Федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
Среднерусский институт управления – филиал
ФАКУЛЬТЕТ «Технологии, товароведение и сервис»
КАФЕДРА «Математика и информационные технологии»

Меркулов Павел Александрович

Подписан: Меркулов Павел Александрович
DN: C=RU, S=Орловская область, L=пр. Орел, T=Директор, OU="СРЕДНЕРУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ - ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ""", СНИЛС=00482216008, ИНН=575206486423, E=it@orel.ranepa.ru, G=Павел Александрович, SN=Меркулов, CN=Меркулов Павел Александрович
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: Среднерусский институт управления

УТВЕРЖДЕНО
Директор Среднерусского института управления – филиала РАНХ и ГС
П.А. Меркулов

ПРОГРАММА БАКАЛАВРИАТА

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ В БИЗНЕСЕ

(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.В.06 Комплексная система защиты информации

(код и наименование РПД)

09.03.02 Информационные системы и технологии

(код и наименование направления подготовки/специальности)

очная, очно-заочная, заочная

(форма (формы) обучения)

Год набора: 2022

Орел, 2022 г.

Автор–составитель:
к.п.н., доцент кафедры математики и информационных технологий А.А. Музалевская

И.о. заведующего кафедрой
математики и информационных технологий, доктор экономических наук, профессор Л.И. Малявкина

РПД Б1.В.06 «Комплексная система защиты информации» одобрена на заседании кафедры математики и информационных технологий, протокол от 26 августа 2022 г., №1.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Объем и место дисциплины в структуре образовательной программы 4
3. Содержание и структура дисциплины 5
4. Материалы текущего контроля успеваемости обучающихся 9
5. Оценочные материалы промежуточной аттестации по дисциплине 12
6. Методические указания для освоения дисциплины 13
7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 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 образовательной программы

1.1 Дисциплина Б1.В.06 «Комплексная система защиты информации» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПК-3	Способен выполнять работы по созданию (модификации) и сопровождению информационных систем	ПК-3.2	Способен сопровождать информационные системы, автоматизирующие задачи организационного управления и бизнес-процессы

1.2 В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ/ трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения
ОТФ С. Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-3.2	на уровне знаний: знает принципы обеспечения информационной безопасности и способы использования безопасных информационных технологий
		на уровне умений: умеет выявлять и оценивать источники, способы и результаты реализации угроз информации в информационной системе предприятия при выполнении работ и управлении работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы
		на уровне навыков: демонстрирует навыки выполнения работ по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности на предприятии

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Общий объем дисциплины в зачетных единицах (академических/астрономических часах): 3 ЗЕ (108/81).
Количество академических/астрономических часов, выделенных на контактную работу:
– по очной форме обучения – 54/40,5 (в т.ч. лекц. – 18 ч., практ. – 36 ч.); на самостоятельную работу обучающихся – 50/37,5;

– по очно-заочной форме обучения – 18/13,5 (в т.ч. лекц. – 6 ч., практ. – 12 ч.); на самостоятельную работу обучающихся – 86/64,5;
– по заочной форме обучения – 18/13,5 (в т.ч. лекц. – 6 ч., практ. – 12 ч.); на самостоятельную работу обучающихся – 86/64,5.

Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам части, формируемой участниками образовательных отношений, Блока 1. «Дисциплины (модули)» учебного плана образовательной программы.

Дисциплина изучается: очная форма обучения – 4 курс, 8 семестр; очно-заочная форма обучения – 5 курс; заочная форма обучения – 5 курс.

Освоение дисциплины опирается на содержание учебных дисциплин: Информационная безопасность; Правовое регулирование в профессиональной деятельности, ИТ-инфраструктура предприятия.

Основные положения дисциплины используются в при прохождении технологической (проектно-технологической) практики, а также во время проведения государственной итоговой аттестации.

