Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Нижегородский институт управления – филиал РАНХиГС
(наименование института (факультета))
Кафедра информатики и информационных технологий
(наименование кафедры)

УТВЕРЖДЕНО
Директор Нижегородского института управления – филиала РАНХиГС

ПРОГРАММА МАГИСТРАТУРЫ

«Информационные технологии в государственном и муниципальном управлении»
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ, реализуемой с применением электронного (онлайн) курса

Б1.В.ДВ.03.02 ПРОГРАММНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ
(индекс и наименование дисциплины, в соответствии с учебным планом)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)
очная, заочная
(форма обучения)

Год набора – 2024

Нижний Новгород, 2024 г.

Автор-составитель:

Заведующий кафедрой информатики и информационных технологий, канд. техн. наук, доцент — И.И. Гребенюк

(ученая степень и(или) ученое звание, должность, наименование кафедры) — *(Ф.И.О.)*

Доцент кафедры информатики и информационных технологий, канд. физ.-мат. наук, доцент — И.Н. Цветкова

(ученая степень и(или) ученое звание, должность, наименование кафедры) — *(Ф.И.О.)*

Заведующий кафедрой информатики и информационных технологий, канд. техн. наук, доцент — И.И. Гребенюк

(ученая степень и(или) ученое звание, должность, наименование кафедры) — *(Ф.И.О.)*

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

Протокол №12 от 20.02.2024 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы 4

2. Объем и место дисциплины в структуре ОП ВО 5

3. Содержание и структура дисциплины 5

4. Материалы текущего контроля успеваемости обучающихся 7

5. Оценочные материалы промежуточной аттестации по дисциплине 9

6. Методические материалы по освоению дисциплины с применением ЭК 11

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 14

7.1 Основная литература 14

7.2 Дополнительная литература 14

7.3 Учебно-методическое обеспечение самостоятельной работы. 14

7.4 Нормативные правовые документы. 15

7.5. Интернет-ресурсы, справочные системы. 15

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 16

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

1.1 Дисциплина «Программно-техническое обеспечение компьютерной безопасности» обеспечивает овладение следующими компетенциями:

Таблица 1.

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента освоения компетенции
ПК-6	Способен выбирать методологию и технологию проектирования ИС с учетом проектных рисков	ПК-6.2	Способен применять методы оценки и управления рисками ИТ-проектов.
ПК-11	Способен проектировать архитектуру и сервисы информационных систем предприятий и организаций в прикладной области	ПК-11.2	Способен использовать инструментарий проектирования архитектуры и сервисов ИС.
ПК-19	Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных информационных систем	ПК-19.2	Способен использовать методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.

1.2 В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2.

ОТФ/ТФ/ профессиональные действия	Код компонента компетенци	Планируемые результаты обучения
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D)	ПК-6.2	На уровне навыков: – оценки и управления рисками проектов проектирования ИС.
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 технологическое обеспечение разработки баз данных ИС (D/17.7).	ПК-11.2	На уровне знаний: – возможности ИС; – архитектура, устройство и функционирование вычислительных систем; – инструменты и методы моделирования бизнес-процессов организации. На уровне навыков: – проектирования и разработки сервисов ИС в прикладных областях.
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D)	ПК-19.2	На уровне навыков: – проведения анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.

2. Объем и место дисциплины в структуре ОП ВО

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 32 ч, в том числе на лекционные занятия – 8 ч, на практические (семинарские) занятия – 24 ч; на самостоятельную работу обучающихся выделено 36 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.

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Таблица 3.

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, и промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО ДОТ*	ПЗ/ ЭО ДОТ*	КСР		
Очная форма обучения								
Тема 1	Постановка задачи комплексного обеспечения ИБ АС	18	2		6		10	О, ПЗ
Тема 2	Методология формирования задач защиты; интеграция средств защиты в технологическую среду	18	2		6		10	О, ПЗ
Тема 3	Типовая структура КСИБ; методы проектирования и оценки качества КСИБ	18	2		6		10	О, ПЗ
Тема 4	Этапы проектирования КСИБ и требования к ним	18	2		6		10	О, ПЗ
Промежуточная аттестация								зачет
Всего (в з.е./акад.часах/астр.часах):		**2/72/54**	**8/6**		**24/18**		**36/27**	
Заочная форма обучения								

