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

Программу составил(и):
Преподователь, Акматов Дамир Русланович

Рецензент(ы):
Преподователь, Исмаилова Жазгул Жыргалбековна

Согласовано РОП:

Рабочая программа дисциплины
Информационные технологии в безопасности

разработана в соответствии с ФГОС 3++:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 20.03.01 Техносферная безопасность (приказ Минобрнауки России от 25.05.2020 г. № 680)

составлена на основании учебного плана:

Направление 20.03.01 - РФ, 760300 - КР Техносферная безопасность
Профиль "Защита в чрезвычайных ситуациях"
утвержденного учёным советом вуза от 26.06.2026 протокол № 11.

Рабочая программа одобрена на заседании Кафедра экологии и защиты в чрезвычайных ситуациях

Протокол от 02.09.2026 г. № 1
Срок действия программы: 2026-2030 уч.г.
Руководитель подразделения: Мамбетов Эрик Мунайтбасович

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
к рабочей программе дисциплины (модуля)
Информационные технологии в безопасности

№ п/п	Основание внесения изменения	Раздел/ пункт	Содержание изменения
1.	Приказ № 456-П от 02.09.2026 г. «О введении новой организационной структуры КыргызскоРоссийского Славянского университета»	«Приказ № 357-П от 24 июня 2026 года считать реализованным в части структурных изменений».	«О преобразовании Естественнотехнического факультета и Факультета архитектуры, дизайна и строительства в Политехнический институт КРСУ»
2.			
3.			
4.			

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.
Уровень 2	
Уровень 3	
Уметь:	
Уровень 1	Работать в команде при решении задач информационной безопасности; распределять роли с учётом требований защиты информации; организовывать безопасный обмен данными между участниками.
Уровень 2	
Уровень 3	
Владеть:	
Уровень 1	Навыками командной работы с использованием информационных технологий; приёмами безопасной коммуникации в цифровой среде.
Уровень 2	
Уровень 3	

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.
Уровень 2	
Уровень 3	
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.
Уровень 2	
Уровень 3	
Владеть:	
Уровень 1	Навыками публичной защиты презентаций; способами аргументированного изложения позиции по вопросам ИБ; приёмами работы с нормативными документами и научной литературой.
Уровень 2	
Уровень 3	

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.
Уровень 2	
Уровень 3	
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.
Уровень 2	
Уровень 3	
Владеть:	
Уровень 1	Навыками работы с информационными системами и базами данных; базовыми приёмами защиты информации; способами соблюдения требований ИБ в профессиональной деятельности.
Уровень 2	
Уровень 3	

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	основные понятия информационной безопасности (информация, критическая информация, угроза, уязвимость, триада ИБ);
3.1.2	классификацию угроз и каналов утечки информации;
3.1.3	роль информационных технологий в предупреждении и ликвидации ЧС;
3.1.4	правовые и организационные основы защиты информации в Кыргызской Республике;
3.1.5	основные методы и средства защиты информации на критически важных объектах;
3.1.6	правила цифровой гигиены и безопасной коммуникации в команде.
3.2	**Уметь:**
3.2.1	анализировать информационные угрозы применительно к объектам защиты и службам спасения;
3.2.2	оценивать последствия нарушения конфиденциальности, целостности и доступности информации;
3.2.3	применять организационные и базовые технические меры защиты информации;
3.2.4	использовать нормативные документы для решения задач ИБ;
3.2.5	готовить устные выступления и письменные материалы по вопросам ИБ;
3.2.6	работать в команде с соблюдением требований информационной безопасности.
3.3	**Владеть:**
3.3.1	анализа рисков информационной безопасности на критически важных объектах;

3.3.2	работы с нормативно-правовыми актами в сфере ИБ;
3.3.3	применения базовых средств защиты информации;
3.3.4	командного взаимодействия с использованием цифровых систем;
3.3.5	подготовки и публичной защиты презентаций по проблемам ИБ;
3.3.6	соблюдения правил цифровой гигиены при работе в условиях ЧС.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем / вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Пр. подг.	Примечание
	Раздел 1. Содержание лекционных занятий							
1.1	Раздел 1. Введение в цифровую среду и интегральную безопасность служб спасения Тема 1.1. Понятие информации и эволюция ИТ в техносфере (1 ч). Понятие информации и «критической» информации в техносферной безопасности. Данные цифрового мониторинга, управленческая информация, каналы оповещения. Пять этапов информационных революций и их значение для служб спасения. Шесть этапов эволюции инструментария ИТ (от ручных до информационного общества). Понятие ИТ-платформы. /Лек/	5	1					
1.2	Тема 1.2. Интегральная безопасность КВО. Триада ИБ (1 ч). Понятие интегральной безопасности: взаимосвязь физической, пожарной и информационной безопасности. Критически важные объекты (КВО) и последствия нарушения их информационной безопасности. Триада ИБ: конфиденциальность, целостность, доступность. Примеры нарушения триады в аварийных службах и их последствия. /Лек/	5	2					
1.3	Тема 1.3. Информационная инфраструктура защиты от ЧС (1 ч). Понятие информационно-телекоммуникационной системы (ИТКС). Структура связи между датчиками мониторинга, серверами и пультами ЕДДС. Роль автоматизированных систем управления (АСУ) и SCADA-систем. Уязвимости инфраструктуры КВО. /Лек/	5	1					

