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)

«Аудит информационной безопасности»

Составитель(и)	**Демина Р.Ю., к.т.н., доц., доцент;**
Согласовано с работодателями:	**Горбатенко С.Ю., заместитель директора ГБУ АО «Инфраструктурный центр электронного правительства»; Лазарев Н.В., инженер 2 категории группы контроля безопасности объектов критической информационной безопасности управления корпоративной защиты ООО «Газпром добыча Астрахань»;**
Направление подготовки / специальность	**10.03.01 Информационная безопасность**
Направленность (профиль) / специализация ОПОП	**«Организация и технология защиты информации»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная, очно-заочная**
Год приёма	**2025**
Курс	**3 (по очной форме)** **4 / (по очно-заочной форме) /**
Семестр(ы)	**6 (по очной форме) /** **8 (по очно-заочной форме) /**

Астрахань – 2025

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) «Аудит информационной безопасности» являются

– изучение теоретических вопросов, основных понятий, определений и категорий, используемых в данной дисциплине, формирование базовых навыков по их применению;

– формирование базовых знаний по основам построения систем информационной безопасности;

– изучение нормативной базы аудита информационной безопасности объектов;

– ознакомление с перечнем основных стандартов, применяемых в области информационной безопасности;

– изучение методики проведения аудита информационной безопасности объектов;

– ознакомление с лицензированием и сертификацией деятельности в области защиты информации;

– применение полученных знаний на практике для проведения аудита информационной безопасности объектов.

1.2. Задачи освоения дисциплины (модуля):

– Изучить основные понятия, термины, определения в сфере аудита информационной безопасности; задачи, функции, структуру, практику проведения аудитов информационной безопасности на предприятии; организационные основы, принципы, методы и технологии управления подразделением аудита информационной безопасности; психологические аспекты подготовки аудитора информационной безопасности;

– Сформировать умения разрабатывать программу аудиторских проверок, план аудита и аудиторский отчёт и использовать методы и передовой опыт проведения аудиторских проверок в сфере информационной безопасности; определить место аудита информационной безопасности в структуре организации и структуре управления информационной безопасностью; определить методы оценки систем обеспечения информационной безопасности, критерии аудита, инструменты проведения аудита, принципы организации труда аудитора, сформировать взгляд на организацию и управление службой защиты информации на предприятии как на систематическую практическую деятельность коллегиальных органов управления предприятия и руководителя службы, направленную на разработку концептуальных и организационных основ ее деятельности и эффективное выполнение возложенных на нее задач.

Сформировать навыки использования методов проведения аудиторских проверок и обработке результатов аудита; проведения аудитов информационной безопасности в системе защиты информации на предприятии.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Аудит информационной безопасности» относится к части, формируемой участниками образовательных отношений и осваивается в 6 семестре при очной форме обучения и в 8семестре при очно-заочной форме обучения.

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

- Информатика.
- Организационное и правовое обеспечение информационной безопасности.

  Знания:
  - основные понятия информатики,
  - структуры систем документационного обеспечения.

Умения:

- использовать программные и аппаратные средства персонального компьютера,
- пользоваться нормативными документами по защите информации.

Навыки:

- поиска информации в глобальной информационной сети Интернет
- работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): методика и техника 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):

- Программно-аппаратные средства защиты информации.
- Проектирование и эксплуатация защищенных информационных систем.
- Комплексное обеспечение защиты информации объекта информатизации.

Также дисциплина «Аудит информационной безопасности» поможет студентам при реализации задач преддипломной практики и написанию бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующей(их) компетенции(ий) в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки / специальности:

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 5 - Способен администрировать средства защиты информации в компьютерных системах и сетях.

Таблица 1. Декомпозиция результатов обучения

Код компетенции	Код и наименование индикатора достижения компетенции[1]	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
ПК-1	ПК-1.1	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	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	методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа

[1] Указываются в соответствии с утвержденными в ОПОП ВО

Код компетенции	Код и наименование индикатора достижения компетенции[1]	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
		от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	методы и средства защиты информации в автоматизированных системах	
ПК-5	ПК-5.1	источники угроз 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	анализировать 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,	навыками управления 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 3 зачетные единицы (108 часов).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной и заочной форм 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
Объем дисциплины в зачетных единицах	3	3
Объем дисциплины в академических часах	108	108
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):		
- занятия лекционного типа, в том числе:	17	15
- практическая подготовка (если предусмотрена)	0	0
- занятия семинарского типа (семинары, практические, лабораторные), в том числе:	51	15
- практическая подготовка (если предусмотрена)	0	0
- консультация (предэкзаменационная)[2]	1	1
- промежуточная аттестация по дисциплине[3]	0,25	0,25
Самостоятельная работа обучающихся (час.)	38,75	76,75
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	экзамен – 6 семестр	экзамен – 8 семестр

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено 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 *[по семестрам]*
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Семестр 1.										
Основы построения систем обеспечения ИБ на предприятии.	1	0	0	0	4	0	0	4	9	Отчет по лабораторной работе 1.
Аудит ИБ. Основные понятия, термины и определения.	1	0	0	0	4	0	0	4	9	Отчет по лабораторной работе 2.
Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	1	0	0	0	4	0	0	4	9	Контрольная работа №1
Критерии аудита информационной безопасности.	1	0	0	0	4	0	0	4	9	Отчет по лабораторной работе 3.