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, и промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО ДОТ*	ПЗ/ ЭО ДОТ*	КСР		
Тема 1	Постановка задачи комплексного обеспечения ИБ АС	16	1		2		13	О, ПЗ
Тема 2	Методология формирования задач защиты; интеграция средств защиты в технологическую среду	18	1		2		15	О, ПЗ
Тема 3	Типовая структура КСИБ; методы проектирования и оценки качества КСИБ	18	1		2		15	О, ПЗ
Тема 4	Этапы проектирования КСИБ и требования к ним	16	1		2		13	О, ПЗ
Промежуточная аттестация		4						зачет
Всего (в з.е./акад.часах/астр.часах):		**2/72/54**	**4/3**		**8/6**		**56/42**	**4/3**

Примечание:
** – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом*
*** – формы текущего контроля успеваемости: опрос (О), тестирование (Т),), оценка доклада (Д), оценка работы с документами в микрогруппе (М),оценка участия в диспуте (Д)с, отчет о выполненнии практического задания (ПЗ), контрольная работа (КР), расчетно-графическая работа (РГР)).*

3.2. Содержание дисциплины

Тема 1 Постановка задачи комплексного обеспечения ИБ АС

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

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

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

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. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.В.ДВ.03.02. «Программно-техническое обеспечение компьютерной безопасности» используются следующие **методы текущего контроля** успеваемости обучающихся:

Таблица 4.

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1. Постановка задачи комплексного обеспечения ИБ АС	Опрос, отчет о выполнении практического задания
Тема 2 Методология формирования задач защиты; интеграция средств защиты в технологическую среду	Опрос, отчет о выполнении практического задания
Тема 3 Типовая структура КСИБ; методы проектирования и оценки качества КСИБ	Опрос, отчет о выполнении практического задания
Тема 4 Этапы проектирования КСИБ и требования к ним	Опрос, отчет о выполнении практического задания

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Вопросы для текущего контроля успеваемости (опросов) по тема дисциплины:

1. Основные понятия и определения информационной безопасности. Общие цели и задачи защиты информации.
2. Принципы организации комплексной системы защиты информации. Системно-концептуальный подход к защите информации.
3. Основные требования и основные задачи защиты информации в автоматизированных системах.
4. Действующие стандарты в области информационной безопасности. Содержание и основные позиции. Документационное сопровождение комплексной системы защиты информации (КСЗИ).
5. Направления работ по созданию КСЗИ. Аспекты планирования инженерно-технического обеспечения КСЗИ.
6. Этапы работ по созданию КСЗИ. Определение и анализ объектов защиты. Базовые понятия и элементы. Формализация описания архитектуры автоматизированной системы.
7. Определение и анализ объектов защиты. Определение исходного уровня защищенности.
8. Классификация защищенности АС в соответствии с РД. Основные требования.
9. Оценка угроз ИБ. Выявление способов НСД и каналов утечки информации.
10. Объективные и субъективные факторы, воздействующие на информацию (по ГОСТ).
11. Виды угроз и основные последствия их реализации.
12. Понятие «нарушителя» и модели нарушителя. Классификации.
13. Модель угроз и принцип ее формирования. Базовая модель угроз безопасности персональных данных (ФСТЭК).
14. Модель угроз и принцип ее формирования. Методология формирования модели

угроз в соответствии с рекомендациями ФСБ.

15. Методики оценки рисков. Применяемые на практике подходы.
16. Структура процесса управления рисками.
17. Средства защиты информации и механизмы обеспечения безопасности информации. Идентификация и аутентификация.
18. Средства защиты информации и механизмы обеспечения безопасности информации. Разграничение доступа. Регистрация и аудит.
19. Средства защиты информации и механизмы обеспечения безопасности информации. Криптографическая подсистема.
20. Средства защиты информации и механизмы обеспечения безопасности информации. Межсетевое экранирование.
21. Планирование мероприятий КСЗИ.
22. Контроль мероприятий КСЗИ. Основные аспекты.
23. Оценка эффективности КСЗИ. Общая характеристика применяемых методов.
24. Оценка эффективности КСЗИ. Оценочные подходы.

Пример практического задания

Задание 1. Изучение содержания и последовательности работ по защите информации.

Изучить содержание и последовательность работ, выполняемых при построении комплексной системы защиты информации.

Задание 2. Изучение методов комплексного исследование объекта информатизации.

Написать отчёт исследования предприятия, закреплённого на практическом занятии №1, содержащий общие сведения о предприятии, о его деятельности и организационной структуре. Изучить стандарты ГОСТ Р ИСО/МЭК 15408-1-2008, ГОСТ Р ИСО/МЭК 15408-2-2008, ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 17799-2005.

