Лебедева
Екатерина
Александровна

Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.23 11:52:42 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 ПРОГРАММНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

(индекс, наименование дисциплины в соответствии с учебным планом)

09.04.03 Прикладная информатика

(код, наименование направления подготовки/специальности)

Информационные технологии в государственном и муниципальном управлении

(наименование образовательной программы)

очная, заочная

(форма обучения)

Год набора – 2026

Нижний Новгород, 2026 г.

Автор(ы)-составитель(и) РПД:
Гребенюк Иван Иванович, канд.тех.наук., доцент, заведующий кафедрой информатики и информационных технологий Нижегородского института управления – филиала РАНХиГС

Цветкова Ирина Николаевна, доцент кафедры информатики и информационных технологий, канд.физ.-мат. наук, доцент

Заведующий кафедрой:

Гребенюк Иван Иванович, канд.тех.наук., доцент, заведующий кафедрой информатики и информационных технологий Нижегородского института управления – филиала РАНХиГС

РПД Б1.В.ДВ.03.02 «Программно-техническое обеспечение компьютерной безопасности» одобрена на заседании кафедры информатики и информационных технологий.

Протокол №16 от 11марта 2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

2. Объем и место дисциплины в структуре образовательной программы

3. Содержание и структура дисциплины

4. Типы оценочных материалов, показатели и критерии их оценивания

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

7. Методические материалы по освоению дисциплины

8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина Б1.В.ДВ.03.02 «Программно-техническое обеспечение компьютерной безопасности» обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС	**Код компетенции**	**Наименование Компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D)	ПК-6	Способен выбирать методологию и технологию проектирования ИС с учетом проектных рисков	ИПК-6.2	*Применяет методы оценки и управления рисками ИТ-проектов.*	*ИПК-6.2 З-1* ***Знает*** *содержание, цели, задачи и принципы разработки системы управления ИТ-рисками организации.* *ИПК-6.2 З-2* ***Знает*** *инструменты и методы управления ИТ-рисками. Например, качественные методы (преимущества и недостатки применения, использование в процедурах идентификации рисков, построения реестров рисков) и количественные методы оценки рисков.*

ОТФ/ТФ и реквизиты ПС	Код компетенции	Наименование Компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
					ИПК-6.2 З-3 ***Знает*** *современные концепции анализа и управления рисками в сфере информационных технологий.* *ИПК-6.2 У-1* ***Умеет*** *выбирать подходящий математический инструментарий для решения задач анализа и оценки ИТ-рисков, в том числе с использованием ЭВМ и прикладных программных продуктов.* *ИПК-6.2 У-2* ***Умеет*** *разрабатывать комплекс мероприятий по управлению рисками ИТ-проектов.* *ИПК-6.2 У-3* ***Умеет*** *использовать специализированное программно*

ОТФ/ТФ и реквизиты ПС	Код компетенции	Наименование Компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
					е обеспечение для проведения анализа ИТ-проектов и формирования планов и отчётности по управлению рисками.
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D); ТФ: • разработка инструментов и методов адаптации бизнес-процессов заказчика к возможностям ИС (D/09.7); • организационное и технологич	ПК-11	Способен проектировать архитектуру и сервисы информационных систем предприятий и организаций в прикладной области	ИПК-11.2	*Использует инструментарий проектирования архитектуры и сервисов ИС.*	*ИПК-11.2 З-1* ***Знает*** *программные средства и платформы инфраструктуры информационных технологий организаций, которые используются в проектировании ИС.* *ИПК-11.2 З-2* ***Знает*** *современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM).* *ИПК-11.2 З-3* ***Знает*** *моделирование как методологи*

ОТФ/ТФ и реквизиты ПС	Код компетенции	Наименование Компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
еское обеспечение разработки баз данных ИС (D/17.7).					*ческую основу проектирования ИС. Средства моделирования, виды моделей и методов моделирования.* *ИПК-11.2 У-1* ***Умеет*** *использовать инструментарий проектирования архитектуры и сервисов информационных систем (ИС).*
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D)	ПК-19	Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных информационных систем	ИПК-19.2	*Использует методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.*	*ИПК-19.2 З-1* ***Знает*** *компоненты концептуальной модели безопасности информации. Угрозы информации, источники угроз, способы их реализации и цели, а также меры защиты информации от неправомерных действий,*

ОТФ/ТФ и реквизиты ПС	Код компетенции	Наименование Компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
					приводящих к нанесению ущерба. *ИПК-19.2 З-2* ***Знает*** *основные направления защиты информации. Правовая, организационная и инженерно-техническая защиты как выразители комплексного подхода к обеспечению информационной безопасности.* *ИПК-19.2 У-1* ***Умеет*** *использовать методы моделирования для анализа значительного набора источников, объектов и действий, нарушающих безопасность.* *ИПК-19.2 У-2* ***Умеет*** *анализировать угрозы информационной*

ОТФ/ТФ и реквизиты ПС	Код компетенции	Наименование Компетенции	Код индикатора достижения компетенций	Наименование индикатора достижения компетенций	Образовательный результат
					безопасности. *ИПК-19.2 У-3* ***Умеет*** *постраивать комплексную систему организационных мер для выбранного государственного или муниципального учреждения (предприятия, организации).*

2. Объем и место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.03.02. «Программно-техническое обеспечение компьютерной безопасности» входит в число дисциплин по выбору части, формируемой участниками образовательных отношений в соответствии с учебным планом.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 академических часа / 54 астрономических часа.

Освоение дисциплины опирается на необходимый объем теоретических знаний и практических навыков в области информационной безопасности.

Дисциплины, на которых базируется данная дисциплина:

Математическое моделирование (Б1.О.02),

Математические и инструментальные методы поддержки принятия решений (Б1.О.03),

Управление внедрением IT-проектов (Б1.О.06),

Тенденции развития Web- пространства (Б1.О.07)

Дисциплины, для которых данная дисциплина является предшествующей:

Разработка баз знаний и экспертных систем (Б1.В.01.02),
Проектирование Web-сервисов информационных систем (Б1.В.01.04),
Правовые основы информационной безопасности (Б1.В.ДВ.04.02),
Научно-исследовательская работа (Б2.В.01(Н))

При ***очной форме обучения*** на контактную работу с преподавателем выделено 28 ч, в том числе на лекционные занятия – 8 ч, на практические (семинарские) занятия – 24 ч, – контактная работа на аттестацию в период экзаменационных сессий – 4 ч; на самостоятельную работу обучающихся выделено 44 ч.

При за***очной форме обучения*** на контактную работу с преподавателем выделено 12 ч, в том числе на лекционные занятия – 4 ч, на практические (семинарские) занятия – 8 ч; на самостоятельную работу обучающихся выделено 56 ч, контроль – 4 ч.

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная/заочная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Очная форма обучения														
Тема 1	Постановка задачи комплексного обеспечения ИБ АС	18	2			6							11	Опрос, контрольные задания с развернутым ответом
Тема 2	Методология формирования задач защиты; интеграция средств защиты в технологическую среду	18	2			6							11	Опрос, контрольные задания с развернутым ответом
Тема 3	Типовая структура КСИБ;	18	2			6							11	Опрос, контрольные задания с развернутым

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
	методы проектирования и оценки качества КСИБ														ответом
Тема 4	Этапы проектирования КСИБ и требования к ним	18	2			6								11	Опрос, контрольные задания с развернутым ответом
Промежуточная аттестация		4								4					зачет
Итого		**72**	**8**			**24**				**4**				**44**	
Заочная форма обучения															
Тема 1	Постановка задачи комплексного обеспечения ИБ АС	16	1			2								13	Опрос, контрольные задания с развернутым ответом

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 2	Методология формирования задач защиты; интеграция средств защиты в технологическую среду	18	1			2								15	Опрос, контрольные задания с развернутым ответом
Тема 3	Типовая структура КСИБ; методы проектирования и оценки качества КСИБ	18	1			2								15	Опрос, контрольные задания с развернутым ответом
Тема 4	Этапы проектирования КСИБ и требования к ним	16	1			2								13	Опрос, контрольные задания с развернутым ответом

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Промежуточная аттестация		4								4					зачет
Итого		**72**	**4**			**8**				**4**				**56**	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

Тема 1 Постановка задачи комплексного обеспечения ИБ АС. ИПК-6.2, ИПК-19.2

Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). Функциональные и обеспечивающие подсистемы, технология, управление. Законодательная, нормативно-методическая и научная базы разработки КСИБ. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС).

