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

Безопасность 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 Безопасность 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 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 «Безопасность WEB-приложений»

1.1 Цели изучения дисциплины Целью освоения дисциплины "Безопасность WEB-приложений" является формирование у студентов теоретических знаний и практических навыков в области защиты web-приложений от различных угроз. Дисциплина направлена на изучение современных методов и технологий обеспечения безопасности web-приложений, включая анализ уязвимостей, разработку защищенного кода и применение средств защиты. В результате освоения дисциплины студенты должны быть готовы к самостоятельной разработке и аудиту безопасности web-приложений.

1.2 Задачи изучения дисциплины Задачи дисциплины:

1. Изучение основных принципов и концепций безопасности web-приложений.

2. Анализ распространенных уязвимостей web-приложений и методов их эксплуатации.

3. Освоение методов защиты web-приложений, включая разработку безопасного кода и настройку средств защиты.

4. Формирование навыков проведения аудита безопасности web-приложений.

5. Развитие умения применять полученные знания на практике для решения задач обеспечения безопасности web-приложений.

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

Код	Результаты освоения ООП	Индикаторы достижения компетенции	Вид оценочного знания
ПК-2	Способен разрабатывать и адаптировать прикладное	ИПК-2.1 Применяет современные технологии разработки и адаптации прикладного ПО.ИПК-2.2 Разрабатывает и адаптирует ПО на современных языках программирования.ИПК-2.3 Применяет	

	программное обеспечение	современные технологии для разработки веб-приложений.	
ПК-3	Способен проектировать информационные системы по видам обеспечения	ИПК-3.1 Обосновывает выбор проектных решений по видам обеспечения ИС.ИПК-3.2 Участвует в проектировании экономических ИС и их модулей.	
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	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. ИУК-2.4 Выполняет задачи в рамках своей ответственности и при необходимости корректирует способы их решения.	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина **«Безопасность WEB-приложений»** входит в обязательную часть Блока Дисциплины (модули) ОПОП ВО и является её базовой частью **(Б1.В.02).** 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 «Безопасность WEB-приложений» планируется студентам Очная формы обучения по направлению «Информационная безопасность».

Объем дисциплины составляет __ зачетные единицы. Всего запланировано 90 часа, из которых: лекции – 16 часов, практические занятия – 14 часов, лабораторные работы 16 часов, иная контактная работа – 32 часа, самостоятельная работа – 42. Всего часов аудиторной нагрузки – 48 часа.

По итогам 3 семестра планируется сдача студентами зачета с оценкой.

3.1 Структура и содержание теоретической части курса

Лекция 1 Введение в безопасность Web-приложений. Основные понятия и угрозы.

Обзор ландшафта угроз web-приложений. Классификация уязвимостей. Нормативно-правовая база в сфере информационной безопасности.

Лекция 2 Атаки на аутентификацию и авторизацию.

Методы аутентификации. Атаки на пароли (подбор, перебор, кража). Управление сессиями и атаки на сессии.

Лекция 3 Внедрение кода (Code Injection) и межсайтовый скриптинг (XSS).

SQL injection. Межсайтовый скриптинг (XSS): типы, методы атаки и защиты. OS Command Injection.

Лекция 4 Межсайтовая подделка запросов (CSRF) и атаки на файлы.

Принципы работы CSRF. Атаки на загрузку файлов и уязвимости, связанные с обработкой файлов.

Лекция 5 Атаки на логику приложений и бизнес-логику.

Уязвимости, связанные с нарушением бизнес-логики. Методы выявления и защиты.

Лекция 6 Безопасность хранения данных. Шифрование и хеширование.

Методы защиты конфиденциальных данных. Использование шифрования и хеширования. Рекомендации по безопасному хранению паролей.

Лекция 7 Безопасность API. Защита от DDoS атак.

Защита API: аутентификация, авторизация, rate limiting. Обзор методов защиты от DDoS.

Лекция 8 Аудит безопасности Web-приложений. Обзор инструментов.

Методология проведения аудита безопасности. Обзор инструментов для автоматизированного сканирования уязвимостей.

Структура и содержание практической части курса

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

Установка и настройка необходимых инструментов (Burp Suite, OWASP ZAP, etc.). Знакомство с интерфейсом и основными функциями.

Практическое занятие 2 Анализ уязвимостей аутентификации. Подбор паролей и перебор учетных записей. (Практика)

Практическое применение инструментов для взлома паролей. Изучение способов защиты от атак.

