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	УТВЕРЖДАЮ И.о. Заведующего кафедрой информационной безопасности
О.Н. Выборнова	В.А. Черкасова
«05» мая 2025 г.	«05» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Составитель(и)	**Шукралиева Д.Э., доцент каф. ИБ, Климов Д.В., ассистент каф. ИБ**
Согласовано с работодателями:	**И.В. Давидюк, доцент, к.т.н., заведующий кафедрой «Информационная безопасность» ФГБОУ ВО «Астраханский государственный университет»; Барсуков В.А., начальник отдела информационной безопасности Управления корпоративной защиты ООО «Газпром добыча Астрахань»**
Направление подготовки / специальность	**10.03.01 Информационная безопасность**
Направленность (профиль) / специализация ОПОП	**Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная, очно-заочная**
Год приёма	**2024**
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

1.1. Целью освоения дисциплины

– 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:

– 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 В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Аудит информационной безопасности» относится к элективным дисциплинам учебного плана и осваивается в 6 семестре при очной форме обучения и в 8 – при очно-заочной.

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

– *Основы информационной безопасности.*

Знания: основные понятия и термины информационной безопасности, механизмы защиты информации, криптографические методы, законодательство в области защиты информации, общие принципы построения систем информационной безопасности.

Умения: анализировать угрозы и риски информационной безопасности, разрабатывать и реализовывать политики защиты информации, использовать стандартные средства защиты данных и криптографические инструменты, оценивать эффективность мер информационной безопасности.

Навыки: проведение оценки уязвимости систем и сети, настройка средств защиты и мониторинга информации, реагирование на инциденты информационной безопасности, подготовка документации и отчетов по информационной безопасности.

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

– Системы искусственного интеллекта.
– Подготовка рефератов, курсовых работ (проектов), бакалаврской работы.
– Дисциплины учебного плана, реализация которых осуществляется с использованием электронной информационно-образовательной среды Астраханского государственного университета им. В. Н. Татищева.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

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

в) профессиональной(ых) (ПК):

– 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);
– Способен администрировать средства защиты информации в компьютерных системах и сетях (ПК-4).

Таблица 1 – Декомпозиция результатов обучения

Код компетенции	Планируемые результаты обучения по дисциплине		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-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 от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в	– 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	– методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа.

Код компетенции	Планируемые результаты обучения по дисциплине		
	Знать (1)	Уметь (2)	Владеть (3)
	автоматизированных системах.	в автоматизированных системах.	
ПК-4	– 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.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 2 зачетные единицы (108 часов).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной формы обучения приведена в таблице 2.1.

Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
Объем дисциплины в зачетных единицах	3	3
Объем дисциплины в академических часах	108	108
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):	69,25	31,25
- занятия лекционного типа, в том числе: - практическая подготовка (если предусмотрена)	17	15
- занятия семинарского типа (семинары, практические, лабораторные), в том числе: - практическая подготовка (если предусмотрена)	51	15
- консультация (предэкзаменационная)	1	1
- промежуточная аттестация по дисциплине	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 представлены в таблице 2.2.

Таблица 2.2. Структура и содержание дисциплины

для очной формы обучения

Раздел, тема дисциплины	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 6										
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	***1***				***4***			***3***	***8***	Отчет по лабораторной работе № 1
Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения.	***1***				***4***			***3,75***	***8,75***	Отчет по лабораторной работе № 2
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	***1***				***4***			***4***	***9***	Контрольная работа №1
Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	***1***				***4***			***4***	***9***	Отчет по лабораторной работе № 3
Тема 5. Критерии аудита информационной	***1***				***4***			***4***	***9***	