Тема 2 Методология формирования задач защиты; интеграция средств защиты в технологическую среду. ИПК-6.2, ИПК-19.2

Параллельная разработка АС и КСИБ. Системный подход к построению КСИБ. Архитектура защищенных АС. Соотношение программных, аппаратных и административных средств в комплексном обеспечении информационной безопасности АС. Разработка и содержание аварийного плана действий в случае нарушения ИБ АС.

Тема 3 Типовая структура КСИБ; методы проектирования и оценки качества КСИБ. ИПК-6.2, ИПК-19.2

Организация доступа к ресурсам АС. Система разграничения доступа к техническим средствам. Система разграничения доступа к программам и данным. Средства блокировки неправомочных действий субъектов. Задача интеграции средств защиты информации в технологическую среду АС. Требования к составу проектной и эксплуатационной документации. Порядок подготовки и проведения аттестации АС. Сертификация программного обеспечения (ПО).

Тема 4 Этапы проектирования КСИБ и требования к ним. ИПК-6.2, ИПК-11.2, ИПК-19.2

Предпроектное обследование: инвентаризация ресурсов. Предпроектное обследование: модели угроз и нарушителя. Предпроектное обследование: анализ рисков. Техническое задание. Техническое и рабочее проектирование. Испытания и внедрение в эксплуатацию, сопровождение. Оценка эффективности. Особенности проектирования на современном уровне и синтез КСИБ.

Автоматизация процесса анализа и управления рисками (с помощью пакета Digital Security Гриф). Моделирование процедуры. Разработка контрмер. Экономическая оценка затрат на защиту информации.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.ДВ.03.02 «Программно-техническое обеспечение компьютерной безопасности» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям)

образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
вариантов предложенных		вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
		ответа (например, 4 текст обоснования).	
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины Б1.В.ДВ.03.02 «Программно-техническое обеспечение компьютерной безопасности» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам): *опрос, контрольное задание открытого типа с развернутым ответом*.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Тема 1 Постановка задачи комплексного обеспечения ИБ АС. ИПК-6.2, ИПК-19.2

Вопросы опроса

№	Вопрос	Ответ
1	Что понимается под информационной безопасностью автоматизированной системы? Как это определение связано с защитой компонентов АС (технических средств, ПО, данных, персонала)?	
2	Какие основные цели обеспечения информационной безопасности АС? Приведите примеры ущерба, который может быть нанесён при нарушении работы АС или целостности информации.	
3	Перечислите ключевые компоненты автоматизированной системы. Как каждый из них влияет на уровень её защищённости?	
4	Что означает комплексный подход к обеспечению ИБ АС? В чём его отличие от фрагментарного подхода? Приведите примеры ситуаций, где комплексный подход особенно важен.	

<u>Контрольные задания с развернутым ответом</u>

ПРАКТИЧЕСКАЯ РАБОТА №1

Разработка технико-экономического обоснования на создания комплексной системы обеспечения информационной безопасности автоматизированных систем.

Цель работы: получить навыки разработки технико-экономического обоснования на создания комплексной системы обеспечения информационной безопасности автоматизированных систем.

Задание

1. Выполнить анализ деятельность предложенного объекта:

- защиты конфиденциальной информации вуза
- защиты конфиденциальной информации администрации Советского района г. Нижний Новгород
- защиты конфиденциальной информации администрации Кстовского района Нижегородской обл.;
- защиты конфиденциальной информации департамента культуры г. Нижний Новгород;
- защиты конфиденциальной информации Министерства имущественных и земельных отношений Нижегородской области
- защиты конфиденциальной информации Территориального органа Федеральной службы государственной статистики по Нижегородской области (Нижегородстат)
- защиты конфиденциальной информации Министерства образования и науки Нижегородской области
- защиты конфиденциальной информации Приволжского таможенного управления;
- защиты конфиденциальной информации Управления Федеральной службы государственной регистрации, кадастра и картографии по Нижегородской области
- защиты конфиденциальной информации Администрации Волжского бассейна внутренних водных путей, ФБУ в Нижнем Новгороде;
- защиты конфиденциальной информации Архива г. Нижнего Новгорода;
- защиты конфиденциальной информации Верхне-Волжского управления по гидрометеорологии и мониторингу окружающей среды в Нижнем Новгороде;
- защиты конфиденциальной информации Государственной жилищной инспекции Нижегородской области;
- защиты конфиденциальной информации Государственной инспекции труда в Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Департамента лесного хозяйства по ПФО в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции Федеральной налоговой службы России по Автозаводскому району в Нижнем Новгороде (;
- защиты конфиденциальной информации Инспекции государственного строительного надзора Нижегородской области в Нижнем Новгороде;

- защиты конфиденциальной информации Нагорного районного отдела занятости населения в Нижнем Новгороде.

2. ***Подготовить исходные данные для технико-экономического обоснования***.

3. *Определить объемы и состав работ, подготовить сметы и сроков их выполнения.*

Тема 2 Методология формирования задач защиты; интеграция средств защиты в технологическую среду. ИПК-6.2, ИПК-19.2

Вопросы опроса

№	Вопрос	Ответ
1	Что такое системный подход в контексте построения систем защиты информации? Как он применяется для оценки рисков и уязвимостей?	
2	Перечислите этапы анализа взаимодействия элементов безопасности при системном подходе. Как связаны между собой угроза, уязвимость, актив, риск, ущерб и контрмеры?	
3	Какие критерии используются при выборе средств защиты информации? Как соотносятся стоимость средств защиты и возможный ущерб от реализации угроз?	
4	Что такое модель нарушителя в контексте информационной безопасности? Какие параметры необходимо учитывать при её конкретизации и расширении?	
5	Какие методы	

№	Вопрос	Ответ
	моделирования используются для анализа угроз и систем защиты? В чём заключается проблема адекватности модели?	

<u>Контрольные задания с развернутым ответом</u>

ПРАКТИЧЕСКАЯ РАБОТА №2

Формирование требований по обеспечению безопасности конфиденциальной информации

Цель работы: получить практические умения формирования требований по обеспечению безопасности конфиденциальной безопасности.

