Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет»

УТВЕРЖДАЮ
Первый проректор Белорусско-Российского университета
_____ Ю.В. Машин
31.08. 2023
Регистрационный № УД-200301/б.1.в.10/р

Информационные технологии в сфере обеспечения техносферной безопасности

(наименование дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 20.03.01 Техносферная безопасность

Направленность (профиль) Техносферная безопасность (общий профиль)

Квалификация Бакалавр

	Форма обучения
	Очная
Курс	3
Семестр	6
Лекции, часы	34
Лабораторные работы, часы	34
Зачёт, семестр	6
Контактная работа по учебным занятиям, часы	68
Самостоятельная работа, часы	40
Всего часов / зачетных единиц	108 / 3

Кафедра-разработчик программы: Автоматизированные системы управления
(название кафедры)

Составитель: Якимов А.И., д. т. н., доц.
(И.О. Фамилия, ученая степень, ученое звание)

Могилев, 2023

Рабочая программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 20.03.01 Техносферная безопасность № 680 от 25.05.2020 , учебным планом рег. № 200301-2.1 от 28.04.2023

Рассмотрена и рекомендована к утверждению кафедрой Автоматизированные системы управления
(название кафедры)
«_27_» ___06___2023 г., протокол № _11_.

Зав. кафедрой _____ А.И. Якимов

Одобрена и рекомендована к утверждению Научно-методическим советом Белорусско-Российского университета

«30» августа 2023 , протокол № 1.

Зам. председателя
Научно-методического совета _____ С.А. Сухоцкий

Рецензент:
заместитель директора по информационным технологиям филиала «Инженерный центр РУП «Могилевэнерго», канд.техн.наук Венберг А.В.
(И.О. Фамилия, должность, ученая степень, ученое звание рецензента)

Рабочая программа согласована:

Зав. кафедрой Техносферная безопасность и производственный дизайн_____ _____ А.В. Щур
(название выпускающей кафедры)

Ведущий библиотекарь О.С. Шушкова

Начальник учебно-методического отдела _____ О.Е. Печковская

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель учебной дисциплины

Цель преподавания дисциплины – формирование у студентов осознанного отношения к безопасности информационных технологий и развитие навыков применения безопасных практик в сфере техносферы.

1.2 Планируемые результаты изучения дисциплины

В результате освоения учебной дисциплины студент должен

знать:

- основные принципы и методы обеспечения безопасности информационных технологий в сфере техносферы;
- основные нормативные и правовые акты, регулирующие обеспечение безопасности информационных технологий в сфере техносферы;
- проблемы и угрозы, связанные с использованием информационных технологий, а также основные пути их предотвращения и минимизации;

уметь:

- разрабатывать и применять стратегии и политики безопасности информационных систем в сфере техносферы;
- реагировать на инциденты безопасности и проводить расследование инцидентов в сфере техносферы;

владеть:

- методами анализа и оценки уязвимостей информационных систем, а также методами контроля и мониторинга безопасности;
- навыками установки, настройки и обслуживания систем безопасности информационных технологий;
- навыками работы с современными информационными технологиями и средствами защиты информации.

1.3 Место учебной дисциплины в системе подготовки студента

Дисциплина относится к Блоку 1 "Дисциплины (модули)" (часть Блока 1, формируемая участниками образовательных отношений).

Перечень учебных дисциплин, изучаемых ранее, усвоение которых необходимо для изучения данной дисциплины:

- Информатика;
- Оценка геоэкологических рисков и основы национальной безопасности.

Перечень учебных дисциплин, которые будут опираться на данную дисциплину:

- Система организации охраны труда на производстве;
- Экспертиза и оценка условий труда.

Кроме того, результаты, полученные при изучении дисциплины на практических (вид занятий) занятиях будут применены при прохождении технологической (проектно-технологической) (название практики) практики, а также при подготовке выпускной квалификационной работы и дальнейшей профессиональной деятельности

1.4 Требования к освоению учебной дисциплины

Освоение данной учебной дисциплины должно обеспечивать формирование следующих компетенций:

Коды формируемых компетенций	Наименования формируемых компетенций
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.
ПК-9	Способен ориентироваться в основных проблемах техносферной безопасности.

