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 СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

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
по дисциплине (модулю)
«ЗАЩИТА СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

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 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.
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	Тестирование. Контроль самостоятельной работы. Отчеты по практическим работам. Контрольная

		информационных систем или их частей (модулей)	работа. Устный опрос.

ТЕМЫ ПИСЬМЕННЫХ РАБОТ
(рефератов, эссе, докладов)

1. Понятие защиты сетевых информационных технологий.
2. Сетевые информационные технологии как объект защиты.
3. Основные угрозы безопасности в сетевых ИТ.
4. Классификация сетевых угроз и атак.
5. Архитектура компьютерных сетей и её влияние на безопасность.
6. Угрозы безопасности на различных уровнях модели OSI.
7. Защита сетевого уровня передачи данных.
8. Протоколы сетевой безопасности и их назначение.
9. Аутентификация и авторизация в сетевых информационных системах.
10. Разграничение доступа в сетях.
11. Межсетевые экраны и их роль в защите сетей.
12. Фильтрация сетевого трафика.
13. Системы обнаружения вторжений (IDS).
14. Системы предотвращения вторжений (IPS).
15. Криптографическая защита сетевых соединений.
16. Использование VPN для защиты сетевых ИТ.
17. Защита беспроводных сетей.
18. Угрозы безопасности беспроводных сетей и методы защиты.
19. Защита сетевых сервисов и серверов.
20. Атаки типа DoS и DDoS и способы противодействия.
21. Защита сетей от вредоносного программного обеспечения.
22. Мониторинг и анализ сетевого трафика.
23. Логирование и аудит событий сетевой безопасности.
24. Управление инцидентами сетевой безопасности.
25. Управление рисками в сетевых информационных технологиях.
26. Защита сетей корпоративных информационных систем.
27. Нормативно-правовые требования к защите сетевых ИТ.
28. Стандарты и рекомендации по сетевой безопасности.
29. Интеграция защиты сетевых ИТ в систему ИБ организации.
30. Современные тенденции и перспективы защиты сетевых информационных технологий.

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

«ЗАЩИТА СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»:

1. Типы информационных систем и их характеристика.
2. Цели и основные обязанности администратора информационных систем.
3. Базовые архитектуры, используемые при построении корпоративных информационных сетей.
4. Функциональные области управления, относящиеся к системному администрированию.
5. Компьютерная сеть, характеристики и области применения сетей.
6. Классификации локальных сетей.
7. Активное и пассивное сетевое оборудование.
8. Топология сетей: шина, кольцо, звезда.
9. Кабельные среды для передачи данных по сети.
10. Пакеты и протоколы.
11. Технология хранения данных.
12. Управление дисками и томами.
13. Реализация RAID.
14. Установка Windows Server.
15. Управление службами Windows Server.
16. Управление периферийными и другими устройствами.
17. Обзор технологий виртуализации.
18. Реализация роли Hyper-V.
19. Модель OSI, стек OSI.
20. Модель TCP/IP, обзор основных протоколов.
21. Утилиты диагностики TCP/IP.
22. Адресация в TCP/IP-сетях. Типы адресов стека TCP/IP.
23. Структура IP-адреса. Классы IP-адресов. Особые IP-адреса.
24. Протоколы IPv6 и ARP.
25. Создание таблиц маршрутизации, протоколы маршрутизации RIP и OSPF.
26. Система доменных имен. Служба DNS.
27. Реализация DHCP в Windows. Параметры DHCP.
28. DHCP-сообщения. Принцип работы DHCP.
29. Реализация доменных служб Active Directory.
30. Управление пользователями, группами и компьютерами.
31. Внедрение групповой политики.
32. Обзор модели многоуровневой защиты.
33. Физическая безопасность.
34. Обзор безопасности Windows.
35. Обеспечение безопасности файлов и папок.
36. Обзор сетевой безопасности.
37. Реализация брандмауэров.
38. Защита доступа к сети.
39. Защита электронной почты.
40. Защита серверов.

Тестовые задания
по дисциплине:

«ЗАЩИТА СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

ПРИМЕРНЫЕ ТЕСТЫ ДЛЯ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ЗНАНИЙ ПО ДИСЦИПЛИНЕ

