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

УТВЕРЖДАЮ
Директор Политехнического института
(должность)
Лопев Г.В.
(ФИО)
05.09.2026 г.

МОДУЛЬ ЦИФРОВЫХ КОМПЕТЕНЦИЙ (DIGITAL)
Информационные технологии в безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Экологии и защиты в чрезвычайных ситуациях**

Учебный план b200301_26_1 тб_зчс.plx
Направление 20.03.01 - РФ, 760300 - КР Техносферная безопасность

Форма обучения очная
Профиль "Защита в чрезвычайных ситуациях"

Общая трудоемкость **4 ЗЕТ**
Часов по учебному плану 144
в том числе:
аудиторные занятия 48
самостоятельная работа 95,9

Виды контроля в семестрах:
зачет с оценкой 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		Итого	
Недель	16 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	32	32	32	32
Контактная работа в период теоретического обучения	0,1	0,1	0,1	0,1
Итого ауд.	48	48	48	48
Контактная работа	48,1	48,1	48,1	48,1
Сам. работа	95,9	95,9	95,9	95,9
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование у обучающихся системы базовых знаний об информационных технологиях и информационной безопасности в сфере техносферной безопасности, необходимых для безопасного применения цифровых систем в профессиональной деятельности специалиста по защите от чрезвычайных ситуаций, а также понимания взаимосвязи киберугроз и техносферных рисков на критически важных объектах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.4.09
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Б1.О.1.05. Безопасность жизнедеятельности
2.1.2	Б1.О.1.06. Основы критического мышления
2.1.3	Б1.О.2.02. Физика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Б1.О.4.03. Управление техносферной безопасностью
2.2.2	Б1.О.4.05. Безопасность и риск. Промышленная экология
2.2.3	Б1.О.4.07. Надежность технических систем и техногенный риск
2.2.4	Б1.О.4.08. Охрана труда
2.2.5	Б1.О.4.02. Защита в чрезвычайных ситуациях
2.2.6	Б3.03(Д). Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.7	Б3.02(Г). Подготовка к сдаче и сдача государственного экзамена
2.2.8	Б1.В.1.ДВ.07.01. Прогнозирование и оценка социально-экономических последствий в чрезвычайных ситуациях
2.2.9	Б1.В.1.ДВ.06.01. Мониторинг и предупреждение в чрезвычайных ситуациях
2.2.10	Б1.В.1.ДВ.02.01. Основы организации и ведения гражданской защиты
2.2.11	Б1.В.1.07. Система связи и оповещения
2.2.12	Б1.В.1.06. Надзор и контроль в сфере безопасности
2.2.13	Б1.В.1.04. Безопасность спасательных работ в ЧС
2.2.14	Б1.В.1.05. Геоинформационные системы и технологии при чрезвычайных ситуациях
2.2.15	Б1.В.1.03. Тактика сил государственной системы гражданской защиты
2.2.16	Б1.В.1.11. Организация и ведение аварийно-спасательных работ
2.2.17	Б1.В.1.09. Устойчивость природных и техногенных объектов и объектов экономики
2.2.18	Б1.В.1.08. Управление рисками, системный анализ и моделирование
2.2.19	Б1.В.1.ДВ.09.01. Методы и приборы контроля окружающей среды и экологический мониторинг

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-3: Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
Знать:	
Уровень 1	Основы командного взаимодействия при ликвидации ЧС с использованием цифровых систем; правила безопасной передачи информации внутри команды; роль каждого участника в обеспечении информационной безопасности.
Уметь:	
Уровень 1	Работать в команде при решении задач информационной безопасности; распределять роли с учётом требований защиты информации; организовывать безопасный обмен данными между участниками.
Владеть:	
Уровень 1	Навыками командной работы с использованием информационных технологий; приёмами безопасной коммуникации в цифровой среде.

УК-4: Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	
Знать:	
Уровень 1	Правила оформления деловой документации и презентаций по вопросам ИБ; основные требования к устной и письменной коммуникации при работе с защищаемой информацией; терминологию информационной безопасности на русском и иностранном языках.
Уметь:	
Уровень 1	Готовить устные выступления и письменные материалы (конспекты, презентации, отчёты) по проблемам информационной безопасности; использовать профессиональную терминологию; вести деловую переписку с соблюдением требований ИБ.
Владеть:	

Уровень 1	Навыками публичной защиты презентаций; способами аргументированного изложения позиции по вопросам ИБ; приёмами работы с нормативными документами и научной литературой.

ОПК-3: Способен осуществлять профессиональную деятельность с учетом государственных требований в области обеспечения безопасности.	
Знать:	
Уровень 1	Классификацию информационных технологий и угроз; правовые и организационные основы ИБ в Кыргызской Республике; методы и средства защиты информации; принципы работы систем мониторинга и оповещения.
Уметь:	
Уровень 1	Применять информационно-коммуникационные технологии для поиска, обработки и анализа информации при решении задач защиты от ЧС; использовать базовые средства защиты информации; оценивать риски нарушения ИБ на объекте.
Владеть:	
Уровень 1	Навыками работы с информационными системами и базами данных; базовыми приёмами защиты информации; способами соблюдения требований ИБ в профессиональной деятельности.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
основные понятия информационной безопасности (информация, критическая информация, угроза, уязвимость, триада ИБ); классификацию угроз и каналов утечки информации; роль информационных технологий в предупреждении и ликвидации ЧС; правовые и организационные основы защиты информации в Кыргызской Республике; основные методы и средства защиты информации на критически важных объектах; правила цифровой гигиены и безопасной коммуникации в команде.	
3.2	**Уметь:**
анализировать информационные угрозы применительно к объектам защиты и службам спасения; оценивать последствия нарушения конфиденциальности, целостности и доступности информации; применять организационные и базовые технические меры защиты информации; использовать нормативные документы для решения задач ИБ; готовить устные выступления и письменные материалы по вопросам ИБ; работать в команде с соблюдением требований информационной безопасности.	
3.3	**Владеть:**
анализа рисков информационной безопасности на критически важных объектах; работы с нормативно-правовыми актами в сфере ИБ; применения базовых средств защиты информации; командного взаимодействия с использованием цифровых систем; подготовки и публичной защиты презентаций по проблемам ИБ; соблюдения правил цифровой гигиены при работе в условиях ЧС.	