Практическое занятие 3 Практикум по SQL-инъекциям. Внедрение кода. (Практика)

Отработка техник SQL injection. Поиск и эксплуатация уязвимостей.

Практическое занятие 4 Межсайтовый скриптинг (XSS). Эксплуатация и защита. (Практика)

Типы XSS атак. Практический анализ и эксплуатация XSS уязвимостей. Методы защиты.

Структура и содержание лабораторной части курса

Лабораторная работа 1 Установка и настройка среды для тестирования безопасности Web-приложений.

Установка и настройка виртуальных машин с уязвимыми Web-приложениями (DVWA, etc.).

Лабораторная работа 2 Использование инструментов для перехвата HTTP-трафика (Burp Suite).

Практическое применение Burp Suite для анализа запросов и ответов.

Лабораторная работа 3 Атака и защита от SQL-инъекций.

Практический анализ и эксплуатация SQL injection. Изучение методов защиты (Prepared Statements).

Лабораторная работа 4 Атака и защита от XSS-атак.

Практический анализ и эксплуатация XSS. Использование различных типов XSS. Применение механизмов защиты (escaping, CSP).

Лабораторная работа 5 Практическая работа с CSRF-атаками.

Эксплуатация CSRF. Рекомендации по защите (CSRF tokens).

Лабораторная работа 6 Анализ и эксплуатация уязвимостей, связанных с загрузкой файлов.

Практическое исследование уязвимостей при загрузке файлов. Рекомендации по защите.

Лабораторная работа 7 Аудит безопасности Web-приложения с использованием сканеров уязвимостей.

Практическое применение сканеров уязвимостей. Анализ отчетов и разработка рекомендаций.

Лабораторная работа 8 Разработка защищенного Web-приложения (с использованием современных фреймворков).

Разработка простого Web-приложения с учетом принципов безопасной разработки.

Структура и содержание КСР

КСР 1 Анализ уязвимостей конкретного Web-приложения (выбор по вариантам).

Выбор и анализ уязвимостей конкретного Web-приложения. Составление отчета.

КСР 2 Разработка плана защиты Web-приложения на основе проведенного анализа.

Разработка плана защиты для выбранного Web-приложения, с учетом выявленных уязвимостей.

КСР 3 Реализация мер защиты от SQL-инъекций (на примере выбранного языка программирования).

Реализация мер защиты от SQL-инъекций на конкретном примере.

КСР 4 Реализация защиты от XSS атак. (Выбор языка программирования).

Реализация защиты от XSS на выбранном языке программирования.

Структура и содержание СРС

СРС 1 Изучение теоретических основ безопасности Web-приложений.

Самостоятельное изучение разделов учебной литературы и статей по безопасности web-приложений.

СРС 2 Подготовка к лабораторным работам и практическим занятиям.

Изучение материала, необходимого для выполнения лабораторных работ и практических заданий.

СРС 3 Поиск и анализ информации по актуальным уязвимостям Web-приложений.

Поиск и анализ информации по новым уязвимостям в Web-приложениях. Изучение способов их эксплуатации и защиты.

СРС 4 Изучение документации по инструментам для тестирования безопасности.

Изучение документации и освоение инструментов для тестирования безопасности Web-приложений.

СРС 5 Выполнение индивидуальных заданий.

Выполнение индивидуальных заданий, направленных на закрепление полученных знаний и навыков.

СРС 6 Подготовка к контрольным мероприятиям.

Подготовка к текущим и итоговым контрольным мероприятиям.

СРС 7 Подготовка к защите отчета по результатам аудита Web-приложения.

Подготовка к защите отчета по результатам аудита Web-приложения. Подготовка презентации.

СРС 8 Разработка отчета по результатам аудита Web-приложения.

Самостоятельная разработка отчета по результатам аудита Web-приложения.