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

[3] 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 *[по семестрам]*
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Национальные стандарты управления информационной безопасностью.										
Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	1	0	0	0	4	0	0	4	9	Отчет по лабораторной работе 4.
Методы оценки безопасности информационных технологий.	2	0	0	0	6	0	0	4	12	Контрольная работа №2
Инструменты проведения аудита информационной безопасности.	2	0	0	0	6	0	0	4	12	Отчет по лабораторной работе 5.
Методика проведения аудита информационной безопасности.	2	0	0	0	7	0	0	4	13	Отчет по лабораторной работе 6.
Организация внутреннего аудита на предприятии.	3	0	0	0	6	0	0	3	12	Контрольная работа №3
Психологические аспекты подготовки аудитора информационной безопасности.	3	0	0	0	6	0	0	3,75	12,75	Итоговое тестирование
Консультации									***1***	
Контроль промежуточной аттестации									**0,25**	**Экзамен**
ИТОГО за семестр:	***17***	***0***	***0***	***0***	***51***	***0***	***0***	***38,75***	***108***	
Итого за весь период	***17***	***0***	***0***	***0***	***51***	***0***	***0***	***38,75***	***108***	

для очно-заочной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации *[по семестрам]*
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Семестр 1.										
Основы построения систем обеспечения ИБ на предприятии.	1	0	0	0	1	0	0	7	9	Отчет по лабораторной работе 1.

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации *[по семестрам]*
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Аудит ИБ. Основные понятия, термины и определения.	1	0	0	0	1	0	0	7	9	Отчет по лабораторной работе 2.
Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	1	0	0	0	1	0	0	7	9	Контрольная работа №1
Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	1	0	0	0	1	0	0	7	9	Отчет по лабораторной работе 3.
Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	1	0	0	0	1	0	0	7	9	Отчет по лабораторной работе 4.
Методы оценки безопасности информационных технологий.	2	0	0	0	2	0	0	8	12	Контрольная работа №2
Инструменты проведения аудита информационной безопасности.	2	0	0	0	2	0	0	8	12	Отчет по лабораторной работе 5.
Методика проведения аудита информационной безопасности.	2	0	0	0	2	0	0	9	13	Отчет по лабораторной работе 6.
Организация внутреннего аудита на предприятии.	2	0	0	0	2	0	0	8	12	Контрольная работа №3
Психологические аспекты подготовки аудитора информационной безопасности.	2	0	0	0	2	0	0	8,75	12,75	Итоговое тестирование
Консультации									***1***	
Контроль промежуточной аттестации									**0,25**	**Экзамен**
ИТОГО за семестр:	***15***	***0***	***0***	***0***	***15***	***0***	***0***	***76,75***	***108***	
Итого за весь период	***15***	***0***	***0***	***0***	***15***	***0***	***0***	***76,75***	***108***	

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

Таблица 3. Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции		Общее количество компетенций
		ПК-1	ПК-5	
Основы построения систем обеспечения ИБ на предприятии.	9	+	+	2
Аудит ИБ. Основные понятия, термины и определения.	9	+	+	2
Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	9	+	+	2
Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	9	+	+	2
Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	9	+	+	2
Методы оценки безопасности информационных технологий.	12	+	+	2
Инструменты проведения аудита информационной безопасности.	12	+	+	2
Методика проведения аудита информационной безопасности.	13	+	+	2
Организация внутреннего аудита на предприятии.	12	+	+	2
Психологические аспекты подготовки аудитора информационной безопасности.	12,75	+	+	2
Итого	**106,75**			

Краткое содержание каждой темы дисциплины (модуля)

Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии

Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.

Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения

Понятие «аудит информационной безопасности». Понятие «критерий аудита информационной безопасности». Аудитор информационной безопасности. Понятие «свидетельство аудита информационной безопасности». Результаты аудита информационной безопасности. Стороны

проведения аудита – «заказчик» и «исполнитель» аудита. Виды аудитов информационной безопасности. Планирование аудита информационной безопасности. Понятия «соответствие» и «несоответствие» критериям аудита информационной безопасности. Программа аудита информационной безопасности. Риски аудита информационной безопасности. Понятие «компетентность аудитора».

Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.

Анализ влияния угроз информационной безопасности на основные виды деятельности организации. Процессный анализ системы управления информационной безопасностью. Анализ рисков информационной безопасности. Анализ ценности и стоимости информационных активов организации. Анализ документов и записей системы управления информационной безопасностью. Анализ архитектуры информационных систем и средств защиты информации. Анализ политик лицензирования автоматизированных и информационных систем. Анализ соответствия ФЗ и требованиям регулирующих органов. Анализ экономических аспектов обеспечения информационной безопасности.

Тема 4.Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.

Стандарты по обеспечению безопасности информационных технологий в России. Гармонизированные стандарты по обеспечению информационной безопасности. Практика оценки соответствия организаций национальным стандартам. Отраслевые стандарты по обеспечению информационной безопасности. Особенности оценки соответствия организаций требования ФЗ РФ и регулятивным требованиям.

Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.

Международные стандарты по обеспечению информационной безопасности. OPSEC – концепция системного подхода к обеспечению защиты конфиденциальной информации. Модели непрерывного совершенствования и корпоративное управление. Компоненты структуры управления рисками ISO 31000. Модель корпоративного управления информационными технологиями ISO/IEC 38500. Семейство стандартов системы управления информационной безопасностью. Понятие «интегрированная система управления», особенность проведения аудитов информационной безопасности интегрированных систем управления. Особенности формирования групп контролей состояния информационной безопасности в финансовых организациях.

Тема 6. Методы оценки безопасности информационных технологий.

Предпосылки введения международного стандарта ISO 15408 «Общие критерии». Основные понятия ISO 15408. Методология оценки безопасности информационных технологий на соответствие ISO 15408. Понятие «уровень доверия». Оценка уровня доверия функциональной безопасности информационной технологии. Классы и семейства ISO 15408. Понятие «Профиль защиты».

Тема 7. Инструменты проведения аудита информационной безопасности.

Анализ видов инструментов для проведения аудитов информационной безопасности. Метод CRAMM. Сканирование уязвимостей автоматизированных и информационных систем. Нагрузочное тестирование и тестирование на устойчивость автоматизированных систем. Анализ уязвимостей CRM и ERP систем. Особенности проведения аудитов информационной безопасности объектов обработки конфиденциальной информации с использованием технических средств.

Тема 8. Методика проведения аудита информационной безопасности.

Понятие «наблюдение» в процессе проведения аудита информационной безопасности. Понятие «свидетельство» аудита информационной безопасности. Методы «выборки» и организация выборочных проверок. Понятие «прослеживаемость процесса» в практике оценки систем управления информационной безопасностью. Анализ метрик информационной безопасности. Анализ корпоративного управления информационной безопасностью. Подготовка и практика

интервьюирования. Методы анализа структур документации и записей системы обеспечения информационной безопасности. «Несоответствие» и методы обработки несоответствий.

Тема 9. Организация внутреннего аудита на предприятии.

Структура подразделения внутреннего аудита. Виды аудитов информационной безопасности. Управление программой аудита информационной безопасности. Типичные виды деятельности при проведении аудита информационной безопасности. Процесс сбора и верификации аудиторской информации. Аудиторский отчёт. Правила согласования аудиторского отчёта. Контроль за деятельностью аудиторов информационной безопасности.

Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.

Профессиональный и нравственно-этический уровень аудитора информационной безопасности. Понятие «Объективная оценка». Понятие «Независимость аудитора». Практика межличностного общения. Материальное вознаграждение. Аудиторский риск. Понятие «Психологический контракт». Принадлежность к профессиональным сообществам. Воздействие на результаты оценки. Профессиональное развитие аудитора информационной безопасности.

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

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

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

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:

- 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:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

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.

Экзамен

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

Оценивание студентов на экзамене 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 экзамена.

На учебном файловом сервере АГУ (fsever) размещены задания для лабораторной и самостоятельной работы студентов, тесты, а также лекционный материал.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Таблица 4. Содержание самостоятельной работы обучающихся

для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Преступления в сфере компьютерной информации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»	4	Отчет по лабораторной работе 1.
Использование поисковиков для сбора информации	4	Отчет по лабораторной работе 2.
Сканирование сети. Получение начальной информации о структуре ЛВС	4	Контрольная работа №1
Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	4	Отчет по лабораторной работе 3.
Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения»	4	Отчет по лабораторной работе 4.
Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»	4	Контрольная работа №2
Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»	4	Отчет по лабораторной работе 5.
ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»	4	Отчет по лабораторной работе 6.
ГОСТ ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий»	3	Контрольная работа №3
ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа	3,75	Итоговое тестирование

