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

« 10 » июля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Разработка и эксплуатация автоматизированных систем в защищенном исполнении
(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

Цель дисциплины - формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации.
- изучение основных угроз безопасности информации в автоматизированных системах и освоение методик оценки данных угроз;
- изучение методов, способов, средств, последовательности и содержания этапов раз-работки автоматизированных систем и подсистем безопасности автоматизирован-ных систем;
- изучение основных мер по защите информации в автоматизированных системах;
- изучение содержания и порядка деятельности персонала по эксплуатации защищен-ных автоматизированных систем и подсистем безопасности автоматизированных систем.

1.2. Изучаемые объекты дисциплины

- модели данных, систем и процессов защиты информации;
- стандарты оценки защищенности автоматизированных систем;
- критерии оценки защищенности автоматизированных систем;
- угрозы безопасности информации в автоматизированных системах;
- базовая модель угроз безопасности информации;
- модель нарушителя в автоматизированной системе;
- методы и модели оценки угроз безопасности автоматизированных систем;
- стадии и этапы разработки автоматизированных систем;
- средства автоматизации проектирования автоматизированных систем;
- состав работ по защите информации на стадиях и этапах создания автоматизирован-ных систем;
- меры по защите информации в автоматизированных системах;
- содержание и порядок деятельности персонала по эксплуатации защищенных авто-матизированных систем и подсистем безопасности автоматизированных систем;
- методы, способы и средства обеспечения отказоустойчивости.

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
ОПК-16	ИД-1ОПК-16	Знает критерии оценки эффективности защищенности автоматизированных систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Отчёт по практическому занятию
ОПК-16	ИД-2ОПК-16	Умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области информационной безопасности	Умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области	Отчёт по практическому занятию
ОПК-16	ИД-3ОПК-16	Владеет навыками определения требований по защите информации в автоматизированных системах	Владеет навыками определения требований по защите информации в автоматизированных системах	Отчёт по практическому занятию
ОПК-17	ИД-1ОПК-17	Знает принципы организации и структуру систем защиты информации автоматизированных систем;	Знает принципы организации и структуру систем защиты информации современных операционных систем; средства защиты информации систем управления базами данных;	Отчёт по практическому занятию
ОПК-17	ИД-2ОПК-17	Умеет проводить установку и настройку современных средств защиты информации автоматизированных систем	Умеет проводить установку и настройку современных операционных систем с учетом требований по обеспечению информационной безопасности; восстанавливать	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
			операционные системы после сбоев; реализовывать политику безопасности в локальной вычислительной сети; конфигурировать средства защиты информации систем управления базами данных	
ОПК-17	ИД-3ОПК-17	Владеет навыками использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем	Владеет навыками использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	48	48
- лекции (Л)	22	22
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	22	22
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	60	60
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

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
8-й семестр				
Введение в дисциплину. История развития, назначение и классификация автоматизированных систем	2	0	2	4
Введение в дисциплину. Основные понятия и положения защиты информации в автоматизированных системах. Этапы развития информационных и автоматизированных систем. Классификация задач, решаемых с использованием автоматизированных систем. Модели данных, систем и процессов защиты информации в автоматизированных системах. Требования к моделям защиты информации в автоматизированных системах.				
Критерии оценки защищенности автоматизированных систем	2	0	2	6
Международные стандарты оценки защищенности. Оценка защищенности на основе отечественных стандартов. История формирования общих критериев. Общий подход к формированию критериев оценки безопасности информационных технологий. Модель разработки объекта оценки. Последовательность формирования требований и спецификаций. Понятие профиля защиты и его особенности. Требования общих критериев и результаты оценки.				
Определение и содержание понятия угрозы безопасности автоматизированных систем	2	0	2	4
Особенности современных автоматизированных систем как объектов информационного воздействия, критерии оценки их защищенности. Уязвимости информационно-технологических ресурсов автоматизированных систем. Основные угрозы безопасности ин-формации автоматизированных систем и их классификация. Понятие модели нарушителя в автоматизированной системе. Мониторинг угроз безопасности автоматизированных систем				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Оценка угроз безопасности автоматизированных систем	2	0	2	4
Цели и задачи оценки угроз безопасности автоматизированных систем. Понятие базовой модели угроз безопасности информации. Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем. Методы и модели анализа угроз. Базовая модель угроз информационной системы персональных данных и порядок ее использования. Оценка угроз безопасности информационных систем персональных данных.				
Стадии и этапы разработки автоматизированных систем	2	0	2	6
Жизненный цикл автоматизированной системы. Методы, способы, средства, последовательность и содержание стадий и этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Задачи и этапы проектирования автоматизированных систем. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. Понятие автоматизированного проектирования. Системы автоматизированного проектирования. Средства автоматизации проектирования автоматизированных систем: общая характеристика, назначение и возможности, классификация. Структура программного обеспечения САПР. Автоматизированные системы проектирования средств и подсистем безопасности.				
Разработка автоматизированных систем в защищенном исполнении	2	0	2	6
Общие требования по разработке автоматизированных систем в защищенном исполнении. Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.				
Реализация моделей безопасности автоматизированных систем	2	0	2	6
Модель реализации многоуровневой защиты автоматизированной системы. Реализация «ядра безопасности». Основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические).				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Механизмы и методы защиты в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.				
Особенности разработки информационных систем персональных данных.	2	0	2	6
Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности. Особенности защиты среды виртуализации				
Общие понятия по эксплуатации автоматизированных систем	2	0	2	6
Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.				
Администрирование информационной безопасности автоматизированных систем	2	0	2	6
Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обя-занности администратора информационной безопасности автоматизированных систем. За-щита носителей информации резервное копирование и восстановление данных. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.				
Особенности эксплуатации автоматизированных систем в защищенном исполнении	2	0	2	6
Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Перечень основных эксплуатационных документов защищенных ав-томатизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Тех-нический паспорт на автоматизированную систему. Методы				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.				
ИТОГО по 8-му семестру	22	0	22	60
ИТОГО по дисциплине	22	0	22	60