@1. Защита сетевых информационных технологий — это
$A) защита программного обеспечения;
$B) защита аппаратных средств;
$C) совокупность мер по обеспечению безопасности сетей и сетевых сервисов;
$D) защита баз данных;
$E) защита пользователей;
@2. К объектам защиты в сетевых ИТ относится
$A) монитор;
$B) клавиатура;
$C) сетевые ресурсы и передаваемая информация;
$D) офисная мебель;
$E) источник питания;
@3. Основной целью защиты сетевых ИТ является обеспечение
$A) скорости передачи данных;
$B) совместимости оборудования;
$C) конфиденциальности, целостности и доступности информации;
$D) масштабируемости сети;
$E) удобства администрирования;
@4. К основным угрозам сетевой безопасности относится
$A) износ оборудования;
$B) сетевые атаки и несанкционированный доступ;
$C) обновление программного обеспечения;
$D) резервное копирование;
$E) аудит безопасности;
@5. На каком уровне модели OSI реализуется маршрутизация?
$A) Канальном;
$B) Сетевом;
$C) Транспортном;
$D) Сеансовом;
$E) Прикладном;
@6. Межсетевой экран предназначен для
$A) хранения данных;
$B) фильтрации сетевого трафика;
$C) резервного копирования;
$D) шифрования файлов;
$E) управления пользователями;
@7. Основная функция IDS — это
$A) блокирование трафика;
$B) шифрование данных;
$C) обнаружение атак и вторжений;
$D) управление доступом;
$E) резервное копирование;
@8. Система IPS отличается от IDS тем, что
$A) анализирует логи;
$B) только фиксирует инциденты;
$C) способна предотвращать атаки в реальном времени;
$D) работает только офлайн;
$E) используется только в локальных сетях;
@9. VPN используется для
$A) увеличения скорости сети;
$B) создания защищённого канала связи;

$C) хранения данных;
$D) фильтрации трафика;
$E) управления пользователями;
@10. К криптографическим методам защиты сетей относится
$A) резервное копирование;
$B) аутентификация пользователей;
$C) шифрование передаваемых данных;
$D) журналирование событий;
$E) управление доступом;
@11. Основная угроза беспроводных сетей — это
$A) перегрев оборудования;
$B) физический износ;
$C) перехват передаваемых данных;
$D) резервное копирование;
$E) отказ сервера;
@12. Для защиты Wi-Fi-сетей используется
$A) FTP;
$B) WEP;
$C) WPA2/WPA3;
$D) HTTP;
$E) SNMP;
@13. Атака типа DoS направлена на
$A) кражу данных;
$B) подмену информации;
$C) отказ в обслуживании сетевого ресурса;
$D) изменение маршрутизации;
$E) перехват паролей;
@14. DDoS-атака отличается от DoS тем, что
$A) проводится вручную;
$B) использует один источник;
$C) осуществляется с множества узлов;
$D) не влияет на доступность;
$E) направлена только на БД;
@15. Сетевой мониторинг предназначен для
$A) управления персоналом;
$B) анализа и контроля сетевого трафика;
$C) шифрования данных;
$D) резервного копирования;
$E) установки обновлений;
@16. Логирование сетевых событий необходимо для
$A) увеличения пропускной способности;
$B) восстановления данных;
$C) анализа инцидентов безопасности;
$D) настройки оборудования;
$E) ускорения работы сети;
@17. Аутентификация в сети — это
$A) назначение прав доступа;
$B) проверка подлинности пользователя;
$C) регистрация событий;
$D) фильтрация трафика;
$E) резервное копирование;
@18. Авторизация означает
$A) ввод логина;
$B) ввод пароля;

$C) предоставление прав доступа;
$D) установку соединения;
$E) шифрование данных;
@19. К средствам защиты сетевых сервисов относится
$A) текстовый редактор;
$B) антивирусное ПО;
$C) веб-сервер;
$D) офисный пакет;
$E) драйвер устройства;
@20. Сетевые черви относятся к
$A) аппаратным сбоям;
$B) программным ошибкам;
$C) вредоносному программному обеспечению;
$D) сетевым протоколам;
$E) средствам защиты;
@21. Управление инцидентами сетевой безопасности включает
$A) только выявление угроз;
$B) только устранение последствий;
$C) выявление, анализ и реагирование;
$D) шифрование данных;
$E) резервное копирование;
@22. Управление рисками в сетевых ИТ направлено на
$A) исключение всех угроз;
$B) устранение уязвимостей оборудования;
$C) снижение вероятности и ущерба от угроз;
$D) увеличение скорости сети;
$E) автоматизацию администрирования;
@23. К организационным мерам защиты сетей относится
$A) шифрование каналов;
$B) настройка межсетевого экрана;
$C) разработка политики сетевой безопасности;
$D) установка антивируса;
$E) настройка маршрутизатора;
@24. Стандарты сетевой безопасности предназначены для
$A) ускорения разработки ПО;
$B) унификации требований к защите сетей;
$C) увеличения производительности;
$D) управления персоналом;
$E) оптимизации трафика;
@25. Основная задача специалиста по защите сетевых ИТ —
$A) администрирование пользователей;
$B) обслуживание оборудования;
$C) обеспечение защищённого функционирования сети;
$D) разработка сайтов;
$E) настройка офисного ПО;

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.