МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ТЕОРИЯ И ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ

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

Год набора на ОПОП
2023

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Теория и проектирование защищенных систем» 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	0000000000EA7C40
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Основной целью освоения дисциплины "Теория и проектирование защищенных систем" является формирование у студентов знаний о защищенных автоматизированных системах, их проектированию, разработке и эксплуатации. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по обеспечению необходимого уровня информационной безопасности автоматизированных систем.

Задачи дисциплины:

-изучение принципов эксплуатации защищенных автоматизированных систем;

- овладение средствами и методами проектирования и разработки защищенных автоматизированных систем;

- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

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-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-14.2к : представляет проектные решения систем защиты, оформлять проектную документацию и проводит оценку их технико-экономического обоснования.	РД1	Знание	Методики разработки архитектуры систем защиты информации
			РД2	Умение	Разрабатывать проектные решения по защите информации с учетом требований конкретной организации
			РД3	Навык	Оформлять проектную документацию согласно установленным стандартам и регламентам
	ОПК-15 : Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг	ОПК-15.3к : понимает стандартные схемы использования межсетевых экранов; особенности подсистем защиты	РД4	Знание	Стандартные схемы установки и конфигурации межсетевых экранов в сетевых инфраструктурах
			РД5	Умение	Конфигурировать межсетевые экраны для фильтрации

	защищенности автоматизированных систем	распространенных СУБД			трафика и предотвращения вторжений

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		
Воспитание уважения к Конституции и законам Российской Федерации	Взаимопомощь и взаимоуважение	Активная жизненная позиция
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Гражданственность	Внимательность к деталям
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Гражданственность	Гибкость мышления
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Взаимопомощь и взаимоуважение	Доброжелательность и открытость

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Теория и проектирование защищенных 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», «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	9	5	91	36	36	0	1	18	89	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	Основные понятия и классификация защищенных автоматизированных систем.	РД1	4	4	0	12	отчет по практической работе, собеседование
2	Основы защиты информации в защищенных автоматизированных системах	РД1	4	4	0	12	практическое задание
3	Угрозы безопасности информации в защищенных автоматизированных системах.	РД1, РД2	4	4	0	12	отчет по практической работе, собеседование
4	Программно-технический уровень защиты автоматизированных систем.	РД2, РД4, РД5	4	4	0	12	практическое задание
5	Основы организации разработки защищенных АС.	РД1, РД3	4	4	0	12	отчет по практической работе, собеседование
6	Общие принципы проектирования защищенных АС.	РД1, РД3	4	4	0	12	отчет по практической работе, собеседование
7	Основы эксплуатации защищенных АС.	РД1, РД2, РД4	4	4	0	12	отчет по практической работе, собеседование
8	Криптографические протоколы обеспечения безопасности	РД1, РД2	4	4	0	12	отчет по практической работе, собеседование
9	Основы администрирования АС.	РД1, РД2, РД3, РД4, РД5	4	4	0	12	отчет по практической работе, собеседование
Итого по таблице			**36**	**36**	**0**	**108**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Основные понятия и классификация защищенных автоматизированных систем.

Содержание темы: Классификация автоматизированных систем (АС). Информационные технологии, используемые в АС. Жизненный цикл АС. Основные угрозы безопасности информации в автоматизированных системах. Отказоустойчивость АС.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Основы защиты информации в защищенных автоматизированных системах.

Содержание темы: Понятия информации и информационных ресурсов. Предмет защиты информации. Объект защиты информации. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС).

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Угрозы безопасности информации в защищенных автоматизированных системах.

Содержание темы: Источники угроз. Окно опасности. Базовые признаки угроз информационной безопасности. Классификация угроз. Доступность информации. Угроза доступности. Целостность информации. Угроза нарушения целостности. Конфиденциальность информации. Угроза нарушения конфиденциальности. Угроза раскрытия параметров АС. Методы обеспечения информационной безопасности. Структуризация методов обеспечения информационной безопасности. Уровни доступа к защищаемой информации. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Программно-технический уровень защиты автоматизированных систем.

Содержание темы: Подходы к обеспечению защиты информации. Сервисы безопасности. Основные и вспомогательные сервисы безопасности. Виды сервисов безопасности Характеристики подходов к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к набору и параметрам механизмов защиты. Необходимые требования. Дополнительные требования. Формализованные требования к защите информации от несанкционированного доступа.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 5 Основы организации разработки защищенных АС.

