МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО НАУКИ, ВЫСШЕГО ОБРАЗОВАНИЯ И ИННОВАЦИЙ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

МОО ВО КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ

имени первого Президента Российской Федерации Б.Н. Ельцина

Высшая школа цифровых технологий

Направление подготовки: 11.03.02 (РФ) / 690300 (КР) Инфокоммуникационные технологии и системы связи

Профиль: «Сети связи и системы коммутации»

Квалификация выпускника: Бакалавр

Форма обучения: Очная

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ФОС)

по дисциплине «Информационная безопасность»

Год начала подготовки: 2026

Семестр изучения: 8 семестр (4 курс)

Общая трудоемкость: 3 ЗЕТ (108 академических часов)

Форма промежуточной аттестации: Зачёт с оценкой (8 семестр)

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению подготовки «Инфокоммуникационные технологии и системы связи» по дисциплине

по дисциплине «Информационная безопасность»

Фонд оценочных средств рассмотрен и утвержден на заседании высшей школы «цифровых технологий»

протокол № 1 от «02» сентября 2026 года.

Директор ВШ «Цифровых технологий» _____ Хмелёва И.В.

Согласовано РОП: к.т.н., доцент Оконов М.О. _____

Исполнители:

Ст. препод. ВШ «Цифровых технологий» _____ Мамадалиева Ж.Б.

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1. Цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) предназначен для проведения текущего контроля успеваемости, рубежного контроля и промежуточной аттестации (зачёта с оценкой) обучающихся по дисциплине «Информационная безопасность». ФОС обеспечивает проверку уровня сформированности компетенции **ПК-8** (*Способен к администрированию средств обеспечения безопасности удаленного доступа, операционных систем и специализированных протоколов*).

1.2. Распределение объема дисциплины по видам занятий (по учебному плану)

- **Общая трудоемкость:** 3 ЗЕТ / 108 академических часов.
- **Лекционные занятия:** 16 часов (в т.ч. в интерактивной форме — 6 часов).
- **Практические занятия:** 16 часов (в т.ч. в форме практической подготовки — 8 часов).
- **Самостоятельная работа студентов (СРС):** 75,9 часа.
- **Контактная работа в период теоретического обучения (КрТО):** 0,1 часа.
- **Вид промежуточной аттестации:** Зачёт с оценкой (8 семестр).

1.3. Матрица связей разделов дисциплины, компетенций и оценочных средств

Раздел дисциплины	Формируемые индикаторы компетенции (ПК-8)	Виды оценочных средств
Раздел 1. Современные угрозы и каналы утечки информации	**Знать:** 3.1.1, 3.1.2 — технологии и топологии сетей связи, современные угрозы и каналы утечки информации **Уметь:** 3.2.1 — применять новые технологии информационной безопасности	Устный опрос (лекции-беседы), Практические работы №1.5, №1.6, №1.11, №1.12, №1.17, №1.18, Задания СРС №1.2, №1.4, №1.7, №1.9, №1.10, №1.13, №1.15, №1.19, №1.21, Рубежный контроль №1

Раздел дисциплины	Формируемые индикаторы компетенции (ПК-8)	Виды оценочных средств
	Владеть: 3.3.2 — ориентироваться на рынке технических средств и услуг безопасности	
Раздел 2. Методы и средства обеспечения безопасности объектов	**Знать:** 3.1.3, 3.1.4 — методы и средства обеспечения информационной безопасности и физической безопасности объектов **Уметь:** 3.2.1, 3.2.2 — применять новые технологии ИБ и безопасности объектов **Владеть:** 3.3.2 — оценка и выбор технических средств защиты объектов	Устный опрос, Практические работы №2.2, №2.3, №2.9, №2.10, Задания СРС №2.4, №2.6, №2.8, Рубежный контроль №2
Раздел 3. Технологии информационной безопасности. Обзор современных технических средств	**Знать:** 3.1.3, 3.1.4 — современные технические средства защиты, стеганографический анализ, проксимити-технологии **Уметь:** 3.2.1, 3.2.2 — оценка скрытности	Устный опрос, Практические работы №3.2, №3.3, №3.7, №3.8, №3.13, №3.14, Задания СРС №3.4, №3.9, №3.11, №3.15, Защита рефератов и докладов, Итоговый зачёт с оценкой

Раздел дисциплины	Формируемые индикаторы компетенции (ПК-8)	Виды оценочных средств
	потоков, настройка аппаратно-программных комплексов **Владеть:** 3.3.1, 3.3.2 — нанотехнологии и проксимити-технологии, анализ рынка средств защиты	

2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КАТЕГОРИИ «ЗНАТЬ» (Контрольные вопросы)

Вопросы сформированы на основе дидактических единиц разделов 4 и 5.1 РПД и используются при текущем опросе на лекционных и практических занятиях, а также при сдаче зачёта с оценкой.

