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

«ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

Составитель(и)	**Шукралиева Д.Э., доцент каф. ИБ, Корякова В.А., 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 «Защита информационных процессов в компьютерных системах» относится к части элективные дисциплины 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:
– Поможет студентам при написании бакалаврской работы

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 техническому обслуживанию защищенных технических средств обработки информации (ПК-2);
–Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем (ПК-3).

Таблица 1 – Декомпозиция результатов обучения

Код компетенции	Планируемые результаты обучения по дисциплине		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-2	– технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям безопасности информации.	– проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.	– методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее.

Код компетенции	Планируемые результаты обучения по дисциплине		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-3	– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации основные меры по защите информации в автоматизированных системах, нормативные правовые акты в области защиты информации.	– администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы.	– методикой анализа структурных и функциональных схем защищенной автоматизированной системы.

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

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
- 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. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	***1***				***5***			***3***	***9***	Отчет по лабораторной работе № 1
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	***2***				***5***			***3,75***	***9,75***	Отчет по лабораторной работе № 2
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	***2***				***5***			***4***	***11***	Отчет по лабораторной работе № 3
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	***2***				***5***			***4***	***11***	Отчет по лабораторной работе № 4

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				
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	***2***				***5***			***4***	***11***	Отчет по лабораторной работе № 5
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	***2***				***6***			***5***	***13***	Отчет по лабораторной работе № 6
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	***2***				***6***			***5***	***13***	Отчет по лабораторной работе № 7
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	***2***				***7***			***5***	***14***	Отчет по лабораторной работе № 8
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	***3***				***7***			***5***	***15***	Итоговая контрольная работа
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. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	***1***				***1***			***7***	***9***	Отчет по лабораторной работе № 1
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно	***1***				***1***			***7,75***	***9,75***	Отчет по лабораторной работе № 2

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				
защищенных баз данных и их оценка по стандарту «Оранжевая книга».										
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	***1***				***1***			***9***	***11***	Отчет по лабораторной работе № 3
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	***2***				***2***			***7***	***11***	Отчет по лабораторной работе № 4
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	***2***				***2***			***7***	***11***	Отчет по лабораторной работе № 5
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	***2***				***2***			***9***	***13***	Отчет по лабораторной работе № 6
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	***2***				***2***			***9***	***13***	Отчет по лабораторной работе № 7
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	***2***				***2***			***10***	***14***	Отчет по лабораторной работе № 8
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	***2***				***2***			***11***	***15***	Итоговая контрольная работа
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-2	ПК-3	
Тема 1. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	9	+	+	2
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	9,75	+	+	2
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	11	+	+	2
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	11	+	+	2
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	11	+	+	2
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	13	+	+	2
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	13	+	+	2
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	14	+	+	2
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	15	+	+	2
Итого	**108**			

Краткое содержание каждой темы дисциплины

Тема 1. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.

Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».

Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.

Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.

Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.

Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.

Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.

Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.

Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

При подготовке к практическим занятиям необходимо воспользоваться учебно-методической литературой из п.8. Практические занятия необходимо проводить с использованием презентаций, созданных в Microsoft PowerPoint.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой, а также пользоваться ресурсами сети Интернет.

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.

Таблица 4. Содержание самостоятельной работы обучающихся

для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Тема 1. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	3	Изучение в рамках программы курса тем и проблем.
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	3,75	Изучение в рамках программы курса тем и проблем.

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	4	Изучение в рамках программы курса тем и проблем.
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в СС и базовые концепции.	4	Изучение в рамках программы курса тем и проблем.
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	4	Изучение в рамках программы курса тем и проблем.
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	5	Изучение в рамках программы курса тем и проблем.
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	5	Изучение в рамках программы курса тем и проблем.
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	5	Изучение в рамках программы курса тем и проблем.
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	5	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. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	7	Изучение в рамках программы курса тем и проблем.
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	7,75	Изучение в рамках программы курса тем и проблем.
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	9	Изучение в рамках программы курса тем и проблем.
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в СС и базовые концепции.	7	Изучение в рамках программы курса тем и проблем.
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	7	Изучение в рамках программы курса тем и проблем.
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	9	Изучение в рамках программы курса тем и проблем.
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	9	Изучение в рамках программы курса тем и проблем.
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	10	Изучение в рамках программы курса тем и проблем.
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	11	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. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение контрольной работы*
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение контрольной работы*
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*
Тема 8. Анализ критичных технологий. Государственная политика в области	*Обзорная лекция*	*Не предусмотрено*	*Выполнение лабораторных работ*

