МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000E97B12
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» является теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой и эксплуатацией защищенных автоматизированных информационных систем в своей профессиональной деятельности; формирование у обучаемых профессиональных компетенций в эксплуатационно-технической и научно-исследовательской областях профессиональной деятельности в соответствии с ОП специальности 10.05.03 - «Информационная безопасность автоматизированных систем».

Задачи дисциплины: К задачам дисциплины относятся ознакомление с теоретическими основами процесса разработки защищенных автоматизированных систем; изучение основ эксплуатации защищенных автоматизированных систем изучение средств описания данных и средств описания действий языков программирования; овладение навыками разработки защищенных автоматизированных систем

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-11 : Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.2к : разрабатывает компоненты комплексных систем защиты информации автоматизированных систем	РД1	Знание	принципы и методы построения защищенных автоматизированных систем
			РД2	Умение	разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
			РД3	Навык	синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
	ОПК-14 : Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных	ОПК-14.1к : понимает основные принципы организации технического, программного обеспечения защищенных информационных систем; оптимального проектирования	РД4	Знание	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ,

	для технико-экономического обоснования проектных решений	защищенных информационных систем; оценки показателей эффективности защищенных информационных систем			метод экспертных структурных вопросников
			РД5	Умение	определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники; оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ); создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем
			РД6	Навык	методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ
	ОПК-5.2 : Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;	ОПК-5.2.2к : интегрирует систему защиты информации в текущую информационно-техническую инфраструктуру	РД7	Знание	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

			РД8	Умение	исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Формирование чувства гордости за достижения России	Гражданственность	Дисциплинированность
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Взаимопомощь и взаимоуважение	Внимательность к деталям
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Гражданственность	Внимательность к деталям
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Взаимопомощь и взаимоуважение	Коммуникабельность

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к базовой части дисциплин учебного плана направления «Информационная безопасность автоматизированных систем».

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Методы проектирования защищенных распределенных информационных систем», «Основы информационной безопасности». На данную дисциплину опираются «Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты», «Производственная преддипломная практика»

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	10	6	98	36	36	0	1	25	118	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Базовые понятия информационной безопасности вычислительных сетей	РД1, РД2, РД3, РД4, РД5	8	8	0	11	Тестовые задания, практические работы
2	Разработка защищенных автоматизированных систем	РД1, РД3, РД4, РД5, РД6	8	8	0	35	Тестовые задания, практические работы
3	Основы эксплуатации защищенных автоматизированных информационных систем	РД3, РД4, РД7	10	10	0	36	Тестовые задания, практические работы

4	Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем	РД2, РД5, РД6, РД7, РД8	10	10	0	36	Тестовые задания, практические работы
Итого по таблице			**36**	**36**	**0**	**118**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Базовые понятия информационной безопасности вычислительных сетей.

Содержание темы: Защищенные автоматизированные системы. Основные понятия и классификация Оценка защищенности автоматизированных систем. Критерии оценки защищенности автоматизированных систем. Определение и содержание понятия угрозы безопасности автоматизированных систем. Оценка угроз безопасности автоматизированных систем.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 2 Разработка защищенных автоматизированных систем.

Содержание темы: Основы организации разработки защищенных автоматизированных систем. Стадии и этапы разработки автоматизированных систем

Общие принципы проектирования защищенных автоматизированных систем. Автоматизированное проектирование. Разработка автоматизированных систем в защищенном исполнении Реализация моделей безопасности автоматизированных систем. Особенности разработки информационных систем персональных данных.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 3 Основы эксплуатации защищенных автоматизированных информационных систем.

Содержание темы: Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 4 Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем.

Содержание темы: Средства диагностирования защищенных автоматизированных информационных систем. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств Технологическое оборудование для ремонта аппаратных средств автоматизированных информационных систем. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования Аппаратно-программные средства диагностики автоматизированных информационных систем Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств Диагностические

