МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство науки, высшего образования и инноваций Кыргызской Республики

Межгосударственная образовательная организация высшего образования

Кыргызско-Российский Славянский университет

им. первого Президента Российской Федерации Б.Н. Ельцина

Политехнический институт

Кафедра «Экология и защита в чрезвычайных ситуациях»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Информационные технологии в сфере безопасности»

Уровень высшего образования: БАКАЛАВРИАТ

Направление подготовки 20.03.01 - РФ, 7603 00 - КР «**Техносферная безопасность»**

Профиль **"Защита в чрезвычайных ситуациях"**

Форма обучения: очная

2026 г.

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению **подготовки:** 20.03.01 - РФ, 760300 - КР «Техносферная безопасность» в процессе подготовки бакалавриата КРСУ в соответствии с ФГОС 3++ по дисциплине «***Информационные технологии в сфере безопасности***».

Фонд оценочных средств рассмотрен и утвержден на заседании

Кафедры «Экологии и защиты в чрезвычайных ситуациях»

протокол № 1 от "02"сентября 2026 г.

Заведующий кафедрой **«Экологии и защиты в чрезвычайных ситуациях»** *к.т.н., доцент* *Мамбетов Эрик Мунайтбасович*
наименование кафедры *подпись* *расшифровка подписи*

Руководитель образовательной программы направления подготовки «Техносферная безопасность» *к.т.н., доцент* *Мамбетов Эрик Мунайтбасович*
наименование РОП *подпись* *расшифровка подписи*

Исполнитель:
преподаватель *Акматов Дамир Русланович*
должность *подпись* *расшифровка подписи*

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств (ФОС) разработан в соответствии с требованиями ФГОС ВО 3++ по направлению подготовки 20.03.01 «Техносферная безопасность» и рабочей программой дисциплины «Информационные технологии в безопасности». ФОС предназначен для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

В результате освоения дисциплины у обучающегося формируются следующие компетенции: УК-3 (способность осуществлять социальное взаимодействие и реализовывать свою роль в команде), УК-4 (способность осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)), ОПК-3 (способность осуществлять профессиональную деятельность с учетом государственных требований в области обеспечения безопасности).

Таблица 1 – Соответствие контролируемых разделов дисциплины, компетенций и оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Раздел 1. Введение в цифровую среду и интегральную безопасность служб спасения (Темы 1.1–1.3)	УК-3, УК-4, ОПК-3	Конспект лекций, устный опрос, защита презентаций (Практики 2–3)
2	Раздел 2. Анатомия цифровых угроз и каналы уязвимостей (Темы 2.1–2.3)	УК-4, ОПК-3	Конспект лекций, устный опрос, ситуационное задание, защита презентаций (Практики 4–6)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
3	Раздел 3. Организационные и технические методы защиты в условиях ЧС (Темы 3.1–3.3)	УК-3, УК-4, ОПК-3	Конспект лекций, устный опрос, защита презентаций (Практики 7–9)
4	Раздел 4. Сохранность данных, гигиена спасателя и законы (Темы 4.1–4.3)	УК-3, УК-4, ОПК-3	Конспект лекций, устный опрос, защита презентаций (Практики 10–11)
5	Итоговый контроль по всем разделам дисциплины	УК-3, УК-4, ОПК-3	Финальный аудит конспектов (Практика 12), зачет с оценкой (собеседование)

2. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

2.1. Критерии оценивания текущего контроля успеваемости

Текущий контроль успеваемости обучающихся осуществляется в ходе практических занятий и включает проверку ведения конспекта лекций, устный опрос, выполнение ситуационного задания и защиту мультимедийных презентаций.

1. Ведение конспекта лекций. Конспект проверяется преподавателем на каждом практическом занятии; финальный аудит конспектов проводится на Практике 12. Отметка «зачтено» выставляется при систематическом ведении записей, наличии основных определений, схем и тезисов по всем прочитанным лекциям. Отметка «не зачтено» выставляется при систематических пропусках тем или отсутствии конспекта, что влияет на допуск к промежуточной аттестации.