1.4	Раздел 2. Анатомия цифровых угроз и каналы уязвимостей Тема 2.1. Классификация современных информационных угроз (1 ч). Четыре типа основных угроз: прерывание, перехват, модификация, подделка (фальсификация). Понятие модели нарушителя. Внутренние и внешние угрозы. Роль человеческого фактора. /Лек/	5	2					
1.5	Тема 2.2. Технические и физические каналы утечки информации (1 ч). Электромагнитные, электрические и параметрические каналы утечки. Понятие «закладных устройств» (жучков). Риски утечки данных через линии пожарно-охранной сигнализации, вентиляции и сети электропитания. /Лек/	5	2					
1.6	Тема 2.3. Вредоносное программное обеспечение в критических системах (1 ч). Классификация компьютерных вирусов (сетевые, резидентные, логические бомбы, троянские программы). Разрушительное воздействие вирусов на аппаратную часть КВО. Примеры исторических кибератак (Stuxnet, атаки на энергосети). /Лек/	5	1					
1.7	Раздел 3. Организационные и технические методы защиты в условиях ЧС Тема 3.1. Методы и средства обнаружения цифровых угроз (1 ч). Обнаружители скрытых камер, радиоизлучений, детекторы вирусов. Применение нелинейных локаторов и анализаторов спектра. Роль систем мониторинга безопасности объектов в реальном времени. /Лек/	5	1					
1.8	Тема 3.2. Управление доступом и аутентификация (1 ч). Функции защиты: идентификация, опознание, проверка полномочий, регистрация (протоколирование). Парольная политика на пультах управления опасными объектами. Биометрические системы идентификации. /Лек/	5	1					

1.9	Тема 3.3. Основы криптографической защиты и стеганографии (1 ч). Ознакомительный обзор алгоритмов шифрования (симметричные и асимметричные). Понятие электронной цифровой подписи (ЭЦП). Стеганография как метод скрытой передачи данных. Применение шифрования для защиты оперативной радиосвязи. /Лек/	5	1					
1.10	Раздел 4. Сохранность данных, гигиена спасателя и законы Тема 4.1. Обеспечение сохранности информации и резервное копирование (1 ч). Понятие целостности данных. Архивация, резервное и страховое копирование оперативных планов эвакуации. Защита серверов от сбоев электропитания (ИБП, UPS). RAID-массивы и распределённое хранение. /Лек/	5	1					
1.11	Тема 4.2. Нормативно-правовое регулирование и стандарты ИБ (1 ч). Правовые меры защиты информации в Кыргызской Республике. Закон КР «О кибербезопасности», Закон КР «Об информации персонального характера», Постановление Кабинета Министров КР №746 о требованиях к системам кибербезопасности объектов КИИ. Понятие стандартов ИТ (ISO). Ответственность за нарушение правил эксплуатации автоматизированных систем. / Лек/	5	1					
1.12	Тема 4.3. Цифровая гигиена сотрудника аварийно-спасательных служб (1 ч). Итоговая лекция-инструктаж. Правила поведения спасателя в цифровом пространстве: использование личных гаджетов в зоне ЧС, защита геолокации, противодействие информационно-психологическим операциям влияния. Профилактика фишинга и социальной инженерии. /Лек/	5	2					
1.13	Практика 1. Вводное занятие. Распределение тем презентаций. Инструктаж по ведению конспектов. /Пр/	5	4					