Содержание темы: Последовательность и содержание этапов разработки АС. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 6 Общие принципы проектирования защищенных АС.

Содержание темы: Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Организация хранения информации в защищенных АС.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 7 Основы эксплуатации защищенных АС.

Содержание темы: Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС. Организация технического обслуживания защищенных АС. Средства диагностирования защищенных АС. Аппаратнопрограммные средства диагностики АС. Аппаратно- программные средства контроля функционирования отдельных элементов, узлов, блоков.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 8 Криптографические протоколы обеспечения безопасности.

Содержание темы: Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/ TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 9 Основы администрирования АС.

Содержание темы: Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования АС. Настройка сетевой подсистемы защищенной АС. Принципы функционирования информационных сервисов АС. Установка и настройка работы информационных сервисов АС. Удаленное администрирование компонентов АС.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

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 4 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. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (Дата обращения - 22.10.2025)

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070 (дата обращения: 15.10.2025).

7.2 Дополнительная литература

1. Зырянова, Т. Ю. Основы криптографии : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 82 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369479 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

2. Рочев, К. В., Архитектура информационных систем : учебное пособие / К. В. Рочев. — Москва : КноРус, 2025. — 205 с. — ISBN 978-5-406-14131-1. — URL: https://book.ru/book/956640 (дата обращения: 26.10.2025). — Текст : электронный.

3. Сорокин, С. А. Архитектура программно-аппаратных комплексов : методические указания / С. А. Сорокин, А. В. Горшков. — Москва : РТУ МИРЭА, 2023. — 61 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/331625 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

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

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "BOOK.ru"
3. Электронно-библиотечная система "ZNANIUM.COM"
4. Электронно-библиотечная система "ЛАНЬ"
5. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/

6. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

7. 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

Программное обеспечение:

- Microsoft Office Professional Plus 2010

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

ТЕОРИЯ И ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ

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

Год набора на ОПОП
2023

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-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-14.2к : представляет проектные решения систем защиты, оформлять проектную документацию и проводит оценку их технико-экономического обоснования.
	ОПК-15 : Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.3к : понимает стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных СУБД

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-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 2.1 – 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-14.2к : представляет проектные решения систем защиты, оформлять проектную документацию и проводит оценку их технико-экономического обоснования.	РД 1	Знание	Методики разработки архитектуры систем защиты информации	решение тестовых заданий
	РД 2	Умение	Разрабатывать проектные решения по защите информации с учетом требований конкретной организации	выполнение практических заданий
	РД 3	Навык	Оформлять проектную документацию согласно установленным стандартам и регламентам	выполнение практических заданий

Компетенция ОПК-15 «Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем»

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-15.3к : понимает стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных СУБД	РД 4	Знание	Стандартные схемы установки и конфигурации межсетевых экранов в сетевых инфраструктурах	решение тестовых заданий
	РД 5	Умение	Конфигурировать межсетевые экраны для фильтрации трафика и предотвращения вторжений	выполнение практических заданий

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 : Методики разработки архитектуры систем защиты информации	1.1. Основные понятия и классификация защищенных автоматизированных систем.	Тест	Экзамен в устной форме
		1.2. Основы защиты информации в защищенных автоматизированных системах	Тест	Экзамен в устной форме
		1.3. Угрозы безопасности информации в защищенных автоматизированных системах.	Тест	Экзамен в устной форме
		1.5. Основы организации и разработки защищенных АС.	Тест	Экзамен в устной форме
		1.6. Общие принципы проектирования защищенных АС.	Тест	Экзамен в устной форме
		1.7. Основы эксплуатации защищенных АС.	Тест	Экзамен в устной форме