безопасности компьютерных систем.			
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем.	*Обзорная лекция*	*Не предусмотрено*	*Выполнение контрольной работы*

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
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
MS Visual Studio Среда разработки программ для ЭВМ	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/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 «Защита информационных процессов в компьютерных системах» 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. Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.	ПК-2, ПК-3	Отчет по лабораторной работе № 1
Тема 2. Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	ПК-2, ПК-3	Отчет по лабораторной работе № 2
Тема 3. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.	ПК-2, ПК-3	Отчет по лабораторной работе № 3
Тема 4. Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.	ПК-2, ПК-3	Отчет по лабораторной работе № 4
Тема 5. Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.	ПК-2, ПК-3	Отчет по лабораторной работе № 5
Тема 6. Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев.	ПК-2, ПК-3	Отчет по лабораторной работе № 6
Тема 7. Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз.	ПК-2, ПК-3	Отчет по лабораторной работе № 7
Тема 8. Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем.	ПК-2, ПК-3	Отчет по лабораторной работе № 8
Тема 9. Разработка политик безопасности для защищенных компьютерных систем. Порядок	ПК-2, ПК-3	Итоговая контрольная работа

Контролируемый раздел, тема дисциплины	Код контролируемой компетенции	Наименование оценочного средства
аттестации защищенных компьютерных систем.		

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 «Информационные технологии и их поддержка. Информационные технологии и информационные системы. Проектирование и разработка защищенных информационных технологий.»

1. Практическое занятие

Вопросы для обсуждения:

Информационные технологии и информационные системы.

Примеры информационных технологий и информационных систем. Типы компьютерных систем, как элементов информационных технологий. Основные принципы успешного функционирования информационной (компьютерной) системы. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений. Основные принципы и методы защиты информационных процессов в компьютерных системах. Проектирование и разработка защищенных информационных технологий

Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении. Государственные

стандарты на разработку и создание информационных систем в защищенном исполнении. CASE-технологии создания информационных систем. Стандарт ITIL.

2. Лабораторная работа 1. Сравнительный анализ различных стандартов в области защиты информационных технологий с точки зрения эффективности достижения цели построения защищенных информационных систем.

Тема «Американские и европейские стандарты по защите информации. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».»

1. Практическое занятие

Вопросы для обсуждения:

Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга». Американский стандарт по защите информации «Оранжевая книга». Понятие гарантии защиты. Критерии оценки защищенности баз данных. Содержание классов защищенности. Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.

2. Лабораторная работа 2. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев

Тема «Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC»

1. Практическое занятие

Вопросы для обсуждения:

Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC. Европейский стандарт по защите информации ITSEC. Понятие гарантии защиты в соответствии с европейским стандартом. Критерии оценки защищенности. Содержание классов защищенности. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения защищенных информационных систем.

2. Лабораторная работа 3. Анализ рисков для информационной системы предприятия (организации) и построение модели угроз безопасности.

Тема «Общие критерии оценки защищенности информационных технологий COMMON CRITERIA (CC). Подход к безопасности компьютерных систем в CC и базовые концепции.»

1. Практическое занятие

Вопросы для обсуждения

Подход к безопасности компьютерных систем в CC и базовые концепции

Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности. Содержание политики безопасности.

2. Лабораторная работа 4. Порядок сертификации средств защиты информации для разработчика СЗИ.

Тема «Классы в системе общих критериев. Гарантии безопасности компьютерных систем в системе общих критериев.»

1. Практическое занятие

Вопросы для обсуждения:

Классы защищенности в системе общих критериев. Понятие аудита политики безопасности. Требования к подсистемам аудита. Подсистемы подтверждения подлинности отправки и получения сообщения. Подсистемы разграничения доступа. Подсистемы идентификации и аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты

ресурсов системы. Подсистемы защиты связи. Требования к подсистемам, предъявляемые в каждом классе защищенности.

Гарантии безопасности компьютерных систем в системе общих критериев

Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

2. Лабораторная работа 5. Порядок сертификации защищенных информационных систем.