Задание 3. Изучение информации, циркулирующей в корпоративной информационной системе.

Построить алгоритм анализа информации, циркулирующей в корпоративной информационной системе. Проанализировать информацию, циркулирующей в корпоративной информационной системе предприятия. Построить полную диаграмму информационных потоков предприятия.

Задание 4. Изучение действующей нормативной документации объекта информатизации.

Составить перечень мероприятий необходимых для построения КСЗИ с учётом нормативно-методических актов. Составить перечень внутренних нормативных документов предприятия, регламентирующих защиту информацию. Провести сравнение имеющегося перечня нормативных документов с необходимым. Написать один из внутренних документов, которые отсутствует на объекте информатизации.

Задание 5. Изучение методов построения комплексной системы организационных и технических мер по защите информации.

Выделите информацию, не подлежащую защите согласно нормативно-правовым актам, и выполнить проектирование организационных и технических мер по защите этой информации. Выполните построение комплексной системы организационных мер для выбранного предприятия.

Задание 6. Изучение методов построения комплексной защиты сетевой файловой системы.

Дайте исходную характеристику сетевой файловой системы, используемой на предприятии. Предложите мероприятия по улучшению имеющейся сетевой ФС и докажите необходимость и эффективность предложенных мер.

Задание 7. Комплексная защита электронной почты и документооборота.

Разработайте проект организации защищенного документооборота в соответствии с закрепленным предприятием.

Задание 8. Изучение методов построения комплексной защиты сетевых приложений и баз данных.

Разработать проект системы защиты базы данных в соответствии с закрепленным *предприятием.*

Задание 9. Изучение методов построения комплексной защиты телекоммуникационной инфраструктуры.

Разработайте проект организации защищенной телекоммуникационной инфраструктуры в соответствии с закрепленным предприятием.

Задание 10. Изучение методов построения комплексной защиты управления информационной безопасностью.

Разработайте проект организации защиты управления информационной безопасностью инфраструктуры в соответствии с закрепленным предприятием.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет проводится с применением следующих методов (средств): проведение устного зачета, включающего теоретическую часть и практико-ориентированное задание, требующее демонстрации уровня владения умениями/навыками.

5.2. Оценочные материалы промежуточной аттестации

Таблица 5.

Показатели и критерии оценивания

Компонент компетенции	Промежуточный индикатор оценивания	Критерий оценивания
ПК-6.2 Способен применять методы оценки и управления рисками ИТ-проектов.	ИПК-6.2 Применяет методы оценки и управления рисками ИТ-проектов.	Использует методы оценки и управления рисками ИТ-проектов.
ПК-11.2 Способен использовать инструментарий проектирования архитектуры и сервисов ИС.	ИПК-11.2 Использует инструментарий проектирования архитектуры и сервисов ИС.	Демонстрирует навыки проектирования архитектуры и сервисов информационных систем
ПК-19.2 Способен использовать методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.	ИПК-19.2 Использует методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.	Применяет методы оценки качества и надежности ИС

Примерные вопросы для подготовки к зачету

1. Комплексный подход к обеспечению информационной безопасности.
2. Характеристика организационно-технических систем.
3. Характеристика видов обеспечения процесса автоматизированного проектирования организационных систем.
4. Исследование состава комплексных систем защиты информации как вида организационно-технических систем.
5. Существующие подходы к автоматизации проектирования комплексных систем защиты информации.

6. Сущность комплексного подхода к разработке системы защиты информации.
7. Систематизация компонентов КСЗИ. Разработка набора типовых вариантов КСЗИ применительно к объекту защиты.
8. Требования к математическому обеспечению САПР КСЗИ.
9. Общий подход к математическому моделированию КСЗИ.
10. Построение математической модели общей оценки угроз безопасности.
11. Построение математической модели оценки рисков реализации угроз безопасности.
12. Варианты решения задачи выбора средств защиты информации в САПР КСЗИ.
13. Анализ используемых методик выбора средств защиты информации в САПР КСЗИ.
14. Типовое вариантное проектирование КСЗИ.
15. Выбор способа представления инженерных знаний в системах параметрического проектирования.
16. Формирование сетевой модели комплексной системы защиты информации на основе типизации её элементов.
17. Разработка структурно-функциональной модели САПР КСЗИ.
18. Анализ объекта защиты на примере высшего учебного заведения.
19. Разработка проекта системы защиты конфиденциальной информации вуз.
20. Анализ результатов работы САПР КСЗИ.

