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)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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
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 автоматизированн-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 основных показателей результативности со-	Отчеты по практическим работам. Устный опрос. Презентация

		здания и применения информационных систем и технологий.	
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-1	**Способен проводить обследование организаций, выявлять ин-формационные потребно-сти пользователей, формировать требования к информационной системе.**	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 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 и оперативного планирования ИС.	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)	практическим работам. Устный опрос. Презентация

ТЕМЫ ПИСЬМЕННЫХ РАБОТ
(рефератов, эссе, докладов)

1. Понятие риска информационной безопасности.
2. Место управления рисками в системе обеспечения ИБ.
3. Объекты управления рисками ИБ.
4. Источники рисков информационной безопасности.
5. Классификация рисков ИБ.
6. Угрозы как фактор формирования риска.
7. Уязвимости информационных систем.
8. Вероятность реализации угрозы.
9. Ущерб и его виды в оценке рисков ИБ.
10. Качественная оценка рисков ИБ.
11. Количественная оценка рисков ИБ.
12. Этапы процесса управления рисками ИБ.
13. Идентификация рисков информационной безопасности.
14. Анализ рисков ИБ.
15. Оценка уровня риска.
16. Критерии приемлемости рисков.
17. Документирование рисков информационной безопасности.
18. Реестр рисков и его назначение.
19. Роль персонала в управлении рисками ИБ.
20. Организационные меры снижения рисков.
21. Технические меры снижения рисков.
22. Экономические аспекты управления рисками ИБ.
23. Взаимосвязь управления рисками и политики ИБ.
24. Мониторинг рисков информационной безопасности.
25. Значение управления рисками для устойчивости ИС.

Тестовые задания
«Информационная безопасность»

@1. Информационная безопасность — это
$A) защита программного обеспечения;
$B) защита аппаратных средств;
$C) состояние защищённости информации от угроз;
$D) защита компьютерных сетей;
$E) защита баз данных;
@2. Основными целями информационной безопасности являются
$A) скорость обработки данных;
$B) удобство пользователей;

$C) конфиденциальность, целостность и доступность информации;
$D) снижение затрат;
$E) автоматизация процессов;
@3. К объектам защиты информационной безопасности относится
$A) монитор;
$B) клавиатура;
$C) информация и информационные ресурсы;
$D) принтер;
$E) источник питания;
@4. Конфиденциальность информации означает
$A) сохранность данных;
$B) защиту от искажения;
$C) защиту от несанкционированного доступа;
$D) постоянную доступность;
$E) резервное копирование;
@5. Целостность информации — это
$A) защита от утечки;
$B) защита от уничтожения;
$C) защита от несанкционированного изменения;
$D) защита каналов связи;
$E) защита оборудования;
@6. Доступность информации означает
$A) возможность её удаления;
$B) возможность копирования;
$C) возможность получения информации уполномоченными пользователями;
$D) шифрование данных;
$E) архивирование информации;
@7. Угроза информационной безопасности — это
$A) сбой оборудования;
$B) потенциальная возможность нарушения ИБ;
$C) антивирусная программа;
$D) резервная копия;
$E) средство защиты;
@8. К внутренним угрозам относится
$A) хакерская атака;
$B) вредоносное ПО;
$C) ошибки персонала;
$D) сетевые черви;
$E) фишинг;
@9. Уязвимость информационной системы — это
$A) угроза;
$B) средство защиты;
$C) слабое место, используемое угрозой;
$D) метод защиты;
$E) инцидент ИБ;
@10. Основной организационный документ в сфере ИБ — это
$A) инструкция пользователя;
$B) политика информационной безопасности;
$C) технический паспорт;
$D) регламент резервного копирования;
$E) сетевой протокол;
@11. К техническим мерам защиты информации относится
$A) обучение персонала;
$B) издание приказов;