1.14	Практика 2. Защита презентаций: «Сбои доступности информационных систем МЧС и их последствия для населения». /Пр/	5	4					
1.15	Практика 3. Защита презентаций: «Устройство и уязвимости современных систем раннего оповещения о ЧС». /Пр/	5	4					
1.16	Практика 4. Защита презентаций: «Риски модификации и фальсификации данных мониторинга (на примере датчиков уровня воды или радиации)». /Пр/	5	2					
1.17	Практика 5. Защита презентаций: «Анализ уязвимостей КВО за счёт побочных излучений и наводок аппаратуры». /Пр/	5	2					
1.18	Практика 6. Защита презентаций: «История разрушительных кибератак на промышленные объекты и гидросооружения». /Пр/	5	2					
1.19	Практика 7. Защита презентаций: «Технические средства поиска каналов утечки информации в штабах ликвидации ЧС». /Пр/	5	2					
1.20	Практика 8. Защита презентаций: «Человеческий фактор: социальная инженерия и фишинг как угроза безопасности КВО». /Пр/	5	2					
1.21	Практика 9. Защита презентаций: «Применение шифрования для защиты оперативной радиосвязи и приказов при ликвидации ЧС». /Пр/	5	2					
1.22	Практика 10. Защита презентаций: «Организация надёжного хранения электронных карт местности и баз данных населения на случай ЧС». /Пр/	5	2					
1.23	Практика 11. Защита презентаций: «Законодательство в сфере защиты критической информационной инфраструктуры». /Пр/	5	2					
1.24	Практика 12. Финальный аудит конспектов лекций. Подведение итогов по посещаемости, выставление зачётов. /Пр/	5	4					
1.25	Подготовка презентации /Ср/	5	8					

1.26	Изучение нормативных документов Изучение Закона КР «О кибербезопасности», Постановления КМ КР №746 и др. /Ср/	5	8					
1.27	Ведение конспекта лекции / КрТО/	5	0,1					
1.28	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.29	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.30	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.31	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.32	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.33	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.34	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.35	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.36	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	8					
1.37	Подготовка презентации, выбор темы, сбор материала, оформление /Ср/	5	7,9					

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Раздел 1. Введение в цифровую среду и интегральную безопасность

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

Какие три составляющие образуют триаду информационной безопасности?

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

Приведите пример нарушения целостности данных мониторинга и опишите последствия.

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

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

Что входит в информационную инфраструктуру критически важного объекта?

Раздел 2. Анатомия цифровых угроз и каналы уязвимостей

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

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

Чем опасны логические бомбы и сетевые черви для аппаратной части КВО?

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

Раздел 3. Организационные и технические методы защиты

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

В чём отличие симметричного и асимметричного шифрования?

Для чего используется электронная цифровая подпись (ЭЦП)?

Что такое стеганография и чем она отличается от криптографии?

Раздел 4. Сохранность данных, гигиена спасателя и законы
Почему резервное копирование критично для служб спасения? Какие устройства защищают серверы от сбоев электропитания? Какие нормативные акты Кыргызской Республики регулируют защиту информации и критической инфраструктуры? Назовите не менее двух.
Перечислите основные правила цифровой гигиены спасателя при работе в зоне ЧС.
Задания для текущего контроля
Задание 1 (Практики 2–11). Подготовить и защитить презентацию по выбранной теме (темы распределены по группам). Требования: 10–12 слайдов, наличие примеров (желательно с привязкой к Кыргызстану), выводы, список источников. Доклад — 5–7 минут.
Задание 2 (каждое практическое занятие). Вести конспект лекций. Конспект проверяется на каждом занятии; отсутствие конспекта влияет на допуск к зачёту.
Задание 3 (Практика 4). Проанализировать гипотетическую ситуацию: «Датчик уровня воды показывает норму, но по данным другого источника уровень растёт. Ваши действия как специалиста по защите от ЧС?» (ответ обосновать с точки зрения триады ИБ).
2. Промежуточная аттестация (зачёт)
Промежуточная аттестация проводится в форме собеседования по вопросам (или итогового аудита конспектов с ответами на 2–3 вопроса). Студент допускается к зачёту при условии посещения не менее 70% занятий, наличия всех конспектов и защиты презентации.
Вопросы к зачёту
Понятие информации и «критической» информации в техносферной безопасности.
Триада информационной безопасности: конфиденциальность, целостность, доступность. Примеры нарушения каждого свойства в аварийных службах.
Понятие интегральной безопасности и её роль для критически важных объектов.
Информационные революции и их значение для служб спасения.
Этапы эволюции инструментария ИТ (от ручных до информационного общества).
Понятие ИТ-платформы. Аппаратный и программный уровни.
Информационная инфраструктура КВО: основные элементы и их уязвимости.
Классификация угроз информационной безопасности (прерывание, перехват, модификация, подделка).
Технические и физические каналы утечки информации. Понятие закладных устройств.
Вредоносное программное обеспечение: виды и воздействие на критические системы.
Методы и средства обнаружения цифровых угроз.
Управление доступом: идентификация, аутентификация, авторизация, протоколирование.
Парольная политика и биометрические системы идентификации.
Основы криптографической защиты: симметричное и асимметричное шифрование.
Электронная цифровая подпись (ЭЦП) и её применение в документообороте аварийных служб.
Стеганография как метод скрытой передачи данных.
Обеспечение сохранности информации: архивация, резервное и страховое копирование.
Защита серверов от сбоев электропитания (ИБП, UPS). RAID-массивы.
Нормативно-правовое регулирование информационной безопасности в Кыргызской Республике (Закон «О кибербезопасности», Постановление КМ №746 и др.).
Цифровая гигиена сотрудника аварийно-спасательных служб: основные правила и рекомендации.
Критерии выставления зачёта
«Зачтено»: студент посетил не менее 70% занятий, имеет все конспекты, защитил презентацию, отвечает на вопросы, демонстрируя понимание базовых понятий и терминов.
«Не зачтено»: систематические пропуски, отсутствие конспектов или незащищённая презентация, неспособность ответить на базовые вопросы.