Форма аттестации: зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
Тема 1	Сущность и задачи комплексной системы защиты информации	14	2		2		10	О
Тема 2	Выявление угроз информационной безопасности на предприятии	18	4		6		10	О,К
Тема 3	Определение компонентов и структуры комплексной системы защиты информации	16	4		10		10	О,К
Тема 4	Принципы организации и этапы разработки комплексной системы защиты информации	14	4		6		10	О
Тема 5	Функционирование комплексной	32	4		12		10	О

	системы защиты информации							
Промежуточная аттестация								З
Всего:		104	18		36		50	

Примечание:
** формы заданий текущего контроля успеваемости: (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.), кейс-задания (КЗ) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.),*
** форма промежуточной аттестации: экзамен (Экз), зачет(З), зачет с оценкой (ЗО)*

Очно-заочная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Сущность и задачи комплексной системы защиты информации	13	1				12	О
Тема 2	Выявление угроз информационной безопасности на предприятии	20	2		2		16	О,К
Тема 3	Определение компонентов и структуры комплексной системы защиты информации	24	2		4		18	О,К
Тема 4	Принципы организации и этапы разработки комплексной системы защиты информации	22			2		20	О
Тема 5	Функционирование комплексной системы защиты информации	25	1		4		20	О
Промежуточная аттестация								З
Всего:		104	6		12		86	

Примечание:
** формы заданий текущего контроля успеваемости: (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.), кейс-задания (КЗ) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.),*
** форма промежуточной аттестации: экзамен (Экз), зачет(З), зачет с оценкой (ЗО)*

Заочная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		

Тема 1	Сущность и задачи комплексной системы защиты информации	13	1				12	О
Тема 2	Выявление угроз информационной безопасности на предприятии	20	2		2		16	О,К
Тема 3	Определение компонентов и структуры комплексной системы защиты информации	24	2		4		18	О,К
Тема 4	Принципы организации и этапы разработки комплексной системы защиты информации	22			2		20	О
Тема 5	Функционирование комплексной системы защиты информации	25	1		4		20	О
Промежуточная аттестация								З
Всего:		104	2		12		86	

Примечание:
** формы заданий текущего контроля успеваемости: (контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол) и т.п.), кейс-задания (КЗ) и виды учебных заданий (эссе (Эс), реферат (Реф), диспут (Д) и др.),*
** форма промежуточной аттестации: экзамен (Экз), зачет(З), зачет с оценкой (ЗО)*

3.2.Содержание дисциплины

Тема 1. Сущность и задачи комплексной системы защиты информации

Понятие, сущность и общее содержание комплексной системы обеспечения безопасности информационных технологий коммерческой организации. Назначение комплексной системы обеспечения информационной безопасности (КСИБ).

Задачи и методологические основы комплексной системы обеспечения информационной безопасности.

Принципы организации КСИБ. Основные факторы, влияющие на организацию КСИБ: организационно-правовая форма и характер основной деятельности предприятия; состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение предприятия; режим функционирования предприятия; конструктивные особенности предприятия; степень автоматизации основных процедур обработки защищаемой информации.

Тема 2. Выявление угроз информационной безопасности на предприятии.

Определение источников дестабилизирующего воздействия на информацию и видов их воздействия. Выявление способов воздействия на информацию. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.

Выявление каналов и определение возможных методов несанкционированного доступа к информации. Анализ потенциальных последствий реализации несанкционированного доступа.

Выявление нарушителей (незаконных пользователей) и состава интересующей их информации. Определение направлений и возможностей доступа нарушителей к защищаемой информации. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.

Тема 3. Определение компонентов и структуры комплексной системы защиты информации.

Объекты защиты как основной фактор, определяющий состав компонентов КСИБ. Выявление состава носителей защищаемой информации. Хранилища носителей информации как объект защиты. Особенности помещений для работы с защищаемой информацией как объектов защиты. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Состав средств обеспечения функционирования предприятия, подлежащих защите. Факторы, определяющие необходимость защиты периметра и здания предприятия. Специфика персонала предприятия как объекта защиты. Выбор компонентов и определение структуры КСИБ.

Состав компонентов КСИБ . Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации.

Тема 4. Принципы организации и этапы разработки комплексной системы защиты информации

Понятие аналитической работы, ее цели и задачи. Результаты аналитической работы как основа формирования системы защиты информации и ее совершенствования.

Принципы построения системы, ее технологичность, иерархичность и факторы эффективности.

Компьютерные технологии и формирование основ системы защиты информации. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях. Комплексность системы защиты. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Основные стадии и этапы разработки КСИБ. Характеристика основных стадий создания КСИБ. Предпроектное обследование. Персонал и информационная технология организации как объект защиты. Определение и нормативное закрепление состава защищаемой информации. Технический проект, рабочий проект. Апробация и ввод в эксплуатацию. Понятие и цели управления КСИБ. Сущность процессов управления КСИБ. Принципы управления КСИБ. Основные стили управления. Структура и содержание общей технологии управления КСИБ.

