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
_____ Лешукович А.И.
«_1_» ___Сентября___2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине (модулю)

БЕЗОПАСНОСТЬ 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
БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
УК-2	**Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы ихрешения, 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.
ПК-2	**Способент разрабатывать и адаптиро-вать прикладное программное обеспечение**	**ИПК-2.1.** Применяет современные технологии разработки и адаптации прикладного программного обеспечения **ИПК-2.2.** Участвует в разработке на современных языках программирования и адаптации прикладного программного обеспечения **ИПК-2.3.** Применяет современные технологии для разработки веб-приложений	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

ПК-3	**Способен проектировать информационные системы по видам обеспечения**	**ИПК-3.1.** Применяет элементы технологий проектирования информационных систем; осуществляет и обосновывает выбор проектных решений по видам обеспечения информационных систем **ИПК-3.2.** Участвует в проектировании экономических информационных систем или их частей (модулей)	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие безопасности WEB-приложений.
2. Архитектура WEB-приложений и её влияние на безопасность.
3. Основные угрозы безопасности WEB-приложений.
4. Модель угроз для WEB-приложений.
5. Уязвимости аутентификации пользователей.
6. Уязвимости авторизации и управления доступом.
7. Управление сессиями в WEB-приложениях.
8. Риски небезопасной обработки пользовательского ввода.
9. SQL-инъекции и причины их возникновения.
10. Межсайтовый скриптинг (XSS).
11. Межсайтовая подделка запросов (CSRF).
12. Уязвимости при загрузке и обработке файлов.
13. Ошибки конфигурации WEB-приложений и серверов.
14. Угрозы утечки данных в WEB-приложениях.
15. Использование HTTPS и его роль в безопасности.
16. Безопасность хранения учетных данных пользователей.
17. Хэширование и защита паролей.
18. Уязвимости сторонних библиотек и компонентов.
19. Безопасность API WEB-приложений.
20. Атаки отказа в обслуживании (DoS/DDoS).
21. Логирование и аудит безопасности WEB-приложений.
22. Тестирование безопасности WEB-приложений.
23. Роль пентестинга в обеспечении WEB-безопасности.
24. Программные средства защиты WEB-приложений.
25. Современные тенденции безопасности 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

«БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ»:

1. Сущность и задачи безопасности WEB-приложений.
2. Классификация угроз безопасности WEB-приложений.
3. Угрозы, связанные с архитектурой WEB-приложений.
4. Аутентификация и типовые ошибки её реализации.
5. Авторизация и разграничение доступа в WEB-приложениях.
6. Управление пользовательскими сессиями и связанные угрозы.
7. SQL-инъекции: механизмы и последствия.
8. Методы защиты от SQL-инъекций.
9. XSS-атаки: виды и способы защиты.
10. CSRF-атаки и методы противодействия.
11. Проверка и валидация пользовательского ввода.
12. Безопасная обработка файлов в WEB-приложениях.
13. Ошибки конфигурации WEB-сервера и приложения.
14. Защита данных при передаче по сети.
15. Использование SSL/TLS в WEB-приложениях.
16. Защита учетных данных и паролей пользователей.
17. Уязвимости сторонних компонентов и управление зависимостями.
18. Безопасность API и REST-сервисов.
19. Атаки DoS/DDoS и их влияние на WEB-приложения.
20. WEB-Application Firewall и его функции.
21. Логирование и мониторинг событий безопасности.
22. Аудит безопасности WEB-приложений.
23. Управление инцидентами безопасности WEB-приложений.
24. Нормативные и стандартные требования к WEB-безопасности.
25. Роль специалиста по ИБ в обеспечении безопасности WEB-приложений.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Понятие безопасности WEB-приложений.
2. Основные угрозы безопасности WEB-приложений.
3. Место безопасности WEB-приложений в системе ИБ.
4. Архитектура WEB-приложений.
5. Клиентская и серверная части WEB-приложения.
6. Угрозы, связанные с архитектурой WEB-приложений.
7. Модель угроз WEB-приложений.
8. Источники атак на WEB-приложения.
9. Классификация атак на WEB-приложения.
10. Аутентификация в WEB-приложениях.
11. Авторизация и управление доступом.
12. Типовые ошибки аутентификации и авторизации.
13. Управление сессиями в WEB-приложениях.
14. Угрозы перехвата и фиксации сессий.
15. Методы защиты пользовательских сессий.
16. Уязвимость SQL-инъекций.
17. Причины возникновения SQL-инъекций.
18. Методы защиты от SQL-инъекций.
19. Межсайтовый скриптинг (XSS).
20. Виды XSS-атак.
21. Методы защиты от XSS.
22. Межсайтовая подделка запросов (CSRF).
23. Механизмы реализации CSRF-атак.
24. Способы защиты от CSRF.
25. Уязвимости управления вводом данных.
26. Проверка и фильтрация пользовательского ввода.
27. Роль валидации данных в безопасности WEB-приложений.
28. Угрозы, связанные с загрузкой файлов.
29. Опасности небезопасной обработки файлов.
30. Методы защиты при работе с файлами.
31. Ошибки конфигурации WEB-приложений.
32. Угрозы небезопасных настроек сервера.
33. Безопасная конфигурация WEB-среды.
34. Защита WEB-приложений от утечки данных.
35. Контроль доступа к данным.
36. Логирование и аудит безопасности WEB-приложений.
37. Использование HTTPS и SSL/TLS.
38. Угрозы при передаче данных по сети.
39. Защита канала передачи данных.
40. Уязвимости сторонних библиотек и компонентов.
41. Управление зависимостями в WEB-приложениях.
42. Риски использования устаревших компонентов.
43. Атаки типа DoS и DDoS на WEB-приложения.
44. Последствия отказа в обслуживании.
45. Методы защиты от DoS/DDoS-атак.
46. Безопасность API WEB-приложений.
47. Типовые уязвимости API.
48. Хранение и защита учетных данных пользователей.
49. Хэширование и соль паролей.
50. Ошибки при хранении паролей.
51. Атаки на стороне клиента.
52. Угрозы, связанные с JavaScript-кодом.

53. Защита клиентской части WEB-приложений.
54. Тестирование безопасности WEB-приложений.
55. Методы анализа уязвимостей.
56. Роль пентестинга в обеспечении безопасности.
57. Программные средства защиты WEB-приложений.
58. WEB-Application Firewall (WAF).
59. Интеграция WAF в систему ИБ.
60. Управление инцидентами безопасности WEB-приложений.
61. Реагирование на атаки и уязвимости.
62. Документирование инцидентов безопасности.
63. Безопасность WEB-приложений в облачной среде.
64. Особенности защиты SaaS-приложений.
65. Риски облачных WEB-решений.
66. Управление рисками безопасности WEB-приложений.
67. Оценка рисков WEB-уязвимостей.
68. Выбор мер защиты на основе анализа рисков.
69. Нормативно-правовые требования к безопасности WEB-приложений.
70. Стандарты и рекомендации по безопасности WEB.
71. Роль стандартов в обеспечении безопасности приложений.
72. Роль специалиста по ИБ в обеспечении безопасности WEB-приложений.
73. Безопасная разработка WEB-приложений (Secure SDLC).
74. Современные тенденции и перспективы 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 « Безопасность WEB-приложений»
для 10.03.01 «Информационная безопасность»
профиль: Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности)
очная

Билет № 1

1. Роль специалиста по ИБ в обеспечении безопасности WEB-приложений.
2. Безопасная разработка WEB-приложений (Secure SDLC).

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.