5.2. Темы курсовых работ (проектов)

Курсовые работы (проекты) учебным планом по дисциплине не предусмотрены. Основными формами самостоятельной работы являются ведение конспекта лекций и подготовка презентаций к практическим занятиям.
Написание эссе и рефератов не является обязательным и может использоваться как форма дополнительной (поощрительной) работы или по выбору студента. При выполнении письменной работы рекомендуется объём: эссе — 3–5 страниц, реферат — 10–15 страниц; оформление — по требованиям вуза; обязательны ссылки на нормативные акты Кыргызской Республики и список источников.

5.3. Фонд оценочных средств

«Зачтено» — студент посетил не менее 70% занятий, имеет все конспекты, защитил презентацию, отвечает на базовые вопросы; «Не зачтено» — систематические пропуски, отсутствие конспектов или незащищённая презентация, неспособность ответить на базовые вопросы.
Фонд оценочных средств по дисциплине оформлен в Приложении 1 к рабочей программе. В разделе приведены паспорт ФОС, перечень оценочных средств, критерии и шкалы оценивания. Контрольные вопросы и темы презентаций представлены в приложении

5.4. Перечень видов оценочных средств

Перечень видов оценочных средств:
Конспект лекций (текущий контроль).
Устный опрос (текущий контроль).
Защита презентации (текущий контроль).
Зачёт в форме собеседования (промежуточная аттестация).
Дополнительно могут использоваться эссе, рефераты и тестовые задания. Курсовые работы учебным планом не предусмотрены.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	Для освоения дисциплины используется лицензионное и свободно распространяемое программное обеспечение: операционная система Windows/Linux, офисный пакет Microsoft Office или LibreOffice (текстовый редактор, презентации, таблицы), браузер, PDF-просмотрщик, антивирус, архиватор, мультимедиа-плеер, а также LMS вуза (при наличии). Специализированное ПО для программирования не требуется.

6.3.2 Перечень информационных справочных систем и программного обеспечения

6.3.2.1	Для освоения дисциплины используются следующие профессиональные базы данных и информационные справочные системы: Централизованный банк данных правовой информации Минюста КР (cbd.minjust.gov.kg), информационно-правовая система «Токтом», официальные сайты МЧС КР (mchs.gov.kg), Национального статистического комитета КР (stat.gov.kg) и портал открытых данных (data.gov.kg), а также научно-образовательные ресурсы eLIBRARY.RU и ЭБС Znanium (при наличии доступа). Доступ к международным базам Scopus и Web of Science возможен при наличии подписки у вуза.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Для проведения лекций и практических занятий используется учебная аудитория, оснащённая мультимедийным проектором, экраном, доской и доступом в Интернет; компьютерный класс (при наличии) с лицензионным/свободно распространяемым ПО (операционная система, офисный пакет, браузер, PDF-просмотрщик, антивирус). Обеспечен доступ к библиотечному фонду, официальным правовым ресурсам КР, сайтам МЧС КР и Нацстаткома КР, научно-образовательным базам (eLIBRARY.RU, ЭБС Znanium — при наличии подписки). Имеются условия для проверки конспектов, защиты презентаций и проведения зачёта.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение дисциплины предполагает регулярное посещение лекций, ведение конспекта, подготовку и защиту презентации, изучение нормативных актов КР и подготовку к зачёту. Конспект проверяется на каждом практическом занятии; презентация должна содержать 12–15 слайдов, примеры и выводы. К зачёту допускаются студенты с посещаемостью не менее 70%, всеми конспектами и защищённой презентацией. Рекомендуется использовать учебное пособие Зимина И.В., официальные сайты МЧС КР, правовые базы КР и научные ресурсы, соблюдать академическую этику и цифровую гигиену.