2. Подготовка и защита презентации. Презентация подготавливается в объеме 10–15 слайдов по утвержденной теме (Практики 2–11) с обязательным включением практических примеров (в том числе с привязкой к Кыргызской

Республике), выводов и списка использованных источников. Регламент устного доклада составляет 5–7 минут. Оценка «отлично» выставляется при полном раскрытии темы, корректном использовании терминологии ИБ, качественном оформлении слайдов и аргументированных ответах на вопросы; «хорошо» – при незначительных недочетах в оформлении или ответах; «удовлетворительно» – при поверхностном изложении материала; «неудовлетворительно» – при несоответствии теме или отказе от защиты.

3. Выполнение ситуационного задания (кейса). При анализе гипотетической аварийной ситуации (Практика 4) оценивается точность идентификации нарушенного свойства триады информационной безопасности, определение типа угрозы и корректность предложенного алгоритма действий специалиста по защите от ЧС.

2.2. Критерии оценивания промежуточной аттестации (зачет с оценкой)

К промежуточной аттестации допускаются студенты, посетившие не менее 70 % учебных занятий, имеющие полный конспект лекций и защитившие презентацию. Промежуточная аттестация проводится в форме устного собеседования по контрольным вопросам.

Таблица 2 – Шкала и критерии оценивания на промежуточной аттестации

Оценка	Критерии оценивания знаний, умений и владений
«Отлично»	Обучающийся выполнил все условия допуска (посещаемость не менее 70 %, наличие всех конспектов, защищенная презентация); дает полные, логически выстроенные и аргументированные ответы на вопросы; свободно оперирует терминологией информационной безопасности и положениями нормативных правовых актов КР; умеет применять теоретические знания для оценки рисков на критически важных объектах.

Оценка	Критерии оценивания знаний, умений и владений
«Хорошо»	Обучающийся выполнил все условия допуска; правильно отвечает на основные вопросы, демонстрируя твердое усвоение программного материала, однако допускает незначительные неточности при формулировке определений или при ответе на дополнительные вопросы преподавателя.
«Удовлетворительно»	Обучающийся выполнил минимальные условия допуска; демонстрирует фрагментарные знания базовых понятий (триада ИБ, классификация угроз, правила цифровой гигиены), испытывает затруднения при приведении практических примеров и ссылках на законодательство КР.
«Неудовлетворительно»	Обучающийся имеет систематические пропуски занятий (более 30 %), не представил конспекты лекций или не защитил презентацию, либо не способен ответить на базовые контрольные вопросы по дисциплине.

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

3.1. Темы презентаций для практических занятий (Практики 2–11)

1. Сбои доступности информационных систем МЧС и их последствия для населения (Практика 2).

2. Устройство и уязвимости современных систем раннего оповещения о чрезвычайных ситуациях (Практика 3).

3. Риски модификации и фальсификации данных мониторинга на примере датчиков уровня воды или радиации (Практика 4).

4. Анализ уязвимостей критически важных объектов за счёт побочных электромагнитных излучений и наводок аппаратуры (Практика 5).

5. История разрушительных кибератак на промышленные объекты и гидросооружения (Практика 6).

6. Технические средства поиска каналов утечки информации в штабах ликвидации чрезвычайных ситуаций (Практика 7).

7. Человеческий фактор: социальная инженерия и фишинг как угроза безопасности критически важных объектов (Практика 8).

8. Применение шифрования для защиты оперативной радиосвязи и приказов при ликвидации ЧС (Практика 9).

9. Организация надёжного хранения электронных карт местности и баз данных населения на случай ЧС (Практика 10).

10. Законодательство Кыргызской Республики в сфере защиты критической информационной инфраструктуры (Практика 11).

3.2. Ситуационное задание (кейс) для Практики 4

Условие задачи: На автоматизированном рабочем месте диспетчера датчик уровня воды на гидротехническом сооружении передает штатные показатели (норма), однако по данным визуального наблюдения и с соседнего гидропоста уровень воды стремительно растёт.

Задание: Обоснуйте ваши первоочередные действия как специалиста по защите от чрезвычайных ситуаций с точки зрения триады информационной безопасности (конфиденциальность, целостность, доступность) и классификации информационных угроз.

3.3. Контрольные вопросы для устного опроса по разделам

Раздел 1. Введение в цифровую среду и интегральную безопасность:

1. Что такое «критическая информация» в техносферной безопасности? Приведите примеры.