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
к информации. Общие технические требования»		

для очно-заочной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Преступления в сфере компьютерной информации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»	7	Отчет по лабораторной работе 1.
Использование поисковиков для сбора информации	7	Отчет по лабораторной работе 2.
Сканирование сети. Получение начальной информации о структуре ЛВС	7	Контрольная работа №1
Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	7	Отчет по лабораторной работе 3.
Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения»	7	Отчет по лабораторной работе 4.
Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»	8	Контрольная работа №2
Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»	8	Отчет по лабораторной работе 5.
ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»	9	Отчет по лабораторной работе 6.
ГОСТ ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий»	8	Контрольная работа №3
ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»	8,75	Итоговое тестирование

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

Лабораторные работы. Для подготовки необходимо изучить теоретический материал по соответствующей теме и разработать программное обеспечение на любом языке программирования. Отчет должен быть представлен в печатном виде и включать в себя описание алгоритма, скриншоты разработанных интерфейсов. При сдаче необходимо продемонстрировать корректно работающее программное обеспечение.

Контрольные работы. Для подготовки к контрольной работе необходимо изучить теоретический материал по соответствующей теме. При написании контрольной работы необходимо развернуто

ответить на вопросы, дать аргументированный ответ, привести примеры, подтверждающие точку зрения.

Тестирование. Для подготовки к тестированию необходимо изучить теоретический материал по соответствующей теме. При написании теста необходимо выбрать правильный вариант ответа из предложенных.

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
Основы построения систем обеспечения ИБ на предприятии.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Аудит ИБ. Основные понятия, термины и определения.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	Лекция - презентация	Не предусмотрено	выполнение контрольной работы
Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Методы оценки безопасности информационных технологий.	Лекция - презентация	Не предусмотрено	выполнение контрольной работы
Инструменты проведения аудита информационной безопасности.	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Методика проведения аудита информационной безопасности.	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Организация внутреннего аудита на предприятии.	Лекция - презентация	Не предусмотрено	выполнение контрольной работы

Психологические аспекты подготовки аудитора информационной безопасности.	Лекция - презентация	Не предусмотрено	выполнение теста

6.2. 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 «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

В соответствии с ОПОП дисциплина должна быть поддержана соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

MS Visual Studio	Среда разработки программ для ЭВМ

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. Научная электронная библиотека eLIBRARY.ru ООО «РУНЭБ» http://elibrary.ru
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС» http://dlib.eastview.com/

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) «Аудит информационной безопасности» 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

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Основы построения систем обеспечения ИБ на предприятии.	ПК-1, ПК-5	Отчет по лабораторной работе 1.
Аудит ИБ. Основные понятия, термины и определения.	ПК-1, ПК-5	Отчет по лабораторной работе 2.
Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	ПК-1, ПК-5	Контрольная работа №1
Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	ПК-1, ПК-5	Отчет по лабораторной работе 3.
Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	ПК-1, ПК-5	Отчет по лабораторной работе 4.
Методы оценки безопасности информационных технологий.	ПК-1, ПК-5	Контрольная работа №2
Инструменты проведения аудита информационной безопасности.	ПК-1, ПК-5	Отчет по лабораторной работе 5.

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Методика проведения аудита информационной безопасности.	ПК-1, ПК-5	Отчет по лабораторной работе 6.
Организация внутреннего аудита на предприятии.	ПК-1, ПК-5	Контрольная работа №3
Психологические аспекты подготовки аудитора информационной безопасности.	ПК-1, ПК-5	Итоговое тестирование

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

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, 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 и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1. Основы построения систем обеспечения ИБ на предприятии.

Лабораторно-практическая работа 1. Command Execution

Цель: Познакомиться с уязвимостью командной строки на веб-сервисах, научиться эксплуатировать данную уязвимость.

Задание:

- скопировать файл /etc/passwd в любую директорию используя данную уязвимость,

- предложить средства защиты от данной уязвимости.

Тема 2. Аудит ИБ. Основные понятия, термины и определения.

Лабораторно-практическая работа 2. Взлом WEB-форм с использованием Tamper Data и crack_web_form.pl.

Цель: Познакомиться с функционалом Tamper Data. Научиться взламывать WEB-формы с помощью crack_web_form.pl.

Задание: изучите принцип эксплуатации уязвимости и применение программного обеспечения crack_web_form.pl.

Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.