Тема «Каналы утечки и их анализ в системе общих критериев. Безопасное функционирование в системе общих критериев»

1. Практическое занятие

Вопросы для обсуждения:

Каналы утечки и их анализ в системе общих критериев

Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.

Безопасное функционирование в системе общих критериев

Управление конфигурацией. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

2. Лабораторная работа 6. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем для руководителя предприятия (организации) – соискателя лицензии

Тема «Технология построения защищенных компьютерных систем. Основные угрозы безопасности информации в компьютерных системах. Модель угроз»

1. Практическое занятие

Вопросы для обсуждения:

Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах. Специфика возникновения угроз в открытых сетях. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных. Анализ рисков. Модель противника, возможности противника. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Основные категории требований к программной и программно- аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

Модель угроз.

2. Лабораторная работа 7. Разработка профиля защиты и построение политик безопасности для компьютерной системы предприятия (организации).

Тема «Анализ критичных технологий. Государственная политика в области безопасности компьютерных систем»

1. Практическое занятие

Вопросы для обсуждения:

Анализ критичных технологий

Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.

Государственная политика в области безопасности компьютерных систем

Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа

2. Лабораторная работа 8. Проведение аттестационных испытаний компьютерных систем в защищенном исполнении и выдача «Аттестата соответствия»

Тема «Разработка политик безопасности для защищенных компьютерных систем. Порядок аттестации защищенных компьютерных систем»

1. Практическое занятие

Вопросы для обсуждения:

Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.

Порядок аттестации защищенных компьютерных систем

Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

2. Итоговая контрольная работа

Вопросы к итоговой контрольной работе:

1. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах.
2. Специфика возникновения угроз в открытых сетях.
3. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных.
4. Анализ рисков. Модель противника, возможности противника.
5. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.
6. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.
7. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.
8. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.
9. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа
10. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.
11. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.
12. Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации.
13. Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.
14. Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

Перечень вопросов и заданий, выносимых на экзамен

1. Примеры информационных технологий и информационных систем.
2. Типы компьютерных систем, как элементов информационных технологий.
3. Основные принципы успешного функционирования информационной (компьютерной) системы.
4. Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
5. Основные принципы и методы защиты информационных

процессов в компьютерных системах.

6. Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий.

7. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.

8. Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.

9. CASE-технологии создания информационных систем.

10. Стандарт ITIL.

11. Американский стандарт по защите информации «Оранжевая книга».

12. Европейский стандарт по защите информации ITSEC.

13. Понятие профиля защиты. Функции поддержки политики безопасности. Гарантии безопасности.

14. Требования по безопасности информационных технологий. Классы защищенности. Компоненты подсистем поддержки политики безопасности.

15. Содержание политики безопасности.

16. Классы защищенности в системе общих критериев.

17. Понятие аудита политики безопасности. Требования к подсистемам аудита.

18. Подсистемы подтверждения подлинности отправки и получения сообщения.

19. Подсистемы разграничения доступа.

20. Подсистемы идентификации и аутентификации.

21. Подсистемы защиты функций защиты.

22. Подсистемы защиты ресурсов системы.

23. Подсистемы защиты связи.

24. Понятие гарантии безопасности. Уровни гарантий. Гарантии проектирования защищенных информационных систем. Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

25. Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности. Методология анализа каналов утечки информации.

26. Управление конфигурацией. Безопасная установка систем защиты информационных технологий. Безопасная модернизация информационных технологий.

27. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах.

28. Специфика возникновения угроз в открытых сетях.

29. Особенности защиты информации на узлах компьютерной сети. Системные вопросы защиты программ и данных.

30. Анализ рисков. Модель противника, возможности противника.

31. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.

32. Основные категории требований к программной и программно-аппаратной реализации средств защиты информации. Требования к защите автоматизированных систем от НСД.

33. Требования, предъявляемые к разработке модели угроз. Структура модели угроз безопасности информации. Анализ критичных технологий обработки информации.

34. Система лицензирования и сертификации средств защиты. Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.

35. Нормативная база и ответственность за защиту информации в компьютерных системах. Руководящие документы ФСТЭК России по оценке защищенности автоматизированных систем от несанкционированного доступа

36. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.

37. Политика мандатного доступа. Политика защиты целостности информационных ресурсов.

38.Понятие аттестации защищенных компьютерных систем. Руководящие документы ФСТЭК России по аттестации.