2 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Вклад дисциплины в формирование результатов обучения выпускника (компетенций) и достижение обобщенных результатов обучения происходит путём освоения содержания обучения и достижения частных результатов обучения, описанных в данном разделе.

2.1 Содержание учебной дисциплины

Номер тем	Наименование тем	Содержание	Коды формируемых компетенций
1	Введение в геоинформационные системы	- Электронные карты и редактирование изображений - Формирование ГИС: программное обеспечение, технические требования - Примеры использования в техносферной безопасности	УК-8, ПК-9
2	Основы криптографии и защиты информации	- Основные принципы криптографии - Симметричное и асимметричное шифрование - Защита информации и алгоритмы шифрования	УК-8, ПК-9
3	Защита компьютерных сетей и информационных систем	- Основные угрозы безопасности компьютерных сетей - Методы и средства защиты сетей - Защита информационных систем от внешних атак	УК-8, ПК-9
4	Анализ и управление рисками в информационных технологиях	- Основные понятия и методы анализа рисков - Оценка уязвимостей и угроз информационных технологий - Стратегии управления рисками и их применение в сфере безопасности	УК-8, ПК-9
5	Этика и правовые аспекты в информационной безопасности	- Основы этики в сфере информационной безопасности - Законодательство и правовые нормы в области информационной безопасности - Этика и правовые аспекты при использовании информационных технологий	УК-8, ПК-9
6	Методы и технологии идентификации и аутентификации	- Основные методы идентификации и аутентификации пользователей - Биометрические методы идентификации - Технологии двухфакторной аутентификации	УК-8, ПК-9
7	Технологии обнаружения и предотвращения атак	- Системы обнаружения интранет-атак - Средства предотвращения атак на информационные системы - Методы анализа и реагирования на инциденты	УК-8, ПК-9
8	Управление информационной безопасностью в организациях	- Организация процесса управления информационной безопасностью - Планирование и внедрение системы управления информационной безопасностью - Нормативная база и стандарты в сфере управления информационной безопасностью	УК-8, ПК-9

2.2 Учебно-методическая карта учебной дисциплины

Итоговая оценка определяется в соответствии с таблицей:

Оценка	Зачтено	Не зачтено

№ недели	Лекции (наименование тем)	Часы	Лабораторные занятия	Часы	Самостоятельная работа часы	Форма контроля знаний	Баллы (max)
Модуль 1							
1	**Тема 1. Введение в геоинформационные системы.**	2	Л. р. № 1. Основы геоинформационных систем.	2	2		
2	**Тема 1. Введение в геоинформационные системы.**	2	Л. р. № 1. Основы геоинформационных систем.	2	2	ЗЛР	7
3	**Тема 2. Основы криптографии и защиты информации.**	2	Л. р. № 2. Криптография и защита информации.	2	2		
4	**Тема 2. Основы криптографии и защиты информации.**	2	Л. р. № 2. Криптография и защита информации.	2	2	ЗЛР	7
5	**Тема 3. Защита компьютерных сетей и информационных систем.**	2	Л. р. № 3. Сетевая безопасность.	2	2		
6	**Тема 3. Защита компьютерных сетей и информационных систем.**	2	Л. р. № 3. Сетевая безопасность.	2	2	ЗЛР	8
7	**Тема 4. Анализ и управление рисками в информационных технологиях.**	2	Л. р. № 4. Анализ угроз и рисков в сфере техносферной безопасности.	2	2	ЗЛР	8
8	**Тема 4. Анализ и управление рисками в информационных технологиях.**	2	Л. р. № 4. Анализ угроз и рисков в сфере техносферной безопасности.	2	2	ПКУ	30
Модуль 2							
9	**Тема 5. Этика и правовые аспекты в информационной безопасности.**	2	Л. р. № 5. Этические аспекты информационной безопасности.	2	2		
10	**Тема 5. Этика и правовые аспекты в информационной безопасности.**	2	Л. р. № 5. Этические аспекты информационной безопасности.	2	2	ЗЛР	7
11	**Тема 6. Методы и технологии идентификации и аутентификации.**	2	Л. р. № 6. Аутентификация и контроль доступа.	2	2		
12	**Тема 6. Методы и технологии идентификации и аутентификации.**	2	Л. р. № 6. Аутентификация и контроль доступа.	2	3	ЗЛР	7
13	**Тема 7. Технологии обнаружения и предотвращения атак.**	2	Л. р. № 7. Безопасность веб-приложений.	2	3		
14	**Тема 7. Технологии обнаружения и предотвращения атак.**	2	Л. р. № 7. Безопасность веб-приложений.	2	3	ЗЛР	8
15	**Тема 8. Управление информационной безопасностью в организациях.**	2	Л. р. № 8. Мониторинг и аудит информационной безопасности.	2	3		
16	**Тема 8. Управление информационной безопасностью в организациях.**	2	Л. р. № 8. Мониторинг и аудит информационной безопасности.	2	3	ЗЛР ТЕСТ	4 4
17	**Тема 8. Управление информационной безопасностью в организациях.**	2	Л. р. № 8. Мониторинг и аудит информационной безопасности.	2	3	ПКУ ПА (Зачет)	30 40
	Итого	**34**		**34**	**40**		**100**

