МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

СОГЛАСОВАНО
Руководитель ОП

Р.И. Дремлюга

«17» июня .2019 г.

УТВЕРЖДАЮ
Директор Школы цифровой экономики

И.Г. Мирин

«17» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ПРОЕКТИРОВАНИЕ И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ СИСТЕМ
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»

Форма подготовки очная

курс 1, 2 семестр 2,3,4
лекции 74 час.
практические занятия 92 час.
лабораторные работы 0 час.
всего часов аудиторной нагрузки 166 час.
самостоятельная работа 158 час.
контрольные работы программой не предусмотрены
курсовая работа/проект – не предусмотрено
зачет с оценкой 2 семестр
экзамен – 3, 4 семестр

Рабочая программа составлена в соответствии составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918.
Рассмотрена и утверждена на заседании Дирекции Школы цифровой экономики «17» июня 2019 года (протокол № 124-01-07-05).

Составитель: к.т.н., с.н.с., Ю.В. Добржинский, С.С. Зотов

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № _____

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ

Б1.В.01.01 ПРОЕКТИРОВАНИЕ И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ СИСТЕМ

Рабочая программа учебной дисциплины «Проектирование и эксплуатация защищенных систем» предназначена для студентов, обучающихся по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры), профиль «Кибербезопасность».

Дисциплина ««Проектирование и эксплуатация защищенных систем» входит в часть, формируемую участниками образовательных отношений, блока «Дисциплины (модули)» (Б1.В.01) учебного плана подготовки магистров, модуля методов и программного обеспечения защиты информации.

Общая трудоемкость освоения дисциплины составляет 11 зачетных единиц, 396 часов. Дисциплина реализуется на 1 и 2 курсе в 2, 3 и 4 семестрах.

Семестр	Аудиторные занятия			Самостоя-тельная работа	Контроль	Всего по дисциплине	
	Лекции	Лабора торные работы	Всего			Часы	Зачетные единицы
2 семестр	18	-	36	54	Зачет с оценкой	108	3
3 семестр	36	-	36	72	Экзамен	180	5
4 семестр	20	-	20	32	Экзамен	108	3
Всего	**74**	**-**	**92**	**158**		**396**	**11**

Цель дисциплины – обучение магистрантов теоретическим основам и практическим навыкам проектирования и эксплуатации защищенных систем с помощью современных методологий и типовых схем проектирования.

Задачи дисциплины:

- формирование знаний о способах проектирования и документального оформления процесса разработки защищенных автоматизированных систем на основе специализированных международных

стандартов

- формирование базовых навыков в области методологии оценки защищенности автоматизированных систем;
- формирование структурированного знания технологического цикла реализации защищенной системы обработки и хранения информации.
- формирование практических навыков, знаний о методах организации и регламентации процесса эксплуатации защищенных автоматизированных систем.

В результате данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-2.1 Знает: модели безопасности компьютерных сетей; виды политик безопасности компьютерных систем и сетей; нормативно-правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации; организационные меры по защите информации ПК-2.2 Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем ПК-2.3 Владеет: навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработки руководящих документов по защите информации в организации
ПК-3 Способен проводить анализ безопасности компьютерных систем	ПК-3.1 Знает: принципы построения компьютерных систем и сетей; уязвимости компьютерных систем и сетей; криптографические методы защиты информации; принципы построения систем управления базами данных; средства анализа конфигураций; национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите

	информации ПК-3.2 Умеет: анализировать компьютерную систему с целью определения уровня защищенности и доверия; прогнозировать возможные пути развития действий нарушителя информационной безопасности; производить анализ политики безопасности на предмет адекватности; проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; составлять и оформлять аналитический отчет по результатам проведенного анализа; разрабатывать предложения по устранению выявленных уязвимостей ПК-3.3 Владеет навыками: определения уровня защищенности и доверия в компьютерных системах; оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; оценки соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	ПК-4.1 Знает: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях ПК-4.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-4.3 Владеет навыками: анализа защищенности компьютерных систем с использованием сканеров безопасности и защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Проектирование защищенных автоматизированных систем

Тема 1. Защищенные АИС. Основные понятия и классификация

1.1. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Классификация АИС. Информационные технологии, используемые в АИС. Жизненный цикл АИС. Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах.