Задание

1. Сформулировать угрозы безопасности для предложенного объекта:

- защиты конфиденциальной информации вуза;
- защиты конфиденциальной информации администрации Советского района г. Нижний Новгород;
- защиты конфиденциальной информации администрации Кстовского района Нижегородской обл.;
- защиты конфиденциальной информации департамента культуры г. Нижний Новгород;
- защиты конфиденциальной информации Министерства имущественных и земельных отношений Нижегородской области;
- защиты конфиденциальной информации Территориального органа Федеральной службы государственной статистики по Нижегородской области (Нижегородстат);
- защиты конфиденциальной информации Министерства образования и науки Нижегородской области;
- защиты конфиденциальной информации Приволжского таможенного управления;
- защиты конфиденциальной информации Управления Федеральной службы государственной регистрации, кадастра и картографии по Нижегородской области;
- защиты конфиденциальной информации Администрации Волжского бассейна внутренних водных путей, ФБУ в Нижнем Новгороде;
- защиты конфиденциальной информации Архива г. Нижнего Новгорода;

- защиты конфиденциальной информации Верхне-Волжского управления по гидрометеорологии и мониторингу окружающей среды в Нижнем Новгороде;
- защиты конфиденциальной информации Государственной жилищной инспекции Нижегородской области;
- защиты конфиденциальной информации Государственной инспекции труда в Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Департамента лесного хозяйства по ПФО в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции Федеральной налоговой службы России по Автозаводскому району в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции государственного строительного надзора Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Нагорного районного отдела занятости населения в Нижнем Новгороде.

2. ***Сформулировать требования по обеспечению безопасности конфиденциальной безопасности***.

Тема 3 Типовая структура КСИБ; методы проектирования и оценки качества КСИБ. ИПК-6.2, ИПК-19.2

Вопросы опроса

№	Вопрос	Ответ
1	**Что включает типовая структура КСИБ?** Перечислите основные компоненты КСИБ (например, подсистемы защиты информации, управления доступом, мониторинга и т. д.). Как соотносятся функциональные и обеспечивающие подсистемы в структуре КСИБ?	
2	**Какие подсистемы обычно входят в техническую составляющую КСИБ?** Приведите примеры подсистем, таких как	

№	Вопрос	Ответ
	антивирусная защита, резервное копирование, защита электронной почты, системы обнаружения атак и др.. Как эти подсистемы взаимодействуют между собой?	
3	**Что представляет собой организационно-распорядительная составляющая КСИБ?** Какие документы входят в её состав (политика безопасности, инструкции, должностные обязанности и т. д.)? Какова роль этих документов в обеспечении информационной безопасности?	
4	**Перечислите этапы проектирования КСИБ.** Охарактеризуйте каждый этап: предпроектное обследование, разработка технического задания, техническое и рабочее проектирование, испытания, внедрение в эксплуатацию, сопровождение. Что происходит на каждом из этих этапов?	

<u>Контрольные задания с развернутым ответом</u>

ПРАКТИЧЕСКАЯ РАБОТА №3

Разработка и утверждение технического задания на создание комплексной системы обеспечения информационной безопасности.

Цель работы: получить навыки разработки и использования технического задания на создание комплексной системы обеспечения информационной безопасности.

Задание

1. Изучить нормативные документы, на основе которых выполняется построение технического задания.

2. Разработать техническое задание на создание комплексной системы обеспечения информационной безопасности для предложенного объекта:

- защиты конфиденциальной информации вуза;
- защиты конфиденциальной информации администрации Советского района г. Нижний Новгород;
- защиты конфиденциальной информации администрации Кстовского района Нижегородской обл.;
- защиты конфиденциальной информации департамента культуры г. Нижний Новгород;
- защиты конфиденциальной информации Министерства имущественных и земельных отношений Нижегородской области;
- защиты конфиденциальной информации Территориального органа Федеральной службы государственной статистики по Нижегородской области (Нижегородстат);
- защиты конфиденциальной информации Министерства образования и науки Нижегородской области;
- защиты конфиденциальной информации Приволжского таможенного управления;
- защиты конфиденциальной информации Управления Федеральной службы государственной регистрации, кадастра и картографии по Нижегородской области;
- защиты конфиденциальной информации Администрации Волжского бассейна внутренних водных путей, ФБУ в Нижнем Новгороде;
- защиты конфиденциальной информации Архива г. Нижнего Новгорода;
- защиты конфиденциальной информации Верхне-Волжского управления по гидрометеорологии и мониторингу окружающей среды в Нижнем Новгороде;
- защиты конфиденциальной информации Государственной жилищной инспекции Нижегородской области;
- защиты конфиденциальной информации Государственной инспекции труда в Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Департамента лесного хозяйства по ПФО в Нижнем Новгороде;

- защиты конфиденциальной информации Инспекции Федеральной налоговой службы России по Автозаводскому району в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции государственного строительного надзора Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Нагорного районного отдела занятости населения в Нижнем Новгороде.

3. Оформить титульный лист с указанием лиц, утверждающих техническое задание.

ПРАКТИЧЕСКАЯ РАБОТА №4
Проектировании комплексной системы обеспечения информационной без опасности от несанкционированного доступа

Цель работы: получить навыки проектировании комплексной системы обеспечения информационной безопасности от несанкционированного доступа

Задание

1. ***Построить диаграмму функционирования комплексной системы обеспечения информационной безопасности от несанкционированного доступа для предложенного объекта:***

- защиты конфиденциальной информации вуза;
- защиты конфиденциальной информации администрации Советского района г. Нижний Новгород;
- защиты конфиденциальной информации администрации Кстовского района Нижегородской обл.;
- защиты конфиденциальной информации департамента культуры г. Нижний Новгород;
- защиты конфиденциальной информации Министерства имущественных и земельных отношений Нижегородской области;
- защиты конфиденциальной информации Территориального органа Федеральной службы государственной статистики по Нижегородской области (Нижегородстат);
- защиты конфиденциальной информации Министерства образования и науки Нижегородской области;
- защиты конфиденциальной информации Приволжского таможенного управления;
- защиты конфиденциальной информации Управления Федеральной службы государственной регистрации, кадастра и картографии по Нижегородской области;
- защиты конфиденциальной информации Администрации Волжского бассейна внутренних водных путей, ФБУ в Нижнем Новгороде;

- защиты конфиденциальной информации Архива г. Нижнего Новгорода;
- защиты конфиденциальной информации Верхне-Волжского управления по гидрометеорологии и мониторингу окружающей среды в Нижнем Новгороде;
- защиты конфиденциальной информации Государственной жилищной инспекции Нижегородской области;
- защиты конфиденциальной информации Государственной инспекции труда в Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Департамента лесного хозяйства по ПФО в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции Федеральной налоговой службы России по Автозаводскому району в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции государственного строительного надзора Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Нагорного районного отдела занятости населения в Нижнем Новгороде.

2. ***Построить диаграммы прецедентов, состояний, взаимодействия на языке UML для проекта комплексной системы обеспечения информационной безопасности от несанкционированного доступа.***

Тема 4 Этапы проектирования КСИБ и требования к ним. ИПК-6.2, ИПК-11.2, ИПК-19.2

Вопросы опроса

№	Вопрос	Ответ
1	Перечислите основные этапы проектирования комплексной системы информационной безопасности (КСИБ). Охарактеризуйте каждый этап, указав его цели и ключевые задачи.	
2	Какие подготовительные мероприятия проводятся перед началом проектирования КСИБ? В чём заключается предпроектное обследование и почему	

№	Вопрос	Ответ
	оно важно?	
3	Что включает в себя технико-экономическое обоснование (ТЭО) при проектировании КСИБ? Какие параметры в нём рассчитываются и кто участвует в его согласовании?	
4	Опишите процесс разработки технического задания (ТЗ) для КСИБ. Какие требования должны быть учтены в ТЗ, и по каким стандартам оно формулируется?	
5	Какие варианты решений предлагаются на этапе технического проектирования КСИБ? Как происходит выбор оптимального варианта и обоснование его эффективности?	