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

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 5 настоящей РПД

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Золотарев, В. В. Разработка и эксплуатация защищенных автоматизированных и телекоммуникационных систем: основные этапы : учебное пособие / В. В. Золотарев, И. А. Лубкин. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2024. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/479330 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.
2. Потехин, Д. С. Разработка программно-аппаратного обеспечения информационных и автоматизированных систем : учебное пособие / Д. С. Потехин, И. Е. Тарасов. — Москва : РТУ МИРЭА, 2022. — 131 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/240098 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем : учебное пособие / Л. Г. Гагарина. — Москва : ФОРУМ : ИНФРА-М, 2021. — 384 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0735-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1214882 (Дата обращения - 05.09.2025)
2. Милюшенко, С. А. Проектирование автоматизированных систем : методические указания / С. А. Милюшенко. — Омск : СибАДИ, 2023. — 13 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/361133 (дата обращения: 09.09.2025). — Режим доступа: для авториз. пользователей.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft OfficeProffessionalPlus 2019 Russian
- Microsoft Windows 2000 Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2024

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-11 : Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.2к : разрабатывает компоненты комплексных систем защиты информации автоматизированных систем
	ОПК-14 : Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14.1к : понимает основные принципы организации технического, программного обеспечения защищенных информационных систем; оптимального проектирования защищенных информационных систем; оценки показателей эффективности защищенных информационных систем
	ОПК-5.2 : Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;	ОПК-5.2.2к : интегрирует систему защиты информации в текущую информационно-техническую инфраструктуру

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-11 «Способен разрабатывать компоненты систем защиты информации автоматизированных систем»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-11.2к : разрабатывает компоненты комплексных систем защиты информации автоматизированных систем	РД 1	Знание	принципы и методы построения защищенных автоматизированных систем	Раскрывает принципы и описывает модели построения защищенных автоматизированных систем
	РД 2	Умение	разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	разрабатывает модели угроз и нарушителей информационной безопасности автоматизированных систем
	РД 3	Навык	синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	анализирует и синтезирует структурные и функциональные схемы защищенных автоматизированных информационных систем

Компетенция ОПК-14 «Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации,

проводить подготовку исходных данных для технико-экономического обоснования проектных решений»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-14.1к : понимает основные принципы организации технического, программного обеспечения защищенных информационных систем; оптимального проектирования защищенных информационных систем; оценки показателей эффективности защищенных информационных систем	РД 4	Знание	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников	Перечисляет методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, раскрывает методы оценки качества КСИБ, метод экспертных структурных вопросников
	РД 5	Умение	определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники; оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ); создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем	определяет риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники; оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ); создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем
	РД 6	Навык	методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ	использует методики рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ

Компетенция ОПК-5.2 «Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;»

Таблица 2.3 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	

ОПК-5.2.2к : интегрирует систему защиты информации в текущую информационно-техническую инфраструктуру	РД 7	Знание	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;	Определяет порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем и содержание работ специалистов;
	РД 8	Умение	исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;	Оценивает эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : принципы и методы построения защищенных автоматизированных систем	1.1. Базовые понятия информационной безопасности вычислительных сетей	Тест	Опрос
		1.2. Разработка защищенных автоматизированных систем	Тест	Опрос
РД2	Умение : разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	1.1. Базовые понятия информационной безопасности вычислительных сетей	Практическая работа	Опрос
		1.4. Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных с	Практическая работа	Опрос

		истем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем		
РД3	Навык : синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	1.1. Базовые понятия информационной безопасности вычислительных сетей	Практическая работа	Опрос
		1.2. Разработка защищенных автоматизированных систем	Практическая работа	Опрос
		1.3. Основы эксплуатации защищенных автоматизированных информационных систем	Практическая работа	Опрос
РД4	Знание : методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников	1.1. Базовые понятия информационной безопасности вычислительных сетей	Тест	Опрос
		1.2. Разработка защищенных автоматизированных систем	Тест	Опрос
		1.3. Основы эксплуатации защищенных автоматизированных информационных систем	Тест	Опрос
РД5	Умение : определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники; оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ) ; создавать модель нарушителя. проводить вероятностный анализ методов и способов воздейств	1.1. Базовые понятия информационной безопасности вычислительных сетей	Практическая работа	Опрос
		1.2. Разработка защищенных автоматизированных систем	Практическая работа	Опрос
		1.4. Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированны	Практическая работа	Опрос

	ия на КСИБ нарушителем	х информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем		
РД6	Навык : методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ	1.2. Разработка защищенных автоматизированных систем	Практическая работа	Опрос
		1.4. Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информацио	Практическая работа	Опрос

