peer	4	3
5.		Какой сервис обеспечивает интернет месенджер? 1) Позволяет общаться удаленным пользователям в режиме реального времени. 2) Обеспечивает удаленный доступ к сетевым устройствам и серверам. 3) Преобразует доменные имена, такие как cisco.com, в IP-адреса. 4) Использует шифрование для обеспечения безопасного удаленного доступа к сетевым устройствам и серверам.	1	2
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

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
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
9.		В чем преимущество использования облачных вычислений в сети?	Возможности сети расширяются, не требуя инвестиций в новую инфраструктуру, персонал или программное обеспечение.	3
10.		Опишите назначение физического уровня модели OSI	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.	3
ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях				
11.	Задание закрытого типа	Администратор сети добавляет новую сеть в филиал организации. Она должна обеспечивать подключение 61 устройства. Какую наименьшую маску администратор может использовать для новой сети? 1) 255.255.255.240 2) 255.255.255.224 3) 255.255.255.192 4) 255.255.255.128	3	5
12.		Какие три требования определяются протоколами, используемыми в сетевых коммуникациях, чтобы разрешить передачу сообщений по сети? 1) Размер сообщения 2) Кодирование сообщения 3) Технические характеристики разъема 4) Выбор среды передачи данных 5) Варианты доставки 6) Установленное оконечное устройство	1, 2, 5	4
13.		Каковы две основные функции подуровня MAC Ethernet? 1) обнаружение ошибок 2) разграничение кадра 3) доступ к среде 4) инкапсуляция данных 5) логическая адресация	3,4	3
14.		Пользователи сообщают о более длительных задержках аутентификации и доступа к сетевым ресурсам в определенные периоды недели. Какую информацию должны проверить сетевые инженеры, чтобы выяснить, является ли эта ситуация частью нормального поведения сети? 1) записи и сообщения системного журнала 2) базовый уровень производительности сети 3) вывод отладки и захват пакетов 4) файлы конфигурации сети	2	3
15.		Клиентский пакет принимается сервером. Пакет имеет номер порта назначения 21. Какой сервис запрашивает клиент?	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		1) FTP 2) LDAP 3) SLP 4) SNMP		
16.	Задание открытого типа	Дайте описание топологии расширенная звезда	Оконечные устройства подключаются к центральному промежуточному устройству, которое, в свою очередь, подключается к другим центральным промежуточным устройствам.	3
17.		Какие основные функции NVRAM коммутатора cisco?	Содержимое сохраняется после отключения питания. Хранится файл стартовой конфигурации	3
18.		Что такое окно TCP?	Окно — это количество байтов, которые отправитель отправит, прежде чем ожидать подтверждения от целевого устройства. Начальное окно согласовывается во время запуска сеанса через трехстороннее рукопожатие между источником и получателем. Он определяется тем, сколько данных целевое устройство сеанса TCP может принять и обработать за один раз.	4
19.		Опишите процесс трехстороннего рукопожатия TCP	Клиент отправляет сообщение SYN. Сервер отвечает – SYN, ACK. Клиент отправляет ACK	3
20.		Охарактеризуйте протокол UDP	UDP — это простой протокол, обеспечивающий основные функции транспортного уровня. У него намного меньше накладных расходов, чем у TCP, потому что он не ориентирован на соединение и не предлагает сложных механизмов повторной передачи, упорядочения и управления потоком, которые обеспечивают надежность.	4

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)

Фонды оценочных средств по дисциплине

Фонд оценочных средств позволяет оценить знания, умения и уровень приобретенных компетенций.

Фонд оценочных средств по дисциплине включает:

- вопросы к зачету;
- набор вариантов контрольных работ и тестов;
- комплект заданий и контрольных вопросов к лабораторным работам.

Оценка качества освоения программы дисциплины включает текущий контроль успеваемости, промежуточную аттестацию, итоговую аттестацию.

Отчет по лабораторной работе

Отчет по лабораторной 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:

- небрежное выполнение,
- отсутствие выводов,
- нарушение сроков предоставления отчета.

Отчет не может быть принят и подлежит доработке в случае:

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

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 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.

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 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 делопроизводства.

В соответствии с балльно-рейтинговой системой БАРСпо 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 самостоятельных и тематических контрольных 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.

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	В соответствии с таблицей 2
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*		3	
6.	*Своевременное выполнение всех заданий*		3	
7.	*Активность студента на занятии*		4	
Всего			**10**	-
ИТОГО			**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)	
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	

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.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

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. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).