Тема 5. Функционирование комплексной системы защиты информации

Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз.

Методики оценки качества КСИБ. Сущность и содержание контроля функционирования. Понятие и виды контроля. Цель проверки контроля. Анализ результатов проведения контрольных мероприятий. Общая характеристика подходов к оценке эффективности. Основные подходы к оценке эффективности. Вероятностный подход. Статистические (экспертные) и качественные методы оценки эффективности. Методы и модели оценки эффективности. Классификация и основные понятия, используемые в различных методах и моделях оценки. Показатели защищенности (эффективности).

Требования к эксплуатационной документации. Положения государственных стандартов, требования к эксплуатационной документации. Нормативно-правовое обеспечение информационной безопасности. Международное и отечественное законодательство в области обеспечение информационной безопасности. Структура государственных организаций, контролирующих защиту информации в стране.

Эксплуатация КСИБ на объекте защиты. Способы и стадии планирования функционирования КСИБ. Структура и общее содержание планов. Организация выполнения планов. Управление КСИБ в условиях чрезвычайных ситуаций. Понятие и виды чрезвычайных ситуаций. Особенности принятия решений в условиях чрезвычайных ситуаций. Мероприятия на случай возникновения чрезвычайных ситуаций.

Правовое обеспечение защиты информационных технологий организаций различных форм собственности.

Политика, концепция и план по обеспечению информационной безопасности на предприятии.

Состав методов и моделей оценки эффективности КСИБ . Выбор показателей эффективности и критериев оптимизации. Подходы к оценке эффективности КСИБ. Перспективы комплексной защиты информации. Методы оптимизации КСИБ

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.В.06 «Комплексная система защиты информации» используются следующие **методы текущего контроля успеваемости** обучающихся:

Тема и/или раздел	Методы текущего контроля успеваемости
Тема 1. Сущность и задачи комплексной системы защиты информации	Опрос
Тема 2. Выявление угроз информационной безопасности на предприятии	Опрос, контрольная работа
Тема 3. Определение компонентов и структуры комплексной системы защиты информации	Опрос, контрольная работа
Тема 4. Принципы организации и этапы разработки комплексной системы защиты информации	Опрос
Тема 5. Функционирование комплексной системы защиты информации	Опрос

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Примерные вопросы для опроса

Тема 1:

1. Какие принципы лежат в основе обеспечения информационной безопасности?
2. Какие требования к СЗИ Вам известны? Дайте им характеристику.
3. Какие средства защиты локальных ПК вам известны? От каких угроз они защищают.
4. Какие средства сетевой защиты Вам известны? Дайте характеристику этих средств
5. Назовите основные принципы построения защищенных КС.
6. Дайте краткую характеристику этапов создания КСЗИ.
7. В чем заключается сущность концепций защиты информации в ИС?
8. Как проводится анализ и классификация организационных и программных средств в ИС?
9. Основные направления развития теории защиты информации
10. В чем заключаются цели и защиты информации в вычислительных системах?

11. Основные концепции защиты информации в ИС. Традиционные меры защиты твердых копий
12. Какая информация является объектом права собственности и какие особенности для нее характерны?

Тема 2:

1. Определить основные виды угроз информационным ресурсам.
2. Понятие нарушителя. Определение направлений и возможностей доступа нарушителей к защищаемой информации.
3. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
4. Охарактеризовать особенности угроз конфиденциальной информации.
5. Дать классификацию удаленных атак.
6. Перечислите основные виды информационных угроз
7. Специфика информационных угроз в различных ИС
8. Что представляет защита от информационных угроз?
9. Какая количественная величина характеризует уязвимость?
10. Дайте понятие основным и косвенным факторам уязвимости информационной системы.
11. Как оценить опасность уязвимости?
12. Какие типы показателей косвенных факторов уязвимости Вы знаете?
13. Какие подходы используются при построении модели нарушителя?

Тема 3:

1. Какими основными компонентами обеспечивается охрана объектов ИС?
2. Охарактеризуйте одноуровневую, многоуровневую и многозвенную модели системы защиты информации.
3. Дайте общую характеристику основных средств и методов защиты информации в ИС.
4. Дать классификацию организационных и программно-аппаратных структур защиты информации в ИС?
5. Раскройте особенности стратегии защиты информации с использованием системного подхода, комплексных решений и принципа интеграции в информационных технологиях.
6. В чем состоит необходимость организационного обеспечения защиты информации?
7. Дайте общую характеристику организационным мероприятиям, направленным на обеспечение информационной безопасности. Что представляет собой персонал организации как источник конфиденциальной информации?