Раздел, тема дисциплины	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				
безопасности. Международные стандарты управления информационной безопасностью.										Отчет по лабораторной работе № 4
Тема 6. Методы оценки безопасности информационных технологий.	***2***				***6***			***4***	***12***	Контрольная работа № 2
Тема 7. Инструменты проведения аудита информационной безопасности.	***2***				***6***			***4***	***12***	Отчет по лабораторной работе № 5
Тема 8. Методика проведения аудита информационной безопасности.	***2***				***7***			***4***	***13***	Отчет по лабораторной работе № 6
Тема 9. Организация внутреннего аудита на предприятии.	***3***				***6***			***4***	***13***	Контрольная работа №3
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	***3***				***6***			***4***	***13***	Итоговое тестирование
Консультации									***1***	
Контроль промежуточной аттестации									***0,25***	**Экзамен**
ИТОГО за семестр:	***17***				***51***			***38,75***	***108***	
Итого за весь период	***17***				***51***			***38,75***	***108***	

для очно-заочной формы обучения

Раздел, тема дисциплины	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 8										
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	***1***				***1***			***6***	***8***	Отчет по лабораторной работе № 1
Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения.	***1***				***1***			***6,75***	***8,75***	Отчет по лабораторной работе № 2
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	***1***				***1***			***7***	***9***	Контрольная работа №1
Тема 4. Критерии аудита информационной безопасности.	***1***				***1***			***7***	***9***	Отчет по лабораторной работе № 3

Раздел, тема дисциплины	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.										
Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	***1***				***1***			***7***	***9***	Отчет по лабораторной работе № 4
Тема 6. Методы оценки безопасности информационных технологий.	***2***				***2***			***8***	***12***	Контрольная работа № 2
Тема 7. Инструменты проведения аудита информационной безопасности.	***2***				***2***			***8***	***12***	Отчет по лабораторной работе № 5
Тема 8. Методика проведения аудита информационной безопасности.	***2***				***2***			***9***	***13***	Отчет по лабораторной работе № 6
Тема 9. Организация внутреннего аудита на предприятии.	***2***				***2***			***9***	***13***	Контрольная работа №3
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	***2***				***2***			***9***	***13***	Итоговое тестирование
Консультации									***1***	
Контроль промежуточной аттестации									***0,25***	**Экзамен**
ИТОГО за семестр:	***15***				***15***			***76,75***	***108***	
Итого за весь период	***15***				***15***			***76,75***	***108***	

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

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

Раздел, тема дисциплины	Кол-во часов	Код компетенции		Общее количество компетенций
		ПК-1	ПК-4	
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	8	+	+	2
Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения.	8,75	+	+	2
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	9	+	+	2
Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	9	+	+	2

Раздел, тема дисциплины	Кол-во часов	Код компетенции		Общее количество компетенций
		ПК-1	ПК-4	
Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	9	+	+	2
Тема 6. Методы оценки безопасности информационных технологий.	12	+	+	2
Тема 7. Инструменты проведения аудита информационной безопасности.	12	+	+	2
Тема 8. Методика проведения аудита информационной безопасности.	13	+	+	2
Тема 9. Организация внутреннего аудита на предприятии.	13	+	+	2
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	13	+	+	2
Итого	**108**			

Краткое содержание каждой темы дисциплины

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

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

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.

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:

- недостаточное выполнение требований задания (например, отсутствие необходимых элементов, неполное выполнение инструкции);
- не ответы на все вопросы или неправильное понимание темы;
- небрежное выполнение.

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.

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.

5.2. Указания для обучающихся по освоению дисциплины

Лекция

Лекция – основной вид обучения в вузе. В лекции излагаются основные положения теории, ее понятия и законы, приводятся факты, показывающие связь теории с практикой.

Накануне лекции необходимо повторить содержание предыдущей лекции (а также теорию по изучаемой теме в школьных учебниках геометрии, если эта тема была представлена в них), а затем посмотреть тему очередной лекции по программе (по плану лекций).

Полезно вести записи (конспекты) лекций: для непонятных вопросов оставлять место при работе над темой лекции с учебными пособиями.

Записи лекций следует вести в отдельной тетради, оставляя место для дополнений во

время самостоятельной работы.

При конспектировании лекций выделяйте главы и разделы, параграфы, подчеркивайте основное.

Лабораторное занятие

Лабораторное занятие – наиболее активный вид учебных занятий в вузе. Он предполагает самостоятельную работу над учебными пособиями, основной литературой, открытыми источниками информации.