		нных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем		
РД7	Знание : содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;	1.3. Основы эксплуатации защищенных автоматизированных информационных систем	Тест	Опрос
		1.4. Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуата	Тест	Опрос

		ционной документации, при организации технического обслуживания защищенных автоматизированных информационных систем		
РД8	Умение : исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений ;	1.4. Аттестация автоматизированных информационных систем по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации Особенности эксплуатации автоматизированных информационных систем на объекте защиты. Требования и рекомендации по защите служебной тайны и персональных данных при работе автоматизированных информационных систем. Порядок обеспечения защиты информации при эксплуатации автоматизированных информационных систем Методы проверки защищенных автоматизированных информационных систем. Содержание и порядок ведения эксплуатационной документации Анализ требований к эксплуатации автоматизированных информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных автоматизированных информационных систем	Практическая работа	Опрос

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого

Лекционные занятия	20			80
Практические занятия		60		
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1. Автоматизированное проектирование это

a. процесс постепенного приближения к выбору окончательного проектного решения

b. процесс проектирования, происходит при взаимодействии человека с компьютером

c. процесс проектирования осуществляется компьютером без участия человека

d. процесс проектирования, происходит без применения вычислительной техники

2. Системы промежуточного уровня (middleware) – это:

a. совокупность технических средств, используемых в автоматизированном проектировании

b. проблемно-ориентированные языки, предназначенные для описания процедур автоматизированного проектирования

c. комплекс регламентирующих документов касаются организационной структуры подразделений, эксплуатирующих САПР

d. набор документов, регламентирующих эксплуатацию САПР

3. Группа признаков качества САПР как объекта эксплуатации

a. учитывают качество выполнения отдельной функциональной задачи

b. характеризует ее приспособленность к изменениям

c. характеризует способности системы к одновременному выполнению всего множества функциональных задач

d. отражает свойства САПР с позиций различных составляющих общего процесса эксплуатации

4. Какими параметрами оперирует проектировщик в процессе проектирования

a. Выходные

b. Внешние

c. Внутренние

d. технологические

5. На этапе технологической подготовки производства решаются следующие задачи

a. инженерные расчеты и проектирование 3D моделей

b. проектирования технологических процессов проектирования управляющих программ и технологической оснастки

c. проектирования 3D моделей и чертежей изделия

d. конструирования изделий и разработка управляющих программ

6. Технико-экономические показатели сложной технической системы это

a. совокупность используемых для достижения эффекта финансовых, материальных, трудовых и временных ресурсов

b. изменение результатов процесса проектирования при замене неавтоматизированного способа его исполнения автоматизированным

c. составляющие эффекта, имеют техническое и экономическое выражение

d. сопоставления эффекта от применения САПР и полных затрат на ее создание и эксплуатацию

7. Какой из представленных вариантов не является разновидностью системного подхода к проектированию

a. структурный подход

b. технологический подход

c. объектно-ориентированный подход

d. блочно-иерархический подход

8. Под угрозой безопасности информации в компьютерной системе (КС) понимают:

a. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b. Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности, обрабатываемой в ней информации.

c. действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

9. Уязвимость информации — это:

a. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b. Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности, обрабатываемой в ней информации.

c. это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 4 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок

4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Практическая работа 1

Модели данных, систем и процессов защиты информации в автоматизированных системах.

Оценка защищенности автоматизированных систем. Определение и содержание понятия угрозы безопасности автоматизированных систем

Практическая работа 2

Исследование надежности и риска нерезервированной технической системы. Исследование надежности информационной восстанавливаемой системы. Составление и отработка технического задания на создание защищенных автоматизированных систем. Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем. Оценка угроз

безопасности информационных систем персональных данных. Стадии и этапы разработки

автоматизированных систем. Автоматизированные системы проектирования средств и подсистем безопасности. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении

Практическая работа 3

Изучение программных средства защиты автоматизированных информационных систем от несанкционированного доступа. Анализ основных документов, определяющих цели, задачи,

порядок проведения аттестации. Анализ требований к эксплуатации автоматизированных

информационных систем на объекте защиты. Анализ этапов обеспечения защиты информации при эксплуатации автоматизированных информационных систем. Анализ содержания и порядка

ведения эксплуатационной документации

Практическая работа 4

Изучение аппаратно-программных средств диагностики автоматизированных

информационных систем. Изучение аппаратно-программных средств контроля функционирования элементов автоматизированных информационных систем