<u>Контрольные задания с развернутым ответом</u>

ПРАКТИЧЕСКАЯ РАБОТА №5

Разработка блочная архитектуры комплексной система обеспечения информационной безопасности

Цель работы: получить навыки разработки блочная архитектуры комплексной система обеспечения информационной безопасности

Задание

1. ***Для комплексной системы обеспечения информационной безопасности для предложенного объекта:***

- защиты конфиденциальной информации вуза;
- защиты конфиденциальной информации администрации Советского района г. Нижний Новгород;
- защиты конфиденциальной информации администрации Кстовского района Нижегородской обл.;
- защиты конфиденциальной информации департамента культуры г. Нижний Новгород;

- защиты конфиденциальной информации Министерства имущественных и земельных отношений Нижегородской области;
- защиты конфиденциальной информации Территориального органа Федеральной службы государственной статистики по Нижегородской области (Нижегородстат);
- защиты конфиденциальной информации Министерства образования и науки Нижегородской области;
- защиты конфиденциальной информации Приволжского таможенного управления;
- защиты конфиденциальной информации Управления Федеральной службы государственной регистрации, кадастра и картографии по Нижегородской области;
- защиты конфиденциальной информации Администрации Волжского бассейна внутренних водных путей, ФБУ в Нижнем Новгороде;
- защиты конфиденциальной информации Архива г. Нижнего Новгорода;
- защиты конфиденциальной информации Верхне-Волжского управления по гидрометеорологии и мониторингу окружающей среды в Нижнем Новгороде;
- защиты конфиденциальной информации Государственной жилищной инспекции Нижегородской области;
- защиты конфиденциальной информации Государственной инспекции труда в Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Департамента лесного хозяйства по ПФО в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции Федеральной налоговой службы России по Автозаводскому району в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции государственного строительного надзора Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Нагорного районного отдела занятости населения в Нижнем Новгороде

выполнить разработку блочной архитектуры.

2. Выполнить детализацию для каждого блока.

ПРАКТИЧЕСКАЯ РАБОТА №6

Моделирование угроз информационной безопасности и защиты

Цель работы: получить навыки моделирования угроз информационной безопасности

Задание 1.

1. Выполнить. разработку частной модели угроз и модели нарушителя информационной безопасности для предложенного объекта:

- защиты конфиденциальной информации вуза;
- защиты конфиденциальной информации администрации Советского района г. Нижний Новгород;
- защиты конфиденциальной информации администрации Кстовского района Нижегородской обл.;
- защиты конфиденциальной информации департамента культуры г. Нижний Новгород;
- защиты конфиденциальной информации Министерства имущественных и земельных отношений Нижегородской области;
- защиты конфиденциальной информации Территориального органа Федеральной службы государственной статистики по Нижегородской области (Нижегородстат);
- защиты конфиденциальной информации Министерства образования и науки Нижегородской области;
- защиты конфиденциальной информации Приволжского таможенного управления;
- защиты конфиденциальной информации Управления Федеральной службы государственной регистрации, кадастра и картографии по Нижегородской области;
- защиты конфиденциальной информации Администрации Волжского бассейна внутренних водных путей, ФБУ в Нижнем Новгороде;
- защиты конфиденциальной информации Архива г. Нижнего Новгорода;
- защиты конфиденциальной информации Верхне-Волжского управления по гидрометеорологии и мониторингу окружающей среды в Нижнем Новгороде;
- защиты конфиденциальной информации Государственной жилищной инспекции Нижегородской области;
- защиты конфиденциальной информации Государственной инспекции труда в Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Департамента лесного хозяйства по ПФО в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции Федеральной налоговой службы России по Автозаводскому району в Нижнем Новгороде;
- защиты конфиденциальной информации Инспекции государственного строительного надзора Нижегородской области в Нижнем Новгороде;
- защиты конфиденциальной информации Нагорного районного отдела занятости населения в Нижнем Новгороде.

2. Выбрать и обосновать выбор методики построения модели угроз.

3. Построить модель угроз в соответствии с выбранной методикой.

***4. Разработать алгоритм для реализации модели угроз*.**

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,3	30
КТ 2	100	0,3	30
Итого:	х	0,6	60

Формула расчета результата контрольной точки:
Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ – 1.

Тема 1 и2

Опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1	Какие методы и средства используются для обеспечения ИБ АС? Классифицируйте их (например, по типу: правовые, организационные, технические, криптографические и т. д.).
2	Что такое модель угроз безопасности информации? Как она формируется и для чего используется при проектировании системы защиты АС?

№ п.п.	Содержание вопроса
3	Какие нормативные правовые акты регулируют вопросы защиты информации в АС в России? Приведите 2–3 примера и кратко охарактеризуйте их значение.
4	Что включает в себя процесс управления информационной безопасностью? Опишите основные этапы циклического процесса управления ИБ.
5	Какие подсистемы могут входить в состав комплексной системы обеспечения ИБ АС? Приведите примеры и поясните их функции.
6	Что такое интегрированная система безопасности (ИСБ)? Перечислите её ключевые компоненты и принципы построения.
7	Какие типы интеграции систем безопасности существуют? Сравните аппаратную, программную и программно-аппаратную интеграцию, укажите их преимущества и недостатки.
8	Какие уровни интеграции могут быть в ИСБ? Охарактеризуйте каждый уровень (например, клиент-сервер, локальный, адресно-серверный, продвинутый).
9	Какие задачи решает ИСБ? Как интеграция систем безопасности влияет на эффективность защиты объекта?
10	Какие требования предъявляются к программному обеспечению для ИСБ? Почему важна масштабируемость и гибкость ПО?

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; технически излагает материал.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко

Диапазон баллов	Описание критерия
	и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

КТ – 2.

Тема 3 и 4

Опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	**Какие методы используются для выявления угроз при проектировании КСИБ?** Как проводится анализ уязвимостей объекта и существующей системы безопасности? Что такое модель угроз и как она используется в проектировании КСИБ?
2.	**Какие методы моделирования применяются при проектировании КСИБ?** Как моделирование помогает в проектировании систем информационной безопасности? Приведите примеры использования математических моделей или симуляций.
3.	**Перечислите методы оценки качества КСИБ.** Охарактеризуйте количественные методы (например, метод оценки риска Фишера, метод оценки уязвимости информации Хофмана). Опишите качественные методы, включая метод экспертных структурных вопросников.
4.	Что такое уязвимость в контексте информационной безопасности? Как оценивается уязвимость информации и системы в целом? Приведите примеры уязвимостей, которые могут быть обнаружены при оценке КСИБ.
5.	Что происходит на этапе рабочего проектирования? Какие документы разрабатываются, и почему проектная документация на этом этапе относится к информации повышенной степени конфиденциальности?
6.	Какие этапы следуют после разработки проекта КСИБ? Охарактеризуйте процессы внедрения, стыковки элементов системы, опытной эксплуатации и приёмочных испытаний.
7.	Какие требования предъявляются к КСИБ с точки зрения

№ п.п.	Содержание вопроса
	нормативно-правовой базы? Назовите ключевые ГОСТы и другие документы, регулирующие проектирование и внедрение КСИБ.
8.	Какие требования предъявляются к обеспечению информационной безопасности в автоматизированных системах (АСУ ТП)? Перечислите основные задачи и функции КСИБ для таких систем.
9.	Какие компоненты должны включаться в КСИБ при её разработке? Охарактеризуйте подсистемы физической защиты, защиты от утечки по техническим каналам, программно-аппаратной и организационно-правовой защиты информации.

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; технически правильно излагает материал.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Обучающемуся разрешается использование компьютера с установленными прикладными программными продуктами

.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме зачета

6.2. Типовые оценочные материалы промежуточной аттестации.

