Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков
« 11 » сентября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Комплексное обеспечение защиты информации объекта информатизации
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Сформировать компетентности в области разработки комплексной системы защиты информации объекта информатизации, на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности подобных систем.

Задачи дисциплины:

1.изучение сущности, целей и задач комплексной системы защиты информации;
2.изучение принципов и этапов разработки комплексной системы защиты информации;
3.освоение технологии установления состава защищаемой информации и объектов защиты информации на объекте информатизации;
4.овладение методами оценки угроз безопасности информации;
5.изучение параметров и структуры комплексной системы защиты информации;
6.установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации;
7.изучение показателей и методик эффективности системы защиты информации

1.2. Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты:
система защиты информации;
анализ и оценки угроз защищаемой информации;
модель процессов защиты информации;
технологическое и организационное построение системы защиты информации;
кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации на объекте информатизации;
планирование и контроль комплексной системы защиты информации на предприятии;
эффективность системы защиты информации;
аттестации объектов информатизации по требованиям безопасности информации.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.2	ИД-1ПК-1.2	Знать понятие, сущность, цели и задачи комплексной системы защиты информации; Знать принципы организации и этапы разработки комплексной системы защиты информации; Знать факторы, влияющие на организацию комплексной системы защиты информации; Знать технологию определения состава защищаемой информации и объектов защиты; Знать методы моделирования, анализа и оценки угроз защищаемой информации; Знать виды моделей, описывающих процессы защиты информации;	Знает организационные меры по защите информации; основные методы управления защитой информации	Отчёт по практическому занятию
ПК-1.2	ИД-2ПК-1.2	Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; Уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; Уметь формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации; Уметь разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих	Умеет разрабатывать предложения по совершенствованию системой управления защитой информации; осуществлять планирование и организацию работы персонала, с учетом требований по защите информации	Индивидуальное задание

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		работу по защите информации на предприятии;		
ПК-1.2	ИД-3ПК-1.2	Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации; Владеть технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии.	Владеет навыками выработки рекомендаций для принятия решения о модернизации систем защиты информации	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	24	24
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	28	28
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	54	54
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
7-й семестр				
Концептуальные основы разработки комплексной системы защиты информации и определения объектов защиты	8	0	8	18
Тема 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации. Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности объекта информатизации. Принципы организации комплексной системы защиты информации. Тема 2. Методологические и концептуальные основы комплексной системы защиты информации. Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации. Достаточность защиты информации. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации. Тема 3. Определение и нормативное закрепление информации ограниченного доступа. Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа. Тема 4. Определение состава объектов защиты. Понятие объекта защиты. Последовательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации. Методика выявления состава носителей защищаемой информации. Основные и вспомогательные технические средства и системы. Особенности помещений как объектов защиты.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Моделирование угроз безопасности информации и процессов защиты информации на объекте информатизации	6	0	8	18
Тема 5. Источники, способы и результаты дестабилизирующего воздействия на информацию. Определение источников дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации. Классификация угроз без-опасности информации для объекта информатизации. Анализ и оценка угроз информационной безопасности объекта. Тема 6. Выявление каналов утечки и методов несанкционированного воздействия на информацию. Сущность утечки информации и несанкционированного воздействия на ин-формацию. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация. Модель технических каналов утечки информатизации на типовом объекте информатизации. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии. Инсайдерские каналы утечки информации и «социальный инжиниринг» Методы «социального инжиниринга». Тема 7. Моделирование процессов защиты информации. Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации. Понятие архитектуры си-стемы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.				
Особенности построения комплексной системы защиты информации объекта информатизации и оценка ее эффективности	10	0	12	18
Тема 8. Технологическое и организационное построение комплексной системы за-щиты информации. Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура техническо-го задания, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию. Тема 9. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации. Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации. Материально-техническое обеспечение защиты информации. Нормативно-методическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии. Тема 10. Планирование и контроль комплексной системы защиты информации. Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов предприятия и функционирования комплексной системы за-щиты информации. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации. Тема 11. Оценка эффективности комплексной системы защиты информации. Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов. Тема 12. Аттестация объектов информатизации по требованиям безопасности информации. Состав и				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
содержание нормативно - правовых актов по аттестации объектов информатизации. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний. Основы проведения поисковых мероприятий по выявлению закладочных устройств.				
ИТОГО по 7-му семестру	24	0	28	54
ИТОГО по дисциплине	24	0	28	54