К каждому лабораторному занятию нужно готовиться. Подготовку следует начинать с повторения теории (по учебному пособию). После этого нужно решать задачи из предложенного домашнего задания.

Организация самостоятельной работы

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

Самостоятельная работа студентов представлена в следующих формах:

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

Таблица 4. Содержание самостоятельной работы обучающихся

для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	***3***	Изучение в рамках программы курса тем и проблем.
Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения.	***3,75***	Изучение в рамках программы курса тем и проблем.
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 6. Методы оценки безопасности информационных технологий.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 7. Инструменты проведения аудита информационной безопасности.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 8. Методика проведения аудита информационной безопасности.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 9. Организация внутреннего аудита на предприятии.	***4***	Изучение в рамках программы курса тем и проблем.
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	***4***	Изучение в рамках программы курса тем и проблем.

для очно-заочной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	***6***	Изучение в рамках программы курса тем и проблем.
Тема 2. Аудит информационной безопасности.	***6,75***	Изучение в рамках программы курса тем

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Основные понятия, термины, определения.		и проблем.
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	***7***	Изучение в рамках программы курса тем и проблем.
Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	***7***	Изучение в рамках программы курса тем и проблем.
Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	***7***	Изучение в рамках программы курса тем и проблем.
Тема 6. Методы оценки безопасности информационных технологий.	***8***	Изучение в рамках программы курса тем и проблем.
Тема 7. Инструменты проведения аудита информационной безопасности.	***8***	Изучение в рамках программы курса тем и проблем.
Тема 8. Методика проведения аудита информационной безопасности.	***9***	Изучение в рамках программы курса тем и проблем.
Тема 9. Организация внутреннего аудита на предприятии.	***9***	Изучение в рамках программы курса тем и проблем.
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	***9***	Изучение в рамках программы курса тем и проблем.

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

Не предусмотрено.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

6.1. Образовательные технологии

Таблица 5. Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины	**Форма учебного занятия**		
	Лекция	**Практическое занятие, семинар**	**Лабораторная работа**
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение контрольной работы*
Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 5. Критерии аудита информационной безопасности.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*

Международные стандарты управления информационной безопасностью.			
Тема 6. Методы оценки безопасности информационных технологий.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение контрольной работы*
Тема 7. Инструменты проведения аудита информационной безопасности.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 8. Методика проведения аудита информационной безопасности.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 9. Организация внутреннего аудита на предприятии.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение контрольной работы*
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение теста*

6.2. Информационные технологии

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

1) использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

2) использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

3) использование возможностей электронной почты преподавателя;

4) 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.);

5) 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);

6) 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

Перечень программного обеспечения (***состав подлежит обновлению при необходимости***)

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
MathCad 14	Система компьютерной алгебры из класса систем автоматизированного проектирования, ориентированная на подготовку интерактивных документов с вычислениями и визуальным сопровождением, отличается лёгкостью использования
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 10 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер

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/catalog/
2. Электронный каталог «Научные журналы АГУ» https://asu-edu.ru/issledovaniya-i-innovacii/11745-nauchnye-jurnaly-agu.html
3. Справочная правовая система КонсультантПлюс http://www.consultant.ru

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

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине «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 и прохождением практик, а в процессе освоения дисциплины – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6. Соответствие разделов, тем дисциплины, результатов обучения по дисциплине и оценочных средств

Контролируемый раздел, тема дисциплины	Код контролируемой компетенции	Наименование оценочного средства
Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.	ПК-1, ПК-4	Отчет по лабораторной работе № 1
Тема 2. Аудит информационной безопасности. Основные понятия, термины, определения.	ПК-1, ПК-4	Отчет по лабораторной работе № 2
Тема 3. Методы оценки систем обеспечения информационной безопасности. Методика процессного анализа систем.	ПК-1, ПК-4	Контрольная работа №1
Тема 4. Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	ПК-1, ПК-4	Отчет по лабораторной работе № 3
Тема 5. Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью.	ПК-1, ПК-4	Отчет по лабораторной работе № 4
Тема 6. Методы оценки безопасности информационных технологий.	ПК-1, ПК-4	Контрольная работа № 2
Тема 7. Инструменты проведения аудита информационной безопасности.	ПК-1, ПК-4	Отчет по лабораторной работе № 5
Тема 8. Методика проведения аудита информационной безопасности.	ПК-1, ПК-4	Отчет по лабораторной работе № 6
Тема 9. Организация внутреннего аудита на предприятии.	ПК-1, ПК-4	Контрольная работа №3