Тема 4:

1. Какие принципы лежат в основе обеспечения информационной безопасности?
2. Какие требования к СЗИ Вам известны? Дайте им характеристику.
3. Какие средства защиты локальных ПК вам известны? От каких угроз они защищают.
4. Какие средства сетевой защиты Вам известны? Дайте характеристику этих средств
5. Назовите основные принципы построения защищенных КС.
6. Дайте краткую характеристику этапов создания КСЗИ.
7. Определите основные этапы создания комплексной системы информационной безопасности и результаты действия на каждом из этапов.

Тема 5:

1. Какими принципами руководствуются при организации системы управления КСЗИ?
2. Какие организационные задачи решаются при эксплуатации КСЗИ?
3. Функциональные процессы, реализуемые комплексной системой защиты информации в процессе эксплуатации
4. Что представляют собой стандартные функциональные профили защищенности?
5. Что представляет собой эффективность КСЗИ? Какие основные требования предъявляются к показателю эффективности?
6. Какие концепции выработки решения используются при выборе критериев эффективности?
7. Что представляют собой стандартные функциональные профили защищенности?
8. Какими принципами руководствуются при организации системы управления КСЗИ?
9. Какие организационные задачи решаются при эксплуатации КСЗИ?

Примерный вариант контрольной работы

Темы 2-3:

1. Подготовить ответ на теоретический вопрос «Технологические системы защиты, обработки и хранения конфиденциальных документов».
2. Практическое задание. Филиал крупного банка имеет следующие отделы: руководство, отдел кадров, бухгалтерия, отдел работы с клиентами. Информационная система филиала представлена в следующем составе:

Руководство – 3 рабочие станции: ПК директора, ПК администратора автоматизированной банковской системы, ПК Администратора ИБ.

Отдел кадров – сервер и ПК начальника отдела кадров

Бухгалтерия – сервер и ПК бухгалтера

Отдел работы с клиентами: Веб-сервер и 3 рабочие станции ПК менеджера.

1) Создать схему территориального расположения структурных подразделений

2) Для каждого структурного подразделения определить информационные активы. Заполнить таблицу.

Вид актива	Наименование актива	Владелец	Гриф конфиденциальности	Угрозы	Уязвимости
Наименование структурного подразделения					

3) Определить зоны доступа к информационным активам, наиболее опасные каналы утечки информации, способы и средства противодействия утечке. Заполнить таблицу

№ п/п	Информационные активы	В какой зоне должны находиться	Наиболее опасные каналы утечки для каждого актива	Способ противодействия утечке	Средство противодействия утечке

Примерная тематика рефератов

1. Сравнительный анализ готовых решений в области КСЗИ.
2. Назначение, структура и методика построения разрешительной системы доступа к ресурсам информационной системы.
3. Средства защиты информации в операционной системе (по выбору).

4. Обеспечение требований информационной безопасности в программных приложениях «1С».
5. Функционирование комплексной системы защиты информации.
6. Программные средства обеспечения защиты информации в локальной сети.
7. Управление и защита информации в информационно-телекоммуникационных сетях.
8. Принципы обеспечения безопасности программного обеспечения
9. Организация работы персонала с конфиденциальными документами и материалами
10. Особенности применения средств криптографической защиты информации коммерческими предприятиями.

Вопросы для самостоятельного изучения:

1. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях.
2. Методологии защиты информационных технологий, их связь с управлением организацией.
3. Правовое обеспечение защиты информационных технологий организаций различных форм собственности
4. Основные факторы, влияющие на организацию КСЗИ.
5. Подходы к созданию комплексной системы защиты конфиденциальной информации в организации.
6. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях.
7. Перспективы комплексной защиты информации.
8. Понятие и виды чрезвычайных ситуаций.
9. Персонал организации как объект защиты.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Экзамен (зачет) проводится с применением следующих методов (средств):

Зачет принимается в устной форме, по билетам. Каждый билет содержит одно практическое задание.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Ключевой индикатор оценивания	Критерии оценивания
ПК-3.2	Способен сопровождать информационные системы, автоматизирующие задачи организационного управления и бизнес-процессы	Демонстрирует умение сопровождать информационные системы, автоматизирующие задачи организационного управления и бизнес-процессы