		1.8. Криптографические протоколы обеспечения безопасности	Тест	Экзамен в устной форме
		1.9. Основы администрирования АС.	Тест	Экзамен в устной форме
РД2	Умение : Разрабатывать проектные решения по защите информации с учетом требований конкретной организации	1.3. Угрозы безопасности информации в защищенных автоматизированных системах.	Практическая работа	Экзамен в устной форме
		1.4. Программно-технический уровень защиты автоматизированных систем.	Практическая работа	Экзамен в устной форме
		1.7. Основы эксплуатации защищенных АС.	Практическая работа	Экзамен в устной форме
		1.8. Криптографические протоколы обеспечения безопасности	Практическая работа	Экзамен в устной форме
		1.9. Основы администрирования АС.	Практическая работа	Экзамен в устной форме
РД3	Навык : Оформлять проектную документацию согласно установленным стандартам и регламентам	1.5. Основы организации и разработки защищенных АС.	Практическая работа	Экзамен в устной форме
		1.6. Общие принципы проектирования защищенных АС.	Практическая работа	Экзамен в устной форме
		1.9. Основы администрирования АС.	Практическая работа	Экзамен в устной форме
РД4	Знание : Стандартные схемы установки и конфигурации межсетевых экранов в сетевых инфраструктурах	1.4. Программно-технический уровень защиты автоматизированных систем.	Практическая работа	Экзамен в устной форме
		1.7. Основы эксплуатации защищенных АС.	Практическая работа	Экзамен в устной форме
		1.9. Основы администрирования АС.	Практическая работа	Экзамен в устной форме
РД5	Умение : Конфигурировать межсетевые экраны для фильтрации трафика и предотвращения вторжений	1.4. Программно-технический уровень защиты автоматизированных систем.	Практическая работа	Экзамен в устной форме
		1.9. Основы администрирования АС.	Практическая работа	Экзамен в устной форме

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	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. Общие характеристики процесса проектирования:

1. Этапность, плановость, коллективность, управляемость, документирование, связь с заказчиком;

2. Творческий подход, инициативность;

3. Демократичность принятия решений;

4. Спонтанное развитие.

2. Определяющий фактор структуры информации и логики ИС:

1. Общефилософский подход;

2. Входные и выходные формы;

3. Скорость разработки проекта;

4. Опыт разработчиков.

3. Исходные данные для проектирования:

1. Заработная плата разработчиков проекта;

2. Квалификация разработчиков проекта;

3. Входные и выходные формы, эффективность работы, надёжность, защита данных, техническая оснащённость и т.п.;

4. Аналогичный продукт/проект другой фирмы.

4. Чем отличается программа от программного продукта той же функциональности?

1. Отлаженностью, качественным интерфейсом;

2. Скоростью работы;

3. Стоимостью;

4. Качеством, оттестированностью, документацией, процедурой приёмки, сопровождением

5. Чем определяется качество программного продукта?

1. Ориентация на стандарты, хорошо организованное сопровождение, проектная документация, и пр.;

2. Гениальная идея;

3. Самоотверженный труд;

4. Скорость подготовки проекта.

6. Что занимает большую часть работы над проектом?

1. Написание программ;

2. Анализ и планирование;

3. Тестирование;

4. Системное тестирование.

7. Функции проектной документации –

1. Повышение авторитета фирмы;

2. Формальное соответствие стандартам;

3. Повышение общности и абстрактности программного продукта;

4. Связь с отделом тестирования, планирование, основания для принятия решений, основа развития продукта.

8. Сопровождение программного продукта это

1. Сервисное обслуживание пользователей, купивших программу (консультации по использованию, обучение, рассылки нововведений и релизов, пропаганда знаний использования и т.п.);

2. Исправление ошибок;

3. Доработка функциональности;

4. Гарантийное обязательство.

9. Внедрение системы – это =

1. Инсталляция на ЭВМ пользователя;

2. Квалифицированная помощь пользователю в запуске и освоении системы, устранение неучтённых особенностей («мелочей»), повышение уровня доверия к системе;

3. Определение особенностей автоматизации объекта;

4. Бюрократическая рутинная процедура завершения проекта.

10. Какие компоненты информационного комплекса подлежат защите? (далее , видимо , список правильных ответов)

1) оборудование

2) средства хранения данных

3) каналы связи

11. Какие существуют категории защиты информации?

1) физическая защита от разрушения

2) логическая защита (ссылочная целостность и пр.)

3) защита от перехвата

4) защита от несанкционированного доступа

5) защита от неправильных действий оператора (от «дурака»)

12. Методы обеспечения физической защиты

1) защита от сбоев питания

2) защита от выхода из строя оборудования (дублирование и резервирование)

3) архивация и резервное копирование данных

4) применение RAID-массивов

5) журнализация

6) административные и дисциплинарные меры (график работы, ограничение доступа к оборудованию, штрафы и т.п.)