Раздел 1. Современные угрозы и каналы утечки информации

1. **Каналы утечки информации:** Охарактеризуйте особенности современных технических каналов утечки информации (акустических, виброакустических, оптических, электромагнитных) и каналов несанкционированного доступа (НСД).
2. **Электрические каналы утечки и ПЭМИН:** Раскройте причины возникновения электрических каналов утечки (наводки на линии связи и цепи электропитания, микрофонный эффект) и побочных электромагнитных излучений и наводок (ПЭМИН).
3. **Пассивные и активные средства разведки:** Приведите сравнительные характеристики пассивных и активных технических средств получения (перехвата) информации.
4. **Классификация угроз и уязвимостей:** Перечислите основные компоненты информационной системы, подверженные угрозам, типы угроз (случайные, преднамеренные, силовое деструктивное воздействие) и основные пути несанкционированного получения информации.
5. **Программные закладки и сетевые угрозы:** Дайте классификацию программных закладок и вредоносного ПО, используемых в глобальной сети Internet и телекоммуникационных сетях.

6. **Концепция безопасности АСОИ:** Сформулируйте основные понятия концепции безопасности автоматизированных систем обработки информации (АСОИ), типовые меры безопасности и нормативно-правовую базу защиты информации.
7. **Аппаратура контроля линий связи и уничтожения закладок:** Опишите назначение и принцип работы анализатора проводных линий связи ССТА-1000, нелинейного детектора ВИЗИР-НЧ и подавителей/уничтожителей закладок BUGROASTER и КОБРА.
8. **Защита каналов передачи данных:** Охарактеризуйте принципы работы системы FS Communication System, сдвоенного канала связи типа V.24/RS-232 и X.21, а также программы управления защитой данных SE-5795.

Раздел 2. Методы и средства обеспечения безопасности объектов

9. **Интегральная защита в компьютерной телефонии:** Раскройте технические возможности реализации интегральной защиты в компьютерной телефонии на примере систем «Калейдоскоп плюс», «МАГ» и интегрального терминального устройства «Индекс».
10. **Комплексная физическая защита объекта:** Опишите структуру комплексной системы безопасности объекта и классификацию датчиков для обеспечения физической защиты периметра и помещений.
11. **Пространственное и линейное зашумление:** Объясните физические принципы работы технических средств акустического, пространственного и линейного зашумления для блокирования каналов утечки информации.
12. **Криптографические методы и стандарты шифрования:** Опишите принципы симметричного и асимметричного шифрования на примере алгоритма DES (Data Encryption Standard), метода Clipper, программного комплекса PGP и стандарта ГОСТ 28147-89.
13. **Защита от НСД и стеганография:** Охарактеризуйте мероприятия по защите от несанкционированного доступа (на примере системы Watchdog 4.1) и основные принципы компьютерной стеганографии.

Раздел 3. Технологии информационной безопасности. Обзор современных технических средств

14. **Носители информации и проксимити-технологии:** Приведите классификацию носителей информации и раскройте принцип действия проксимити-технологий (бесконтактной идентификации RFID/NFC) в системах контроля и управления доступом (СКУД).
15. **Генераторы шума и средства зашумления:** Сравните назначение и характеристики генераторов шума в акустическом диапазоне (WNG-023, SP-21B, ГНОМ-3, ГШ-1000,

ТУМАН-1) и средств создания маскирующих помех в сетях электропитания (NG-201, СОПЕРНИК).

16. **Многофункциональные устройства защиты:** Опишите функциональные возможности многофункциональных устройств защиты информации от утечки по техническим каналам СОНАТА-ДУ и ГРОМ-ЗИ-4.
17. **Статистический стегоанализ:** Раскройте суть методов оценки скрытности встраивания данных в контейнеры (по критерию хи-квадрат χ^2, по количеству переходов и группированию серий в потоке наименее значимых бит — НЗБ).

3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КАТЕГОРИИ «УМЕТЬ» (Практические задания)

Задания сформированы в соответствии с пунктами 4 и 5.1 «Уметь» РПД и выполняются на практических занятиях в формате разбора примеров и на зачёте.