Тема 1 Постановка задачи комплексного обеспечения ИБ АС. ИПК-6.2, ИПК-19.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос	Ответ
1.	Что понимается под комплексной системой обеспечения информационной безопасности (КСИБ)? Перечислите её ключевые компоненты и цели.	
2.	Какие этапы включает процесс постановки задачи комплексного обеспечения ИБ АС? Охарактеризуйте каждый этап.	
3	Какие методы и инструменты используются для анализа угроз информационной безопасности в автоматизированных системах? Приведите примеры.	
4	Что такое политика информационной безопасности? Опишите её роль в проектировании КСИБ и основные элементы, которые она должна включать.	
5	Какие нормативные документы регулируют обеспечение информационной безопасности	

№ п.п.	Вопрос	Ответ
	в России? Назовите ключевые законы и стандарты, влияющие на проектирование КСИБ.	
6	Чем отличаются организационные, технические и правовые меры обеспечения ИБ? Приведите примеры каждого типа мер.	
7	Что такое риск информационной безопасности? Объясните процесс оценки рисков и методы их минимизации.	

1.2. Контрольные задания с ключами правильных ответов.

Задание 1. Анализ объекта защиты.

Выберите тип организации (например, банк, больница, промышленное предприятие). Определите объекты защиты в АС этой организации, включая информационные ресурсы, технические средства, персонал. Классифицируйте информацию по уровням конфиденциальности.

Задание 2. Построение модели угроз.

Для выбранного объекта из предыдущего задания идентифицируйте потенциальные угрозы ИБ (внешние и внутренние). Для каждой угрозы оцените вероятность возникновения и возможный ущерб. Сформируйте модель угроз с указанием уязвимостей и потенциальных нарушителей.

Задание 3. Разработка политики безопасности.

Составьте краткую политику информационной безопасности для небольшой компании. Включите разделы о целях, области действия, ролях и обязанностях сотрудников, основных мерах защиты.

Задание 4. Выбор средств защиты.

Подберите программно-аппаратные средства для защиты АС от выявленных угроз (например, межсетевые экраны, системы обнаружения вторжений, антивирусное ПО). Обоснуйте выбор с учётом специфики организации.

2. Задания закрытого типа.

2.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Что понимается под информационной безопасностью автоматизированной системы?

а) Защита системы и всех её составляющих от преднамеренного или непреднамеренного нежелательного воздействия.

б) Обеспечение доступности информации для всех пользователей.

в) Использование исключительно криптографических методов защиты.

г) Регулярное обновление программного обеспечения.

2. Какие ключевые компоненты включает автоматизированная система?

а) Технические средства, программное обеспечение, специалисты, информация.

б) Только технические средства и программное обеспечение.

в) Только информация и специалисты.

г) Сетевые протоколы и базы данных.

3. Какова основная цель обеспечения безопасности автоматизированной системы?

а) Защита участников информационного взаимодействия от ущерба, который они могут понести в результате вмешательства в работу системы или воздействия на информацию.

б) Обеспечение бесперебойной работы системы.

в) Предотвращение утечек данных.

г) Соблюдение нормативных требований.

4. Что относится к задачам системы обеспечения информационной безопасности АС?

а) Защита от вмешательства посторонних лиц, разграничение доступа пользователей, регистрация действий пользователей, контроль целостности среды исполнения программ, защита от несанкционированной модификации программных средств, защита информации от утечки и разглашения, аутентификация пользователей, оперативное реагирование на угрозы.

б) Только защита от хакерских атак.

в) Только контроль доступа к данным.

г) Только обеспечение физической безопасности помещений.

5. Какой подход рекомендуется применять для поддержания информационной безопасности в надлежащем состоянии?

а) Комплексный подход, который объединяет разнородные методы и средства защиты и предполагает внедрение менеджмента информационной безопасности.

б) Фрагментарный подход с выборочным внедрением мер защиты.

в) Опора исключительно на технические средства защиты.

г) Использование только правовых методов регулирования.

6. Что включает формирование требований к защите информации в автоматизированной системе управления?

а) Анализ целей создания АС, определение критически важной информации, оценку возможных последствий её нарушения, анализ нормативных актов, классификацию АС по требованиям защиты информации, определение угроз безопасности и разработку модели угроз.

б) Только установку антивирусного ПО.

в) Только разработку политики информационной безопасности.

г) Исключительно настройку сетевых фильтров.

7. Какие стандарты регулируют создание автоматизированных систем в защищённом исполнении в России?

а) ГОСТ Р 51583, ГОСТ Р 51624, ГОСТ Р ИСО/МЭК 27000 и другие.

б) Только международные стандарты ISO.

в) Только стандарты, разработанные ФСБ России.

г) Стандарты, регулирующие только физическую безопасность.

8. Что такое комплексная система обеспечения информационной безопасности (КСОИ)?

а) Система, которая отвечает на все вопросы регуляторов и включает организационное, лингвистическое, математическое, программное, техническое, информационное и нормативное обеспечение.

б) Набор отдельных технических средств защиты.

в) Только организационные меры по защите информации.

г) Система, ориентированная исключительно на защиту от внешних угроз.

9. Что включает этап планирования при внедрении системы менеджмента информационной безопасности (СМИБ)?

а) Формирование политики информационной безопасности, определение области действия СМИБ, оценка рисков ИБ, выбор и формирование планов реализации защитных мер.

б) Только закупку технических средств защиты.

в) Исключительно обучение персонала.

г) Только мониторинг текущих угроз.

10. Что такое модель угроз безопасности информации?

а) Документ, который описывает потенциальные угрозы, их источники, способы реализации и возможные последствия для АС.

б) Список всех возможных технических сбоев системы.

в) План действий при возникновении инцидента.

г) Документ, регулирующий доступ к информации.

Тема 2 Методология формирования задач защиты; интеграция средств защиты в технологическую среду. ИПК-6.2, ИПК-19.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос	Ответ
1.	Объясните суть системного подхода к построению системы защиты информации. Как он учитывает взаимодействие элементов безопасности, внешней среды и объекта оценки? Приведите пример последовательности анализа рисков в рамках этого подхода.	
2.	Что такое модель угроз информационной безопасности? Перечислите её основные задачи и этапы создания. Как модель угроз помогает в разработке мер безопасности?	
3	Сравните неформальный (описательный) и формальный подходы к построению защищённых систем. В чём заключается их суть и какие преимущества/недостатки у каждого из них?	
4	Какие критерии используются при выборе средств защиты информации? Как соотносятся эффективность и стоимость средств защиты при их внедрении?	
5	Опишите принципы проектирования интегрированных систем безопасности (ИСБ).	

1.2. Контрольные задания с ключами правильных ответов.

Задание 1.

Представьте, что вам нужно защитить информационную систему компании. Сформулируйте перечень потенциальных угроз, используя модель STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Для каждой угрозы предложите меру противодействия.

Задание 2.

Рассмотрите ситуацию сближения ИТ и АСУ ТП. Какие архитектурные риски могут возникнуть при таком сопряжении? Приведите примеры и предложите меры по их минимизации.

Задание 3.

Вам поручено интегрировать систему контроля и управления доступом (СКУД) с системой противоаварийной защиты (ПАЗ) на промышленном объекте. Опишите, какие функции должна выполнять такая интеграция и какие технические решения могут быть использованы.

Задание 4.

Проведите анализ уязвимостей гипотетической информационной системы. Используйте методы внешнего и внутреннего сканирования. Представьте результаты в виде таблицы с указанием типа уязвимости, её критичности и рекомендаций по устранению.

Задание 5.

Разработайте план митигирующих мероприятий для защиты от DDoS-атак. Укажите ответственные лица, сроки реализации и ожидаемый результат.

2. Задания закрытого типа.

2.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Что является первым этапом при формировании задач защиты информации?

A) Выбор конкретных средств защиты.

