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
_____ Лещукович А.И.
«_1_» Сентября___2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине (модулю)

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

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
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
ОПК-2	**Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности**	ИОПК-2.1. Способен выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ИОПК-2.2. Применяет современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
ОПК-9	**Способен принимать участие в реализации профессиональных коммуникаций с заинтересованными участниками проектной деятельности и в рамках проектных групп**	ИОПК-9.1. Использует инструменты и методы коммуникаций в проектах; каналы коммуникаций в проектах; модели коммуникаций в проектах; технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии, технологии подготовки и проведения презентаций. ИОПК-9.2. Осуществляет взаимодействие с заказчиком в процессе реализации проекта; принимать участие в командообразовании и развитии персонала. ИОПК-9.3. Участвует в проведении презентаций, переговоров, публичных выступлений	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
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	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

		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	
ПК-2	**Способент разрабатывать и адаптиро-вать прикладное про-граммное обеспечение**	**ИПК-2.1.** Применяет совре-менные технологии разработки и адаптации прикладного про-граммного обеспечения **ИПК-2.2.** Участвует в разра-ботке на современных языках программирования и адапта-ции прикладного программно-го обеспечения **ИПК-2.3.** Применяет совре-менные технологии для разра-ботки веб-приложений	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие программно-аппаратных средств защиты информации.
2. Место программно-аппаратных средств в системе ИБ.
3. Классификация средств защиты информации.
4. Аппаратные средства защиты информации.
5. Программные средства защиты информации.

6. Программно-аппаратные комплексы защиты.
7. Средства идентификации и аутентификации.
8. Аппаратные средства контроля доступа.
9. Программные средства разграничения доступа.
10. Биометрические средства защиты информации.
11. Аппаратные криптографические средства.
12. Программные криптографические средства.
13. Средства защиты от несанкционированного доступа.
14. Средства антивирусной защиты.
15. Средства защиты сетевых соединений.
16. Межсетевые экраны как программно-аппаратные средства защиты.
17. Системы обнаружения и предотвращения вторжений.
18. Аппаратные средства защиты каналов связи.
19. Программные средства резервного копирования.
20. Аппаратные модули доверенной загрузки.
21. Защита информации на рабочих станциях.
22. Защита информации на серверах.
23. Эксплуатация программно-аппаратных средств защиты.
24. Оценка эффективности программно-аппаратных средств защиты.
25. Перспективы развития программно-аппаратных средств защиты информации.

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 промежу-

точный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

по дисциплине

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»:

1. Назначение программно-аппаратных средств защиты информации.
2. Классификация программно-аппаратных средств защиты.
3. Аппаратные средства защиты информации и их особенности.
4. Программные средства защиты информации.
5. Программно-аппаратные комплексы защиты информации.
6. Средства идентификации, аутентификации и авторизации.
7. Аппаратные ключи и токены безопасности.
8. Биометрические системы защиты информации.
9. Криптографические программно-аппаратные средства.
10. Аппаратные средства шифрования информации.
11. Программные средства шифрования данных.
12. Средства защиты от несанкционированного доступа.
13. Межсетевые экраны и их функции.
14. Программно-аппаратные системы обнаружения вторжений.
15. Средства защиты сетевых соединений.
16. Аппаратные средства защиты каналов передачи информации.
17. Защита информации в локальных сетях.
18. Защита информации в распределённых системах.
19. Средства антивирусной защиты информации.
20. Средства резервного копирования и восстановления данных.
21. Аппаратные средства доверенной загрузки.
22. Эксплуатация и администрирование средств защиты.
23. Сертификация программно-аппаратных средств защиты.
24. Оценка эффективности средств защиты информации.
25. Роль программно-аппаратных средств в комплексной системе ИБ.

. ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Понятие программно-аппаратных средств защиты информации.
2. Классификация средств защиты информации.
3. Аппаратные средства защиты информации.
4. Программные средства защиты информации.
5. Средства идентификации и аутентификации.
6. Аппаратные средства контроля доступа.
7. Программно-аппаратные комплексы защиты информации.
8. Средства разграничения доступа.
9. Управление правами пользователей.
10. Аппаратные криптографические средства защиты.
11. Программные криптографические средства защиты.
12. Шифрование информации.
13. Средства защиты от несанкционированного доступа.
14. Аппаратные ключи и токены безопасности.
15. Биометрические средства защиты информации.
16. Межсетевые экраны как программно-аппаратные средства защиты.
17. Защита сетевых соединений.
18. Фильтрация сетевого трафика.
19. Системы обнаружения вторжений.
20. Системы предотвращения вторжений.
21. Анализ сетевых атак.

22. Антивирусные программно-аппаратные средства защиты.
23. Защита от вредоносного программного обеспечения.
24. Обновление средств защиты информации.
25. Аппаратные модули доверенной загрузки.
26. Защита загрузочного процесса.
27. Контроль целостности программной среды.
28. Защита информации на рабочих станциях.
29. Программно-аппаратные средства защиты АРМ.
30. Эксплуатационные требования к средствам защиты.
31. Защита информации на серверах.
32. Программно-аппаратные средства серверной защиты.
33. Администрирование средств защиты информации.
34. Резервное копирование данных.
35. Аппаратные средства хранения резервных копий.
36. Восстановление информации после инцидентов.
37. Защита информации в локальных сетях.
38. Защита информации в распределённых системах.
39. Сетевые программно-аппаратные средства защиты.
40. Эксплуатация программно-аппаратных средств защиты.
41. Мониторинг и журналирование событий безопасности.
42. Анализ эффективности средств защиты.
43. Аппаратные средства защиты каналов передачи информации.
44. Криптографическая защита каналов связи.
45. Защита беспроводных соединений.
46. Биометрические системы идентификации пользователей.
47. Надёжность и ограничения биометрических методов.
48. Применение биометрии в системах ИБ.
49. Аппаратные средства контроля физического доступа.
50. Программные средства контроля доступа.
51. Интеграция средств контроля доступа.
52. Защита информации на автоматизированных рабочих местах.
53. Программно-аппаратные средства защиты АРМ.
54. Требования к защите пользовательских данных.
55. Комплексная система защиты информации.
56. Роль программно-аппаратных средств в КСЗИ.
57. Взаимодействие средств защиты в системе ИБ.
58. Критерии выбора программно-аппаратных средств защиты.
59. Оценка эффективности средств защиты информации.
60. Экономическая эффективность защиты информации.
61. информации в корпоративных информационных системах.
62. Программно-аппаратные средства корпоративной ИБ.
63. Администрирование корпоративных средств защиты.
64. Аппаратные средства защиты носителей информации.
65. Защита съёмных носителей данных.
66. Контроль доступа к носителям информации.
67. Программные средства защиты данных.
68. Защита файловых систем.
69. Контроль целостности данных.
70. Эксплуатация и сопровождение средств защиты информации.
71. Обновление и модернизация программно-аппаратных средств.
72. Анализ инцидентов информационной безопасности.
73. Современные программно-аппаратные средства защиты информации.
74. Тенденции и перспективы развития средств защиты.
75. Роль специалиста по ИБ в эксплуатации средств защиты.

БИЛЕТЫ

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

МОУ ВО РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Факультет Естественнонаучный

Кафедра Информатики и ИТ

по «Программно-аппаратные средства защиты информации»

для 10.03.01 «Информационная безопасность»

профиль: Безопасность компьютерных систем

(по отрасли или в сфере профессиональной деятельности)

очная

Билет № 1

1. Тенденции и перспективы развития средств защиты.
2. Роль специалиста по ИБ в эксплуатации средств защиты.

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.