1. **Обнаружение угроз в проводных линиях связи:** Определить порядок проведения инструментального контроля телефонных и выделенных линий связи с использованием анализатора ССТА-1000 и выявления нелинейных элементов с помощью детектора ВИЗИР-НЧ.
2. **Анализ сетевых угроз и противодействия в сети Internet:** Провести сравнительный анализ векторов сетевых атак (перехват трафика, подмена пакетов, внедрение программных закладок) и подобрать адекватные программно-аппаратные средства противодействия.
3. **Выбор средств защиты телефонных линий:** По заданным параметрам абонентской телефонной линии выбрать и обосновать схему подключения многофункционального устройства индивидуальной защиты от несанкционированного прослушивания.
4. **Нейтрализация закладных устройств:** Разработать алгоритм действий специалиста по применению устройств локализации и уничтожения электронных закладок (BUGROASTER, КОБРА) при обследовании выделенного помещения.
5. **Построение модели системы безопасности объекта:** Разработать структурную модель комплексной системы безопасности узла связи, включающую рубежи физической защиты, датчики контроля пространства и технические средства защиты информации.
6. **Расчет зон акустического и виброакустического зашумления:** Подобрать комплект генераторов акустического и вибрационного шума (ГШ-1000, ТУМАН-1, СОНАТА-ДУ) для защиты выделенного переговорного помещения заданной площади и конфигурации.
7. **Криптографическая защита файлов и сообщений:** Выполнить шифрование и проверку электронной подписи конфиденциального документа с использованием

криптографического программного средства PGP и оценить стойкость применяемых алгоритмов (DES, ГОСТ 28147-89).

8. **Защита от высокочастотного (ВЧ) навязывания и помех по сети питания:** Выбрать схему включения сетевых фильтров и генераторов маскирующих помех (NG-201, СОПЕРНИК, ГРОМ-ЗИ-4) для нейтрализации утечки по цепям электропитания и от ВЧ-навязывания.
9. **Проведение стеганографического анализа по критерию χ^2:** По заданной гистограмме распределения пар значений пикселей графического контейнера вычислить статистику критерия хи-квадрат (χ^2) и сделать вывод о наличии скрытого сообщения в потоке НЗБ.
10. **Оценка скрытности по переходам в потоке НЗБ:** Проанализировать битовую последовательность наименее значимых бит (НЗБ) методом подсчета переходов и группирования серий для выявления признаков стеганографического встраивания.

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КАТЕГОРИИ «ВЛАДЕТЬ» (Комплексные практические кейсы)

Задания соответствуют пунктам 3.3 и 5.1 «Владеть» РПД и проверяются при защите практических работ и на итоговом зачёте.

- **Кейс 1. Аудит защищенности и проектирование системы защиты телекоммуникационного узла**

Задание: На основе исходных данных об архитектуре корпоративной телекоммуникационной сети (типы каналов связи V.24/RS-232, X.21, IP-телефония, выделенные помещения) выявить потенциальные технические каналы утечки информации и угрозы НСД, после чего сформировать спецификацию средств активной и пассивной защиты (анализаторы линий, генераторы шума, системы разграничения доступа).

- **Кейс 2. Противодействие высокочастотному навязыванию и утечке по проводным каналам**

Задание: Разработать комплекс мероприятий и схему размещения технических средств защиты проводных линий связи, телефонных аппаратов («Калейдоскоп плюс», «МАГ», «Индекс») и цепей электропитания (NG-201, СОПЕРНИК, ГРОМ-ЗИ-4) от утечки информации за счет ПЭМИН, наводок и высокочастотного навязывания.

- **Кейс 3. Применение криптографических и программных средств защиты информации в АСОИ**

Задание: Настроить политику управления доступом и криптографической защиты данных в автоматизированной системе обработки информации с использованием программных комплексов (SE-5795, Watchdog 4.1, PGP), обеспечив конфиденциальность и целостность передаваемых и хранимых данных.

- **Кейс 4. Инструментальная и математическая оценка скрытности информационных потоков (Стегоанализ)**

Задание: Провести комплексное исследование цифрового файла-контейнера на наличие скрытых вложений в наименее значимых битах (НЗБ) с применением критерия согласия Пирсона (χ^2), анализа количества переходов и группирования серий; оформить протокол экспертизы.

- **Кейс 5. Подбор современных технических средств и проксимити-систем на рынке безопасности**

Задание: Провести сравнительный маркетингово-технический анализ современных средств обеспечения безопасности объектов (проксимити-СКУД, инфракрасные датчики, многофункциональные комплексы защиты) и обосновать выбор оптимального решения по критерию «эффективность / стоимость».

5. ТЕМАТИКА РЕФЕРАТОВ НА САМОСТОЯТЕЛЬНУЮ РАБОТУ (СРС)

Перечень из 10 тем соответствует пункту 5.2 РПД. Тема выбирается обучающимся по согласованию с преподавателем и оформляется в соответствии с требованиями раздела 8 РПД.

1. Назначение технического устройства «Спринт».
2. Назначение технического устройства BUGROASTER.
3. Назначение технического устройства «СОПЕРНИК».
4. Алгоритм шифрования DES (Data Encryption Standard).
5. Инфракрасные датчики контроля пространства.
6. Назначение технического устройства «КОБРА».
7. Технические средства обеспечения безопасности объектов инфокоммуникаций.
8. Назначение технического устройства ГШ-1000.
9. Метод шифрования информации по технологии Clipper.
10. Назначение технического устройства «СМОГ».