Вопросы к контрольной работе № 1

1. Деятельность по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности.
2. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности.
3. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.
4. Понятие «аудит информационной безопасности». Понятие «критерий аудита информационной безопасности».
5. Аудитор информационной безопасности. Понятие «свидетельство аудита информационной безопасности».
6. Результаты аудита информационной безопасности. Стороны проведения аудита – «заказчик» и «исполнитель» аудита.
7. Виды аудитов информационной безопасности.
8. Планирование аудита информационной безопасности. Понятия «соответствие» и «несоответствие» критериям аудита информационной безопасности.
9. Программа аудита информационной безопасности.
10. Риски аудита информационной безопасности. Понятие «компетентность аудитора».
11. Анализ влияния угроз информационной безопасности на основные виды деятельности организации.
12. Процессный анализ системы управления информационной безопасностью. Анализ рисков информационной безопасности.
13. Анализ ценности и стоимости информационных активов организации. Анализ документов и записей системы управления информационной безопасностью.

14. Анализ архитектуры информационных систем и средств защиты информации. Анализ политик лицензирования автоматизированных и информационных систем.

15. Анализ соответствия ФЗ и требованиям регулирующих органов. Анализ экономических аспектов обеспечения информационной безопасности.

Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.

Лабораторно-практическая работа 3. Manual SQL Injection, John the Ripper.

Цель: Научиться проводить SQL-инъекции, понять базовые принципы проведения SQL-инъекций, освоить программу John the Ripper.

Задание: самостоятельно изучить работу программы John the Ripper восстановить пароли по его хэшу.

Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.

Лабораторно-практическая работа 4. SQLMAP.

Цель: Познакомиться с SQLMAP, изучить базовые возможности SQLMAP, научиться автоматизировать процесс SQL-инъекций.

Задание: самостоятельно изучить работу программы SQLMAP и получить доступ к тестовой базе данных.

Тема 6. Методы оценки безопасности информационных технологий.

Вопросы к контрольной работе № 2

1. Стандарты по обеспечению безопасности информационных технологий в России.
2. Гармонизированные стандарты по обеспечению информационной безопасности.
3. Практика оценки соответствия организаций национальным стандартам.
4. Отраслевые стандарты по обеспечению информационной безопасности. Особенности оценки соответствия организаций требования ФЗ РФ и регулятивным требованиям.
5. Международные стандарты по обеспечению информационной безопасности.
6. OPSEC – концепция системного подхода к обеспечению защиты конфиденциальной информации.
7. Модели непрерывного совершенствования и корпоративное управление. Компоненты структуры управления рисками ISO 31000.
8. Модель корпоративного управления информационными технологиями ISO/IEC 38500. Семейство стандартов системы управления информационной безопасностью.
9. Понятие «интегрированная система управления», особенность проведения аудитов информационной безопасности интегрированных систем управления.
10. Особенности формирования групп контролей состояния информационной безопасности в финансовых организациях.
11. Предпосылки введения международного стандарта ISO 15408 «Общие критерии». Основные понятия ISO 15408.
12. Методология оценки безопасности информационных технологий на соответствие ISO 15408. Понятие «уровень доверия».

13. Оценка уровня доверия функциональной безопасности информационной технологии. Классы и семейства ISO 15408. Понятие «Профиль защиты».

Тема 7. Инструменты проведения аудита информационной безопасности.

Лабораторно-практическая работа 5. 'union exploit, create_user.php, John The Ripper.

Цель: Научиться проводить SQL-инъекции с помощью команды union, понять базовые принципы таких атак.

Задание:

- Разобраться в скрипте создания нового пользователя,

- Восстановить пароли из хэша с помощью John the Ripper

- Предложить средства защиты от SQL-инъекций.

Тема 8. Методика проведения аудита информационной безопасности.

Лабораторно-практическая работа 6. CSRF.

Цель: Познакомиться с CSRF атаками, понять принцип их работы, научиться проводить CSRF атаки, узнать способы защиты от CSRF атак.

Задание:

- написать свою альтернативу фейковой страницы,

- рассказать про способы защиты от CSRF атак.

Тема 9. Организация внутреннего аудита на предприятии.

Вопросы к контрольной работе №3

1. Анализ видов инструментов для проведения аудитов информационной безопасности. Метод CRAMM.
2. Сканирование уязвимостей автоматизированных и информационных систем. Нагрузочное тестирование и тестирование на устойчивость автоматизированных систем.
3. Анализ уязвимостей CRM и ERP систем. Особенности проведения аудитов информационной безопасности объектов обработки конфиденциальной информации с использованием технических средств.
4. Понятие «наблюдение» в процессе проведения аудита информационной безопасности. Понятие «свидетельство» аудита информационной безопасности.
5. Методы «выборки» и организация выборочных проверок. Понятие «прослеживаемость процесса» в практике оценки систем управления информационной безопасностью.
6. Анализ метрик информационной безопасности. Анализ корпоративного управления информационной безопасностью.
7. Подготовка и практика интервьюирования. Методы анализа структур документации и записей системы обеспечения информационной безопасности.
8. «Несоответствие» и методы обработки несоответствий.
9. Структура подразделения внутреннего аудита. Виды аудитов информационной безопасности.