B) Анализ угроз и рисков.

C) Внедрение системы мониторинга.

D) Обучение персонала.

2. Какой принцип предполагает, что защита должна охватывать все компоненты информационной системы?

A) Принцип избыточности.

B) Принцип эшелонированной обороны.

C) Принцип минимальной необходимости.

D) Принцип максимальной доступности.

3. Что означает интеграция средств защиты в технологическую среду?

A) Установка всех защитных механизмов в одном месте.

B) Обеспечение совместимости и взаимодействия средств защиты с существующей инфраструктурой.

C) Полное замещение существующей инфраструктуры новыми защитными решениями.

D) Использование только аппаратных средств защиты.

4. Какой документ определяет цели, задачи и основные подходы к защите информации в организации?

A) Инструкция по эксплуатации оборудования.

B) Политика информационной безопасности.

C) Должностная инструкция администратора.

D) Отчёт о проведённом аудите.

5. Что такое «модель угроз» в контексте информационной безопасности?

A) Список всех возможных технических сбоев в системе.

B) Описание потенциальных угроз, их источников и способов реализации.

C) План действий при возникновении чрезвычайной ситуации.

D) Перечень сотрудников, имеющих доступ к информации.

6. Какой метод позволяет оценить эффективность внедряемых средств защиты?

A) Увеличение количества установленных антивирусов.

B) Проведение тестирования на проникновение (пентеста).

C) Сокращение числа пользователей с правами доступа.

D) Замена всех устаревших компьютеров.

7. Что подразумевается под «непрерывностью защиты»?

A) Защита работает только в рабочее время.

B) Защитные меры действуют постоянно, без перерывов.

C) Защита активируется только при обнаружении угрозы.

D) Защитные механизмы обновляются раз в год.

8. Какой подход предполагает распределение защитных механизмов по разным уровням системы?

A) Централизованный подход.

B) Эшелонированный подход.

C) Локальный подход.

D) Временный подход.

9. Что необходимо сделать перед внедрением новых средств защиты?

A) Провести пилотное тестирование в ограниченной среде.

B) Сразу развернуть на всех рабочих станциях.

C) Отключить все старые защитные механизмы.

D) Ничего не делать, оставить как есть.

10. Какой фактор является ключевым при выборе средств защит ы для конкретной технологической среды?

A) Минимальная цена решения.

B) Совместимость с существующей инфраструктурой и бизнес-проц ессами.

C) Наличие максимального количества функций.

D) Популярность бренда на рынке.

Тема 3 Типовая структура КСИБ; методы проектирования и оценки качества КСИБ. ИПК-6.2, ИПК-19.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос	Ответ
1.	**Какие критерии используются для оценки эффективности КСИБ?** Перечислите ключевые показатели, такие как функциональность, надёжность, устойчивость к внешним угрозам, соответствие нормативным требованиям. Как эти критерии измеряются?	
2.	**Как проводится аттестация КСИБ по требованиям безопасности?** Что включает процесс аттестации? Какие документы и процедуры требуются для успешной аттестации?	
3	**Какие проблемы могут возникнуть при оценке качества КСИБ и как их решать?** Перечислите типичные сложности (например, субъективность экспертных	

№ п.п.	Вопрос	Ответ
	оценок, недостаток данных для статистического анализа). Предложите способы минимизации этих проблем.	
4	**Как технологии влияют на проектирование и оценку КСИБ?** Приведите примеры современных технологий, которые используются в КСИБ (например, машинное обучение, блокчейн, квантовые вычисления). Как эти технологии меняют подходы к проектированию и оценке систем информационной безопасности?	

1.2. Контрольные задания с ключами правильных ответов.

Задание 1.

Проанализируйте существующую систему безопасности в организации (реальной или гипотетической). Выявите слабые места и предложите улучшения с учётом современных методов проектирования и оценки качества КСИБ.

Задание 2.

Составьте техническое задание на разработку КСИБ для объекта определённого типа (например, для банка или промышленного предприятия), включив ключевые требования к системе.

2. Задания закрытого типа.

2.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать верный ответ.

1. ***Какие подсистемы обычно входят в состав КСИБ?***

a) Подсистема антивирусной защиты.

b) Подсистема резервного копирования и архивирования.

c) Подсистема защиты электронной почты.

d) Подсистема обнаружения атак.

e) Подсистема управления доступом (идентификации и аутентификации пользователей).

f) Подсистема регистрации и учёта.

g) Подсистема обеспечения целостности.

h) Подсистема защиты информации в ЛВС.

2. ***Какие компоненты относятся к организационно-распорядительной составляющей КСИБ?***

a) Политика информационной безопасности.

b) Организационно-распорядительные документы (приказы, инструкции).

c) Должностные инструкции и эксплуатационная документация средств защиты информации.

3. ***Какие элементы включает техническая составляющая КСИБ?***

a) Средства защиты информации (межсетевые экраны, системы обнаружения вторжений и т. д.).

b) Системы мониторинга и аудита событий ИБ.

c) Средства управления доступом и идентификации пользователей.

d) Средства защиты каналов передачи данных

Тест 2.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать верный ответ.

1. ***Какие этапы включает проектирование КСИБ?***

a) Предпроектное обследование.

b) Разработка технического задания.

c) Техническое проектирование.

d) Рабочее проектирование.

e) Испытания и внедрение в эксплуатацию.

f) Сопровождение.

2. ***Что включает этап предпроектного обследования?***

a) Аудит информационной безопасности объекта.

b) Анализ текущих угроз и уязвимостей.

c) Оценка существующих мер защиты.

d) Формирование модели угроз.

3. ***Какие факторы необходимо учитывать при выборе технических средств для КСИБ?***

a) Совместимость с информационными технологиями и техническими средствами объекта.

b) Класс защищённости информационной системы.

c) Стоимость и эффективность средств защиты.

d) Наличие сертификатов соответствия требованиям безопасности информации.

4. ***Какие методы используются для моделирования КСИБ на этапе проектирования?***

a) Математическое моделирование.

b) Построение графов атак и уязвимостей.

c) Использование виртуальных моделей объектов для размещения средств защиты.

Тест 3.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать верный ответ.

1. ***Какие методы оценки качества КСИБ упоминаются в литературе?***

a) Метод нормативного функционального наполнения.

b) Метод экспертных структурных вопросников.

c) Метод оценки уязвимости информации Хоффмана.

d) Метод оценки риска Фишера.

2. ***Что включает оценка риска в контексте КСИБ?***

a) Идентификация угроз.

b) Оценка вероятности их реализации.

c) Оценка потенциального ущерба от реализации угроз.

d) Разработка мер по снижению рисков.

3. ***Какие критерии используются для комплексной оценки защищённости информации?***

a) Уровень соответствия нормативным требованиям.

b) Эффективность средств защиты.

c) Надёжность систем мониторинга и аудита.

d) Уровень подготовки персонала в области ИБ.

Тема 4 Этапы проектирования КСИБ и требования к ним. ИПК-6.2, ИПК-11.2, ИПК-19.2

1. Задания открытого типа.

1.1. Вопросы открытого типа.

№ п.п.	Вопрос	Ответ
1.	Какие требования предъявляются к мониторингу и контролю функционирования КСИБ? Как осуществляется	

№ п.п.	Вопрос	Ответ
	регистрация инцидентов, анализ журналов учёта действий пользователей и обеспечение реагирования на сигналы угроз?	
2.	Какие факторы необходимо учитывать при проектировании КСИБ для объектов критической информационной инфраструктуры (КИИ)? Как происходит категорирование таких объектов?	
3	Какие требования предъявляются к средствам защиты информации, используемым в КСИБ? Как происходит их выбор с учётом класса защищённости системы, совместимости с информационными технологиями и другими параметрами?	
4	Какие меры должны предусматриваться для сопровождения и эксплуатации КСИБ после внедрения? В чём заключается регулярное обслуживание, обновление ПО, сертификация средств защиты и другие аспекты эксплуатации?	
5	Какие риски и проблемы могут возникнуть при проектировании и внедрении КСИБ? Как их можно минимизировать или устранить?	