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 баллов
		Лек	Прак	КСР	Лаб	СРС	ИКР		
1	Введение в безопасность Web-приложений. Основные понятия и угрозы.	2	2	2	2	8			12.5

2	Атаки на аутентификацию и авторизацию.	2	2	2	2	6			12.5
3	Внедрение кода (Code Injection) и межсайтовый скриптинг (XSS).	2	2	2	2	6			12.5
4	Межсайтовая подделка запросов (CSRF) и атаки на файлы.	2	2	2	2	6			12.5
5	Атаки на логику приложений и бизнес-логику.	2			2	4			
6	Безопасность хранения данных. Шифрование и хеширование.	2			2	4			
7	Безопасность	2			2	4			

	API. Защита от DDoS атак.								
8	Аудит безопасности Web-приложений. Обзор инструментов.	2			2	4			
Итого:		**16**	**8**	**8**	**16**	**42**	**0**		**50**

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 **2 -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 2 -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	Тема СРС	Форма и вид результатов самостоятельной работы	Форма контроля

1.			Вопросы 1-4. Описание технологии разработки, реферат	Опрос
2.			Вопросы 5-8. Презентация методов	Выступление
3.			Вопросы 8-10. Презентация, доклад	Выступление
4.			Вопросы 11-13. Выполнение задания 1 (1-10).	Защита работы. Выступление
5.			Выполнение задания 1. Конспект, презентация (вопросы 14-15)	Опрос, Выступление
6.			Выполнение задания 2	Защита работы.
7.			Вопросы 16-17. Выполнение задания 3	Защита работы.
8.			Вопросы 16-17. Выполнение задания 4	Защита работы.
9.			Выполнение задания 5	Защита работы.
10.			Вопросы 18-25. Выполнение задания 6	Защита работы.
11.			Вопросы 26-29. Выполнить задания 2 и описать в терминах классов.	Опрос. Защита работы
12.			Вопросы 30-31. Реферат. Выполнение задания 7	Защита реферата. Защита работы
13.			Вопросы 32-37. Презентация	Опрос. Выступление
14.			Вопросы 38-40. Выполнение задания 8 (1-4)	Защита работы
15.			Вопросы 41-44. Выполнение задания 9	Защита раз боты
16.			Вопросы 45-46. Выполнение задания 8 (4-10)	Защита работы
17.			Вопросы 50-51. Выполнение задания 10	Защита работы
18.			Вопросы 52-54. Выполнение задания 11	Защита работы

19.			Вопросы 55-59. Выполнение задания 11	Защита работы
20.			Вопросы 60-62. Выполнение задания 12	Защита работы
21.			Вопросы 63-64. Выполнение задания 13	Защита работы
22.			Вопросы 65-66. Выполнение задания 14	Защита работы
23.			Вопросы 67-68. Выполнение задания 15	Защита работы
24.			Вопросы 69-74. Презентация, доклад	Выступление

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. Щербаков А.Ю. Безопасность Web-приложений. Учебное пособие. М.: ДМК Пресс, 2020. 336 с.

2. Гольман М. А. Защита web-приложений: Практическое руководство. СПб.: Питер, 2019. 288 с.

3. Макаров А. С. Web-безопасность. Учебник для вузов. М.: Издательство Юрайт, 2020. 256 с.

4. Скворцов А.В. Безопасность web-приложений на практике. М.: ДМК Пресс, 2018. 200 с.

5. Самсонов А.В. Основы защиты web-приложений. Учебное пособие. СПб.: БХВ-Петербург, 2019. 224 с.

6. Богатырев С. Ю. Аудит безопасности web-приложений. М.: Издательство «Наука», 2019. 184 с.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. М.: Триумф, 2019. 816 с.

5.2. Учебники и учебные пособия в сети Интернет:

1. 1. Кузнецов С.Д. Технологии разработки web-приложений. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2018.

2. Евстратов С.А. Основы информационной безопасности. М.: Издательство «Флинта», 2017.

3. Таненбаум Э. Архитектура компьютера. СПб.: Питер, 2019.

4. Макконнелл С. Совершенный код. М.: Питер, 2018.

5. Кнут Д. Искусство программирования. Том 1. Основные алгоритмы. М.: Вильямс, 2018.

6. Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. М.: Вильямс, 2019.

7. Кнут Д. Искусство программирования. Том 3. Сортировка и поиск. М.: Вильямс, 2020.

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. 1. OWASP (Open Web Application Security Project): https://owasp.org/

2. NIST (National Institute of Standards and Technology): https://www.nist.gov/

3. CISA (Cybersecurity and Infrastructure Security Agency): https://www.cisa.gov/

4. Хабр: https://habr.com/

5. Stack Overflow: https://stackoverflow.com/

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 «Безопасность 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 «Безопасность 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 «Безопасность 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	Неудовлетворительно
F	0	0-44	

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.