$C) использование межсетевых экранов;
$D) распределение обязанностей;
$E) контроль доступа по должности;
@12. Идентификация пользователя — это
$A) проверка прав доступа;
$B) установление личности пользователя;
$C) регистрация инцидента;
$D) блокировка доступа;
$E) шифрование данных;
@13. Аутентификация — это
$A) определение имени пользователя;
$B) проверка подлинности пользователя;
$C) назначение прав доступа;
$D) регистрация событий;
$E) контроль сетевого трафика;
@14. Авторизация означает
$A) ввод пароля;
$B) подтверждение личности;
$C) предоставление прав доступа;
$D) шифрование данных;
$E) резервное копирование;
@15. К программным средствам защиты информации относится
$A) биометрический сканер;
$B) аппаратный ключ;
$C) антивирусное программное обеспечение;
$D) контроллер доступа;
$E) источник бесперебойного питания;
@16. К аппаратным средствам защиты информации относится
$A) операционная система;
$B) межсетевой экран;
$C) аппаратный криптографический модуль;
$D) антивирус;
$E) система резервного копирования;
@17. Инцидент информационной безопасности — это
$A) установка ПО;
$B) событие, нарушающее требования ИБ;
$C) обновление системы;
$D) резервное копирование;
$E) аудит безопасности;
@18. Антивирусная защита предназначена для
$A) защиты каналов связи;
$B) защиты от несанкционированного доступа;
$C) обнаружения и устранения вредоносного ПО;
$D) резервного копирования;
$E) управления доступом;
@19. Криптографическая защита информации используется для
$A) хранения данных;
$B) защиты оборудования;
$C) защиты информации при хранении и передаче;
$D) управления пользователями;
$E) анализа рисков;
@20. Межсетевой экран предназначен для
$A) хранения данных;
$B) анализа угроз;

$C) фильтрации сетевого трафика;
$D) резервного копирования;
$E) мониторинга пользователей;
@21. Управление рисками ИБ включает
$A) только идентификацию угроз;
$B) только выбор средств защиты;
$C) идентификацию, анализ и обработку рисков;
$D) шифрование информации;
$E) аудит безопасности;
@22. Социальная инженерия основана на
$A) технических уязвимостях;
$B) программных ошибках;
$C) психологическом воздействии на людей;
$D) сбоях оборудования;
$E) сетевых атаках;
@23. Резервное копирование используется для
$A) защиты от утечки;
$B) защиты от изменения;
$C) восстановления данных после потерь;
$D) контроля доступа;
$E) анализа рисков;
@24. Аудит информационной безопасности предназначен для
$A) обучения персонала;
$B) оценки эффективности мер защиты;
$C) шифрования информации;
$D) администрирования сети;
$E) резервного копирования;
@25. Основная задача специалиста по информационной безопасности —
$A) разработка программ;
$B) обслуживание техники;
$C) обеспечение защиты информации и ИС;
$D) администрирование БД;
$E) разработка интерфейсов;
$B) защиты оборудования;
$C) защиты информации при хранении и передаче;
$D) управления пользователями;
$E) анализа рисков;
@20. Межсетевой экран предназначен для
$A) хранения данных;
$B) анализа угроз;
$C) фильтрации сетевого трафика;
$D) резервного копирования;
$E) мониторинга пользователей;
@21. Управление рисками ИБ включает
$A) только идентификацию угроз;
$B) только выбор средств защиты;
$C) идентификацию, анализ и обработку рисков;
$D) шифрование информации;
$E) аудит безопасности;
@22. Социальная инженерия основана на
$A) технических уязвимостях;
$B) программных ошибках;
$C) психологическом воздействии на людей;

$D) сбоях оборудования;
$E) сетевых атаках;
@23. Резервное копирование используется для
$A) защиты от утечки;
$B) защиты от изменения;
$C) восстановления данных после потерь;
$D) контроля доступа;
$E) анализа рисков;
@24. Аудит информационной безопасности предназначен для
$A) обучения персонала;
$B) оценки эффективности мер защиты;
$C) шифрования информации;
$D) администрирования сети;
$E) резервного копирования;
@25. Основная задача специалиста по информационной безопасности —
$A) разработка программ;
$B) обслуживание техники;
$C) обеспечение защиты информации и ИС;
$D) администрирование БД;
$E) разработка интерфейсов;

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

«УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»:

1. Сущность и цели управления рисками информационной безопасности.
2. Понятие риска ИБ и его основные характеристики.
3. Модель управления рисками в системе ИБ организации.
4. Классификация рисков информационной безопасности.
5. Взаимосвязь угроз, уязвимостей и рисков.
6. Источники угроз информационной безопасности.
7. Методы идентификации рисков ИБ.
8. Качественные методы анализа рисков.
9. Количественные методы анализа рисков.
10. Оценка вероятности и ущерба при анализе рисков.
11. Критерии оценки и ранжирования рисков ИБ.
12. Понятие приемлемого риска.
13. Методы обработки рисков информационной безопасности.
14. Снижение риска как метод управления.
15. Передача риска и её особенности.
16. Принятие риска и условия его допустимости.
17. Избежание риска в системе ИБ.
18. Выбор мер защиты на основе оценки рисков.
19. План обработки рисков информационной безопасности.
20. Контроль эффективности мер управления рисками.
21. Мониторинг и пересмотр рисков ИБ.
22. Документирование процесса управления рисками.
23. Стандарты и подходы к управлению рисками ИБ.
24. Роль управления рисками в системе ИБ организации.
25. Современные проблемы и перспективы управления рисками ИБ.
26. 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.