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 УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
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 УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

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	Отчеты по практическим работам. Устный опрос. Презентация
УК-3	**Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде**	**ИУК-3.1**. Определяет свою роль в социальном взаимодействии и командной работе, исходя из знания социологии и социальной психологии, методов развития личности этических норм профессионального взаимодействия с коллективом **ИУК-3.2.** При реализации своей роли в социальном взаимодействии и командной работе учитывает особенности поведения и интересы других участников **ИУК-3.3.** Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает статусные позиции других членов команды для достижения поставленной цели **ИУК-3.4.** Соблюдает нормы и установленные правила внутригруппового взаимодействия; несет личную ответственность за результат	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	Отчеты по практическим работам. Устный опрос. Презентация

		развитии персонала. ИОПК-9.3. Участвует в проведении презентаций, переговоров, публичных выступлений	
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 естественно-науч-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
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)	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 УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»:

1. Понятие управления информационной безопасностью.
2. Цели и задачи управления информационной безопасностью.
3. Место управления ИБ в системе управления организацией.
4. Объекты управления информационной безопасностью.
5. Субъекты управления информационной безопасностью.
6. Политика информационной безопасности и её назначение.
7. Структура политики информационной безопасности.
8. Организационная структура управления ИБ.
9. Роль руководства в обеспечении информационной безопасности.
10. Ответственность персонала в системе управления ИБ.
11. Управление рисками как элемент управления ИБ.
12. Планирование мероприятий по обеспечению ИБ.
13. Документирование процессов управления ИБ.
14. Контроль выполнения требований информационной безопасности.
15. Мониторинг состояния информационной безопасности.
16. Управление инцидентами информационной безопасности.
17. Аудит информационной безопасности.
18. Оценка эффективности системы управления ИБ.
19. Нормативно-правовая база управления ИБ.
20. Стандарты в области управления информационной безопасностью.

21. Интеграция управления ИБ в бизнес-процессы.
22. Обучение и повышение осведомлённости персонала по ИБ.
23. Управление изменениями с точки зрения ИБ.
24. Непрерывное совершенствование системы управления ИБ.
25. Роль специалиста по ИБ в системе управления информационной безопасностью.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Сущность и содержание управления информационной безопасностью.
2. Цели и принципы управления информационной безопасностью.
3. Система управления информационной безопасностью (СУИБ).
4. Политика информационной безопасности: назначение и структура.
5. Организационные основы управления информационной безопасностью.
6. Роль высшего руководства в управлении ИБ.
7. Полномочия и ответственность участников управления ИБ.
8. Управление рисками в системе управления ИБ.
9. Планирование и реализация мер обеспечения ИБ.
10. Документирование системы управления ИБ.
11. Контроль соблюдения требований информационной безопасности.
12. Мониторинг и анализ состояния ИБ.
13. Управление инцидентами информационной безопасности.
14. Аудит системы управления информационной безопасности.
15. Оценка эффективности системы управления ИБ.
16. Нормативно-правовое обеспечение управления ИБ.
17. Международные и национальные стандарты управления ИБ.
18. Взаимосвязь управления ИБ и корпоративного управления.
19. Информационная безопасность как элемент устойчивого развития организации.
20. Обучение персонала и формирование культуры ИБ.
21. Управление изменениями в информационных системах с учётом ИБ.
22. Реагирование на нарушения требований ИБ.
23. Непрерывное улучшение системы управления ИБ.
24. Современные проблемы управления информационной безопасностью.
25. Перспективы развития систем управления информационной безопасностью.

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 управления информационной безопасностью »
для 10.03.01 «Информационная безопасность»
профиль: Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности)
очная

Билет № 1

1. Современные проблемы управления информационной безопасностью.
2. Перспективы развития систем управления информационной безопасностью.

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.