Краткие методические указания

На выполнение одной практической работы отводится не менее трех двухчасовых занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	12-15	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	8-11	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	4-7	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-3	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Примерные вопросы

1. Понятие сложной системы. Элементы подсистемы. Управление и информация. Случайнее факторы. Самоорганизация
2. Понятие качества и эффективности сложных систем. Эффективность. Надежность. Помехозащищенность. Устойчивость. Сложность.
3. Порядок разработки сложной системы. Этапы разработки. Системотехника. Обоснование технического задания.
4. Что такое информационная система? Классификация информационных систем. Разработка и производство информационных систем. Структура информационной системы и принципы ее функционирования.
5. Принципы построения системы защиты информации. Типовые компоненты информационной системы. Проблемы защиты информационной системы.
6. Проблемы защиты открытых систем клиент/сервер.
7. Защита для открытых информационных систем. Структура и задачи органов, осуществляющих защиту информации.
8. Определение информационных и технических ресурсов, подлежащих защите. Оценка угроз и рисков
9. Политика информационной безопасности, принципы и виды политики
10. безопасности. Организационно-технические мероприятия. Организация секретного делопроизводства. Организация мероприятий по защите информации.
11. Внедрение и использование средств защиты в автоматизированной системе. Принятие административных решений по уровням обеспечения защиты информации.
12. Порядок выполнения работ по защите информации. Этапы выполнения работ по созданию и внедрению средств защиты информации.
13. Программно-технические методы и средства защиты информации. Службы и механизмы защиты. Управление доступом. Контроль за работой пользователей. Управление доступом к рабочим места.
14. Регламентация парольного доступа. Защита целостности программ. Управление системой защиты информации. Принципы организации и контроля системы защиты.
15. Реализация политики безопасности. Управление защитой в распределенных сетях. Методы разработки защищенных информационных систем. Модели управления доступом.
16. Проблемы внедрения систем управления доступом. Основные понятия секретной информации. Порядок отнесения информации к государственной тайне. Защита государственной тайны.
17. Сведения, составляющие коммерческую тайну. Определение степени секретности информации. Оценка уязвимости и рисков. Анализ рисков. Разработка методологии оценки. Этапы оценки.
18. Определение и анализ угроз. Требования к системам защиты информации. Организационные требования. Требования к техническому обеспечению. Требования к программному обеспечению.
19. Выбор средств защиты. Модель информационной системы как объекта защиты. Механизмы обеспечения безопасности. (перечислить и рассмотреть один из механизмов.)
20. Внедрение и использование выбранных мер защиты. Основные решения по обеспечению защиты безопасности. Содержание и последовательность работ по защите информации.
21. Построение системы защиты информации. (перечислить этапы и рассмотреть один из этапов) Порядок проведения работ по защите информации. Этапы выполнения

работ по созданию средств защиты информации. (перечислить этапы и рассмотреть один из этапов)

22. Реализация организационных и технических мер защиты. Приемка, определение полноты и качества. Контроль целостности средств защиты информации. Сертификация продукции. Процесс сертификации.
23. Сертификация программного обеспечения на соответствие требованиям безопасности. Общие сведения об устройстве биологического нейрона и нервной системы человека.
24. Общий вид базового элемента искусственных нейронных сетей (формального нейрона). Режимы функционирования искусственных нейронных сетей. Классификация искусственных нейронных сетей по структуре связей, примеры соответствующих НС.
25. Динамические и статические искусственные нейронные сети, примеры соответствующих НС. Классификация искусственных нейронных сетей по способам обучения, примеры соответствующих НС.
26. Коннекционизм. Правило Хебба. Сеть Хопфилда: принципы работы. Сеть Хопфилда с синхронной динамикой. Предельное состояние. Сеть Хопфилда с асинхронной динамикой. Предельное состояние.
27. Обучение сети Хопфилда для решения задачи классификации. Сеть Кохонена: принципы работы. Сеть Кохонена: способ обучения.
28. Нейронные сети с радиально-базисными функциями активации: принцип работы, способ обучения. Персептрон: принцип работы, способ обучения. Статические многослойные нейронные сети: принцип работы. Функции активации. Задача построения аппроксимации отображения по примерам.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.