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Комплексная система защиты информации на объекте информатизации и принципы ее организации (СЗ)
2	Оценка факторов, влияющих на организацию комплексной системы защиты информации (ПЗ)
3	Этапы работы по выявлению состава защищаемой информации на объекте информатизации (ПЗ)
4	Определение состава объектов защиты на предприятии (ПЗ)
5	Анализ и оценка угроз информационной безопасности объекта информатизации (ПЗ)
6	Выявление каналов утечки информации на предприятии (ПЗ)
7	Задачи и этапы моделирования в процессе построения комплексной системы защиты информации (СЗ)
8	Моделирование процессов защиты информации (ПЗ)
9	Технологическое и организационное построение комплексной системы защиты информации (СЗ)
10	Разработка нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии (ПЗ)
11	Организация планирования и контроля комплексной системы защиты информации на предприятии (СЗ)
12	Применение методов и моделей оценки эффективности систем защиты информации (ПЗ)

№ п.п.	Наименование темы практического (семинарского) занятия
13	Состав и содержание нормативно - правовых актов по аттестации объектов информатизации (СЗ)
14	Организация и проведение процедур аттестации объектов информатизации по требованиям безопасности информации (ПЗ)

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

Проведение практических занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		

1	Грибунин В.Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов / В.Г. Грибунин, В.В. Чудовский. - Москва: Академия, 2009.	23
2	Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. - М.: Гелиос АРВ, 2007.	10
3	Садердинов А. А. Информационная безопасность предприятия : учебное пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. - Москва: Дашков и К, 2004.	13
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Игнатьев В.А. Защита информации в корпоративных информационно-вычислительных сетях: монография / В. А. Игнатьев.— Старый Оскол: ТНТ, 2005	1
2	Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - Москва: Академия, 2009.	10
3	Обеспечение информационной безопасности машиностроительных предприя-тий : учебное пособие для вузов : в 2 ч. / С. А. Клейменов [и др.].— Старый Оскол : ТНТ, Ч. 1.— 2011	1
4	Северин В.А. Правовая защита информации в коммерческих организациях: учебное пособие для вузов / В.А. Северин; Под ред. Б.И. Пугинского.— Москва: Академия, 2009	4
5	Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - Москва: ДМК Пресс, 2017.	3
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Титов А. А. Инженерно-техническая защита информации / Титов А. А. - Москва: ТУСУР, 2010.	http://elib.pstu.ru/Record/lan4959	сеть Интернет; авторизованный доступ
Методические указания для студентов по освоению дисциплины	Круглов Р. С. Обнаружение радиопередающих закладных устройств детектором СВЧ-поля и металлодетектором / Круглов Р. С. - Москва: ТУСУР, 2008.	http://elib.pstu.ru/Record/lan11409	сеть Интернет; авторизованный доступ

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Основная литература	Грибунин В.Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов / В.Г. Грибунин В.В. Чудовский .— Москва : Академия, 2009	http://elib.pstu.ru/Record/RUPSTUbooks128778	сеть Интернет; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных уязвимостей CVE Mitre	https://cve.mitre.org/
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	проектор	1
Практическое занятие	ПК Intel	6
Практическое занятие	проектор	1

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Комплексное обеспечение защиты информации объекта информатизации»
Приложение к рабочей программе дисциплины

Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы:	Организация и технология защиты информации
Квалификация выпускника:	Бакалавр
Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы:	Безопасность открытых информационных систем
Квалификация выпускника:	Специалист
Форма обучения:	Очная

Курс: 4 **Семестр**: 7

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Экзамен: 7 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (7-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим заданиям и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ПЗ**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знать принципы организации и этапы разработки комплексной системы защиты информации объекта информатизации.		ТО1	ПЗ3	Т		ТВ
Освоенные умения						
У.1 Уметь реализовывать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации			ПЗ 5 ПЗ 4 ПЗ 10 ПЗ 11 ПЗ14	Т		ПЗ
Приобретенные владения						
В.1 Владеть навыками и методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации			ПЗ 6 ПЗ 7 ПЗ 8 ПЗ 9 ПЗ 12 ПЗ 13 ПЗ 14	Т		КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1. Характер и степень влияния различных факторов на организацию системы защиты информации на объекте информатизации.