39.Порядок аттестации. Принципы и методы аттестационных испытаний защищенных компьютерных систем по требованиям безопасности.

40.Содержание этапов аттестационных испытаний. Контроль эффективности защитных мероприятий в системе аттестации.

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-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации*				
1.	Задание закрытого типа	В каком году был принят Международный стандарт ISO 17799? 1.1998 2.2000 3.2002 4.2010	2	2
2.		В каком году в Германии вышло "Руководство по защите информационных технологий для базового уровня", дальнейшем, которое было оформлено в виде германского стандарта BSI. 1. 1998 2. 2000 3. 2002 4. 2010	1	2
3.		Какие аспекты затрагивает гарантированность в стандарте "Гармонизированные критерии европейских стран" 1. эффективность 2. корректность средств безопасности 3. мощность 4. надежность 5. быстродействие 6. производительность	1, 2	2
4.		По каким критериям оценивается степень доверия по стандарту «Критерии оценки надежности компьютерных систем» 1. Политика безопасности 2. Уровень гарантированности 3. Уровень безопасности 4. Уровень секретности 5. Концепция безопасности	1,2	2
5.		По стандарту "Гармонизированные критерии европейских стран" определяются следующие градации мощности 1. базовая 2. средняя 3. высокая 4. низкая 5. основная 6. дополнительная	1, 2, 3	2
6.	Типы АИС	Типы АИС по структуре	Для определения последствий нарушения безопасности	5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
	по структуре		рекомендуется проделать следующие шаги: зафиксировать инцидент с помощью записи сетевою трафика, снятия копий файлов журналов, активных учетных записей и сетевых подключений; ограничить дальнейшие нарушения путем отключения учетных записей, отсоединения сетевого оборудования от локальной сети и от Интернета; провести резервное копирование скомпрометированных систем для проведения детального анализа повреждений и метода атаки; попытаться найти другие подтверждения компрометации (часто при компрометации системы оказываются затронутыми другие системы и учетные записи); хранить и просматривать файлы журналов устройств безопасности и сетевого мониторинга, так как они часто являются ключом к определению метода атаки.	
7.		Типы АИС по структуре	По структуре АИС подразделяются на три типа: 1) на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (АРМ); 2) комплексы АРМ, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные системы); 3) комплексы АРМ и (или) локальных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).	6
8.		Класс, которые присваивается типовой информационной системе по результатам анализа исходных данных	По результатам анализа исходных данных типовой информационной системе	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
			присваивается один из следующих классов: • класс 1 (К1) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных; • класс 2 (К2) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к средним негативным последствиям для субъектов персональных данных; • класс 3 (К3) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных; • класс 4 (К4) – системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.	
9.		Основные направления деятельности в области аудита безопасности информации	Основными направлениями деятельности в области аудита безопасности информации являются: 1. Аттестация объектов информатизации по требованиям безопасности информации. 2. Контроль защищенности информации ограниченного доступа. 3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН). 4. Проектирование объектов в защищенном исполнении	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
10.		Масштабы проведения аудита	Масштабы проведения аудита: 1. Аудит безопасности всей фирмы в комплексе. 2. Аудит безопасности отдельных зданий и помещений (выделенные помещения). 3. Аудит оборудования и технических средств конкретных типов и видов. 4. Аудит отдельных видов и направлений деятельности:	8
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем				
11.	Задание закрытого типа	Действия против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей – 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна	1	2
12.		Диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна	4	2
13.		Монитор обращений (по стандарту «Критерии оценки надежности компьютерных систем») должен обладать следующими качествами: 1. Изолированность 2. Полнота 3. Верифицируемость 4. Надежность 5. Безопасность 6. Подлинность	1, 2, 3	2
14.		Назовите средства радиоэлектронной борьбы 1. аппаратные средства 2. средства подавления связи 3. оперативные технические средства 4. средства борьбы с системами управления противника 5. программные средства 6. экономические средства	1, 2, 3	2
15.		В «Оранжевой книге» рассматривается несколько видов гарантированности 1. операционная 2. технологическая 3. информационная 4. техническая 5. безопасная	1, 2	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
		6. подлинная		
16.	Задание открытого типа	Аспекты ИБ в соответствии со стандартом BS 7799	Аспектами ИБ в соответствии со стандартом BS 7799 являются: • Политика безопасности. • Организация защиты. • Классификация и управление информационными ресурсами. • Управление персоналом. • Физическая безопасность. • Администрирование компьютерных систем и сетей. • Управление доступом к системам. • Разработка и сопровождение систем. • Планирование бесперебойной работы организации. • Проверка системы на соответствие требованиям ИБ.	3
17.		Какие тома должны входить в комплект документации надежной системы согласно "Оранжевой книге"?	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.	3
18.		Элементы, которые должна обязательно включать в себя политика безопасности согласно «Оранжевой книге»	Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы: • произвольное управление доступом; • безопасность повторного использования объектов; • метки безопасности; • принудительное управление доступом.	8
19.		Согласно «Оранжевой книге» дать определение политики безопасности	Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в мин)
			наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия	
20.		Согласно «Оранжевой книге» дать определение уровня гарантированности	Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.	2