10. Управление программой аудита информационной безопасности. Типичные виды деятельности при проведении аудита информационной безопасности.
11. Процесс сбора и верификации аудиторской информации. Аудиторский отчёт.
12. Правила согласования аудиторского отчёта. Контроль за деятельностью аудиторов информационной безопасности.
13. Профессиональный и нравственно-этический уровень аудитора информационной безопасности.
14. Понятие «Объективная оценка». Понятие «Независимость аудитора».
15. Практика межличностного общения. Материальное вознаграждение. Аудиторский риск.
16. Понятие «Психологический контракт». Принадлежность к профессиональным сообществам.
17. Воздействие аудитора на результаты оценки. Профессиональное развитие аудитора информационной безопасности.

Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.

Вопросы итогового теста

1. Перечислите основные виды аудита информационной безопасности:
   - экспертный аудит безопасности;
   - оценка соответствия рекомендациям международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии);
   - инструментальный анализ защищенности ИС;
   - комплексный аудит,
   - функциональный аудит,
   - композиционный аудит.
2. Расставьте в правильной последовательности этапы проведения аудита ИБ:
   - Разработка регламента проведения аудита
   - Сбор исходных данных
   - Анализ полученных данных с целью оценки текущего уровня безопасности
   - Разработка рекомендаций по повышению уровня защищенности ИС.
3. Сочетание вероятности события и его последствий
   - Риск
   - Атака
   - Актив
   - Угроза
4. Возможная причина нежелательного инцидента, который может нанести ущерба системе или организации
   - Атака
   - Анализ
   - Угроза
   - Воздействие
5. Напишите основную задачу регламента ИБ _____.
6. Дайте определение аудита информационной безопасности _____.

Перечень вопросов к экзамену

1. Деятельность по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности.

2. Принципы и форма деятельности по обеспечению информационной безопасности.
3. Методы деятельности по обеспечению информационной безопасности.
4. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.
5. Понятие «аудит информационной безопасности».
6. Понятие «критерий аудита информационной безопасности».
7. Аудитор информационной безопасности.
8. Понятие «свидетельство аудита информационной безопасности».
9. Результаты аудита информационной безопасности. Стороны проведения аудита – «заказчик» и «исполнитель» аудита.
10. Виды аудитов информационной безопасности.
11. Планирование аудита информационной безопасности. Понятия «соответствие» и «несоответствие» критериям аудита информационной безопасности.
12. Программа аудита информационной безопасности.
13. Риски аудита информационной безопасности. Понятие «компетентность аудитора».
14. Анализ влияния угроз информационной безопасности на основные виды деятельности организации.
15. Процессный анализ системы управления информационной безопасностью.
16. Анализ рисков информационной безопасности.
17. Анализ ценности и стоимости информационных активов организации.
18. Анализ документов и записей системы управления информационной безопасностью.
19. Анализ архитектуры информационных систем и средств защиты информации. Анализ политик лицензирования автоматизированных и информационных систем.
20. Анализ соответствия ФЗ и требованиям регулирующих органов. Анализ экономических аспектов обеспечения информационной безопасности.
21. Стандарты по обеспечению безопасности информационных технологий в России.
22. Гармонизированные стандарты по обеспечению информационной безопасности.
23. Практика оценки соответствия организаций национальным стандартам.
24. Отраслевые стандарты по обеспечению информационной безопасности.
25. Особенности оценки соответствия организаций требования ФЗ РФ и регулятивным требованиям.
26. Международные стандарты по обеспечению информационной безопасности.
27. OPSEC – концепция системного подхода к обеспечению защиты конфиденциальной информации.
28. Модели непрерывного совершенствования и корпоративное управление. Компоненты структуры управления рисками ISO 31000.
29. Модель корпоративного управления информационными технологиями ISO/IEC 38500. Семейство стандартов системы управления информационной безопасностью.
30. Понятие «интегрированная система управления», особенность проведения аудитов информационной безопасности интегрированных систем управления.
31. Особенности формирования групп контролей состояния информационной безопасности в финансовых организациях.
32. Предпосылки введения международного стандарта ISO 15408 «Общие критерии». Основные понятия ISO 15408.
33. Методология оценки безопасности информационных технологий на соответствие ISO 15408. Понятие «уровень доверия».
34. Оценка уровня доверия функциональной безопасности информационной технологии.
35. Классы и семейства ISO 15408. Понятие «Профиль защиты».

36. Анализ видов инструментов для проведения аудитов информационной безопасности. Метод CRAMM.

37. Сканирование уязвимостей автоматизированных и информационных систем.

