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)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 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.
ОПК-5	**Способен инсталлировать программное и аппаратное обеспечение для информа-ционных и автоматизированных систем**	ИОПК-5.1. Применяет основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем. ИОПК-5.2. Выполняет параметрическую настройку информационных и автоматизирован-ных систем ИОПК-5.3. Выполняет инсталляцию программного и аппаратного обеспечения информаци-онных и автоматизированных систем.	Отчеты по практическим работам. Устный опрос. Презентация
ОПК-6	**Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования**	ИОПК-6.1. Использует основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования. ИОПК-6.2. Применяет методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий. ИОПК-6.3. Проводит инженерные расчеты	Отчеты по практическим работам. Устный опрос. Презентация

		основных показателей результативности создания и применения информационных систем и технологий.	
ОПК-1	**Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального иссле-дования в профессиональной деятельности**	ИОПК-1.1. Применяет основы математики, физики, вычислительной техники и программи-рования в профессиональной деятельности. ИОПК-1.2. Решает стандартные профессиональные задачи с применением естественнонауч-ных и общеинженерных знаний, методов математического анализа и моделирования. ИОПК-1.3. Использует методы теоретического и экспериментального исследования объек-тов профессиональной деятельности.	Отчеты по практическим работам. Устный опрос. Презентация

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие и цели информационной безопасности.
2. Информация как объект защиты.
3. Основные принципы обеспечения ИБ.
4. Классификация угроз информационной безопасности.
5. Внутренние и внешние источники угроз.
6. Роль персонала в системе ИБ.
7. Конфиденциальность, целостность и доступность информации.
8. Понятие уязвимости информационных систем.
9. Методы минимизации уязвимостей.
10. Модель нарушителя информационной безопасности.
11. Объекты и субъекты защиты информации.
12. Организационные меры обеспечения ИБ.
13. Политика информационной безопасности организации.
14. Структура и содержание политики ИБ.
15. Ответственность за нарушение требований ИБ.
16. Технические средства защиты информации.
17. Классификация средств защиты информации.
18. Комплексный подход к обеспечению ИБ.
19. Антивирусные средства защиты информации.
20. Типы вредоносного программного обеспечения.
21. Методы противодействия вредоносным программам.
22. Межсетевые экраны: назначение и функции.
23. Классификация межсетевых экранов.
24. Защита информации в компьютерных сетях.
25. Системы обнаружения и предотвращения вторжений.
26. Основные типы атак на информационные системы.
27. Реагирование на инциденты ИБ.
28. Криптографические методы защиты информации.

29. Симметричное шифрование и его особенности.
30. Асимметричное шифрование и его применение.
31. Электронная цифровая подпись и ее функции.
32. Хэш-функции и контроль целостности данных.
33. Управление ключевой информацией.
34. Контроль и управление доступом к информации.
35. Аутентификация и авторизация пользователей.
36. Идентификация в информационных системах.
37. Защита информации в корпоративных ИС.
38. Информационная безопасность бизнес-процессов.
39. Риски информационной безопасности.
40. Защита информации в государственных ИС.
41. Требования к обеспечению ИБ в организациях.
42. Аудит информационной безопасности.
43. Информационная безопасность в условиях цифровой экономики.
44. Современные угрозы ИБ.
45. Перспективы развития систем защиты информации.
46. Социальная инженерия как угроза ИБ.
47. Методы противодействия социальной инженерии.
48. Обучение персонала вопросам ИБ.
49. Инциденты информационной безопасности и их классификация.
50. Порядок реагирования на инциденты ИБ.
51. Документирование инцидентов.
52. Защита персональных данных.
53. Угрозы утечки персональной информации.
54. Меры обеспечения безопасности персональных данных.
55. Информационная безопасность в облачных технологиях.
56. Риски использования облачных сервисов.
57. Механизмы защиты данных в облаке.
58. Комплексная система обеспечения информационной безопасности.
59. Взаимосвязь организационных и технических мер защиты.
60. Роль ИБ в устойчивом развитии организации.

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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»:

1. Понятие информационной безопасности и ее роль в деятельности организации.
2. Основные цели и задачи обеспечения информационной безопасности.
3. Классификация информации по уровню доступа.
4. Виды угроз информационной безопасности и их характеристика.
5. Источники внутренних и внешних угроз информации.
6. Понятие уязвимости информационных систем.
7. Объекты и субъекты защиты информации.
8. Принципы обеспечения информационной безопасности.
9. Модель «конфиденциальность – целостность – доступность».
10. Организационные меры защиты информации.
11. Политика информационной безопасности: структура и назначение.
12. Ответственность персонала за нарушение требований ИБ.
13. Технические средства защиты информации.
14. Антивирусная защита и ее функции.
15. Межсетевые экраны и их назначение.
16. Системы обнаружения и предотвращения вторжений.
17. Основы криптографической защиты информации.
18. Электронная цифровая подпись и области ее применения.
19. Информационная безопасность в корпоративных информационных системах.
20. Роль информационной безопасности в условиях цифровой экономики.

САМОСТОЯТЕЛЬНЫЕ ЗАДАНИЯ

Задание 1 Разработать электронную форму документа «Журнал учёта инцидентов информационной безопасности» (дата, тип инцидента, объект защиты, описание, уровень критичности, ответственный, статус).

Задание 2 Разработать электронную форму документа «Справочник угроз информационной безопасности» (наименование угрозы, источник, тип угрозы, возможные последствия, уровень риска).

Задание 3 Разработать электронную форму документа «Акт регистрации нарушения требований информационной безопасности» (дата, подразделение, сотрудник, описание нарушения, принятые меры, ответственное лицо).

Задание 4 По разработанным электронным формам документов спроектировать базу данных обеспечения информационной безопасности организации и реализовать её на ПЭВМ с использованием языка SQL (создание таблиц, ограничений целостности, связей).

Задание 5 Для разработанной базы данных сформировать SQL-запросы, обеспечивающие: выборку инцидентов за период, анализ инцидентов по типам угроз, отчёт по подразделениям, выявление наиболее критичных угроз поиск нарушений по сотруднику.

Задание 6 Для разработанной базы данных определить функциональные зависимости между атрибутами основных таблиц (инциденты, угрозы, сотрудники, подразделения).

Задание 7 Для разработанной базы данных определить потенциальные ключи и выбрать из них первичные и внешние ключи, обосновав их использование с точки зрения обеспечения целостности и безопасности данных.

Задание 8 Выполнить нормализацию базы данных (до 3-й нормальной формы), обосновав устранение избыточности и повышение надёжности хранения данных информационной безопасности.

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 «Основы информационной безопасности»

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.