МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ

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) «Технология построения защищенных распределенных приложений» 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	0000000000EAAAB1
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Технология построения защищенных распределенных приложений» является теоретическая и практическая подготовка специалистов к деятельности, связанной с аттестацией объектов информатизации критически важных объектов: обучение методам проектирования и разработки защищенных распределенных приложений, соответствующим требованиям нормативных документов.

Задачи дисциплины:

- изучение нормативных документов по организации жизненного цикла, обеспечению функциональной и информационной безопасности разрабатываемых приложений;
- освоение методов обеспечения взаимодействия распределенных компонент разрабатываемых приложений;
- освоение методов обеспечения безопасности разрабатываемых приложений;
- изучение системы документационного обеспечения аттестации объектов информатизации.

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-12 : Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.2к : использует средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем	РД1	Знание	принципы построения распределенных систем, распределенного программного обеспечения; CASE-технологии для проектирования защищенного программного обеспечения; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования
			РД3	Умение	использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных 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	РД2	Знание	нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты
			РД4	Умение	применять нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты
			РД5	Навык	методами и средствами определения технологической безопасности функционирования распределенной информационной системы
			РД6	Навык	методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения

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 истории и культуре России	Гражданственность	Активная жизненная позиция
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Взаимопомощь и взаимоуважение	Любознательность
Формирование научного мировоззрения и культуры мышления		
Развитие творческих способностей и умения решать нестандартные задачи	Гражданственность	Внимательность к деталям
Формирование коммуникативных навыков и культуры общения		

Воспитание культуры диалога и уважения к мнению других людей	Взаимопомощь и взаимоуважение	Гибкость мышления

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Технология построения защищенных распределенных приложений» относится к базовой части дисциплин учебного плана направления 10.05.03 «Информационная безопасность автоматизированных систем». Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Криптографические методы защиты информации», «Технологии и методы программирования». На данную дисциплину опираются «Разработка и эксплуатация защищенных автоматизированных систем»

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	8	5	91	36	0	36	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	Основы построения защищенных распределенных приложений	РД1, РД2, РД3, РД4, РД5, РД6	12	0	12	30	Лабораторная работа

2	Взаимодействие компонент распределенных приложений	РД1, РД2, РД3, РД4, РД5, РД6	12	0	12	30	Лабораторная работа
3	Обеспечение безопасности распределенных приложений	РД1, РД2, РД3, РД4, РД5, РД6	12	0	12	30	Лабораторная работа
Итого по таблице			**36**	**0**	**36**	**90**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Основы построения защищенных распределенных приложений.

Содержание темы: Понятие распределенной системы. Типовые архитектуры распределенных систем. Понятие распределенных приложений. Требования к распределенным приложениям. Программные компоненты распределенных приложений. Понятие промежуточной среды распределенных приложений. Модели взаимодействия компонент распределенных приложений. Обмен сообщениями. Дальний вызов процедур. Использование удаленных объектов. Распределенные события. Распределенные транзакции. Жизненный цикл программного обеспечения: стандарты жизненного цикла ПО. Процессы жизненного цикла ПО. Стадии жизненного цикла ПО, взаимосвязь между процессами и стадиями. Модели жизненного цикла ПО. Методологии разработки ПО. Проектирование и моделирование программного обеспечения: язык графического описания для объектного моделирования в области разработки программного обеспечения UML. Программные средства поддержки жизненного цикла ПО. Технология внедрения CASE-средств. Характеристики CASE-средств. Обеспечение функциональной безопасности распределенных приложений: проблемы обеспечения функциональной безопасности. Основные понятия и факторы, определяющие функциональную безопасность. Характеристики среды, для которой должна обеспечиваться функциональная безопасность. Ресурсы для обеспечения функциональной безопасности. Обеспечение информационной безопасности распределенных приложений: критерии оценки безопасности информационных технологий. Методология оценки безопасности информационных технологий. Уровни целостности систем и программных средств .

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

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 2 Взаимодействие компонент распределенных приложений.

Содержание темы: Программный интерфейс сокетов, сетевое взаимодействие по протоколам UDP и TCP: понятие и типы сокетов. Понятие и назначение сетевого адреса и сетевого порта. Реализация программного интерфейса сокетов в .NET Framework. Сравнение возможностей протоколов TCP и UDP. Реализация сетевого взаимодействия по протоколу UDP в .NET Framework. Реализация сетевого взаимодействия по протоколу TCP в .NET Framework. Одноранговые сети: основы функционирования и технологии построения одноранговых сетей. Протоколы FEC и MDC. Проблемы безопасности одноранговых сетей.

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

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

Тема 3 Обеспечение безопасности распределенных приложений.

Содержание темы: Создание безопасного кода программного обеспечения: обеспечение безопасности данных. Безопасность доступа к методам. Безопасность кода программы-оболочки. Безопасность и поля-массивы с общим доступом только для чтения. Безопасность обработки исключений. Безопасность и ввод данных пользователем. Вопросы безопасности при удаленном взаимодействии. Безопасность и сериализация. Безопасность и конфликты. Безопасность на основе ролей и применение политик в .NET Framework. Объекты Principal и Identity. Объекты PrincipalPermission. Службы криптографии Задачи криптографии. Криптографические примитивы. Хеширование. Симметричное шифрование. Асимметричное шифрование. Сертификаты ключей. Цифровые подписи. Генерация случайных чисел. Разновидности алгоритмов хеширования, реализованных в .NETFramework. Создание хеша. Проверка хеша. Симметричное шифрование: разновидности алгоритмов симметричного шифрования, реализованных в.NETFramework. Режимы шифрования. Создание и хранение симметричных ключей. Асимметричное фрование Разновидности алгоритмов асимметричного шифрования, реализованных в.NETFramework. Режимы шифрования. Создание и хранение асимметричных ключей. .

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

Виды самостоятельной подготовки студентов по теме: подготовка к лабораторной работе.

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. Гагарина, Л. Г. Технология разработки программного обеспечения : учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова-Виснадул ; под ред. Л.Г. Гагариной. — Москва : ФОРУМ : ИНФРА-М, 2023. — 400 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0707-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1971872 (Дата обращения - 22.10.2025)

2. Современные технологии разработки программного обеспечения : учебно-методическое пособие / составитель Н. А. Федькова. — Брянск : Брянский ГАУ, 2022. — 58 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/305087 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.

3. Чернышев, С. А. Принципы, паттерны и методологии разработки программного обеспечения : учебник для вузов / С. А. Чернышев. — Москва : Издательство Юрайт, 2025. — 176 с. — (Высшее образование). — ISBN 978-5-534-14383-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567946 (дата обращения: 15.10.2025).

7.2 Дополнительная литература

1. Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 189 с. — ISBN 978-5-406-08880-7. — URL: https://book.ru/book/941751 (дата обращения: 26.10.2025). — Текст : электронный.

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
- Проектор

Программное обеспечение:

- Microsoft Office 2010 Standart

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ

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-12 : Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.2к : использует средства операционных систем для обеспечения эффективного и безопасного функционирования 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

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-12 «Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке 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-12.2к : использует средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем	РД 1	Знание	принципы построения распределенных систем, распределенного программного обеспечения; CASE-технологии для проектирования защищенного программного обеспечения; требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования	решение тестовых заданий
	РД 3	Умение	использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем	выполнение лабораторной работы

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 2	Знание	нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты	решение тестовых заданий
	РД 4	Умение	применять нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты	выполнение лабораторной работы
	РД 5	Навык	методами и средствами определения технологической безопасности функционирования распределенной информационной системы	выполнение лабораторной работы
	РД 6	Навык	методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения	выполнение лабораторной работы

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 построения распределенных систем, распределенного программного обеспечения; CASE-технологии для проектирования защищенного программного обеспечения; требования к архитектуре информационных систем и их компонентам для обеспеч	1.1. Основы построения защищенных распределенных приложений	Тест	Экзамен в устной форме
		1.2. Взаимодействие компонент распределенных приложений	Тест	Экзамен в устной форме
		1.3. Обеспечение безопасности распределенных приложений	Тест	Экзамен в устной форме

	ения безопасности функ ционирования			
РД2	Знание : нормативные д окументы по метрологи и, стандартизации и сер тификации программны х и аппаратных средств защиты	1.1. Основы построения защищенных распредел енных приложений	Тест	Экзамен в устной форме
		1.2. Взаимодействие ко мпонент распределенны х приложений	Тест	Экзамен в устной форме
		1.3. Обеспечение безопа сности распределенных приложений	Тест	Экзамен в устной форме
РД3	Умение : использовать т ехнологии автоматизиро ванного проектирования и структурный подход п ри проектировании инф ормационных систем	1.1. Основы построения защищенных распредел енных приложений	Лабораторная рабо та	Экзамен в устной форме
		1.2. Взаимодействие ко мпонент распределенны х приложений	Лабораторная рабо та	Экзамен в устной форме
		1.3. Обеспечение безопа сности распределенных приложений	Лабораторная рабо та	Экзамен в устной форме
РД4	Умение : применять нор мативные документы по метрологии, стандартиз ации и сертификации пр ограммных и аппаратны х средств защиты	1.1. Основы построения защищенных распредел енных приложений	Лабораторная рабо та	Экзамен в устной форме
		1.2. Взаимодействие ко мпонент распределенны х приложений	Лабораторная рабо та	Экзамен в устной форме
		1.3. Обеспечение безопа сности распределенных приложений	Лабораторная рабо та	Экзамен в устной форме
РД5	Навык : методами и сре дствами определения те хнологической безопасн ости функционирования распределенной информ ационной системы	1.1. Основы построения защищенных распредел енных приложений	Лабораторная рабо та	Экзамен в устной форме
		1.2. Взаимодействие ко мпонент распределенны х приложений	Лабораторная рабо та	Экзамен в устной форме
		1.3. Обеспечение безопа сности распределенных приложений	Лабораторная рабо та	Экзамен в устной форме
РД6	Навык : методами сниж ения угроз безопасности информационных систе м, вызванных ошибками на этапе проектировани я, разработки и внедрен ия	1.1. Основы построения защищенных распредел енных приложений	Лабораторная рабо та	Экзамен в устной форме
		1.2. Взаимодействие ко мпонент распределенны х приложений	Лабораторная рабо та	Экзамен в устной форме
		1.3. Обеспечение безопа сности распределенных приложений	Лабораторная рабо та	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	Лабораторна я работа	Экзаме н	Ито го
Лекционные занятия	20			20
Практические занятия		60		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 Пример заданий на лабораторную работу

Лабораторная работа №1

Цель: Исследование технологий дальнего вызова процедур и использование удаленных объектов для обеспечения взаимодействия компонент распределенных приложений.

Содержание лабораторной работы: Исследовать технологии дальнего вызова процедур и использования удаленных объектов для обеспечения взаимодействия компонент распределенных приложений

Лабораторная работа №2

Цель: Изучить нормативные акты регулирующие данный аспект профессиональной деятельности

Содержание лабораторной работы: Изучение нормативных актов, определяющих процессы жизненного цикла программных средств.

Лабораторная работа №3

Цель: Проектирование и моделирование программного обеспечения.

Содержание лабораторной работы: Спроектировать и смоделировать программное обеспечение с применением UML и использованием CASE-средств.

Лабораторная работа №4

Цель: Изучение нормативных актов, определяющих обеспечение функциональной безопасности

Содержание лабораторной работы: Изучить нормативные акты, определяющих обеспечение функциональной безопасности распределенных приложений.

Лабораторная работа №5

Цель: Разработать распределенное приложение.

Содержание лабораторной работы: Разработка распределенного приложения с взаимодействием компонент через программный интерфейс сокетов.

Лабораторная работа №6

Цель: Разработка распределенного приложения

Содержание лабораторной работы: Разработка распределенного приложения, построенного по технологии одноранговой сети

Лабораторная работа №7

Цель: Разработка распределенного приложения

Содержание лабораторной работы: Разработка распределенного приложения с взаимодействием компонент через службу обмена сообщениями MSMQ.