2. Какие три составляющие образуют триаду информационной безопасности?

3. Приведите пример нарушения доступности информации в аварийной службе и опишите последствия.

4. Приведите пример нарушения целостности данных мониторинга и опишите последствия.

5. Назовите пять информационных революций и укажите, какая из них позволила впервые передавать сигналы бедствия быстрее физического перемещения человека.

6. Из каких двух уровней состоит ИТ-платформа автоматизированного диспетчерского пункта?

7. Что входит в информационную инфраструктуру критически важного объекта?

Раздел 2. Анатомия цифровых угроз и каналы уязвимостей:

1. Перечислите четыре типа основных угроз информационной безопасности (прерывание, перехват, модификация, подделка).

2. Что такое «закладное устройство»? Через какие каналы возможна утечка информации (линии сигнализации, вентиляция, электропитание)?

3. Чем опасны логические бомбы и сетевые черви для аппаратной части критически важных объектов?

4. Приведите пример исторической кибератаки на промышленный объект и кратко опишите её последствия.

Раздел 3. Организационные и технические методы защиты:

1. Назовите основные функции управления доступом (идентификация, аутентификация, авторизация, протоколирование).

2. В чём отличие симметричного и асимметричного шифрования?

3. Для чего используется электронная цифровая подпись (ЭЦП)?

4. Что такое стеганография и чем она отличается от криптографии?

Раздел 4. Сохранность данных, гигиена спасателя и законы:

1. Почему резервное копирование критично для служб спасения? Какие устройства защищают серверы от сбоев электропитания?

2. Какие нормативные акты Кыргызской Республики регулируют защиту информации и критической инфраструктуры? Назовите не менее двух.

3. Перечислите основные правила цифровой гигиены спасателя при работе в зоне чрезвычайной ситуации.

3.4. Темы дополнительных письменных работ (эссе, рефераты)

Написание эссе (рекомендуемый объем 3–5 страниц) и рефератов (10–15 страниц) является необязательным видом самостоятельной работы и используется по выбору обучающегося как поощрительная форма контроля. Обязательным требованием является наличие ссылок на нормативные правовые акты Кыргызской Республики и списка использованной литературы.

1. Обеспечение кибербезопасности объектов энергетической инфраструктуры Кыргызской Республики.

2. Реализация требований Постановления Кабинета Министров КР № 746 на критически важных объектах техносферы.

3. Противодействие информационно-психологическим операциям влияния в условиях ликвидации крупных ЧС.

4. Защита автоматизированных систем управления технологическими процессами (SCADA) от целевых кибератак.

4. ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЕТ С ОЦЕНКОЙ)

1. Понятие информации и «критической» информации в техносферной безопасности.

2. Триада информационной безопасности: конфиденциальность, целостность, доступность. Примеры нарушения каждого свойства в аварийных службах.

3. Понятие интегральной безопасности и её роль для критически важных объектов.

4. Информационные революции и их значение для служб спасения.

5. Этапы эволюции инструментария информационных технологий (от ручных средств до информационного общества).

6. Понятие ИТ-платформы. Аппаратный и программный уровни.

7. Информационная инфраструктура критически важных объектов: основные элементы и их уязвимости.

8. Классификация угроз информационной безопасности (прерывание, перехват, модификация, подделка).

9. Технические и физические каналы утечки информации. Понятие закладных устройств.

10. Вредоносное программное обеспечение: виды и воздействие на критические системы.

11. Методы и средства обнаружения цифровых угроз.

12. Управление доступом: идентификация, аутентификация, авторизация, протоколирование.

13. Парольная политика и биометрические системы идентификации.

14. Основы криптографической защиты: симметричное и асимметричное шифрование.

15. Электронная цифровая подпись (ЭЦП) и её применение в документообороте аварийных служб.

16. Стеганография как метод скрытой передачи данных.

17. Обеспечение сохранности информации: архивация, резервное и страховое копирование.

18. Защита серверов от сбоев электропитания (ИБП, UPS). RAID-массивы.

19. Нормативно-правовое регулирование информационной безопасности в Кыргызской Республике (Закон КР «О кибербезопасности», Постановление КМ КР № 746 и др.).

20. Цифровая гигиена сотрудника аварийно-спасательных служб: основные правила и рекомендации.