Тема 2. Основы организации проектирования защищенных АИС

2.1. Последовательность и содержание этапов проектирования АИС. Методы, способы и средства проектирования автоматизированных систем и подсистем безопасности автоматизированных систем.

2.2. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АИС. Методы обеспечения информационной безопасности АИС.

Тема 3. Общие принципы проектирования защищенных АИС

3.1. Проектирование защищенных АИС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания.

3.2. Построение комплексной защиты АИС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АИС. Технологии создания отказоустойчивых систем.

Тема 4. Средства автоматизации проектирования автоматизированных информационных систем. Средства построения пользовательского интерфейса

Раздел II. Эксплуатация защищенных автоматизированных систем.

Тема 5. Основы эксплуатации защищенных АИС

5.1. Аттестация АИС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АИС на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС. Порядок обеспечения защиты информации при эксплуатации АИС.

5.2. Технические и программные средства защиты АИС от несанкционированного доступа. Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации. Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации.

Тема 6. Диагностика программных и аппаратных средств АИС

6.1. Средства диагностирования защищенных АИС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АИС. Технологическое оборудование для ремонта аппаратных средств АИС.

6.2. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования. Аппаратно-программные средства диагностики АИС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.

Тема 7. Проектные структуры управления: понятие «проектная структура управления». Виды проектных структур управления.

Тема 8. Контроль и регулирование при реализации проекта. Обеспечение качества проекта. Качество программного и аппаратного обеспечения.

Тема 9. Управление завершением проекта. Технологии и методы управления проектами.

II. СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНОЙ И ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практическая работа

Практическое занятие № 1 Тема: Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах.

Практическое занятие № 2 Тема: Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем

Практическое занятие № 3 Тема Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Методы обеспечения информационной безопасности АИС

Семинарское занятие № 4 Тема: Методы проектирования защищенных АИС. Структура и содержание технического задания

Семинарское занятие № 5 Тема: Основы проектирования комплексной защиты информационной безопасности от НСД. Технологии создания отказоустойчивых систем.

Семинарское занятие № 6 Тема Аттестация АИС по требованиям безопасности. Особенности эксплуатации АИС на объекте защиты. Порядок обеспечения защиты информации при эксплуатации АИС

Семинарское занятие № 7 Тема Технические и программные средства защиты АИС от несанкционированного доступа. Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации.

Семинарское занятие № 8 Тема Аппаратно-программные средства диагностики АИС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.

Семинарское занятие № 9 Тема Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0. –

Семинарское занятие № 10 Тема Оценка общих критериев и определение класса защищенности автоматизированной системы.

Семинарское занятие № 11 Тема – Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Семинарское занятие № 12 Тема Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия. Анализ реализации модулей автоматизированных систем . Анализ полноты проектной документации

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине ««Проектирование и эксплуатация защищенных систем» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства – наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Проектирование защищенных автоматизированных систем	ПК-2, ПК-3, ПК-4	знает	ПР-7	1-7
			умеет	ПР-5	1-7
			владеет	ПР-5	1-7
2	Раздел II. Эксплуатация защищенных автоматизированных систем.	ПК-2, ПК-3, ПК-4	знает	ПР-7	8-13
			умеет	ПР-5	8-13
			владеет	ПР-5	8-13

Фонд оценочных средств, определяющий процедуру оценивания знаний, умений и навыков и (или) опыта деятельности; критерии и показатели, необходимые для оценки знаний, умений, навыков, а также оценочные средства для промежуточной аттестации и список вопросов на зачет представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература
(электронные и печатные издания)

1. Комплексная защита информации в корпоративных системах: учебное пособие для вузов / В. Ф. Шаньгин. - М.: ФОРУМ, 2012 ; М. : ИНФРА-М, 2012. - 592 с.

2. Полковников А.В. Управление проектами. Полный курс MBA / А.В. Полковников, М.Ф. Дубовик. – М.: ЗАО «Олимп-Бизнес», 2015 – 552 с. \

3. Фуфаев Д.Э., Фуфаев Э.В. Разработка и эксплуатация автоматизированных информационных систем Учебник. — 3-е изд., стер. — М.: Академия, 2014. — 304 с. — (Профессиональное образование). — ISBN 978-5-4468-1097-0.