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*	8 / 4	32	Указан в Moodle
2.	*Выполнение контрольной работы*	1 / 8	8	
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. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).

2. Политики безопасности компании при работе в Интернет [Электронный ресурс] / С.А. Петренко, В.А. Курбатов - М. : ДМК Пресс, 2018. - http://www.studentlibrary.ru/book/ISBN9785937000576.html.

3. Введение в программную инженерию [Электронный ресурс]: учебное пособие / Соловьев Н.А. - Оренбург: ОГУ, 2017. - http://www.studentlibrary.ru/book/ISBN9785741016855.html.

8.2. Дополнительная литература

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202572.html (ЭБС «Консультант студента»).

2. Интеллектуальные системы защиты информации : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785942756673.html (ЭБС «Консультант студента»).

3. Интеллектуальные интерактивные системы и технологии управления удаленным доступом (Методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intranet): Учебное пособие / Ботуз С.П. - 3-е изд., доп. - М. : СОЛОН-ПРЕСС, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785913591326.html (ЭБС «Консультант студента»).

4. Куприянова, А.И. Основы защиты информации: доп. УМО по образованию в области авиации, ракетостроения и космоса в качестве учеб.пособ. для студ., обуч. по спец. "Радиоэлектронные системы", "Средства радиоэлектронной борьбы" и "Информационные системы и технологии" / А. И. Куприянова, Сахаров, А.В., Шевцов, В.А. - - М. : Академия, 2008. - 256 с. (11 экз.)

5. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: Рек. УМО вузов по университетскому п/тех. образованию в качестве учеб. пособ. для вузов... по

специальности "Информатика и вычислительная техника" / П. Б. Хорев,. - М.: Акдемия, 2005. - 256 с. (69 экз.)

6. Садердинов, А.А. Информационная безопасность предприятия: Учеб. пособ. - 2-е изд. - М.: Дашков и К, 2005. - 336 с. (45 экз.)

7. Девянин, П.Н. Модели безопасности компьютерных систем : Доп. УМО объединением вузов по образованию в области информационной безопасности в качестве учеб. пособ. для вузов... по специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / П. Н. Девянин. - М. : Академия, 2005. - 144 с. (50 экз.)

4. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html (ЭБС «Консультант студента»).

8. Галатенко, В.А. Основы информационной безопасности : Курс лекций. Учебное пособие. Рек. для вузов ... по специальностям в области информационных технологий / В. А. Галатенко ; Под ред. В.Б. Бетелина. - Изд. 3-е. - М. : ИНТУИТ. РУ "Интернет-университет Информационных Технологий", 2004 - 264 с. (45 экз.)

5. Технологии борьбы с компьютерными вирусами. Практическое пособие. - М.: СОЛОН-ПРЕСС, 2009. - 352 с.: ил. - URL: http://www.studentlibrary.ru/book/ISBN9785913590596.html (ЭБС «Консультант студента»).

6. Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. - М. : Компания АйТи; ДМК Пресс. 2004. - 288 с.: ил. - (Информацион ные технологии для инженеров). URL: http://www.studentlibrary.ru/book/ISBN5940742483.html (ЭБС «Консультант студента»).

7. Марьенков А.Н., Лим В.Г., Обеспечение информационной безопасности вычислительных сетей: Учебно-методическое пособие для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» (учебно-методическое пособие). Сорокин Роман Васильевич, Астрахань, 2018. 72с. (5 экз).

8.3. Интернет-ресурсы, необходимые для освоения дисциплины

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).