38. Нагрузочное тестирование и тестирование на устойчивость автоматизированных систем. Анализ уязвимостей CRM и ERP систем.

39. Особенности проведения аудитов информационной безопасности объектов обработки конфиденциальной информации с использованием технических средств.

40. Понятие «наблюдение» в процессе проведения аудита информационной безопасности.

41. Понятие «свидетельство» аудита информационной безопасности.

42. Методы «выборки» и организация выборочных проверок.

43. Понятие «прослеживаемость процесса» в практике оценки систем управления информационной безопасностью.

44. Анализ метрик информационной безопасности. Анализ корпоративного управления информационной безопасностью.

45. Подготовка и практика интервьюирования. Методы анализа структур документации и записей системы обеспечения информационной безопасности.

46. «Несоответствие» и методы обработки несоответствий.

47. Структура подразделения внутреннего аудита. Виды аудитов информационной безопасности.

48. Управление программой аудита информационной безопасности. Типичные виды деятельности при проведении аудита информационной безопасности.

49. Процесс сбора и верификации аудиторской информации. Аудиторский отчёт.

50. Правила согласования аудиторского отчёта. Контроль за деятельностью аудиторов информационной безопасности.

51. Профессиональный и нравственно-этический уровень аудитора информационной безопасности. Понятие «Объективная оценка». Понятие «Независимость аудитора».

52. Практика межличностного общения. Материальное вознаграждение. Аудиторский риск.

53. Понятие «Психологический контракт». Принадлежность к профессиональным сообществам.

54. Воздействие аудитора на результаты оценки. Профессиональное развитие аудитора информационной безопасности.

Перечень практических заданий к экзамену

1) УК РФ. Ответственность за преступления в сфере компьютерной информации.
2) Службы DNS, DHCP. Принципы функционирования.
3) Протокол ARP. Назначение. Принцип функционирования.
4) Метод кодирования информации Base64.
5) Сетевые маски. Назначение. Разбиение сети на подсети.
6) Принципы функционирования сетевых устройств (повторитель (Repeater), концентратор (Hub), сетевой мост (Network Bridge), Коммутатор (Switch), маршрутизатор (Router)).
7) Поиск узлов в сети, определение функционирующих служб и версии ОС при помощи сканера NMAP (Продемонстрировать).
8) Google Hack (Продемонстрировать).
9) Поиск Web приложений на сервере.
10) AXFR запрос (Продемонстрировать).
11) Определение платформы Web приложения, версии Web сервера, CMS, Framework (Продемонстрировать).

12) OWASP TOP 10.
13) SQL Injection (Продемонстрировать).
14) XSS (Продемонстрировать).
15) Directory traversal/File Include (Продемонстрировать).
16) Поиск уязвимостей в WordPress и Joomla. Сканеры wpscan и joomscan (Продемонстрировать).
17) Поиск уязвимостей в Web приложениях. Сканер OWAP-ZAP (Продемонстрировать)
18) Работа с Sqlmap (Продемонстрировать).
19) Поиск уязвимых сетевых сервисов. Сканер OpenVas (Продемонстрировать).
20) Работа с системой эксплуатации уязвимостей metasploit framework (Продемонстрировать).
21) BufferOverflow.
22) Атака man in the middle. Реализация при помощи ARP spoofing.
23) Безопасность WiFi сети.
24) Восстановление исходной информации по хешам. Утилита john the ripper.
25) Понятия: персональные данные, обработка персональных данных, информационная система персональных данных.
26) Условия обработки персональных данных.
27) Уведомление об обработке персональных данных.
28) Определение уровня защищенности ИСПДн.
29) Классификация АС.
30) Нормативные документы, определяющие требования к защите ПДн и КИ.