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Модели данных, систем и процессов защиты информации в автоматизированных системах (ПЗ)
2	Критерии оценки защищенности автоматизированных систем
3	Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем
4	Оценка угроз безопасности информационных систем персональных данных (ПЗ)
5	Стадии и этапы разработки автоматизированных систем
6	Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении
7	Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем
8	Порядок разработки информационных систем персональных данных (ПЗ)
9	Задачи, функции и обязанности администратора информационной безопасности автоматизированных систем.
10	Особенности эксплуатации автоматизированных систем в защищенном исполнении
11	Особенности ведения эксплуатационной документации (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.

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	Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. - Москва [и др.]: ДиаСофт, 2002.	7
2	Информационная безопасность и защита информации : учебное пособие для вузов / Ю. Ю. Громов [и др.]. - Старый Оскол: ТНТ, 2010.	5
3	Липаев В.В. Программно-технологическая безопасность информационных систем / В.В.Липаев. - М.: Изд-во МИФИ, 1997.	1

4	Малюк А. А. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - Москва: Горячая линия-Телеком, 2001.	11
5	Михайлов С. Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции : учебное пособие / С. Ф. Михайлов, В. А. Петров, Ю. А. Тимофеев. - Москва: Изд-во МИФИ, 1995.	1
6	Чипига А.Ф. Информационная безопасность автоматизированных систем : учебное пособие для вузов / А.Ф. Чипига. - Москва: Гелиос АРВ, 2010.	2
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Бондарев В. В. Введение в информационную безопасность автоматизированных систем : учебник / В. В. Бондарев. - Москва: Изд-во МГТУ им. Н. Э. Баумана, 2016.	2
2	Васильков А. В. Безопасность и управление доступом в информационных системах : учебное пособие для среднего профессионального образования / А. В. Васильков, И. А. Васильков. - Москва: ФОРУМ, 2010.	3
3	Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И.Т.Л. Попов. - М.: ФОРУМ, 2009.	5
4	Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013.	11
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	Правовые основы организации защиты персональных данных	https://books.ifmo.ru/file/pdf/1570.pdf	сеть Интернет; свободный доступ

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

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Среды разработки, тестирования и отладки	Microsoft Visual Studio (подп. Azure Dev Tools for Teaching)

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-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

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 «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»

Приложение к рабочей программе дисциплины

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы:	Безопасность открытых информационных систем
Квалификация выпускника:	Специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	Очная

Курс: 4 **Семестр**: 8

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

Форма промежуточной аттестации:
Экзамен: 8 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 (8-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенции **ОПК-14**: способен осуществлять разработку, внедрение и эксплуатацию автоматизированной системы с учетом требований по защите информации и проводить подготовку исходных данных для технико-экономического обоснования проектных решений. З*нать, 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 Знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах **З.2 Знает** принципы организации и структуру систем защиты информации автоматизированных систем		ТО1	ПЗ1 ПЗ2 ПЗ7	Т		ТВ
Освоенные умения						
У.1 Умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; определять структуру системы защиты информации автоматизированной системы в соответствии с			ПЗ 2 ПЗ 3 ПЗ 6 ПЗ 8 ПЗ 10	Т		ПЗ