13. Методы защиты от перехвата и несанкционированного доступа

1.криптозащита (шифрование)

2. электронно-цифровая подпись

3. использование защищенных протоколов передачи данных (SSL)

4. формирование защищенных каналов передачи (туннелирование)

5. персональная идентификация пользователей, желательно единая в рамках всей системы

6. использование дополнительных средств идентификации (штрих-код, магнитные и proximity-карты)

7. категоризация пользователей

8. протоколирование действий пользователей

9. ограничение и протоколирование условий доступа (HID, MAC, IP, время получения доступа)

10. хранение истории изменений свойств объектов

11. настройка интерфейса в зависимости от прав пользователя или группы

14. Что служит основой для формирования требований к ТЗ (техническому заданию)?

1) входные и выходные формы

2) вид деятельности оператора

3) способ и интенсивность работы со средствами ввода

4) способ получения и восприятия информации

5) ограничения безопасности

6) защита от «дурака»

7) понятие эффективности

8) понятие оптимальности

9) сведения о квалификации операторов

15. Какие существуют концептуальные подходы к проектированию?

1) Нисходящее проектирование

2) Восходящее проектирование

3) Низ-восходящее проектирование

4) Экстремальное проектирование (программирование)

16. Преимущества нисходящего проектирования

1) очень удобное документирование

2) высокая надёжность

3) управляемость процессом проектирования

4) лёгкость создания тестов

17. Недостатки нисходящего проектирования

1) многие из реальных проблем не иерархические

2) слишком строгая формализация может замедлить процесс разработки

3) обилие тестов

18. Когда следует использовать нисходящее проектирование?

1. Всегда

2. Когда задачи имеют ясно выраженный иерархический характер

3. Когда требует заказчик

4. Когда задача плохо формализована

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

Задание 1. Проектирование защищенной распределенной информационной системы для организации на базе технологий виртуальных частных сетей VPN.

Задание 2. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов SSL, TSL, IP sec, S-HTTP

Задание 3. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности.

Задание 4. Проектирование защищенной распределенной информационной системы для организации базе технологий централизованного хранения данных сервера безопасности.

Задание 5. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов TSL

Задание 6. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов IP- sec

Задание 7. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов S-HTTP

Задание 8. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов SSL, TSL

Задание 9. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности. базе технологий протоколов SSL, TSL, IP sec, S-HTTP

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. 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	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

1. Привести и охарактеризовать модель взаимодействия открытых систем, размещение услуг и механизмов защиты на уровнях модели.

2. Привести понятие процесса проектирования. Указать особенности постановки задачи управления процессом проектирования.

3. Характеризовать распределенную информационную систему как объект обеспечения безопасности.

4. Привести и охарактеризовать состав оборудования распределенных информационных систем

5. Привести и охарактеризовать основные протоколы взаимодействия распределенных информационных систем.

6. Трафик и качество функционирования распределенных информационных систем

7. Оптимизация трафика в распределенных информационных системах, типы трафика

8. Привести классификацию угроз безопасности. Дать общую характеристику нарушителей информационной безопасности в распределенных информационных системах. Привести особенности формирование общих требований информационной безопасности к организации.

9. Охарактеризовать общие принципы построения защищенных распределенных информационных систем

10. Указать особенности предпроектного обследование при разработке распределенных защищенных систем

11. Указать особенности формирования технического задания при проектировании распределенных защищенных систем

12. Указать особенности рабочего проектирования распределенных защищенных систем

13. Указать особенности построения защищенного решения для распределенных информационных систем на базе технологий виртуальных частных сетей VPN.

14. Указать и охарактеризовать способы построения сервера безопасности

15. Порядок использования протоколов SSL,TSL ,IPsec, PPP, SSH, S-HTTP. Протоколы аутентифицированного распределения ключей.

16. Указать особенности стандарта X.509. Указать особенности протоколов электронной цифровой подписи.

17. Указать и охарактеризовать принципы проектирования VPN, варианты технической реализации

18. Базовые технологии обеспечения качества трафика

19. Указать и охарактеризовать принципы проектирования VPN для сети на базе технологии многопротокольной коммутации по меткам.

20. Указать и охарактеризовать методы криптографической защиты протокола VPN; принципы функционирования протоколов PPTP, L2F.

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.