Баллы	51-100	0-50

Принятые обозначения:
ЗЛР – защита лабораторной работы;
ПКУ – промежуточный контроль успеваемости;
ПА – промежуточная аттестация.
ТЕСТ – тестовое задание

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении дисциплины используется модульно-рейтинговая система оценки знаний студентов. Применение форм и методов проведения занятий при изучении различных тем курса представлено в таблице.

№ п/п	Форма проведения занятия	Вид аудиторных занятий		Всего часов
		Лекции	Лабораторные занятия	
1	Мультимедиа	Тема 1 – 8		34
2	С использованием ЭВМ		Л. р. 1 – Л. р. 8	34
	ИТОГО	34	34	68

4 ОЦЕНОЧНЫЕ СРЕДСТВА

Используемые оценочные средства по учебной дисциплине представлены в таблице и хранятся на кафедре.

№ п/п	Вид оценочных средств	Количество комплектов
1	Вопросы к зачету	1
2	Контрольные вопросы для защиты лабораторных работ	8
3	Тестовые задания для оценки знаний студентов	1

5 МЕТОДИКА И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ СТУДЕНТОВ

5.1 Уровни сформированности компетенций.

№ п/п	Уровни сформированности компетенции	Содержательное описание уровня	Результаты обучения
Компетенция УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.			
ИУК-8.9 Способен использовать современные информационные технологии для обеспечения безопасности на производстве и в непроизводственной сфере.			
1	Пороговый уровень	Понятие о техносфере, основных принципах криптографии, основных угрозах безопасности компьютерных сетей, основах этики в сфере информационной безопасности, основных методах идентификации и аутентификации пользователей.	Имеет представление о техносфер основных принципах криптографи основных угрозах безопасност компьютерных сетей, основах этики сфере информационной безопасност основных методах идентификации аутентификации пользователей.
2	Продвинутый уровень	Знает и понимает безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества.	Владеет методами анализа и оценки уязвимостей информационных систем, а также методами контроля и мониторинга безопасности.
3	Высокий уровень	Знает и понимает безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении	Владеет необходимыми навыками установки, настройки и обслуживания систем безопасности информационных технологий.