Примеры практико-ориентированных (практических) заданий к зачету

ПК-6.2 - способен применять методы оценки и управления рисками ИТ-проектов:

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» построить модель угроз ИСПДн государственного или муниципального учреждения (предприятия, организации).

ПК-11.2 - способен использовать инструментарий проектирования архитектуры и сервисов ИС:

Разработайте проект организации защиты управления информационной безопасностью инфраструктуры государственного или муниципального учреждения (предприятия, организации).

ПК-19.2 - способен использовать методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности:

Выделите информацию, не подлежащую защите согласно нормативно-правовым актам, и выполнить проектирование организационных и технических мер по защите этой информации. Выполните построение комплексной системы организационных мер для выбранного государственного или муниципального учреждения (предприятия, организации).

Шкала оценивания

Промежуточная аттестация проводится в форме зачета без применения балльно-рейтинговой системы оценивания - посредством аттестационных испытаний в форме традиционного зачета.

Результаты промежуточной аттестации оцениваются: по бинарной системе оценивания («зачтено», «не зачтено»).

Наряду с оцениванием учебных достижений обучающихся по принятой образовательной организации системе оценок и использованием ее при оформлении официальных дипломов Академии о высшем образовании, вводят повышенный («Excellent» и «Good») и базовый («Very good» и «Satisfactory») уровень оценок «отлично» и «хорошо» для использования при оформлении ЕПД, согласно Положению об оформлении и выдаче ЕПД.

Таблица 6

Соответствие академической оценке

Академическая оценка		Оценка по шкале ESTS	
зачтено	отлично	Passed	A (Excellent)
			B (Very Good)
	хорошо		C (Good)
			D (Satisfactory)
	удовлетворительно		E (Sufficient)
не зачтено	неудовлетворительно	-	-

Критерии оценивания на зачете

Оценка **«зачтено»** выставляется обучающемуся, если он твердо знает материал, четко и логически стройно излагает его на зачете, умеет тесно увязывать теорию с практикой, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами заданий, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение.

Оценка **«не зачтено»** выставляется обучающемуся, если он не знает значительной части программного материала, допускает неточности, недостаточно правильные формулировки, выполнение практических заданий неуверенно, с большими затруднениями

6. Методические материалы по освоению дисциплины с применением ЭК

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.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1 Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 16.04.2024). – Режим доступа: по подписке.
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 16.04.2024). - Режим доступа: по подписке.
3. 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, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016 (дата обращения: 16.04.2024). – Режим доступа: по подписке.

7.2 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: 16.04.2024). – Режим доступа: по подписке.
2. 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: 02.03.2024). – Режим доступа: по подписке.

7.3 Учебно-методическое обеспечение самостоятельной работы.

1. 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: 02.03.2024). — Режим доступа: для авториз. пользователей.
2. 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: 02.03.2024). — Режим доступа: для авториз. пользователей.

3. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861659 (дата обращения: 02.03.2024). – Режим доступа: по подписке.

4. 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: 02.03.2024). – Режим доступа: по подписке.

5. 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: 02.03.2024). — Режим доступа: для авториз. пользователей.

6. Электронные информационно-образовательные ресурсы Нижегородского института управления – филиала РАНХиГС - http://sdo.niu.ranepa.ru/

7.4 Нормативные правовые документы.

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации"

2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)

3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями)

4. 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»

5. 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).

7.5. Интернет-ресурсы, справочные системы.

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/

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

8.1. 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.

8.2. 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.

8.3. Информационные справочные системы:

1. https://www.urait.ru –Электронно-библиотечная система [ЭБС] Юрайт;
2. http://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «IPR SMART» (ранее – IPRBooks)
3. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».

4. https://znanium.com - Электронно-библиотечная система [ЭБС] «Znanium.com».
5. https://www.book.ru - Электронно-библиотечная система [ЭБС] «Book.ru».
6. https://ibooks.ru - Электронно-библиотечная система [ЭБС] «ibooks.ru».
7. https://www.ezproxy.ranepa.ru:2443/login?url=https://dlib.eastview.com/ – East View. Полные тексты российских научных и практических журналов, а так же газет центральной прессы России.
8. https://www.ezproxy.ranepa.ru:2443/login?url=https://grebennikon.ru/ - Полные тексты 38 научно-практических журналов по маркетингу, менеджменту, финансам и управлению персоналом ИД «Гребенников»
9. http://www.consultant.ru/ - Справочно-правовая система «Консультант».
10. http://www.garant.ru/ Справочно-правовая система «Гарант».