требованиями нормативных правовых документов в области информационной безопасности **У.2 Умеет** проводить установку и настройку современных средств защиты информации автоматизированных систем						
Приобретенные владения						
В.1 Владеет навыками определения требований по защите информации в автоматизированных системах **В.2 Владеет навыками** использования средств операционных систем для обеспечения безопасного функционирования автоматизированных систем			ПЗ 4 ПЗ 5 ПЗ 7 ПЗ 9 ПЗ 11	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:

Раздел 1, модуль 1

Тема 1. Общие требования по безопасности информации в автоматизированной системе.

Тема 2. Последовательность формирования требований по безопасности информации.

Тема 3.Разработка частной модели угроз безопасности информации.

Тема 4.Оценка угроз безопасности информации в автоматизированной системе.

Раздел 2, модуль 2

Тема 5. Организация работ по созданию автоматизированной системы.

Тема 6. Автоматизация проектирования автоматизированной системы.

Тема 7. Техническое задание на создание автоматизированной системы в защищенном исполнении.

Тема 8. Требования к автоматизированной системе по защите от НСД.

Раздел 3, модуль 3

Тема 9. Средства обеспечения отказоустойчивости автоматизированной системы.

Тема 10. Порядок выполнения обязанностей администратора информационной безопасности автоматизированной системы.

Тема 11. Эксплуатационная документация защищенной автоматизированной системы.

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 11 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. Понятие автоматизированной системы (АС), ее основное предназначение.
2. Разновидности классификации и варианты реализации АС.
3. Понятие автоматизированной системы обработки данных и ее особенности.
4. Исторические этапы развития информационных систем.
5. Модели данных, систем и процессов защиты информации в АС.
6. Стандарты в области информационной безопасности. Оценочные стандарты и спецификации.
7. Международные стандарты оценки защищенности АС.
8. Отечественные стандарты и руководящие документы о защите информации в АС.
9. Критерии оценки безопасности информационных технологий. Среда безопасности объекта оценки.
10. Особенности современных АС как объектов защиты.
11. Актуальные угрозы безопасности информации АС и их классификация.
12. Разработка модели угроз безопасности информации в АС. Модель нарушителя.
13. Базовая модель угроз ИС ПДн, содержание и порядок использования.
14. Цель, задачи и этапы оценки угроз безопасности информации. Разработка частной модели угроз ИС ПДн.
15. Общая характеристика стадий, этапов и задач разработки АС.
16. Содержание предпроектной группы стадий и этапов разработки АС.
17. Содержание группы стадий и этапов работ по проектированию АС.
18. Содержание группы стадий и этапов работ по вводу в эксплуатацию АС.
19. Особенности и основные понятия автоматизированного проектирования.
20. Структура системы автоматизированного проектирования (САПР). Классификация САПР.
21. Автоматизированное проектирование систем (подсистем) безопасности и защиты информации.

22. Понятие системы защиты АС в защищенном исполнении и требования к ней.

23. Участники работ по созданию (модернизации) АС в защищенном исполнении.

24. Общие требования по разработке АС в защищенном исполнении.

25. Состав комплекса работ по созданию системы ЗИ АС в защищенном исполнении.

26. Работы по защите информации на стадии разработки АС: «Формирование требований».

27. Работы по защите информации на стадии разработки АС: «Разработка концепции АС».

28. Работы по защите информации на стадии разработки АС: «Техническое задание».

29. Работы по защите информации на стадии разработки АС: «Эскизный проект».

30. Работы по защите информации на стадии разработки АС: «Технический проект».

31. Работы по защите информации на стадии разработки АС: «Рабочая документация».

32. Работы по защите информации на стадии разработки АС: «Ввод в действие».

33. Работы по защите информации на стадии разработки АС: «Сопровождение АС».

34. Требования по защите сведений о создаваемой АС. Перечень информации о создаваемой (модернизируемой) АС, подлежащей защите.

35. Содержание модели многоуровневой защиты информации в АС.

36. Модель реализации «ядра безопасности» в АС. Монитор обращений. Условие гарантированного выполнения политики безопасности.

37. Моделирование систем управления доступом. Способы представления информации о правах доступа.