Тема 2. Порядок организации нормативного закрепления информации

ограниченного доступа.
Тема 3. Особенности помещений как объектов защиты.
Тема 4. Базовые модели угроз безопасности различных видов информации ограниченного доступа.
Тема 5. Методы «социального инжиниринга».
Тема 6. Формальные модели безопасности.
Тема 7. Апробация системы защиты информации и ввод ее в эксплуатацию.
Тема 8. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.
Тема 9. Основные контрольные мероприятия по защите информации
Тема 10. Разработка плана проведения контрольных мероприятий по защите информации на объекте информатизации.
Тема 11. Разработка перечня мероприятий по оценке эффективности комплексной системы защиты информации на объекте информатизации.
Тема 12. Разработка модели подготовки и организации аттестационных испытаний объекта информатизации предприятия.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 14 практических занятий. Темы практических занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Сущность комплексной системы защиты информации и принципы ее организации.
2. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия.
3. Принципы организации комплексной системы защиты информации.
4. Методологические и концептуальные основы комплексной системы защиты информации.
5. Методология защиты информации и ее основные задачи.
6. Уровень обеспечения безопасности информации.
7. Достаточность защиты информации.
8. Варианты построения комплексной системы защиты.
9. Методологические и концептуальные основы комплексной системы защиты информации.
10. Основные факторы, влияющие на организацию комплексной системы защиты информации.
11. Характер и степень влияния различных факторов на организацию системы защиты информации.
12. Определение и нормативное закрепление информации ограниченного доступа.
13. Классификация информации по видам тайны и степеням конфиденциальности.
14. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава защищаемой информации.
15. Порядок организации нормативного закрепления информации ограниченного доступа.
16. Определение состава объектов защиты. Понятие объекта защиты. Последовательность определения объекта защиты.
17. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации.
18. Определение состава объектов защиты. Понятие объекта защиты. Методика выявления состава носителей защищаемой информации.
19. Основные и вспомогательные технические средства, и системы. Особенности помещений как объектов защиты.
20. Источники, способы и результаты дестабилизирующего воздействия на информацию. Определение источников дестабилизирующего воздействия на информацию.
21. Источники, способы и результаты дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов.
22. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации.
23. Понятие угрозы безопасности информации. Классификация угроз безопасности информации для объекта информатизации.

24. Понятие угрозы безопасности информации. Анализ и оценка угроз информационной безопасности объекта.
25. Выявление каналов утечки и методов несанкционированного воздействия на информацию.
26. Сущность утечки информации и несанкционированного воздействия на информацию.
27. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация.
28. Модель технических каналов утечки информатизации на типовом объекте информатизации.
29. Выявление каналов утечки и методов несанкционированного воздействия на информацию. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии.
30. Инсайдерские каналы утечки информации и «социальный инжиниринг». Методы «социального инжиниринга».
31. Моделирование процессов защиты информации. Понятие модели и объекта моделирования.
32. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации.
33. Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации.
34. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.
35. Технологическое и организационное построение комплексной системы защиты информации. Общее содержание работ по организации комплексной системы защиты информации.
36. Характеристика технологического и организационного направлений создания комплексной системы защиты информации. Содержание стадий построения комплексной системы защиты информации.
37. Технологическое и организационное построение комплексной системы защиты информации. Общее содержание работ по организации комплексной системы защиты информации.
38. Предпроектное обследование. Назначение и структура технического задания, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.
39. Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации.
40. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации. Материально-техническое обеспечение защиты информации.

41. Нормативно-методическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.
42. Планирование и контроль комплексной системы защиты информации. Понятие, принципы и методы планирования комплексной системы защиты информации.
43. Планирование и контроль комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования.
44. Планирование и контроль комплексной системы защиты информации. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов.
45. Планирование и контроль комплексной системы защиты информации. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации.
46. Оценка эффективности комплексной системы защиты информации. Понятие эффективности и эффективности защиты информации. Требование по защите информации.
47. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации.
48. Оценка эффективности комплексной системы защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии.
49. Оценка эффективности комплексной системы защиты информации. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
50. Аттестация объектов информатизации по требованиям безопасности информации. Состав и содержание нормативно - правовых актов по аттестации объектов информатизации.
51. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации.
52. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа
53. Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок.
54. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний.

55. Аттестационные испытания выделенных помещений. Основы проведения поисковых мероприятий по выявлению закладочных устройств.

Типовые практические задания для контроля освоенных умений:

1. Определить основные бизнес-процессы на объекте информатизации.
2. Определить факторы, влияющие на организацию комплексной системы защиты информации на объекте информатизации.
3. Сформировать перечень сведений конфиденциального характера на объекте информатизации.
4. Определить объекты защиты на объекте информатизации.
5. Провести классификацию угроз безопасности информации для объекта информатизации на объекте информатизации.
6. Разработать модель технического канала утечки информатизации на типовом объекте информатизации предприятия.
7. Разработать модель подсистем защиты информации.
8. Разработать технико-экономическое обоснование комплексной системы защиты информации.
9. Разработать комплект организационно-распорядительных документов, регламентирующих работу по защите информации на объекте информатизации.
10. Разработать план проведения контрольных мероприятий по защите информации на объекте информатизации.
11. Разработать перечень мероприятий по оценке эффективности комплексной системы защиты информации на объекте информатизации.
12. Разработать модель подготовки и организации аттестационных испытаний объекта информатизации предприятия.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.