

**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)

Защита информации от утечки по техническим каналам

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
«Защита информации от утечки по техническим каналам»**

Код компетенции	Содержание компетенции	Перечень планируемых результатов обучения по дисциплине (индикаторы достижения компетенций)	Виды оценочных средств
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	<p>ИУК-2.1. Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение.</p> <p>ИУК-2.2. Определяет ресурсное обеспечение для достижения поставленной цели;</p> <p>ИУК-2.3. Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</p> <p>ИУК-2.4. Выполняет задачи в рамках своей ответственности в соответствии с запланированными результатами, при необходимости корректирует способы решения задач</p>	Тестирование. Контроль самостоятельно работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
ПК-2	Способен разрабатывать и адаптировать прикладное программное обеспечение	<p>ИПК-2.1. Применяет современные технологии разработки и адаптации прикладного программного обеспечения</p> <p>ИПК-2.2. Участвует в разработке на современных языках программирования и адаптации прикладного программного обеспечения</p> <p>ИПК-2.3. Применяет современные технологии для разработки веб-приложений</p>	Тестирование. Контроль самостоятельно работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
ПК-3	Способен проектировать информационные системы по видам обеспечения	<p>ИПК-3.1. Применяет элементы технологий проектирования информационных систем; осуществляет и обосновывает выбор проектных решений по видам обеспечения информационных систем</p> <p>ИПК-3.2. Участвует в проектировании экономических информационных систем или</p>	Тестирование. Контроль самостоятельно работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ (рефератов, письменных работ)

1. Понятие утечки информации по техническим каналам.
2. Классификация технических каналов утечки информации.
3. Акустические каналы утечки информации.
4. Виброакустические каналы утечки информации.
5. Электромагнитные каналы утечки информации.
6. Паразитные электромагнитные излучения и наводки (ПЭМИН).
7. Оптические каналы утечки информации.
8. Радиоканалы утечки информации.
9. Технические средства разведки и перехвата информации.
10. Закладные устройства и их классификация.
11. Методы обнаружения технических каналов утечки.
12. Пассивные и активные методы защиты информации.
13. Экранирование как метод защиты информации.
14. Заземление и фильтрация в системах защиты информации.
15. Маскирующие помехи и их применение.
16. Организационные меры защиты от утечки информации.
17. Нормативно-правовое обеспечение защиты информации от утечки.
18. Аттестация объектов информатизации по требованиям безопасности.
19. Оценка эффективности мер защиты от утечки информации.
20. Роль специалиста по информационной безопасности в защите от технических каналов утечки.

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 кон-

трольных 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 **«Защита информации от утечки по техническим каналам»:**

1. Сущность и особенности утечки информации по техническим каналам.
2. Основные виды технических каналов утечки информации.
3. Акустические и виброакустические каналы утечки: источники и способы реализации.
4. Электромагнитные каналы утечки информации.
5. Паразитные электромагнитные излучения и наводки.
6. Радиоканалы утечки информации и их особенности.
7. Оптические каналы утечки информации.
8. Технические средства негласного получения информации.
9. Классификация закладных устройств.
10. Методы выявления и локализации технических каналов утечки.
11. Активные методы защиты информации от утечки.
12. Пассивные методы защиты информации от утечки.
13. Экранирование и его роль в системе защиты информации.
14. Фильтрация и заземление как меры защиты информации.
15. Применение генераторов помех для защиты информации.
16. Организационно-технические меры защиты информации.
17. Нормативные требования к защите информации от утечки.
18. Аттестация и контроль защищённости объектов информатизации.
19. Комплексная система защиты информации от утечки по техническим каналам.
20. Современные проблемы и перспективы развития защиты информации от технических каналов утечки.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Информационная безопасность: сущность, цели и задачи.
2. Информация как объект защиты. Виды защищаемой информации.
3. Угрозы информационной безопасности и их классификация.
4. Модель нарушителя информационной безопасности.
5. Уязвимости информационных систем и способы их минимизации.
6. Основные принципы обеспечения информационной безопасности.
7. Конфиденциальность, целостность и доступность информации.
8. Организационные методы защиты информации.
9. Политика информационной безопасности организации.
10. Роль персонала в обеспечении информационной безопасности.
11. Технические средства защиты информации.
12. Антивирусные средства защиты и их классификация.
13. Межсетевые экраны: назначение и виды.
14. Системы обнаружения вторжений.

15. Криптографические методы защиты информации.
16. Симметричное и асимметричное шифрование.
17. Электронная цифровая подпись и ее функции.
18. Защита информации в локальных и глобальных сетях.
19. Обеспечение информационной безопасности в государственных и корпоративных ИС.
20. Современные проблемы и тенденции развития информационной безопасности.

БИЛЕТЫ

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

МОУ ВО РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Факультет Естественнонаучный

Кафедра Информатики и ИТ

по «Защита информации от утечки по техническим каналам»

для 10.03.01 «Информационная безопасность»

профиль: Безопасность компьютерных систем

(по отрасли или в сфере профессиональной деятельности)

очная

Билет № 1

1. Конфиденциальность, целостность и доступность информации.
2. Организационные методы защиты информации.

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	$95 \leq A \leq 100$	отлично
A-	3,67	$90 \leq A < 95$	
B+	3,33	$85 \leq B < 90$	хорошо
B	3	$80 \leq B < 85$	
B-	2,67	$75 \leq B < 80$	
C+	2,33	$70 \leq C < 75$	удовлетворительно
C	2	$65 \leq C < 70$	
C-	1,67	$60 \leq C < 65$	
D+	1,33	$55 \leq D < 60$	
D	1	$50 \leq D < 55$	
Fx	0	$45 \leq Fx < 50$	неудовлетворительно
F	0	$0 < F < 45$	

Критерии выведения итоговой оценки промежуточной аттестации:

«Отлично» - средняя оценка $\geq 3,67$.

«Хорошо» - средняя оценка $\geq 2,67$ и $\leq 3,33$.

«Удовлетворительно» - средняя оценка $\geq 1,0$ и $\leq 2,33$.

«Неудовлетворительно» - средняя оценка < 0 .