38. Основные рекомендуемые меры по защите информации в АС (в соответствии с СТР-К).

39. Состав общих требований по защите персональных данных в информационных системах.

40. Состав и содержание организационных и технических мер по защите ПДн в ИС ПДн.

41. Порядок формирования базовых требований по защите ПДн, в соответствии с уровнем защищенности.

42. Порядок адаптации и уточнения мер по обеспечению безопасности ПДн. Требования к применяемым средствам обработки и защиты информации.

43. Цели, задачи и принципы администрирования в АС. Функции и задачи администратора АС.

44. Административный персонал АС и работа с пользователями.

45. Управление эксплуатацией АС. Принципы управляемости.

46. Автоматизация управления сетью. Сетевая служба.

47. Общие обязанности администратора информационной безопасности АС.

48. Общие требования по обеспечению безопасности объектов КИИ.

49. Мероприятия по защите объектов КИИ при разработке и эксплуатации.

50. Требования к мерам по защите информации, в соответствии с категорией значимости объекта КИИ.

Типовые практические задания для контроля освоенных умений:

1. Определить виды информации ограниченного доступа и состав носителей информации обрабатываемые в автоматизированной системе.

2. Изучить порядок формирования и структуру Банк данных уязвимостей информационных систем.

3. Классифицировать состав угроз информационной безопасности. Определить состав актуальных угроз безопасности информации для автоматизированной системы на основе БДУ.

4. Разработать модель угроз безопасности информации ИС ПДн.

5. Разработать макет технического задания (ТЗ) на автоматизированную систему в защищенном исполнении в составе основных разделов.

6. Определить состав применяемых сервисов безопасности программно-технического уровня для варианта автоматизированной системы, с учетом особенностей объекта информатизации.

7. Представить вариант модели данных, систем и процессов защиты информации в автоматизированной системе.

8. Разработать модель многоуровневой защиты автоматизированной системы с учетом рубежей безопасности на уровнях:

- административном;
- процедурном;
- программно-техническом.

В составе программно-технического уровня защиты автоматизированной системы предусмотреть:

- уровень защиты периметра (firewall, СОВ);
- уровень защиты внутренней сети (VLAN: IPSec, персональные МЭ);
- уровень защиты узлов (серверов и АРМ, конфигурация, ПО НСД);
- уровень защиты приложений (настройки, обновления, АЗ);
- уровень защиты данных (файловая система, шифрование).

9. Разработать модель разрешительной системы доступа к ресурсам автоматизированной системы одним из способов представления информации о правах доступа в информационной системе:

- по спискам полномочий субъектов доступа;
- по спискам управления доступом к объекту.

10. Сформировать матрицу полномочий доступа для варианта информационной системы.

11. Сформировать перечень основных мер по обеспечению безопасности информации для ИСПДн 1,2,3,4 УЗ.

12. Предложить состав мер по противодействию утечке информации в автоматизированной системе.

13. Определить класс защиты СВТ для:
- ГИС 1 класса защищенности;
- АСУ 2 класса защищенности;
- ИС ПДн 1 уровня защищенности;
- ИС ПДн 3 уровня защищенности;
- ИС ПДн 4 уровня защищенности.

11. Определить класс защиты СОВ и АВЗ для:
- ИС, содержащей сведения, отнесенные к ГТ «Секретно», АВЗ типа «А»;
- ГИС, не содержащих сведения, отнесенных к ГТ, АВЗ типа «Б»;
- ИС ПДн 2 уровня защищенности, АВЗ типа «В».

12. Определить класс защиты СДЗ для:
- ИС, содержащей сведения, отнесенные к ГТ «Совершенно секретно»;
- ГИС 3 класса, взаимодействующих с сетями МИО;
- ИС ПДн 3 уровня защищенности, без доступа к сетям МИО.

13. Определить класс защиты средств КСН для:
- ИС, не содержащей сведения, отнесенные к ГТ;
- ГИС 2 класса;
- ИС ПДн 4 уровня защищенности.

14. Осуществить подбор межсетевого экрана для:
- ГИС 1 класса защищенности, типа «А»;
- АСУ 2 класса защищенности, типа «Д»;
- ИС ПДн 1 уровня защищенности, типа «Б»;
- ИС ПДн 3 уровня защищенности, типа «Г»;
- ИС ПДн 4 уровня защищенности, типа «В».

15. Разработать технический паспорт и перечень эксплуатационной документации на автоматизированную систему в защищенном исполнении.

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.