1.2. Контрольные задания с ключами правильных ответов.

Задание 1.

Опишите этапы проектирования КСИБ и приведите пример задачи для каждого этапа.

Задание 2.

Составьте модель угроз для гипотетического объекта информатизации (например, для государственного учреждения или промышленного предприятия).

Задание 3.

Разработайте краткое техническое задание для КСИБ конкретного объекта (укажите тип организации, основные виды обрабатываемой информации, предполагаемые угрозы).

Задание 4.

Опишите, какие документы должны быть подготовлены на этапе внедрения КСИБ, и поясните их назначение.

2. Задания закрытого типа.

2.1. Тестовые задания.

Тест 1.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать верный ответ.

1. Какие основные этапы включает проектирование комплексной системы информационной безопасности (КСИБ)?

А) Анализ угроз, разработка технического задания, внедрение, эксплуатация.

Б) Технико-экономическое обоснование, техническое проектирование, рабочее проектирование, внедрение, опытная эксплуатация, приёмочные испытания.

В) Моделирование угроз, выбор средств защиты, настройка параметров безопасности.

Г) Аудит текущей системы, разработка политики ИБ, обучение персонала.

2. Что такое технико-экономическое обоснование (ТЭО) в контексте создания КСИБ?

А) Документ, описывающий характеристики требуемой системы безопасности.

Б) Процесс выбора средств защиты информации.

В) Документ, в котором обосновывается целесообразность создания системы, определяются сроки и порядок работ, а также указывается стоимость.

Г) Этап внедрения системы.

3. Какие требования предъявляются к техническому заданию (ТЗ) на разработку КСИБ?

А) Учёт всех исходных данных, включая цели, задачи, границы системы, требования к функциональности и безопасности.

Б) Описание только технических характеристик системы.

В) Указание только сроков и стоимости проекта.

Г) Отсутствие ссылок на нормативные документы.

4. Что включает в себя рабочее проектирование КСИБ?

А) Детализация проектных решений, составление должностных инструкций, подготовка документации.

Б) Только выбор аппаратных средств защиты.

В) Проведение приёмочных испытаний.

Г) Обучение персонала.

5. Какие нормативные документы регулируют разработку и эксплуатацию КСИБ в России?

А) ГОСТ Р 72118-2025, ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации», приказы ФСТЭК.

Б) Только ISO/IEC 27001.

В) Только внутренние стандарты организации.

Г) Только ФЗ-152 «О персональных данных».

6. Что такое конструктивная информационная безопасность (КИБ) согласно ГОСТ Р 72118-2025?

А) Безопасность, достигаемая применением конструктивных подходов, включая учёт опыта блокирования и исправления уязвимостей.

Б) Безопасность, обеспечиваемая только внешними средствами защиты.

В) Безопасность, основанная исключительно на криптографических методах.

Г) Безопасность, реализуемая после завершения разработки системы.

7. Какие принципы должны соблюдаться при проектировании КСИБ для АСУ ТП (автоматизированных систем управления технологическими процессами)?

А) Законность, непрерывность, комплексность обеспечения безопасности, приоритет предотвращения компьютерных атак.

Б) Только принцип минимизации привилегий.

В) Только использование сертифицированных средств защиты.

Г) Отсутствие необходимости в мониторинге системы.

8. Что включает в себя модель угроз безопасности информации при проектировании КСИБ?

А) Описание возможных угроз, их источников, сценариев реализации, вероятностей и потенциального ущерба.

Б) Только перечень технических уязвимостей.

В) Только анализ внешних угроз.

Г) Только описание мер противодействия угрозам.

9. Какие меры должны быть предусмотрены для реагирования на инциденты информационной безопасности в КСИБ?

А) Регистрация инцидентов, передача информации о них по заданному сценарию, прерывание обработки данных, уничтожение информации в подключённых к защищённым данным съёмных носителях, принятие мер для задержания нарушителя.

Б) Только автоматическое обнаружение угроз.

В) Только уведомление руководства.

Г) Отсутствие каких-либо действий до проведения полного расследования.

10. Что такое система менеджмента информационной безопасности (СМИБ)?

А) Система, основанная на оценке рисков ИБ, предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа и улучшения мер безопасности.

Б) Только набор технических средств защиты.

В) Только документация по ИБ.

Г) Система, не требующая регулярного обновления.

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается	20-29

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
несколько ошибок в содержании ответа и решении практических заданий.	
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий.

Обучающемуся разрешается использование компьютера с установленными прикладными программными продуктами

7. Методические материалы по освоению дисциплины (модуля)

Обучение по дисциплине «*Программно-техническое обеспечение компьютерной безопасности*» предполагает изучение курса в ходе контактной работы обучающихся с преподавателем по видам учебных занятий (лекции, семинарские занятия) и самостоятельной работы магистров. Семинарские занятия дисциплины «*Программно-техническое обеспечение компьютерной безопасности*» предполагают их проведение в различных формах, в том числе в виде защиты исследовательских проектов, с целью выявления полученных знаний, умений, навыков в рамках заявленных компетенций.

Подготовка к лекции:

- повторение материала предыдущей лекции;
- определение с темы предстоящей лекции (в рабочей программе учебной дисциплины);
- ознакомление с учебными материалами по данной теме в соответствии с предложенным в рабочей программе списком литературы учебной дисциплины или с электронными материалами, предложенными лектором;
- подготовить возможные вопросы, которые можно будет задать лектору.

Подготовка к практическим (семинарским) занятиям:

- внимательно прочитать материал лекций и раздела учебника по теме занятия;

− изучить план семинарского занятия и рекомендации преподавателя по подготовке к нему;

− изучить рекомендованные по данной теме источники и литературу и подготовить ответы в соответствии с планом занятия;

− готовиться к семинарским занятиям можно как индивидуально, так и в составе малой группы.

Рабочую программу учебной дисциплины необходимо использовать в качестве основного ориентира в организации обучения. Электронная версия рабочей программы по дисциплине размещена на сайте Нижегородского института управления, и предоставлен авторизованный доступ.

Самостоятельная работа обучающихся призвана закрепить теоретические знания и практические навыки, полученные студентами на лекциях, практических и семинарских занятиях.

Самостоятельная работа обучающихся проводится с целью:

− систематизации и закрепления полученных теоретических знаний и практических умений студентов;

− углубления и расширения теоретических знаний;

− формирования умений использовать справочную документацию и специальную литературу;

− развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

− формированию самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

− развития исследовательских умений.

Эффективность лекционных, семинарских и практических занятий по дисциплине во многом зависит от качества самостоятельной работы студентов, от их самоподготовки. Часть времени, отведенного на самостоятельную работу должна использоваться на подготовку к аудиторным занятиям, другая часть на выполнение домашней работы, осмысление и оформление результатов практических занятий.

При подготовке к занятиям студенту полезно:

− изучить теоретический материал по данной теме (конспект занятия);

− ознакомиться с литературой, рекомендованной преподавателем;

− выполнить задания, предложенные преподавателем, к занятию;

− составить перечень вопросов, вызывающих затруднения, неясности или сомнения, обсудить их с преподавателем или на занятии;

− заниматься самостоятельным поиском дополнительной литературы по изучаемой теме.

