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)
МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ 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
МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Код компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения	Вид оценочного знания
УК-1	**Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	ИУК-1.1 Анализирует задачу, выделяя ее базовые составляющие ИУК-1.2. Демонстрирует знание особенностей системного и критического мышления и готовность к нему ИУК-1.3. Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение ИУК-1.4. Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки	Отчеты по практическим работам. Устный опрос. Презентация
ОПК-2	**Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной дея-тельности**	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.	Отчеты по практическим работам. Устный опрос. Презентация
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 коммуни-каций в проектах; модели коммуникаций в проектах; технологии межличностной и группо-вой коммуникации в деловом взаимодействии, основы конфликтологии, технологии подго-товки 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	Отчеты по практическим работам. Устный опрос. Презентация

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	Отчеты по практическим работам. Устный опрос. Презентация

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие криптографической защиты информации.
2. Цели и задачи криптографии в системе ИБ.
3. История развития криптографических методов.
4. Основные термины и понятия криптографии.
5. Классификация криптографических методов.
6. Симметричные криптографические алгоритмы.
7. Асимметричные криптографические алгоритмы.
8. Криптографические хэш-функции.
9. Электронная цифровая подпись.
10. Управление криптографическими ключами.
11. Генерация и распределение ключей.
12. Хранение и защита ключевой информации.
13. Криптографические протоколы.
14. Криптография в сетевых технологиях.
15. Криптографическая защита каналов связи.
16. Программные средства криптографической защиты.
17. Аппаратные средства криптографической защиты.
18. Программно-аппаратные криптографические средства.
19. Сертификация и лицензирование средств криптографической защиты.
20. Нормативно-правовое обеспечение криптографической защиты.
21. Криптографические атаки и методы криптоанализа.
22. Стойкость криптографических алгоритмов.
23. Роль криптографии в защите персональных данных.
24. Применение криптографии в информационных системах.
25. Перспективы развития криптографических методов 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 промежуточный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

по дисциплине

«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»:

1. Определить вид криптографического алгоритма (симметричный или асимметричный) по заданному описанию.
2. Выбрать криптографический метод для защиты данных при хранении и обосновать выбор.
3. Выбрать криптографический метод для защиты данных при передаче.
4. Сравнить симметричное и асимметричное шифрование по заданным критериям.
5. Определить назначение хэш-функции в системе ИБ.
6. Проанализировать схему использования электронной цифровой подписи.
7. Определить этапы генерации и распределения ключей.
8. Выявить возможные угрозы компрометации ключевой информации.
9. Определить меры защиты ключей в информационной системе.
10. Проанализировать криптографический протокол обмена ключами.
11. Определить область применения симметричных алгоритмов.
12. Определить область применения асимметричных алгоритмов.
13. Оценить криптографическую стойкость алгоритма по заданным параметрам.
14. Проанализировать последствия использования слабых ключей.
15. Определить роль криптографии в защите сетевых соединений.
16. Выбрать средство криптографической защиты для корпоративной сети.
17. Проанализировать использование криптографии в электронной почте.

18. Определить функции криптографических модулей безопасности.
19. Проанализировать требования к сертификации средств криптозащиты.
20. Выявить возможные криптографические атаки в заданной ситуации.
21. Определить методы противодействия криптографическим атакам.
22. Проанализировать использование криптографии при защите персональных данных.
23. Выбрать криптографический метод для электронного документооборота.
24. Оценить эффективность применения криптографических средств в ИС.
25. Сформулировать выводы о целесообразности использования криптографической защиты в заданной системе.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Понятие криптографической защиты информации.
2. Цели и задачи криптографии в системе ИБ.
3. Основные термины и понятия криптографии.
4. История развития криптографических методов.
5. Классификация криптографических методов.
6. Роль криптографии в обеспечении информационной безопасности.
7. Симметричные криптографические алгоритмы.
8. Преимущества и недостатки симметричного шифрования.
9. Области применения симметричных алгоритмов.
10. Асимметричные криптографические алгоритмы.
11. Преимущества и недостатки асимметричного шифрования.
12. Области применения асимметричных алгоритмов.
13. Сравнение симметричных и асимметричных методов шифрования.
14. Гибридные криптографические схемы.
15. Использование гибридных схем в ИС.
16. Криптографические хэш-функции.
17. Назначение и свойства хэш-функций.
18. Применение хэш-функций в ИБ.
19. Электронная цифровая подпись.
20. Принципы формирования и проверки ЭЦП.
21. Области применения ЭЦП.
22. Управление криптографическими ключами.
23. Генерация криптографических ключей.
24. Распределение и хранение ключей.
25. Компрометация криптографических ключей.
26. Угрозы ключевой информации.
27. Методы защиты криптографических ключей.
28. Криптографические протоколы.
29. Протоколы обмена ключами.
30. Роль криптографических протоколов в ИБ.
31. Криптографическая защита каналов связи.
32. Использование криптографии в сетевых протоколах.
33. Защищённые сетевые соединения.
34. Программные средства криптографической защиты информации.
35. Аппаратные средства криптографической защиты информации.
36. Программно-аппаратные криптографические средства.
37. Криптографические модули безопасности.
38. Аппаратные криптографические устройства.
39. Области их применения.
40. Сертификация средств криптографической защиты.
41. Требования к криптографическим средствам.
42. Лицензирование в области криптографической 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 « Методы и средства криптографической защиты информации»
для 10.03.01 «Информационная безопасность»
профиль: Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности)
очная

Билет № 1

1. Программно-аппаратные криптографические средства.
2. Криптографические модули безопасности.

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.