Типовые оценочные материалы промежуточной аттестации

Варианты практических (ситуационных) заданий для проведения зачета

Вариант 1. Для заданной предметной области создать перечень конфиденциальных сведений и перечень конфиденциальных документов

Вариант 2. Для заданной предметной области предложить инженерно-техническую подсистему КСЗИ
Вариант 3. Для заданной предметной области предложить программную подсистему КСЗИ
Вариант 4. Для заданной предметной области составить матрицу ответственности (работы и исполнители) по созданию КСЗИ
Вариант 5. Для заданной предметной области составить сетевой график выполнения работ по созданию КСЗИ
Вариант 6. Для заданной предметной области написать техническое задание на разработку КСЗИ
Вариант 7. Для заданной предметной области создать информационную модель КСЗИ
Вариант 8. Для заданной предметной области создать структурную модель КСЗИ
Вариант 9. Для заданной предметной области создать функциональную модель КСЗИ
Вариант 10. Для заданной предметной области описать политику информационной безопасности

6. Методические указания для освоения дисциплины

Обучение по дисциплине предполагает изучение курса на аудиторных (лекционных, практических) занятиях, самостоятельную работу обучающихся и проведение контрольных мероприятий (текущей и промежуточной аттестации).

В начале учебного курса рекомендуется ознакомиться с рабочей программой дисциплины, обратив внимание на следующие ключевые моменты:

– перечень знаний, умений и навыков, которыми обучающийся должен овладеть в результате освоения дисциплины;

– тематический план проведения занятий;

– формы и материалы для проведения текущего контроля;

– учебники и учебные пособия по дисциплине, а также электронными ресурсы;

– оценочные материалы для проведения промежуточной аттестации.

С целью обеспечения успешного освоения курса обучающийся должен готовиться к лекционным и практическим занятиям.

На лекционных занятиях рекомендуется конспектировать основные положения излагаемого преподавателем материала. При подготовке к занятиям целесообразно самостоятельно прорабатывать лекционный материал, особое внимание следует уделять возникающим при этом вопросам, выделяя или выписывая указанные моменты для дальнейшего уточнения и обсуждения на последующих занятиях. В случае необходимости обращаться к преподавателю за консультацией. Таким образом, подготовка к лекции заключается в:

– внимательном прочтении материала предыдущей лекции;

– знакомстве с темой предстоящей лекции (по тематическому плану или информации лектора);

– предварительном знакомстве с учебным материалом по учебнику и учебным пособиям;

– уяснении места изучаемой темы в своей профессиональной подготовке;

– записи возможных вопросов преподавателю.

Практические занятия предполагают их проведение в различных формах (в том числе с использованием информационно-коммуникационных технологий) с целью систематизации, углубления и конкретизации полученных теоретических знаний, а также формирования навыков их применения при решении практических задач. Подготовка к практическим занятиям заключается в:

– внимательном прочтении теоретического материала лекций, относящихся к

данному занятию, изучении учебного материала в рекомендуемых учебно-методических пособиях;

– ответе на приведенные в рабочей программе дисциплины вопросы для самостоятельной подготовки к занятиям лекционного, практического (семинарского) типов, лабораторным работам;

– выполнении заданий для самостоятельной работы по соответствующей теме.

В рамках практических занятий предусмотрено проведение мероприятий текущего контроля с целью выявления уровня освоения полученных знаний, умений, навыков и компетенций. Для осуществления текущего контроля в рабочей программе предусмотрены различные формы. При подготовке к контрольным мероприятиям рекомендуется ознакомиться с представленными в рабочей программе типовыми материалами для проведения текущего контроля успеваемости обучающихся.

Изучение дисциплины предполагает самостоятельное освоение обучающимся части учебного материала в соответствии с перечнем вопросов для самостоятельного изучения.

Одной из форм самостоятельной работы является подготовка реферата в соответствии с приведенной в рабочей программе тематикой. Тематика может быть расширена с учетом интересов обучающегося.

Структура реферата:

– Введение – это вступительная часть реферата, предваряющая текст. Оно должно содержать следующие элементы:

а) краткое освещение актуальности темы

б) степень ее изученности (краткий анализ научных, экспериментальных или практических достижений в той области, которой посвящен реферат);

в) определение объекта, предмета исследования;

в) цель данной работы;

г) задачи, требующие решения.