4. Малюк А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. – М.: ГЛТ, 2015. – 230 с

Дополнительная литература
(печатные и электронные издания)

1. Бондарев В. Введение в информационную безопасность автоматизированных систем: Учебное пособие / В. Бондарев. – МГТУ им. Н.А. Баумана, 2016. – 252 с.

2. Казарин О.В. Надежность и безопасность программного обеспечения: Учебное пособие для бакалавриата и магистратуры / О.В. Казарин, И.Б. Шубинский, 2018. – 342 с.

3. Управление проектными рисками: учебно-методическое пособие для практических занятий [Электронный ресурс] / сост. О. И. Бабина. – Электрон. дан. – Красноярск: Сиб. федер. Ун-т, 2013.

4. Сравнительный анализ средств защиты информации от несанкционированного доступа [Электронный ресурс]. URL: https://interactive-plus.ru/ru/action/150/action_articles?page=4

5. Щеглов А. Ю. Компьютерная безопасность. Как выбрать средство защиты информации? // Информационные технологии в бизнесе URL: http://www.npp-itb.spb.ru/publications/15.html.

6. Баранова Е. Информационная безопасность и защита: Учебное пособие / Е. Баранова, А.Бабаш. – РИОР, Инфра-М, 2017. – 324 с.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество часов, отведенных на изучение дисциплины «Проектирование и эксплуатация защищенных систем», составляет 288 часов. На самостоятельную работу – 157 часов.

Аудиторная нагрузка состоит из 36 лекционных часов и 72 часов практических и лабораторных работ. На лекционных занятиях обучающийся получает теоретические знания, усвоение которых необходимо для дальнейшего выполнения практических работ. Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

Подготовка к практическим работам предполагает повторение лекционного материала. В результате выполнения работы студент предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы, результаты и выводы о проделанной работе.

В рамках указанной дисциплины итоговой формой аттестации является зачет. Вопросы к зачету/экзамену соответствуют темам, изучаемым на лекционных занятиях. Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников из списка литературы и материалов по практическим работам.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения лекционных, практических и практических занятий необходима оборудованная персональными компьютерами аудитория с мультимедиа проектором.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебная аудитория для занятий семинарского типа 690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10 Здание ФЭК корпус А, лит О, ауд. G468	Комплект специализированной мебели: доска аудиторная – 1 шт.; парты – 30 шт.; стул -30 шт.; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi,; Системный блок с монитором. Процессор: Intel I5-8600k 3.6Ghz, оперативная память: 32gb, жесткий диск: 1ТБ, графический ускоритель: Nvidia GTX 1080 Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS).

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Проектирование и эксплуатация защищенных систем»
Направление подготовки 09.04.01 Информатика и вычислительная техника
Магистерская программа
«Кибербезопасность»
Форма подготовки очная

Владивосток
2018

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-4 неделя обучения	Подготовка практического задания (выполнение отчета к работе №1)	4	Отчеты о выполнении
2	5-8 неделя обучения	Подготовка практического задания (выполнение отчета к работе №2)	4	Отчеты о выполнении
3	9-12 неделя обучения	Подготовка практического задания (выполнение отчета к работе №3)	5	Отчет о выполнении
4	12-14 неделя обучения	Подготовка к семинарному занятию (выполнение отчета к работе №4)	5	Отчет о выполнении
5	15-17 неделя обучения	Подготовка семинарному занятию (выполнение отчета к работе №5)	5	Отчеты о выполнении
6	18 неделя обучения	Подготовка к зачету	8	Зачет

Подготовка отчета по практическим работам предполагает повторение лекционного материала и выполнение задания для практических работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Самостоятельная работа при подготовке к зачету/экзамену включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к зачету, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Проектирование и эксплуатация защищенных систем»
Направление подготовки 09.04.01 Информатика и вычислительная техника
Магистерская программа
«Кибербезопасность»

