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

ЕСТЕСТВЕННОНАУЧНЫЙ ФАКУЛЬТЕТ
Кафедра «Информатика и ИТ»

«Утверждаю»
Декан естественнонаучного факультета
_____ Пешукович А.И.
«_1_» __Сентября___2026 г.
.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине (модулю)

ПРОЕКТИРОВАНИЕ БЕЗОПАСНЫХ WEB-ПРИЛОЖЕНИЙ

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

ДУШАНБЕ 2026

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
Проектирование безопасных WEB-приложений

Код компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения	Вид оценочного знания
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 в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение. **ИУК-2.2.** Определяет ресурсное обеспечение для достижения поставленной цели; **ИУК-2.3.** Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **ИУК-2.4.** Выполняет задачи в рамках своей ответственности в соответствии с запланированными результатами, при необходимости корректирует способы решения задач	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
УК-3	**Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде**	ИУК-3.1. Определяет свою роль в социальном взаимодействии и командной работе, исходя из знания социологии и социальной психологии, методов развития личности этических норм профессионального взаимодействия с коллективом ИУК-3.2. При реализации своей роли в социальном взаимодействии и командной работе учитывает особенности поведения и интересы других участников ИУК-3.3. Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает статусные позиции других членов команды для достижения поставленной цели ИУК-3.4. Соблюдает нормы и установленные правила внутригруппового взаимодействия; несет личную ответственность за результат	Отчеты по практическим работам. Устный опрос. Презентация

ПК-1	**Способен проводить обследование организаций, выявлять ин-формационные потребно-сти пользователей, формировать требования к информационной систе-ме.**	ИПК-1.1. Использует методику проведения обследования организации и выявления информационных потребностей пользователей ИПК-1.2. Анализирует деятельности предприятий, и выявляет участки производства, нуждающиеся в автоматизации ИПК-1.3. Осуществляет широкой общей подготовкой (базовыми знаниями) для решения практических задач в области информационных систем и технологий; теоретическими знаниями о роли компьютерных систем управления информационными потоками; типовыми разработанными средствами защиты информации и возможностями их использования в реальных задачах создания и внедрения информационных систем; навыками выбора класса ИС для автоматизации предприятия в соответствии с требованиями к ИС и ограничениями; способами автоматизации для конкретного предприятия; способами выбора ИС на основании преимуществ и недостатков существующих способов; расчета совокупной стоимости владения ИС; способами организации стратегического и оперативного планирования ИС.	Отчеты по практическим работам. Устный опрос. Презентация

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие безопасного WEB-приложения.
2. Цели и задачи проектирования безопасных WEB-приложений.
3. Принципы безопасного проектирования программных систем.
4. Архитектура WEB-приложений с точки зрения безопасности.
5. Модель угроз при проектировании WEB-приложений.
6. Учет требований безопасности на этапе проектирования.
7. Безопасность клиентской и серверной частей WEB-приложений.
8. Проектирование механизмов аутентификации пользователей.
9. Проектирование авторизации и разграничения доступа.
10. Управление сессиями при проектировании WEB-приложений.
11. Безопасная обработка пользовательского ввода.
12. Предотвращение SQL-инъекций на этапе проектирования.
13. Предотвращение XSS-уязвимостей на этапе проектирования.
14. Предотвращение CSRF-атак на уровне архитектуры.
15. Проектирование безопасной работы с файлами.
16. Защита данных при передаче и хранении.
17. Использование криптографических механизмов в WEB-приложениях.
18. Проектирование журналирования и аудита безопасности.

19. Безопасная обработка ошибок и исключений.
20. Учет безопасности сторонних библиотек и компонентов.
21. Проектирование защищённых API.
22. Безопасная конфигурация WEB-приложений.
23. Интеграция требований безопасности в жизненный цикл разработки.
24. Документирование требований безопасности WEB-приложений.
25. Современные подходы к проектированию безопасных WEB-приложений.

Критерии оценки выполнения самостоятельной работы.

В основу разработки балльно рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Студентам выставляются следующие баллы за выполнение задания к ПК:

- **оценка «отлично» (10 баллов):** контрольные тесты, а также самостоятельно выполненные семестровые задания, выполненные полностью и сданные в срок в соответствии с предъявляемыми требованиями;
- **оценка «хорошо» (8-9 баллов):** задание выполнено и в целом отвечает предъявляемым требованиям, но имеются отдельные замечания в его оформлении или сроке сдачи;
- **оценка «удовлетворительно» (6-7 баллов):** задание выполнено не до конца, отсутствуют ответы на отдельные вопросы, имеются отклонения в объеме, содержании, сроке выполнения;
- **оценка «неудовлетворительно» (5 и ниже):** отсутствует решение задачи, задание переписано (скачано) из других источников, не проявлена самостоятельность при его выполнении.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;
- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;
- выполнение контрольной работы и обсуждение результатов;
- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;
- написание и презентация доклада;
- написание самостоятельной (контрольной) работы.

Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен. Общее количество баллов по дисциплине - 100 баллов. Распределение баллов на текущий и промежуточный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

по дисциплине

«Проектирование безопасных WEB-приложений»:

1. Сущность и особенности проектирования безопасных WEB-приложений.
2. Принципы secure-by-design и defense-in-depth.
3. Учет информационной безопасности на этапе проектирования.
4. Архитектурные решения для повышения безопасности WEB-приложений.
5. Моделирование угроз WEB-приложений.
6. Проектирование системы аутентификации пользователей.
7. Проектирование механизмов авторизации и ролей.
8. Безопасное управление пользовательскими сессиями.
9. Проектирование защиты от SQL-инъекций.

10. Проектирование защиты от XSS-атак.
11. Проектирование защиты от CSRF-атак.
12. Валидация и фильтрация входных данных.
13. Проектирование безопасной загрузки и хранения файлов.
14. Защита конфиденциальных данных в WEB-приложениях.
15. Использование HTTPS и TLS на этапе проектирования.
16. Применение криптографических методов в WEB-приложениях.
17. Проектирование безопасных API и REST-сервисов.
18. Учет безопасности сторонних компонентов и библиотек.
19. Проектирование логирования и мониторинга безопасности.
20. Безопасная обработка ошибок и сообщений об ошибках.
21. Проектирование защиты от утечек информации.
22. Проектирование защиты от атак отказа в обслуживании.
23. Интеграция требований безопасности в Secure SDLC.
24. Оценка рисков на этапе проектирования WEB-приложений.
25. Роль проектирования в обеспечении безопасности WEB-приложений.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Понятие и цели проектирования безопасных WEB-приложений.
2. Принципы secure-by-design при разработке WEB-приложений.
3. Принцип defense-in-depth в архитектуре WEB-приложений.
4. Архитектура WEB-приложений и её влияние на безопасность.
5. Моделирование угроз на этапе проектирования WEB-приложений.
6. Учет требований информационной безопасности при проектировании.
7. Проектирование безопасной клиент-серверной архитектуры.
8. Проектирование механизмов аутентификации пользователей.
9. Проектирование авторизации и ролевой модели доступа.
10. Безопасное управление пользовательскими сессиями.
11. Проектирование защиты от SQL-инъекций.
12. Проектирование защиты от XSS-атак.
13. Проектирование защиты от CSRF-атак.
14. Валидация и фильтрация пользовательского ввода на уровне проектирования.
15. Проектирование безопасной обработки файлов.
16. Защита данных при хранении в WEB-приложениях.
17. Защита данных при передаче по сети.
18. Использование криптографических механизмов в WEB-приложениях.
19. Проектирование безопасного хранения учетных данных пользователей.
20. Проектирование журналирования и аудита безопасности.
21. Безопасная обработка ошибок и исключений.
22. Учет безопасности сторонних библиотек и компонентов.
23. Проектирование защищённых API и REST-сервисов.
24. Безопасная конфигурация WEB-приложений и серверной среды.
25. Проектирование защиты от утечки информации.
26. Проектирование защиты от атак отказа в обслуживании.
27. Интеграция требований безопасности в Secure SDLC.
28. Оценка рисков на этапе проектирования WEB-приложений.
29. Документирование требований безопасности WEB-приложений.
30. Роль этапа проектирования в обеспечении безопасности WEB-приложений.

БИЛЕТЫ

ДЛЯ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ЗНАНИЙ ПО ДИСЦИПЛИНЕ
(ДЛЯ ЗАЧЕТА – ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ)

МОУ ВО РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ
Факультет Естественнонаучный
Кафедра Информатики и ИТ
по «Проектирование безопасных WEB-приложений»
для 10.03.01 «Информационная безопасность»
профиль: Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности)
очная

Билет № 1

1. Информационная безопасность: сущность, цели и задачи.
2. Обеспечение информационной безопасности в государственных и корпоративных ИС.

Утверждено на заседании кафедры _
протокол № 4 от «16» Ноября 2026г.
Заведующий кафедрой/_____/ Лешукович А.И.

Итоговые оценки студентов

Буквенное обозначение итоговых оценок студентов и их цифровые эквиваленты:

Буквенная оценка	Цифра	Общий балл	Традиционная оценка
A	4	95<A<100	отлично
A-	3,67	90≤A-<95	
B+	3,33	85≤B+<90	хорошо
B	3	80≤B<85	
B-	2,67	75≤B-<80	
C+	2,33	70≤C+<75	удовлетворительно
C	2	65<C<70	
C-	1,67	60≤C-<65	
D+	1,33	55<D+<60	
D	1	50≤D<55	
Fx	0	45≤Fx<50	неудовлетворительно
F	0	0<F<45	

Критерии выведения итоговой оценки промежуточной аттестации:

«Отлично» - средняя оценка ≥ 3,67.
«Хорошо» - средняя оценка ≥ 2,67 и ≤ 3,33.
«Удовлетворительно» - средняя оценка ≥ 1,0 и ≤ 2,33.
«Неудовлетворительно» - средняя оценка < 0.