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	Ввод имени пользователя при входе в систему 1) идентификация 2) аутентификация 3) мониторинг 4) риск	1	2
2.		Стандартное средство проверки подлинности пользователя – пароль 1) идентификация 2) аутентификация 3) мониторинг 4) риск	2	3
3.		Система, которая «управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право	1	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		читать, записывать, создавать и удалять информацию 1) безопасная 2) опасная 3) доверенная 4) защищенная		
4.		Система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа 1) безопасная 2) опасная 3) доверенная 4) защищенная	3	3
5.		Совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности 1) доверенная вычислительная база 2) защищенная вычислительная база 3) безопасная система 4) опасная система	1	3
6.	Задание открытого типа	Категории, на которые делятся средства подотчетности согласно «Оранжевой книге»	Средства подотчетности согласно «Оранжевой книге» делятся на три категории: идентификация и аутентификация; предоставление доверенного пути; анализ регистрационной информации.	5
7.		Основное назначение доверенной вычислительной базы	Основное назначение доверенной вычислительной базы – выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (пользователями) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.	6
8.		Произвольное управление доступом	Произвольное управление доступом – это метод разграничения доступа к	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.	
9.		Принудительное (или мандатное) управление доступом	Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов объектов, оказываются зафиксированными и права доступа.	8
10.		Какие тома согласно "Оранжевой книге" должны входить в комплект документации надежной системы	Согласно "Оранжевой книге" в комплект документации надежной системы должны входить следующие тома: Руководство пользователя по средствам безопасности. Руководство администратора по средствам безопасности. Тестовая документация. Описание архитектуры.	8
ПК-5. Способен администрировать средства защиты информации в компьютерных системах и сетях				
11.	Задание закрыт	Форма независимого, нейтрального контроля какого-либо направления деятельности коммерческого предприятия, широко используемая в практике рыночной	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
	ого типа	экономики, особенно в сфере бухгалтерского учета 1) Аудит 2) Мониторинг 3) Анализ 4) Оценка		
12.		Компьютерная распределённая система для получения информации о доменах 1) DNS 2) DHCP 3) NAT 4) PHP	1	2
13.		Сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP 1) DNS 2) DHCP 3) HTML 4) PHP	2	2
14.		Протокол DHCP предоставляет три способа распределения IP-адресов: 1) Ручное распределение 2) Автоматическое распределение 3) Динамическое распределение 4) Статистическое распределение 5) Автоматизированное распределение 6) Смешанное распределение	1, 2, 3	2
15.		Механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов 1) DNS 2) DHCP 3) NAT 4) PHP	3	2
16.	Задание открытого типа	Цели проведения аудита безопасности	Целями проведения аудита безопасности являются: анализ рисков, связанных с возможностью осуществления угроз безопасности в от- ношении ресурсов; оценка текущего уровня защищенности ИС; локализация узких мест в системе защиты ИС;	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			оценка соответствия ИС существующим стандартам в области информационной безопасности; выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.	
17.		Принцип работы сетевого концентратора	Концентратор работает на первом (физическом) уровне сетевой модели OSI, ретранслируя входящий сигнал с одного из портов в сигнал на все остальные (подключённые) порты, реализуя, таким образом, свойственную Ethernet топологию общая шина, с разделением пропускной способности сети между всеми устройствами и работой в режиме полудуплекса. Коллизии (то есть попытка двух и более устройств начать передачу одновременно) обрабатываются аналогично сети Ethernet на других носителях - устройства самостоятельно прекращают передачу и возобновляют попытку через случайный промежуток времени, говоря современным языком, концентратор объединяет устройства в одном домене коллизий	3
18.		Принцип работы сетевого моста	Сетевой мост работает на канальном уровне сетевой модели OSI, при получении из сети кадра, сверяет MAC-адрес последнего и, если он не принадлежит данной подсети, передаёт (транслирует) кадр дальше в тот сегмент, которому предназначался данный кадр; если кадр принадлежит данной подсети, мост ничего не делает	8
19.		Принцип работы сетевого коммутатора	Сетевой коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			уровень OSI). Коммутатор передаёт данные только непосредственно получателю. Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется	
20.		Принцип работы маршрутизатора	Маршрутизаторы работают на более высоком «сетевом» (третьем) уровне сетевой модели OSI, нежели коммутатор (или сетевой мост) и концентратор (хаб), которые работают соответственно на втором и первом уровнях модели OSI. Обычно маршрутизатор использует адрес получателя, указанный в заголовке пакета, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается. Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/расшифрование передаваемых данных и т.п.	

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

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

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	6/4	24	
2.	Выполнение контрольной работы	3/4	12	
3.	Тест	1/4	4	
Всего			**40**	-
Блок бонусов				
4.	Посещение занятий без пропусков	1	3	
5.	Своевременное выполнение всех заданий	1	3	
6.	Активность студента на занятии	1	4	
Всего			**10**	-
Дополнительный блок**				
7.	*Зачет (Диф.зачет) / Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11. Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1

Показатель	Балл
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)	Не зачтено

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. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский - М. : ФЛИНТА, 2016. - http://www.studentlibrary.ru/book/ISBN9785976512771.html

2. Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин - М. : ФЛИНТА, 2016. - http://www.studentlibrary.ru/book/ISBN9785976512733.html

8.2. Дополнительная литература

1. Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М. : ЦИПСиР, 2011. - http://www.studentlibrary.ru/book/ISBN9785961413649.html

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.

Материально-техническое обеспечение дисциплины включает в себя учебные лаборатории и классы, оснащенные современными компьютерами, объединенными локальными вычислительными сетями с выходом в Интернет. Учащимся предоставляется возможность

практической работы на ЭВМ различной архитектуры (на базе одноядерных, многоядерных, параллельных процессоров).

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).