Объем введения – 2 страницы.

– Основная часть (как правило, 2-3 раздела)

В основной части реферата обучающийся дает письменное изложение материала по предложенному плану, используя источники из библиографического списка. В этом разделе работы формулируются основные понятия, их содержание, подходы к анализу, существующие в литературе, точки зрения на суть проблемы, ее характеристики. В соответствии с поставленной задачей делаются выводы и обобщения.

– Заключение

Заключение подводит итог работы. Оно может включать повтор основных тезисов работы, чтобы акцентировать на них внимание, содержать общий вывод, к которому пришел автор реферата, предложения по дальнейшей научной и практической разработке вопроса и т.п.

– Библиографический список

Объём реферата должен составлять 25-30 страниц формата А4. Для визуализации содержания и основных выводов по реферату обучающийся может подготовить презентацию с использованием соответствующего программного обеспечения.

Подготовка к промежуточной аттестации. предполагает целенаправленную, регулярную, систематическую работу при изучении дисциплины в рамках аудиторных занятий и самостоятельной работы. Систематическое выполнение учебной работы на лекциях и практических занятиях, а также в рамках самостоятельной работы позволит успешно освоить дисциплину и создать хорошую базу для успешного прохождения промежуточной аттестации. Непосредственно подготовку к процедуре аттестации рекомендуется осуществлять в соответствии с приведенным в рабочей программе перечнем типовых оценочных материалов для проведения промежуточной аттестации.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература

1. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095 . — Режим доступа: для авториз. пользователей.
2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184. — Режим доступа: для авториз. пользователей.

7.2. Дополнительная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022 . – Режим доступа: по подписке.
2. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 224 с. - ISBN 978-5-9515-0429-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1230827 . – Режим доступа: по подписке.
3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843184 . – Режим доступа: по подписке.

7.3. Нормативные правовые документы.

1. Национальная программа «Цифровая экономика Российской Федерации» (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7). – URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer =https%3a%2f%2fwww.yandex.ru%2f
2. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» – URL: http://www.kremlin.ru/acts/bank/41919

7.4. Интернет-ресурсы

1. Официальный портал СИУ РАНХиГС – URL: http://orel.ranepa.ru.
2. Образовательная платформа Юрайт – URL: https://urait.ru/
3. ЭБС Лань – URL: https://e.lanbook.com/
4. ЭБС Znanium – URL: https://znanium.com/
5. Официальный сайт компании «Консультант Плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/, свободный.
6. Информационно-правовой портал [Электронный ресурс]. – Режим доступа: http://www.garant.ru, свободный.

7.5. Иные источники.

Не предусмотрены

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

Материально-техническая база

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель, проекционное оборудование, доска,
Учебная аудитория для проведения занятий семинарского типа, лабораторных занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель, проекционное оборудование, доска.
Компьютерный класс (аудитория для выполнения самостоятельной работы) /Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная мебель, проекционное оборудование, компьютеры, доска. Компьютеры с выходом в сеть «Интернет» и ЭИОС СИУ РАНХиГС
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

Программное обеспечение

Наименование программного обеспечения	Назначение и тип лицензии программного обеспечения
7-Zip	Архиватор с высокой степенью сжатия Свободная лицензия
Adobe reader – Russian	Просмотр, печать и внесение аннотаций в документы PDF. Свободная лицензия
Adobe Acrobat Reader DC– Russian	Чтение, печать и рецензирование файлов PDF. Свободная лицензия
Google Chrome	Браузер Свободная лицензия
Mozilla FireFox	Браузер. Свободная лицензия
Opera	Браузер. Свободная лицензия
Yandex Браузер	Браузер Свободная лицензия
Apache Open Office	Свободный пакет офисных приложений. Свободная лицензия
Windows 7 Professional Windows 8 Pro Windows 8.1 Pro Windows 10 Pro	Операционные системы. Лицензированная версия
Office Professional Plus 2007 Office Professional Plus 2010 Office Standard 2007 Office Standard 2010 Office Standard 2013	Пакет офисных приложений. Лицензированная версия
Лицензия на право исполь-	Работа с электронными подписями

зования "КриптоАРМ Стандарт" версии 5	
Лицензия на право использования "КриптоПро CSP" версия 4.0.99	Работа с электронными подписями
Консультант Плюс	Справочно-правовая система