Форма подготовки очная

Владивосток
2018

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-2.1 Знает: модели безопасности компьютерных сетей; виды политик безопасности компьютерных систем и сетей; нормативно-правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации; организационные меры по защите информации ПК-2.2 Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем ПК-2.3 Владеет: навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработки руководящих документов по защите информации в организации
ПК-3 Способен проводить анализ безопасности компьютерных систем	ПК-3.1 Знает: принципы построения компьютерных систем и сетей; уязвимости компьютерных систем и сетей; криптографические методы защиты информации; принципы построения систем управления базами данных; средства анализа конфигураций; национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации ПК-3.2 Умеет: анализировать компьютерную систему с целью определения уровня защищенности и доверия; прогнозировать возможные пути развития действий нарушителя информационной безопасности; производить анализ политики безопасности на предмет адекватности; проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; составлять и оформлять аналитический отчет по результатам проведенного анализа; разрабатывать предложения по устранению выявленных уязвимостей ПК-3.3 Владеет навыками: определения уровня защищенности и доверия в компьютерных системах; оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; оценки соответствия механизмов безопасности компьютерной системы

	требованиям существующих нормативных документов, а также их адекватности существующим рискам
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	ПК-4.1 Знает: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях ПК-4.2 Умеет: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет ПК-4.3 Владеет навыками: анализа защищенности компьютерных систем с использованием сканеров безопасности и защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства – наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Проектирование защищенных автоматизированных систем	ПК-2, ПК-3, ПК-4	знает	ПР-7	1-7
			умеет	ПР-5	1-7
			владеет	ПР-5	1-7
2	Раздел II. Эксплуатация защищенных автоматизированных систем.	ПК-2, ПК-3, ПК-4	знает	ПР-7	8-13
			умеет	ПР-5	8-13
			владеет	ПР-5	8-13

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачет.

Для допуска к зачету обучающийся должен получить оценку «зачтено» по всем практическим работам курса. Критерии оценивания практических работ представлены далее в данном Приложении.

Зачет проводится в форме собеседования (УО-1), вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на зачете обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;

- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для промежуточной аттестации
Список вопросов на зачет/экзамен

1. Планирование проекта. Общие сведения, подходы к планированию, блок-схема результата
2. Планирование проекта. Деятельность планирования, распределение ресурсов, использование программных средств для планирования
3. Организация проекта. Общие сведения, программы и проекты, определение заинтересованных лиц и их проблемы, организационная структура, желательные характеристики менеджера проекта, офис-поддержки проектов.
4. Организация проекта. Команда проекта, управление таблиц, построение таблицы, динамика команд, стили управления, методы связи.
5. Информационные технологии, используемые в АИС.
6. Основные угрозы безопасности информации в автоматизированных системах.
7. Модели нарушителя в автоматизированных системах.
8. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизиро- ванных систем.
9. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
10. Методы обеспечения информационной безопасности АИС.
11. Методы и этапы проектирования защищенных АИС.
12. Построение комплексной защиты АИС.
13. Основы проектирования комплексной защиты информационной безопасности от НСД.
14. Средства обеспечения надежности защищенных АИС.
15. Технологии создания отказоустойчивых систем.
16. Аттестация АИС по требованиям безопасности.
17. Особенности эксплуатации АИС на объекте защиты.
18. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС.
19. Порядок обеспечения защиты информации при эксплуатации АИС.
20. Технические и программные средства защиты АИС от несанкционированного доступа.
21. Организация технического обслуживания защищенных АИС.
22. Методы проверки защищенных АИС.

23. Средства диагностирования защищенных АИС.

24. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АИС.

25. Технологическое оборудование для ремонта аппаратных средств АИС

26. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования.

27. Аппаратно-программные средства диагностики АИС.

28. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.

Каждый студент должен ответить на два вопроса из списка выше. Результаты зачета оцениваются по двухбалльной системе («зачтено», «не зачтено») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- знание основных терминов и понятий курса;
- знание и владение методами и средствами решения задач;
- последовательное изложение материала курса;
- умение формулировать некоторые обобщения по теме вопросов;
- достаточно полные ответы на вопросы;
- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«зачтено».** Хорошее знание основных терминов и понятий курса. Хорошее знание и владение методами и средствами решения задач. Последовательное изложение материала курса. Умение формулировать некоторые обобщения по теме вопросов. Достаточно полные ответы на вопросы. Умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«не зачтено».** Неудовлетворительное знание основных терминов и понятий курса. Неумение решать задачи. Отсутствие логики и последовательности в изложении материала курса. Неумение формулировать отдельные выводы и обобщения по теме вопросов. Неумение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для текущей аттестации

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся практические работы. Темы практические работ

представлены в Разделе II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Критерий
Зачтено	Отчёт по практической работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ.
Незачтено	Отчёт по практической работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ.