МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан естественнонаучного факультета
_____ Пещукович А.И.
«____»_____2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Проектирование безопасных WEB-приложений

Направление подготовки - 10.03.01 «Информационная безопасность»
Профиль подготовки – Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Форма подготовки – Очная
Уровень подготовки – Бакалавриат

ДУШАНБЕ - 2026

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» **(**уровень Бакалавриат), утвержденного приказом Министерства образования и науки РФ №524 от 08.06.2017 г., Концепции преподавания Проектирование безопасных WEB-приложений для специальностей и направлений подготовки, реализуемых в образовательных организациях высшего образования, утвержденной протоколом Экспертного совета по развитию исторического образования Минобрнауки РФ от 06.08.2024 г. №ВФ/35-ПР

При разработке рабочей программы учитываются

- содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;
- новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Кафедра информатики и информационных технологий протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена УМС естественнонаучного факультета протокол №1 от «___» _____ 2025 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от «___» _____ 2025 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Актуальность изучения дисциплины «Проектирование безопасных WEB-приложений»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Проектирование безопасных WEB-приложений" является формирование у студентов теоретических знаний и практических навыков по проектированию и разработке безопасных веб-приложений. В рамках дисциплины студенты изучат современные подходы к обеспечению безопасности веб-приложений, методы защиты от распространенных угроз и уязвимостей, а также научатся применять эти знания на практике. Дисциплина направлена на подготовку специалистов, способных разрабатывать безопасные и надежные веб-приложения, соответствующие современным требованиям.

1.2 Задачи изучения дисциплины {Изучение принципов безопасной разработки веб-приложений.} {Освоение методов защиты от распространенных веб-угроз (XSS, CSRF, SQL-инъекции и т.д.).} {Формирование навыков анализа уязвимостей и проведения тестирования безопасности веб-приложений.} {Ознакомление с современными инструментами и технологиями обеспечения безопасности веб-приложений.} {Развитие навыков командной работы и решения практических задач по обеспечению безопасности веб-приложений.}

1.3 В результате изучения дисциплины «Проектирование безопасных WEB-приложений» у обучающихся формируются следующие универсальные и общепрофессиональные компетенции:

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из	"ИУК-2.1 Формулирует совокупность взаимосвязанных задач. ИУК-2.2 Определяет ресурсное обеспечение. ИУК-2.3 Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач.	

	действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.4 Выполняет задачи в рамках своей ответственности и при необходимости корректирует способы их решения."	
УК-3.	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	"ИУК-3.1 Определяет свою роль в команде. ИУК-3.2 Учитывает особенности поведения и интересы других участников. ИУК-3.3 Осуществляет обмен информацией и опытом. ИУК-3.4 Соблюдает нормы внутригруппового взаимодействия и несёт ответственность за результат."	
ПК-1.	Способен проводить обследование организаций и формировать требования к информационной системе	ИПК-1.1 Использует методики обследования организации и выявления информационных потребностей пользователей. ИПК-1.2 Анализирует деятельность предприятия и выявляет участки, нуждающиеся в автоматизации. ИПК-1.3 Выбирает класс ИС, способы автоматизации, оценивает совокупную стоимость владения ИС, планирует стратегическое и оперативное развитие ИС.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Проектирование безопасных WEB-приложений»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.06).** В процессе преподавания данного курса учитываются знания студентов по таким дисциплинам, как история таджикского народа, история первобытного общества, история древнего мира и средних веков, изучавшихся ими в общеобразовательной средней школе.

2.2 Преподавание данной дисциплины является необходимым для дальнейшего освоения студентами дисциплин в структуре ОПОП бакалавриата по направлению **«Информационная безопасность».**

Таблица 2.

№ п/п	Название дисциплины	Семестр	Место дисциплины в структуре ОПОП
-	—	—	Предшествующая дисциплина
-	—	—	Последующая дисциплина

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам, указанных в Таблице 2. Дисциплины взаимосвязаны с данной дисциплиной, они изучаются параллельно. Теоретическими дисциплинами, для которых освоение данной дисциплины необходимо как предшествующее являются:

3. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА, КРИТЕРИИ НАЧИСЛЕНИЯ БАЛЛОВ

Преподавание курса «Проектирование безопасных WEB-приложений» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 180 часа, из которых: лекции – 16 часов, практические занятия – 16 часов, лабораторные работы 16 часов, иная контактная работа – 32 часа, самостоятельная работа – 116. Всего часов аудиторной нагрузки – 64 часа.

По итогам 5 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в безопасность веб-приложений. Обзор угроз и уязвимостей.

Основные понятия безопасности веб-приложений. Классификация угроз. Обзор распространенных уязвимостей (XSS, CSRF, SQL Injection, Authentication/Authorization, Session Management)

Лекция 2 Аутентификация и авторизация. Методы и лучшие практики.

Принципы аутентификации и авторизации. Различные методы аутентификации (пароли, многофакторная аутентификация, OAuth). Рекомендации по обеспечению безопасности аутентификации и авторизации.

Лекция 3 Защита от межсайтового скриптинга (XSS).

Механизм XSS-атак. Типы XSS-атак (Stored, Reflected, DOM-based). Методы защиты от XSS: фильтрация входных данных, экранирование вывода, использование Content Security Policy (CSP).

Лекция 4 Защита от межсайтовой подделки запроса (CSRF).

Механизм CSRF-атак. Методы защиты от CSRF: использование CSRF-токенов, проверка Referer-заголовков. Разбор практических примеров.

Лекция 5 SQL-инъекции. Методы выявления и защиты.

Механизм SQL-инъекций. Техники SQL-инъекций. Методы защиты от SQL-инъекций: параметризованные запросы, проверка типов данных, использование Web Application Firewall (WAF).

Лекция 6 Безопасность хранения данных. Шифрование и хеширование.

Принципы шифрования и хеширования. Защита конфиденциальных данных (пароли, личная информация). Использование современных алгоритмов хеширования (bcrypt, Argon2).

Лекция 7 Безопасность сессий. Управление сессиями и куки.

Принципы управления сессиями. Методы защиты от угона сессий. Безопасное использование куки: атрибуты SameSite, Secure, HttpOnly.

Лекция 8 Тестирование безопасности веб-приложений. Обзор инструментов.

Методы тестирования безопасности: сканирование уязвимостей, пентестинг. Обзор инструментов для тестирования (Burp Suite, OWASP ZAP).

Структура и содержание практической части курса

Практическое занятие 1 Настройка среды разработки и инструментов безопасности. (Практика)

Установка и настройка необходимых инструментов (IDE, анализаторы кода, браузерные расширения для безопасности). Настройка тестовой среды.

Практическое занятие 2 Анализ и исправление XSS уязвимостей. (Практика)

Практическое задание по поиску и устранению XSS-уязвимостей. Использование различных методов защиты (фильтрация, экранирование).

Практическое занятие 3 Реализация защиты от CSRF атак. (Практика)

Практическое задание по реализации защиты от CSRF атак. Использование CSRF токенов и других методов защиты.

Практическое занятие 4 Выявление и устранение SQL-инъекций. (Практика)

Практическое задание по поиску и устранению SQL-инъекций. Использование параметризованных запросов и других методов защиты.

Практическое занятие 5 Практикум по безопасной аутентификации и авторизации. (Практика)

Реализация безопасной системы аутентификации и авторизации. Использование современных методов и библиотек.

Практическое занятие 6 Аудит и улучшение безопасности сессий. (Практика)

Аудит текущей системы управления сессиями. Внедрение лучших практик и улучшение безопасности сессий.

Практическое занятие 7 Использование инструментов тестирования безопасности (Burp Suite). (Практика)

Практическое применение Burp Suite для выявления уязвимостей. Анализ результатов сканирования.

Практическое занятие 8 Использование инструментов тестирования безопасности (OWASP ZAP). (Практика)

Практическое применение OWASP ZAP для выявления уязвимостей. Анализ результатов сканирования и формирование отчетов.

Структура и содержание КСР

КСР 1 Анализ требований к безопасности веб-приложения. Формирование ТЗ.

Анализ предоставленных требований к веб-приложению и формирование требований к безопасности. Разработка технического задания (ТЗ).

КСР 2 Проектирование безопасной архитектуры веб-приложения.

Разработка архитектуры веб-приложения с учетом требований безопасности. Выбор технологий и подходов к реализации.

КСР 3 Разработка плана тестирования безопасности веб-приложения.

Разработка плана тестирования безопасности: определение целей, scope, методов и инструментов тестирования.

КСР 4 Проведение статического анализа кода.

Применение инструментов статического анализа кода для выявления уязвимостей.

КСР 5 Проведение динамического анализа безопасности веб-приложения.

Проведение динамического анализа с использованием инструментов (Burp Suite, OWASP ZAP).

КСР 6 Анализ результатов тестирования и формирование отчета.

Анализ результатов тестирования безопасности веб-приложения. Формирование отчета с описанием найденных уязвимостей и рекомендациями по их устранению.

КСР 7 Разработка рекомендаций по устранению уязвимостей.

Разработка конкретных рекомендаций по устранению выявленных уязвимостей и повышению безопасности веб-приложения.

КСР 8 Защита разработанного веб-приложения от угроз и атак.

Разработка и реализация мер по защите веб-приложения от угроз и атак. Обзор и внедрение мер защиты, рассмотрение различных угроз и их воздействия.

Структура и содержание СРС

СРС 1 Изучение нормативных документов по безопасности веб-приложений.

Самостоятельное изучение стандартов и нормативных документов, регулирующих безопасность веб-приложений (ISO 27001, PCI DSS).

СРС 2 Подготовка реферата по теме "Современные методы защиты от DDoS атак".

Самостоятельное изучение современных методов защиты от DDoS атак и подготовка реферата.

СРС 3 Анализ уязвимостей веб-приложений на примере OWASP Top 10.

Самостоятельное изучение OWASP Top 10 и анализ уязвимостей веб-приложений.

СРС 4 Разработка сценариев тестирования безопасности веб-приложений.

Самостоятельная разработка сценариев тестирования безопасности для конкретных веб-приложений.

СРС 5 Изучение методов защиты от SQL-инъекций на конкретных примерах.

Самостоятельное изучение методов защиты от SQL-инъекций на конкретных примерах кода.

СРС 6 Самостоятельное изучение современных технологий аутентификации и авторизации.

Самостоятельное изучение современных технологий аутентификации и авторизации, таких как OAuth, OpenID Connect.

СРС 7 Разработка безопасного веб-приложения (индивидуальное задание).

Самостоятельная разработка безопасного веб-приложения с использованием изученных методов и технологий.

СРС 8 Подготовка презентации по теме "Лучшие практики обеспечения безопасности веб-приложений".

Подготовка презентации по теме "Лучшие практики обеспечения безопасности веб-приложений" на основе изученного материала.

СРС 9 Разработка отчета о тестировании безопасности веб-приложения.

Составление отчета по результатам проведенного тестирования безопасности веб-приложения, включая найденные уязвимости и рекомендации по их устранению.

СРС 10 Анализ уязвимостей конкретного веб-приложения и подготовка отчета.

Самостоятельный анализ уязвимостей конкретного веб-приложения, подготовка отчета о выявленных уязвимостях и рекомендации по их устранению.

СРС 11 Изучение передовых технологий защиты веб-приложений.

Изучение и анализ новых подходов и инструментов защиты веб-приложений, включая WAF, системы обнаружения атак.

СРС 12 Подготовка доклада на тему современных угроз веб-безопасности.

Подготовка и представление доклада о современных угрозах веб-безопасности, включая актуальные атаки и способы защиты от них.

СРС 13 Реализация защиты от XSS-атак в существующем веб-приложении.

Самостоятельная реализация защиты от XSS-атак в существующем веб-приложении, используя изученные методы.

СРС 14 Внедрение многофакторной аутентификации (MFA) в веб-приложении.

Внедрение многофакторной аутентификации (MFA) для повышения безопасности доступа к веб-приложению.

СРС 15 Разработка рекомендаций по повышению безопасности веб-приложения.

Разработка конкретных рекомендаций по повышению безопасности веб-приложения на основе проведенного анализа и тестирования.

СРС 16 Подготовка к итоговому тестированию.

Подготовка к итоговому тестированию по материалам курса.

СРС 17 Работа над индивидуальным проектом.

Работа над индивидуальным проектом по проектированию безопасного веб-приложения.

СРС 18 Рецензирование кода и анализ отчетов о безопасности.

Проведение взаимного рецензирования кода и анализа отчетов о безопасности, обмен опытом и знаниями.

СРС 19 Разбор реальных примеров успешных веб-атак.

Анализ реальных примеров успешных веб-атак, изучение способов их реализации и предотвращения.

СРС 20 Изучение современных методов защиты от SQL инъекций.

Самостоятельное изучение продвинутых методов защиты от SQL инъекций, включая использование Prepared Statements.

СРС 21 Анализ защищенности веб-приложения с помощью статического анализатора кода.

Использование статического анализатора кода для оценки безопасности веб-приложения и выявления уязвимостей.

СРС 22 Разработка пользовательских модулей безопасности для веб-приложений.

Самостоятельная разработка пользовательских модулей безопасности для веб-приложений, например, для защиты от CSRF.

СРС 23 Практическая работа по применению Content Security Policy.

Практическое применение Content Security Policy (CSP) для защиты от XSS атак в веб-приложении.

СРС 24 Оптимизация производительности веб-приложения с учетом безопасности.

Изучение методов оптимизации производительности веб-приложений с учетом требований безопасности.

СРС 25 Анализ защищенности веб-приложения с помощью динамического сканирования.

Проведение динамического сканирования веб-приложения для выявления уязвимостей, используя различные инструменты.

СРС 26 Разработка плана действий в случае обнаружения инцидента безопасности.

Разработка плана действий для реагирования на инциденты безопасности в веб-приложениях.

СРС 27 Создание отчета о тестировании безопасности веб-приложения.

Самостоятельное составление отчета о тестировании безопасности веб-приложения, включая обнаруженные уязвимости и рекомендации по их устранению.

СРС 28 Изучение и применение техник обфускации кода для защиты от reverse engineering.

Изучение и применение техник обфускации кода для защиты веб-приложения от reverse engineering.

СРС 29 Разработка и внедрение системы логирования и мониторинга безопасности.

Разработка и внедрение системы логирования и мониторинга для отслеживания событий безопасности в веб-приложении.

СРС 30 Оценка рисков безопасности веб-приложения.

Проведение оценки рисков безопасности веб-приложения для определения приоритетов и мер защиты.

СРС 31 Изучение современных методов тестирования на проникновение (Penetration Testing).

Изучение современных методов тестирования на проникновение для оценки безопасности веб-приложения.

СРС 32 Практикум по внедрению безопасных HTTP-заголовков.

Настройка и использование безопасных HTTP-заголовков для защиты от различных атак.

СРС 33 Подготовка презентации на тему 'Будущее веб-безопасности'.

Подготовка презентации, посвященной будущему веб-безопасности, с обсуждением новых угроз и технологий защиты.

СРС 34 Работа над проектом: разработка безопасного веб-приложения.

Работа над завершением проекта: разработка безопасного веб-приложения с учетом всех изученных принципов и практик.

СРС 35 Подготовка к экзамену.

Систематизация знаний и подготовка к итоговому экзамену по дисциплине.

СРС 36 Практическое задание: создание отчета о тестировании безопасности веб-приложения.

Практическое создание детального отчета о проведенном тестировании безопасности, включая анализ уязвимостей и рекомендации.

СРС 37 Рефакторинг и аудит существующего веб-приложения.

Проведение рефакторинга и аудита существующего веб-приложения с целью повышения его безопасности и производительности.

СРС 38 Анализ и устранение уязвимостей в open source веб-приложениях.

Самостоятельный анализ и устранение уязвимостей в open source веб-приложениях.

СРС 39 Разработка рекомендаций по безопасности для конкретного веб-проекта.

Формулирование конкретных рекомендаций по обеспечению безопасности для выбранного веб-проекта.

СРС 40 Подготовка к защите проекта.

Подготовка к защите итогового проекта, включая написание реферата и презентации.

СРС 41 Разработка плана реагирования на инциденты безопасности для веб-приложения.

Разработка детального плана действий в случае обнаружения инцидентов безопасности в веб-приложении.

СРС 42 Изучение новых технологий и тенденций в веб-безопасности.

Самостоятельное изучение актуальных технологий и трендов в веб-безопасности.

СРС 43 Анализ существующих решений по защите веб-приложений.

Анализ существующих решений по защите веб-приложений, включая WAF и другие технологии.

СРС 44 Разработка и внедрение системы обнаружения вторжений (IDS) для веб-приложения.

Практическая работа по разработке и внедрению системы обнаружения вторжений для веб-приложения.

СРС 45 Обучение и работа с реальными данными уязвимостей.

Практическая работа с реальными данными уязвимостей и их анализом.

СРС 46 Подготовка к итоговому экзамену и защита проекта.

Подготовка к итоговому экзамену и защита проекта.

СРС 47 Заключительное занятие: разбор сложных кейсов и вопросов.

Разбор сложных кейсов, ответы на вопросы студентов, обсуждение перспектив веб-безопасности.

Структура и содержание теоретической, лабораторной части курса, КСР и СРС

Таблица 3.

№ п/п	Наименование темы	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Лит-ра	Количество
		Лек	Прак	КСР	Лаб	СРС	ИКР		
1	Введение в безопасность веб-приложений. Обзор угроз и уязвимостей.	2			2	4		1	12
	Настройка среды разработки и инструментов безопасности.		2					4	
2	Анализ требований к безопасности веб-приложения. Формирование ТЗ.			2		4		3	12
3	Аутентификация и авторизация. Методы и лучшие практики.	2			2			6	12
	Анализ и исправление XSS уязвимостей.		2			4		5	
4	Проектирование безопасной архитектуры веб-приложения.			2				4	12
5	Защита от межсайтового скриптинга (XSS).	2			2	4		2	12
	Реализация защиты от CSRF атак.		2					5	
6	Разработка плана тестирования безопасности веб-приложения.			2		4		7	12
7	Защита от межсайтовой подделки запроса (CSRF).	2			2			2	12
	Выявление и устранение SQL-инъекций.		2					2	
8	Проведение статического анализа кода.			2		4		1	12
9	SQL-инъекции. Методы выявления и защиты.	2			2			4	12

	Практикум по безопасной аутентификации и авторизации.		2			2		5	
10	Проведение динамического анализа безопасности веб-приложения.			2				3	12
11	Безопасность хранения данных. Шифрование и хеширование.	2			2	4		2	12
	Аудит и улучшение безопасности сессий.		2					5	
12	Анализ результатов тестирования и формирование отчета.			2		4		6	12
13	Безопасность сессий. Управление сессиями и куки.	2			2			5	12
14	Использование инструментов тестирования безопасности (Burp Suite).		2			4		6	12
15	Разработка рекомендаций по устранению уязвимостей.			2				5	12
	Тестирование безопасности веб-приложений. Обзор инструментов.	2			2	2		4	
16	Использование инструментов тестирования безопасности (OWASP ZAP).		2					5	12
	Защита разработанного веб-приложения от угроз и атак.			2		2		2	
Итого:		16	16	16	16	42	0		20

Формы контроля и критерии начисления баллов

Контроль усвоения студентом каждой темы осуществляется в рамках балльно-рейтинговой системы (БРС), включающей текущий, рубежный и итоговый контроль. Студенты **3 -го курса**, обучающиеся по кредитно-рейтинговой системе обучения, могут получить максимально возможное количество баллов - 300. Из них на текущий и рубежный контроль выделяется 200 баллов или 49% от общего количества.

На итоговый контроль знаний студентов выделяется 51% или 100 баллов.

Порядок выставления баллов: 1-й рейтинг (1-7 недели до 12,5 баллов+12,5 баллов (8 неделя – Рубежный контроль №1) = 100 баллов), 2-й рейтинг (9-15 недели до 12,5 баллов+12,5 баллов (16 неделя – Рубежный контроль №2) = 100 баллов), итоговый контроль 100 баллов.

К примеру, за текущий и 1-й рубежный контроль выставляется 100 баллов:

лекционные занятия – 21 балл, за практические занятия (КСР, лабораторные) – 31,5 балл, за СРС – 17,5 баллов, требования ВУЗа – 17,5 баллов, рубежный контроль – 12,5 баллов.

В случае пропуска студентом занятий по уважительной причине (при наличии подтверждающего документа) в период академической недели деканат факультета обращается к проректору по учебной работе с представлением об отработке студентом баллов за пропущенные дни по каждой отдельной дисциплине с последующим внесением их в электронный журнал.

Итоговая форма контроля по дисциплине (зачет, экзамен) проводится как в форме тестирования, так и в традиционной (устной) форме. Тестовая форма итогового контроля по дисциплине предусматривает: для естественнонаучных направлений – 10 тестовых вопросов на одного студента, где правильный ответ оценивается в 10 баллов, для гуманитарных направлений – 25 тестовых вопросов, где правильный ответ оценивается в 4 балла. Тестирование проводится в электронном виде, устный экзамен на бумажном носителе с выставлением оценки в ведомости по аналогичной системе с тестированием.

Таблица 4.

Неделя	Активное участие на лекционных занятиях, написание конспекта и выполнение других видов работ*	Активное участие на практических (семинарских) занятиях, КСР	СРС Написание реферата, доклада, эссе Выполнение других видов работ	Выполнение положения высшей школы (установленная форма одежды, наличие рабочей папки, а также других пунктов устава высшей школы)	РК №1	Всего
1	2	3	4	5	6	7
1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Первый рейтинг	21	31,5	17,5	17,5	12,5	100
1	2	3	4	5	6	7

1	3	4,5	2,5	2,5	-	12,5
2	3	4,5	2,5	2,5	-	12,5
3	3	4,5	2,5	2,5	-	12,5
4	3	4,5	2,5	2,5	-	12,5
5	3	4,5	2,5	2,5	-	12,5
6	3	4,5	2,5	2,5	-	12,5
7	3	4,5	2,5	2,5	-	12,5
8	-	-	-	-	12,5	12,5
Второй рейтинг	21	31,5	17,5	17,5	12,5	100
Итог						200

Формула вычисления результатов дистанционного контроля и итоговой формы контроля по дисциплине за семестр для студентов 3 -го курсов:

$$ИБ = \left[\frac{(P_1 + P_2)}{2}\right] \cdot 0{,}49 + Эи \cdot 0{,}51 \ ,$$

где ИБ –итоговый балл, P_1- итоги первого рейтинга, P_2- итоги второго рейтинга, *Эи*– результаты итоговой формы контроля (экзамен).

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы обработки информации» включает в себя:

1. план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

2. характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

3. требования к представлению и оформлению результатов самостоятельной работы;

4. критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

4.1. План-график выполнения самостоятельной работы по дисциплине

№	Объем СРС, ч.	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля
1	4	Понятие и архитектура WEB-приложений	Вопросы 1–4. Описание технологии разработки, реферат	Опрос
2	4	Основные угрозы безопасности WEB-приложений	Вопросы 5–8. Презентация методов	Выступление
3	6	Модель угроз и анализ рисков WEB-приложений	Вопросы 8–10. Презентация, доклад	Выступление
4	6	Уязвимости OWASP Top 10	Вопросы 11–13. Выполнение задания 1 (1–10)	Защита работы, выступление
5	4	Безопасное проектирование архитектуры WEB-приложений	Выполнение задания 1. Конспект, презентация (вопросы 14–15)	Опрос, выступление
6	4	Аутентификация и управление сессиями	Выполнение задания 2	Защита работы
7	6	Авторизация и контроль доступа	Вопросы 16–17. Выполнение задания 3	Защита работы
8	6	Защита от XSS, CSRF и SQL-инъекций	Вопросы 16–17. Выполнение задания 4	Защита работы
9	4	Безопасная работа с пользовательским вводом	Выполнение задания 5	Защита работы
10	4	Криптографическая защита данных в WEB-приложениях	Вопросы 18–25. Выполнение задания 6	Защита работы
11	4	Логирование и мониторинг безопасности	Вопросы 26–29. Выполнить задания 2 и описать в терминах классов	Опрос, защита работы
12	4	Тестирование безопасности WEB-приложений	Вопросы 30–31. Реферат. Выполнение задания 7	Защита реферата, защита работы
13	4	Безопасность API и микросервисов	Вопросы 32–37. Презентация	Опрос, выступление
14	4	Защита WEB-приложений в облачной среде	Вопросы 38–40. Выполнение задания 8 (1–4)	Защита работы
15	4	Безопасность DevOps и CI/CD	Вопросы 41–44. Выполнение задания 9	Защита работы
16	4	Комплексное проектирование безопасного WEB-приложения	Вопросы 45–46. Выполнение задания 8 (4–10)	Защита работы

4.2 Характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе «Содержание и структура дисциплины». Конспекты и задания можно выполнить в отдельном тетради или в

лекционной (практической) тетради в произвольной форме.

4.3 Критерии оценки выполнения самостоятельной работы.

Критерии оценки выполнения самостоятельной работы является полнота освещения вопроса, логичность изложения, проявления самостоятельность в обработке материала.

4.4. Критерии оценки выполнения самостоятельной работы.

Самостоятельная работа прививает студентам навыки работы с источниками и учебной литературой, помогает повысить уровень знаний по предмету, которые можно использовать на практике.

Оценка «отлично» выставляется студенту, если индивидуальное задание выполнено полностью и по данной теме защищена лабораторная работа.

Оценка «хорошо» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено с отдельными замечаниями.

Оценка «удовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

Оценка «неудовлетворительно» выставляется студенту, если лабораторная работа по теме индивидуального задания не защищена, а само индивидуальное задание выполнено не до конца, т.е. не полностью.

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕ- ЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература:

1. 1. Макконнелл С. Совершенный код. – СПб.: Питер, 2018. – 896 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходный код в С. – М.: Триумф, 2019. – 816 с.
3. Стивенс Р., Коллинз М., Карниц Дж. HTTP. Подробное руководство. – М.: Символ-Плюс, 2017. – 688 с.
4. Гольденберг С. HTTP. Полное руководство. – М.: ДМК Пресс, 2019. – 448 с.
5. Болтон Д. Безопасность веб-приложений. Руководство для разработчиков. – СПб.: Питер, 2019. – 432 с.

6. Варгас Э. Веб-безопасность для профессионалов. – М.: ДМК Пресс, 2019. – 480 с.
7. Паттерсон, Д. Компьютерные сети. – СПб.: Питер, 2020. – 1024 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Керри Джонс. SQL для чайников. – М.: Диалектика, 2020. – 352 с.
2. Лоуренс П. Веб-сервисы. – М.: Вильямс, 2016. – 336 с.
3. Кинг, К. Программирование сетевых приложений. – М.: ДМК Пресс, 2018. – 480 с.
4. Х. Храмова, А. Хорев. Защита от DDoS-атак. – М.: ДМК Пресс, 2018. – 288 с.
5. Блэкберн Дж., Боско В. Атака на Java-приложения. – М.: ДМК Пресс, 2016. – 368 с.
6. Седжвик Р., Уэйн К. Алгоритмы на Java. – М.: Вильямс, 2017. – 848 с.
7. Гарсия-Молина Г., Ульман Дж., Уидом Дж. Системы баз данных. Полный курс. – М.: Вильямс, 2015. – 1088 с.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. OWASP (Open Web Application Security Project): https://owasp.org/
2. SANS Institute: https://www.sans.org/
3. PortSwigger Web Security Academy: https://portswigger.net/web-security
4. Web Security Initiative: https://www.websecurityinitiative.org/
5. NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для обеспечения систематической и регулярной работы по изучению дисциплины «Проектирование безопасных WEB-приложений» и успешного

прохождения текущих и итоговых контрольных испытаний студенту рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.

2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.

3. Согласовывать с преподавателем виды работы по изучению дисциплины.

4. По завершении отдельных тем передавать выполненные работы (рефераты) преподавателю.

Обучение по дисциплине «Проектирование безопасных WEB-приложений» строится следующим образом. На лекциях преподаватель дает общую характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

При подготовке к практическому занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее рефератами, докладами и презентациями.

Самостоятельная работа должна соответствовать графику прохождения программы дисциплины. Самостоятельная работа по дисциплине

«Проектирование безопасных WEB-приложений» включает:

а) работу с литературой;

б) подготовку устного выступления на практическом занятии;

в) подготовку к занятию в интерактивной форме;

г) подготовку реферата с презентацией;

д) подготовку к дискуссии;

е) заполнение хронологической таблицы;

ж) подготовку к текущей и итоговой аттестации по дисциплине.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, которая может осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа студентов предполагает самостоятельное изучение отдельных тем, дополнительную подготовку студентов к каждому практическому занятию.

Самостоятельная работа студентов является важной формой образовательного процесса. Она реализуется непосредственно в процессе аудиторных занятий, в контакте с преподавателем, а также в библиотеке, дома, при выполнении студентом учебных и творческих задач.

Цель самостоятельной работы студентов - научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

При изучении дисциплины организация самостоятельной работы студентов форм представлена следующим образом:

1) внеаудиторная самостоятельная работа;

2)аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя.

Аудиторная самостоятельная работа может реализовываться при проведении практических занятий и во время чтения лекций.

На практических занятиях различные виды самостоятельной работы

позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

Для проведения занятий необходимо иметь большой банк заданий, причем эти задания могут быть дифференцированы по степени сложности.

На каждом этапе самостоятельной работы следует разъяснять цели работы, контролировать понимание этих целей студентами, постепенно формируя у них умение самостоятельной постановки задачи и выбора цели.

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов

путем проведения экспресс-опросов по конкретным темам.

На практических занятиях различные виды самостоятельной работы позволяют сделать процесс обучения более интересным и поднять активность значительной части студентов в группе.

На практических занятиях нужно не менее 1 часа из двух (50% времени) отводить на самостоятельное рассмотрение заданий.

По результатам самостоятельного рассмотрения задания следует выставлять по каждому занятию оценку. Оценка предварительной подготовки студента к практическому занятию может быть сделана путем экспресс-опроса в течение 5, максимум - 10 минут.

По материалам раздела целесообразно выдавать студенту домашнее задание и на последнем практическом занятии по разделу подвести итоги его изучения (например, провести контрольную работу), обсудить оценки каждого студента, выдать дополнительные задания тем студентам, которые хотят повысить оценку.

Результативность самостоятельной работы студентов во многом определяется наличием активных методов ее контроля. Существуют следующие виды контроля:

- входной контроль знаний и умений студентов при начале изучения очередной дисциплины;

- текущий контроль, то есть регулярное отслеживание уровня усвоения материала на лекциях, практических занятиях;

- самоконтроль, осуществляемый студентом в процессе изучения дисциплины при подготовке к контрольным мероприятиям;

- итоговый контроль по дисциплине в виде зачета, зачета с оценкой (в устной форме).

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИТ РТСУ имеются 4 компьютерных классов. Для занятий используются лицензионное программное обеспечение ОС Windows -7/8/10/11 и программное обеспечение открытого доступа (Open source), среды программирования (Denwer, CodeBlock, Dev_C++ и др.). Для разработки моделей проекта ИС используются CASE – средства: ERWin, Visual UML, Rational Rose и т.д.

В Университете созданы специальные условия для обучающихся с ограниченными возможностями здоровья - специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания организаций и другие условия, без которых невозможно или затруднено освоение дисциплины обучающимися с ограниченными возможностями здоровья.

Обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература, а также обеспечивается:

- наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проёмов, лифтов).

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования. Защита курсового проекта: представляется пояснительная записка и презентация выступления.

Текущий контроль студентов осуществляется путем защиты лабораторных работ, выполнения самостоятельного задания, обсуждения теоретических вопросов.

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине.

Тестовые задания для промежуточного контроля знаний по дисциплине;

Методические рекомендации и тематика курсового проектирования.

Также указаны критерии оценки курсового проекта.

Итоговая система оценок по кредитно-рейтинговой системе с использованием буквенных символов

Оценка по буквенной системе	Диапазон соответствующих наборных баллов	Численное выражение оценочного балла	Оценка по традиционной системе
A	10	95-100	Отлично
A-	9	90-94	
B+	8	85-89	Хорошо
B	7	80-84	
B-	6	75-79	
C+	5	70-74	Удовлетворительно
C	4	65-69	
C-	3	60-64	
D+	2	55-59	
D	1	50-54	
Fx	0	45-49	

F	0	0-44	Неудовлетвори-тельно

Содержание текущего контроля, промежуточной аттестации, итогового контроля раскрываются в фонде оценочных средств, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС ВО.

ФОС по дисциплине является логическим продолжением рабочей программы учебной дисциплины. ФОС по дисциплине прилагается.