Лабораторная работа №8

Цель: Изучение межсетевого экранирования. Разработка распределенного приложения.

Содержание лабораторной работы: Межсетевое экранирование. Разработка распределенного приложения с взаимодействием компонент через промежуточную среду COM+.

Лабораторная работа №9

Цель: Разработка распределенного приложения

Содержание лабораторной работы: Разработка распределенного приложения с взаимодействием компонент через промежуточную среду ASP.NET.

Лабораторная работа №10

Цель: Изучение правил создания безопасного кода программного обеспечения.

Содержание лабораторной работы: Практическая реализация правил создания безопасного кода программного обеспечения.

Лабораторная работа №11

Цель: Разработка распределенного приложения

Содержание лабораторной работы: Разработка распределенного приложения с взаимодействием компонент через промежуточную среду .NET Remoting.

Лабораторная работа №12

Цель: Исследовать различных промежуточных сред при построении защищенных распределенных приложений и их взаимосвязей.

Содержание лабораторной работы: Исследование различных промежуточных сред при построении защищенных распределенных приложений и их взаимосвязей.

Краткие методические указания

На выполнение одной лабораторной 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.

5.2 Вопросы к экзамену

1. Понятие и структура ИС.
2. Понятия и структура программного обеспечения (далее, ПО).
3. Построение проекта программного обеспечения. Требования к эффективности и надежности
проектных решений.
4. Жизненный цикл программного обеспечения. Модели Жизненного цикла.
5. Основные компоненты технологии проектирования ПО.
6. Методы и средства проектирования защищенного распределенного ПО.
7. Архитектуры распределенного ПО (централизованные, децентрализованные).
8. Методы межсетевого взаимодействия.
9. Протоколы межсетевого взаимодействия программного обеспечения: SOAP, RPC, Socket.
10. Стадии и этапы процесса проектирования программного обеспечения: состав работ на
предпроектной стадии, стадии технического и рабочего проектирования.
11. Стадии и этапы процесса проектирования программного обеспечения: стадии ввода в
действие ИС, эксплуатации и сопровождения.
12. Состав проектной документации. Методологии моделирования предметной области.
13. Организационные структуры проектирования программного обеспечения.
14. Планирование и контроль проектных работ. Среды разработки IDE. Системы версий SVN.
15. ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27001.16. семейства ГОСТ 34, ГОСТ 9х.
17. Oracle CDM.
18. Rational Unified Process.
19. Microsoft Solution Framework (MSF).
20. Extreme Programming (XP).
21. IEEE Guide to the Software Engineering Body of Knowledge
22. CASE-средства. Основные принципы CASE-технологии.
23. Основные понятия и подходы к построению защищенного программного обеспечения.
24. Unified Modeling Language (UML).
25. Проектирование диаграмм классов.
26. Проектирование временных диаграмм.
27. Средства моделирования и построения защищенного программного обеспечения с
использованием UML.
28. Инструменты рефакторинга (модернизации) программного кода.
29. Генераторы программного кода.
30. Анализ основных угроз защищенного программного обеспечения.
31. Методы защиты данных.
32. Методы защиты программного обеспечения.
33. Методы защиты межсетевого взаимодействия.
34. РД ФСТЭК.

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.

5.3 Контрольный тест

1. Что означает аббревиатура PKI в контексте информационной безопасности?

A) Public Key Infrastructure (Инфраструктура открытых ключей)

B) Private Key Identification (Идентификация закрытых ключей)

C) Password Knowledge Interface (Интерфейс парольной аутентификации)

D) Personal Key Integration (Интеграция персональных ключей)

2. Что такое сессионный ключ в криптографии?

A) Постоянный секретный ключ, используемый в течение длительного времени

B) Открытый ключ, предназначенный для шифрования данных

C) Ключи, используемые для подписи цифровых сертификатов

D) Временный ключ, генерируемый для одноразового сеанса коммуникации

3. Какой протокол защищает передачу данных в HTTP-протоколе?