Подготовка к зачету. К зачету необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по

данной дисциплине. В самом начале учебного курса познакомиться со следующими учебно-методическими материалами:

- рабочей программой данной дисциплины и содержащимися в ней
  - перечнем знаний и умений, которыми магистр должен владеть;
  - тематическими планами лекций, семинарских занятий;
  - списком рекомендованной литературы и электронных материалов;
- содержанием тем лекционных и семинарских занятий, а также методическими рекомендациями по освоению дисциплины;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов для подготовки к зачету.

Систематическое выполнение всех видов заданий на лекциях, семинарских занятиях, а также самостоятельная работа позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

Вопросы для самостоятельной подготовки к занятиям

1. Перечислите основные этапы построения КСЗИ.
2. Назовите ГОСТ с учётом которых должны быть разработаны требования к системе защиты информации.
3. Перечислите основные понятия которые будут определены при проектировании КСЗИ.
4. Перечислите основное содержание эксплуатационной документации КСЗИ.
5. Перечислите этапы внедрения системы защиты информации.
6. Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.
7. Какие существуют виды обследования защищённости?
8. Назовите порядок проведения аттестации объектов информатизации по требованиям безопасности информации?
9. Какие документы предоставляет заявитель для проведения испытаний органу по аттестации?
10. Какие функции осуществляет ФСТЭК в рамках системы аттестации?
11. Назовите закон о защите персональных данных.
12. Каким документом определяются требования к защите персональных данных?
13. Назовите перечень документов используемых для защиты персональных данных.
14. Назовите документ регламентирующий использование криптографических средств защиты в информационных системах.
15. Какие показатели необходимо рассчитать для построения модели угроз ПДн?
16. Что обозначает коэффициент реализуемости угрозы?

17. Какие угрозы являются актуальными?

18. В соответствии с каким нормативным документом строится модель угроз?

19. В соответствии с каким нормативным документом, и в каких случаях строится модель нарушителя?

20. Назовите структуру нормативных документов предприятия.

21. Какой документ по защите информации является первичным нормативным актом на предприятии?

22. Перечислите законы, регулирующие порядок работы с конфиденциальной информацией.

23. Что регулирует закон об архивном деле?

24. Что регулирует Федеральный закон "О защите персональных данных"?

25. Что регулирует Федеральный закон "О коммерческой тайне"?

26. Что регулирует Федеральный закон "О связи"?

27. Перечислите общий список внутренних нормативных документов, которые должны быть на любом объекте информатизации?

28. Какими документами должен руководствоваться специалист по защите информации при составлении плана мероприятий по улучшению защищённости объекта информатизации?

29. Дайте определение политики информационно безопасности.

30. Из каких основных документов состоит политика информационной безопасности?

31. Назовите общее содержание политики разрешения доступа к технологическим ресурсам.

32. Что включает в себя политика пользования электронной почтой?

33. Назовите общее содержание антивирусная политика.

34. Назовите общее содержание политика подготовки, обмена и хранения документов.

35. Что включает в себя политика информационно-технической поддержки?

36. Что включает в себя политика серверной безопасности?

37. Опишите структуру сетевой файловой системы.

38. Дайте характеристику использования симметричных алгоритмы шифрования в сетевой ФС.

39. Дайте характеристику средств аутентификации в сетевой ФС.

40. Дайте характеристику средств авторизации доступа.

41. Дайте характеристику средств аудита.

42. Опишите способы построения защищенного канала связи.

43. Что такое защищенный документооборот?

44. Назовите основные компоненты необходимые для организации электронного документооборота.

45. Какие мероприятия необходимы для организации защищенного электронного документооборота?

46. Назовите основной метод обнаружения вредоносных программ.
47. Перечислите методики обнаружения вредоносных программ.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233509 (дата обращения: 17.04.2026). – Режим доступа: по подписке.

2. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2026. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2241407 (дата обращения: 17.04.2026). – Режим доступа: по подписке.

3. Техническая защита информации : практикум / сост. А. С. Кравченко, В. А. Мельник, С. Л. Сахаров ; ФКОУ ВО Воронежский институт ФСИН России. - Иваново : Издательско-полиграфический комплекс «ПресСто», 2023. - 80 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2158325 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва : Директ-Медиа, 2020. - 270 с. - ISBN 978-5-4499-0496-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1908082 (дата обращения: 16.04.2026). – Режим доступа: по подписке.

2. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва : Директ-Медиа, 2020. - 270 с. - ISBN 978-5-4499-0496-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1908082 (дата обращения: 02.03.2026). – Режим доступа: по подписке.

3. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 17.04.2026). – Режим доступа: по подписке.

4. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91449 (дата обращения: 02.03.2026). — Режим доступа: для авториз. пользователей.

5. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 02.03.2026). — Режим доступа: для авториз. пользователей.

6. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/185333 (дата обращения: 02.03.2026). — Режим доступа: для авториз. пользователей.

7. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 02.03.2026). – Режим доступа: по подписке.

8.3. Нормативные правовые документы и иная правовая информация

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ. // Справочная правовая система КонсультантПлюс: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 14.04.2025).
2. Приказ Министерства науки и высшего образования Российской Федерации от 06.04.2021 №245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры» // Справочная правовая система КонсультантПлюс: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_393023/ (дата обращения: 14.04.2025).
3. Приказ РАНХиГС Об утверждении положения о единой балльно-рейтинговой системе оценивания успеваемости студентов Академии и ее использовании при проведении текущей и промежуточной аттестации от 12.12.2024 №02-2531.
4. Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 №916 (зарегистрировано в Министерстве юстиции Российской Федерации 10.10.2017, регистрационный номер № 48495).
5. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)
6. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями)

8.4 Интернет-ресурсы

1. Портал http://www.interface.ru/
2. Федеральный портал Российское образование http://www.edu.ru/
3. Российский портал открытого образования https://eduopenru.ru/
4. Управление внедрением информационных систем http://www.intuit.ru/studies/courses/2196/267/info
5. Основы управления проектами http://www.intuit.ru/studies/courses/2194/272/info
6. Стратегический аудит информационных систем http://www.intuit.ru/studies/courses/482/338/info

7. Портал о защите персональных данных [Электронный ресурс]. – Режим доступа: www.reignvox.ru
8. Официальный сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: www.fstec.ru.
9. Официальный сайт ФСБ России [Электронный ресурс]. – Режим доступа: www.fsb.ru.
10. Интернет-сайт «Российской газеты» [Электронный ресурс]. – Режим доступа: www.rg.ru.
11. Интернет-ресурс «Искусство управления информационной безопасностью» [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/zaschita-personalnyh-dannyh/

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

9.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов.
2. Компьютерные классы для выполнения групповых тестовых и иных заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно-образовательную среду организации.
3. Специализированные аудитории и лаборатории.
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека).
5. Читальный зал.
6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

9.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.

2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средства работы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

9.3. Информационные справочные системы:

1. https://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «IPRSMART» (ранее – IPRBooks)
2. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».
3. Электронно-библиотечная система [ЭБС] «Znanium.com».
4. https://www.book.ru - Электронно-библиотечная система [ЭБС] «Book.ru».
5. https://ibooks.ru - Электронно-библиотечная система [ЭБС] «ibooks.ru».
6. https://ranepalib.miflib.ru - Электронная библиотека издательства «МИФ».
7. https://eivis.ru – Ивис. Полные тексты российских научных и практических журналов, а также газет центральной прессы России. Доступ с ip-адресов локальной сети Института.
8. http://www.consultant.ru/ - Справочно-правовая система «Консультант».
9. http://www.garant.ru/ Справочно-правовая система «Гарант».