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
_____Пешукович А.И.
«_1_» _Сентября___2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине (модулю)
ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ
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 В ОПЕРАЦИОННЫХ СИСТЕМАХ

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**	**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.
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	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.
ПК-3	**Способен проекти-ровать 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	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная работа. Устный опрос.

		их частей (модулей)	

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
«ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ»
(рефератов, письменных работ)

1. Администрирование информационных систем: цели, задачи и место в управлении ИС.
2. Роль системного администратора в современной организации.
3. Архитектура информационной системы и её влияние на процессы администрирования.
4. Управление пользователями и правами доступа в информационных системах.
5. Администрирование серверных и клиентских компонентов информационных систем.
6. Резервное копирование данных и восстановление работоспособности ИС.
7. Обеспечение отказоустойчивости и надёжности информационных систем.
8. Мониторинг и сопровождение информационных систем.
9. Информационная безопасность в процессе администрирования ИС.
10. Защита данных и контроль доступа в корпоративных информационных системах.
11. Администрирование сетевой инфраструктуры информационных систем.
12. Управление обновлениями и сопровождение программного обеспечения.
13. Администрирование информационных систем в условиях удалённого доступа.
14. Виртуализация и облачные технологии в администрировании ИС.
15. Документирование процессов администрирования информационных систем.
16. Типовые ошибки администрирования ИС и их последствия.
17. Роль администрирования ИС в обеспечении устойчивости бизнеса.
18. Современные тенденции развития администрирования информационных систем

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 ПО ДИСЦИПЛИНЕ «ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ»

1. Понятие защиты информации в операционных системах.
2. Операционная система как объект защиты.
3. Основные угрозы безопасности операционных систем.
4. Классификация уязвимостей операционных систем.
5. Модель безопасности операционной системы.
6. Идентификация пользователей в ОС.
7. Аутентификация пользователей в ОС.
8. Авторизация и разграничение прав доступа.
9. Управление учетными записями пользователей.
10. Механизмы защиты файловых систем.
11. Права доступа к файлам и каталогам.
12. Защита памяти в операционных системах.
13. Изоляция процессов как механизм защиты.
14. Защита ядра операционной системы.
15. Контроль целостности системных файлов.
16. Журналирование и аудит событий безопасности в ОС.
17. Защита операционных систем от вредоносного ПО.
18. Обновление и патч-менеджмент как мера защиты ОС.
19. Роль пользователя и администратора в обеспечении безопасности ОС.
20. Современные тенденции развития защиты операционных систем.

САМОСТОЯТЕЛЬНЫЕ ЗАДАНИЯ

Задание 1. Разработать электронную форму документа (накладная на материалы) для предприятия.
Задание 2. Разработать электронную форму документа (справочник материалов) для предприятия.
Задание 3. Разработать электронную форму документа (приходный ордер на материалы) для предприятия.
Задание 4. По электронным формам документов разработать базу данных и реализовать её на ПЭВМ с помощью языка программирования SQL.
Задание 5. Для разработанной базы данных сформировать запросы на языке запросов SQL.
Задание 6. Для разработанной базы данных определить все функциональные зависимости.
Задание 7. Для разработанной базы данных определить потенциальные ключи и из них выбрать первичные и внешние ключи.
Задание 8. Нормализовать разработанную базу данных.

Контрольные тестовые вопросы ПО ДИСЦИПЛИНЕ ПО ДИСЦИПЛИНЕ «ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ»

@1. Защита в операционных системах направлена на
$A) повышение производительности;
$B) оптимизацию ресурсов;
$C) обеспечение конфиденциальности, целостности и доступности;
$D) модернизацию оборудования;
$E) удобство интерфейса;
@2. Операционная система как объект защиты включает
$A) только аппаратные средства;

$B) только программное обеспечение;
$C) ядро, службы и пользовательскую среду;
$D) только прикладные программы;
$E) сетевое оборудование;
@3. К основным угрозам безопасности ОС относится
$A) резервное копирование;
$B) плановое обновление;
$C) несанкционированный доступ;
$D) аудит безопасности;
$E) журналирование;
@4. Идентификация пользователя — это
$A) проверка подлинности;
$B) назначение прав доступа;
$C) установление личности по идентификатору;
$D) блокировка учетной записи;
$E) регистрация событий;
@5. Аутентификация означает
$A) ввод логина;
$B) проверку подлинности пользователя;
$C) выдачу прав доступа;
$D) шифрование данных;
$E) резервное копирование;
@6. Авторизация — это
$A) подтверждение личности;
$B) предоставление прав доступа;
$C) регистрация пользователя;
$D) ввод пароля;
$E) контроль целостности;
@7. Разграничение доступа в ОС предназначено для
$A) ускорения работы;
$B) защиты оборудования;
$C) ограничения прав пользователей;
$D) резервного копирования;
$E) мониторинга сети;
@8. Защита файловой системы обеспечивает
$A) резервное копирование;
$B) контроль доступа к файлам и каталогам;
$C) ускорение ввода-вывода;
$D) шифрование каналов связи;
$E) мониторинг процессов;
@9. Изоляция процессов используется для
$A) повышения производительности;
$B) предотвращения влияния процессов друг на друга;
$C) резервного копирования;
$D) шифрования данных;
$E) управления пользователями;
@10. Защита памяти в ОС предназначена для
$A) увеличения объема ОЗУ;
$B) предотвращения несанкционированного доступа к памяти;
$C) ускорения работы приложений;
$D) резервного копирования данных;
$E) управления файлами;
@11. Контроль целостности системных файлов позволяет
$A) ускорить загрузку ОС;

$B) обнаружить несанкционированные изменения;
$C) увеличить объем памяти;
$D) улучшить интерфейс;
$E) управлять пользователями;
@12. Журналирование событий безопасности используется для
$A) резервного копирования;
$B) анализа инцидентов безопасности;
$C) ускорения работы системы;
$D) шифрования данных;
$E) управления памятью;
@13. К средствам защиты ОС относится
$A) текстовый редактор;
$B) антивирусное программное обеспечение;
$C) офисный пакет;
$D) графический редактор;
$E) медиаплеер;
@14. Обновление операционной системы необходимо для
$A) изменения интерфейса;
$B) устранения уязвимостей безопасности;
$C) увеличения объема памяти;
$D) установки приложений;
$E) резервного копирования;
@15. Патч-менеджмент — это
$A) управление пользователями;
$B) процесс установки обновлений безопасности;
$C) резервное копирование данных;
$D) мониторинг сети;
$E) контроль доступа;
@16. Привилегированный режим работы ОС предназначен для
$A) выполнения пользовательских программ;
$B) работы ядра и системных процессов;
$C) запуска офисных приложений;
$D) управления файлами пользователя;
$E) просмотра мультимедиа;
@17. Защита ядра ОС необходима для
$A) ускорения загрузки;
$B) предотвращения компрометации системы;
$C) удобства пользователей;
$D) резервного копирования;
$E) управления интерфейсом;
@18. Антивирусная защита ОС направлена на
$A) защиту от аппаратных сбоев;
$B) обнаружение и удаление вредоносного ПО;
$C) контроль сетевого трафика;
$D) резервное копирование;
$E) управление доступом;
@19. Администратор ОС отвечает за
$A) только работу приложений;
$B) настройку и контроль параметров безопасности;
$C) ввод данных;
$D) разработку программ;
$E) тестирование интерфейса;
@20. Основная цель защиты в операционных системах —
$A) повышение скорости работы;

$B) снижение энергопотребления;
$C) обеспечение безопасного функционирования ОС и данных;
$D) модернизация оборудования;
$E) улучшение дизайна интерфейса.

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.