A) SSL/TLS

B) FTP

C) SSH

D) SMTP

4. Что представляет собой атака man-in-the-middle (MITM)?

A) Атака, связанная с перебором паролей методом грубой силы

B) Атака, осуществляемая путем перехвата и модификации данных в процессе их передачи

C) Атака, направленная на проникновение через уязвимости нулевого дня

D) Атака, основанная на фишинге

5. Какая техника шифрования используется для ускорения симметричного шифрования?

A) RSA

B) AES

C) MD5

D) SHA-256

6. Что такое cross-site scripting (XSS)?

A) Техника для обхода ограничений доступа

B) Метод для кражи файлов cookie

C) Способ повышения привилегий пользователя

D) Атака, позволяющая внедрить вредоносный код в веб-сайт, загружаемый браузером пользователя

7. Что такое OAuth?

A) Протокол шифрования каналов связи

B) Стандарт для безопасной передачи данных

C) Алгоритм хеширования

D) Протокол делегированной авторизации и аутентификации

8. Какая угроза связана с отсутствием валидаторов ввода в веб-приложениях?

A) SQL-инъекции

B) Cross-Site Request Forgery (CSRF)

C) Man-In-The-Middle (MITM)

D) Buffer Overflow

9. Что такое Kerberos?

A) Брандмауэр

B) Антивирусное ПО

C) Шлюз VPN

D) Система централизованной аутентификации и предоставления билетов доступа

10. Какой стандарт определяет форматы и процедуры цифровой подписи электронной почты?

A) OpenPGP

B) TLS

C) IPsec

D) S/MIME

11. Что такое JWT (JSON Web Token)?

A) Формат сжатия данных

B) Механизм хэширования

C) Средство защиты от спама

D) Стандарт токенов аутентификации и авторизации на основе JSON

12. Что представляет собой CSRF-токен?

A) Техническое средство блокировки входа в аккаунт

B) Токен, подтверждающий подлинность пользователя

C) Уникальный случайный маркер, предотвращающий подделку межсайтового запроса

D) Электронная подпись

13. Какая атака направлена на перегрузку системы большим количеством ложных запросов?

A) Denial of Service (DoS)

B) Phishing

C) Social engineering

D) Watering hole attack

14. Что такое Trusted Platform Module (TPM)?

A) Устройство хранения больших объемов данных

B) Микроконтроллер для осуществления аутентификации

C) Аппаратный модуль, хранящий ключи и сертификаты

D) Интерфейс взаимодействия с устройствами USB

15. Что такое HMAC (Hash-based Message Authentication Code)?

A) Код аутентичности сообщения, созданный на основе хэш-функции

B) Хэш-код файла

C) Сертификат открытого ключа

D) Методы стеганографии

16. Какой режим работы шифра используют для предотвращения повторения блоков в шифротексте?

A) ECB (Electronic Codebook mode)

B) CBC (Cipher Block Chaining mode)

C) OFB (Output Feedback mode)

D) CTR (Counter mode)

17. Что такое Zero-day vulnerability?

A) Уязвимость операционной системы Windows XP

B) Тип уязвимости, исправленный производителем

C) Уязвимость, известная разработчикам и пользователям

D) Уязвимость, неизвестная производителю программного обеспечения и не имеющая готового патча

18. Что такое SAML (Security Assertion Markup Language)?

A) Язык разметки для описания бизнес-процессов

B) Спецификация для обмена информацией об аутентификации и авторизации между системами

C) API-интерфейс для взаимодействия приложений

D) Интернет-протокол высокого уровня

19. Что такое nonce?

A) Количество попыток подбора пароля

B) Имя домена второго уровня

C) Временный номер, используемый в качестве одноразового маркера

D) Список разрешенных IP-адресов

20. Какая рекомендация относится к практике «безопасности по умолчанию» (security by default)?

A) Открытие максимального количества портов

B) Установка минимального количества обновлений безопасности

C) Ограничение прав доступа и предоставление полномочий только по мере необходимости

D) Хранение всех конфиденциальных данных в открытом доступе

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 3 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