Контролируемый раздел, тема дисциплины	Код контролируемой компетенции	Наименование оценочного средства
Тема 10. Психологические аспекты подготовки аудитора информационной безопасности.	ПК-1, ПК-4	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

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 SQLинъекций, 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 и заданий, выносимых на экзамен

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.

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 мин)
Код и наименование проверяемой компетенции *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	2	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
		3) мониторинг 4) риск		
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 читать, записывать, создавать и удалять информацию 1) безопасная 2) опасная 3) доверенная 4) защищенная	1	3
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	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
			доступом – это метод разграничения доступа к 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-4. Способен администрировать средства защиты информации в компьютерных системах и сетях				
11.	Задание закрытого типа	Форма независимого, нейтрального контроля какого-либо направления деятельности коммерческого предприятия, широко	1	2
12.		Компьютерная распределённая система для получения информации о доменах	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
		1) DNS 2) DHCP 3) NAT 4) PHP		
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 отношении ресурсов; оценка текущего уровня защищенности ИС; локализация узких мест в системе защиты ИС; оценка соответствия ИС существующим стандартам в области информационной безопасности; выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.	3
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	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
			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 оду ном домене коллизий	
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 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	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
			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 рабоу тают 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 уровней и другая информация,	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
			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 (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины, и в Центре мониторинга и аудита качества обучения.

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

Таблица 10. Технологическая карта рейтинговых баллов по дисциплине

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	6 / 4	24	Указан в Moodle
2.	*Выполнение контрольной работы*	3 / 4	12	
3.	*Тест*	1 / 4	4	
Всего			**40**	-
Блок бонусов				
4.	*Посещение всех занятий*	5	5	По расписанию
5.	*Своевременное выполнение всех заданий*	5	5	Указан в Moodle
Всего			**10**	-
Дополнительный блок				
7.	*Экзамен*		**50**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Пропуски занятий без уважительной причины (за одно занятие)	- 1

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

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 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

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

Для проведения **лекционных занятий**:

1. Используется аудитория, оборудованная необходимым количеством столов, стульев, доской маркерной и электронной.
2. Аудитория должна иметь следующие нормы освещенности:
   - СНиП 23-05-95 «Естественное и искусственное освещение» норма освещенности аудиторий ВУЗов 400 Лк;
   - СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий» пункт 3.3.3. «Общее освещение в помещениях общественных зданий должно быть равномерным».
3. Электронная доска должна быть подключена к сети Интернет.

Для проведения **лабораторных занятий**:

1. Лабораторные занятия проводятся с группами или подгруппами не более 15 человек.
2. Аудитория должна быть оснащена необходимым количеством столов, стульев, доской маркерной и электронной.
4. Аудитория должна иметь следующие нормы освещенности:
   - СНиП 23-05-95 «Естественное и искусственное освещение» норма освещенности аудиторий ВУЗов 400 Лк;
   - СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий» пункт 3.3.3. «Общее освещение в помещениях общественных зданий должно быть равномерным».
5. В аудитории должно быть не менее 15 компьютеров, находящихся в исправном состоянии.
6. Расположение компьютеров в аудитории должно позволять преподавателю подойти к рабочему месту студента.
7. Компьютеры должны быть соединены локальной сетью со скоростью не менее 1 Гбит/с и подключены к сети Интернет.

8. Компьютеры должны обладать минимальными характеристиками:
   - Материнская плата H610M H DDR 4;
   - Процессор 12th Gen Intel(R) Core(TM) i3-12100;
   - Видеоадаптер Intel(R) UHD Graphics 730.

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

Рабочая программа дисциплины 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).