(Примечание: Курсовые работы и курсовые проекты по данной дисциплине учебным планом не предусмотрены).

6. ПЕРЕЧЕНЬ ВИДОВ ОЦЕНОЧНЫХ СРЕДСТВ И ТЕХНОЛОГИЧЕСКАЯ КАРТА КОНТРОЛЯ

В соответствии с разделами 5.4 и 8.1 РПД для оценки качества освоения дисциплины используются следующие оценочные средства:

1. **Контрольные вопросы (устный опрос):**

Текущая проверка усвоения теоретического материала на лекциях (в том числе в интерактивной форме лекции-беседы) и практических занятиях.

2. **Задания практических и лабораторных занятий (16 практических занятий, 16 часов):**

Выполнение и защита заданий в формате разбора конкретных примеров и творческих заданий по обнаружению угроз, настройке средств защиты и стегоанализу.

3. **Задания самостоятельной работы (75,9 часа СРС):**

Самостоятельная проработка теоретических вопросов (радиомониторинг, система «ОПАС», защита от ПЭМИН и силового деструктивного воздействия, нормативно-правовая база), подготовка докладов и написание рефератов.

4. **Рубежный контроль (контрольные работы и доклады по разделам):**

Проверка освоения материала по итогам изучения каждого из трех разделов дисциплины.

5. **Промежуточная аттестация — Зачёт с оценкой (8 семестр):**

Итоговая комплексная проверка уровня сформированности компетенции ПК-8 (уровни «Знать», «Уметь», «Владеть»).

7. КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЁТ С ОЦЕНКОЙ)

7.1. Балльно-рейтинговая система оценивания

В соответствии с разделом 8.1 рабочей программы дисциплины оценка итоговой успеваемости осуществляется по 100-балльной шкале с последующим переводом в пятибалльную академическую оценку. Для получения зачёта с оценкой сумма баллов, полученная студентом по результатам прохождения текущего и рубежного контроля, должна составлять **60 и более баллов**.

7.2. Шкала перевода баллов и дескрипторы оценивания (ПК-8)

Шкала баллов 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	**Академическая оценка 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf**	**Требования к уровню сформированности компетенции ПК-8 (Знать, Уметь, Владеть)**
85 – 100 баллов	**Отлично (5)**	Обучающийся демонстрирует глубокие, системные знания современных

Шкала баллов 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Академическая оценка 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Требования к уровню сформированности компетенции ПК-8 (Знать, Уметь, Владеть)
		угроз, технических каналов утечки информации (электрических, акустических, ПЭМИН), методов криптографической защиты, стегоанализа и принципов работы технических средств безопасности; безошибочно подбирает и обосновывает комплексы защиты линий связи и объектов, проводит оценку скрытности потоков НЗБ по критерию χ^2; в полном объеме выполнил и защитил все практические работы, доклад и реферат, оформленный в строгом соответствии с требованиями.
70 – 84 балла	**Хорошо (4)**	Обучающийся твердо знает теоретический

Шкала баллов 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Академическая оценка 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Требования к уровню сформированности компетенции ПК-8 (Знать, Уметь, Владеть)
		материал по всем трем разделам дисциплины, допускает незначительные неточности при ответе на дополнительные вопросы по характеристикам специализированных устройств защиты или алгоритмам шифрования; уверенно решает типовые задачи по выявлению угроз безопасности и выбору средств защиты каналов связи; выполнил и защитил все практические задания и реферат с незначительными замечаниями.
60 – 69 баллов	**Удовлетворительно (3)**	Обучающийся усвоил только основной базовый материал (классификацию угроз, основные каналы утечки

Шкала баллов 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Академическая оценка 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Требования к уровню сформированности компетенции ПК-8 (Знать, Уметь, Владеть)
		информации, базовые методы физической и криптографической защиты); испытывает затруднения при самостоятельном проведении математического стегоанализа и проектировании комплексных систем защиты; практические работы и задания СРС выполнены в минимально необходимом объеме с помощью преподавателя.
Менее 60 баллов	**Неудовлетворительно (2)**	Обучающийся не знает классификации каналов утечки информации, методов и технических средств обеспечения информационной безопасности и защиты объектов; не владеет

Шкала баллов 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Академическая оценка 2026-2027_b110302_26_1 итисс_plx_Информационная безопасность_Сети связи и системы коммутации.pdf	Требования к уровню сформированности компетенции ПК-8 (Знать, Уметь, Владеть)
		практическими навыками оценки угроз и работы со средствами защиты информации; имеет невыполненные практические работы и академические задолженности по контрольным точкам.