		чрезвычайных ситуаций и военных конфликтов.	
Компетенция ПК-9: Способен ориентироваться в основных проблемах техносферной безопасности.			
ИПК-9.4 Способен использовать в профессиональной деятельности информационные технологии в сфере обеспечения техносферной безопасности.			
1	Пороговый уровень	Минимальные требования о применении основных принципов и методов обеспечения безопасности информационных технологий в сфере техносферы.	Имеет представление о применении основных принципов и методов обеспечения безопасности информационных технологий в сфере техносферы.
2	Продвинутый уровень	Знает и понимает основные нормативные и правовые акты, регулирующие обеспечение безопасности информационных технологий в сфере техносферы, организацию процесса управления информационной безопасностью.	Владеет методами разработки и применения стратегии и политики безопасности информационных систем в сфере техносферы, реагирования на инциденты безопасности и проведения расследований инцидентов в сфере техносферы
3	Высокий уровень	Знает и понимает проблемы и угрозы, связанные с использованием информационных технологий, а также основные пути их предотвращения и минимизации.	Владеет необходимыми навыками работы с современными информационными технологиями и средствами защиты информации, с методами анализа и реагирования на инциденты.

5.2 Методика оценки знаний, умений и навыков студентов

Результаты обучения	Оценочные средства
Компетенция УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.	
Имеет представление о техносфере, основных принципах криптографии, основных угрозах безопасности компьютерных сетей, основах этики в сфере информационной безопасности, основных методах идентификации и аутентификации пользователей.	Контрольные вопросы к лабораторным работам. Вопросы к зачету. Тестовое задание
Владеет методами анализа и оценки уязвимостей информационных систем, а также методами контроля и мониторинга безопасности.	Контрольные вопросы к лабораторным работам. Вопросы к зачету. Тестовое задание
Владеет необходимыми навыками установки, настройки и обслуживания систем безопасности информационных технологий.	Контрольные вопросы к лабораторным работам. Вопросы к зачету. Тестовое задание
Компетенция ПК-9: Способен ориентироваться в основных проблемах техносферной безопасности.	
Имеет представление о применении основных принципов и методов обеспечения безопасности информационных технологий в сфере техносферы.	Контрольные вопросы к лабораторным работам. Вопросы к зачету. Тестовое задание
Владеет методами разработки и применения стратегии и политики безопасности информационных систем в сфере техносферы, реагирования на инциденты безопасности и проведения расследований инцидентов в сфере техносферы	Контрольные вопросы к лабораторным работам. Вопросы к зачету. Тестовое задание
Владеет необходимыми навыками работы с современными информационными технологиями и средствами защиты информации, с методами анализа и реагирования на инциденты.	Контрольные вопросы к лабораторным работам. Вопросы к зачету. Тестовое задание

5.3 Критерии оценки лабораторных работ

Каждая выполненная и защищенная лабораторная работа оценивается в диапазоне от 5 до 8 баллов. При этом 5 баллов начисляется за выполнение работы и 2 или 3 балла за оформление отчета и защиту работы в зависимости от качества оформления и уровня знаний студента по тематике работы. Если по окончанию модуля лабораторная работа выполнена, но не защищена, то баллы по ней не начисляются и она попадает в разряд задолженности.

5.4 Критерии оценки зачета

Допустимые погрешности и ошибки при определении учебных достижений студентов на зачетах:

Шкала соответствия	Уровень соответствия	Баллы	Количество ошибок, погрешности / несущественные / существенные
Соответствие	Высокий	40	0/0/0
		39	1/1/0
		38	2/1/1
		37	3/2/1
	Средний	36	5/2/1
		35	6/3/1
		34	6/4/1
		33	7/1/1
		32	7/2/1
		31	7/3/1
		30	7/4/1
		29	7/1/2
	Достаточный	28	7/2/1
		27	7/2/1
		26	7/3/1
		25	7/4/1
		24	4/1/2
		23	5/2/2
		22	6/3/2
		21	6/4/2
		20	6/5/2
		19	7/1/2
		18	7/2/2
		17	7/3/2
		16	7/4/2
	Минимально необходимый	15	7/4/3
Несоответствие	Низкий	<14	8/5/4

5.5 Критерии оценки тестовых заданий

Каждая выполненное тестовое задание оцениваются от 3 до 4 баллов. Критерием определения количества баллов является количество правильных ответов на тестовые вопросы, определяемое в процентах. За выполнение менее 50% тестовых вопросов баллы не начисляются и она попадает в разряд задолженности.

Баллы определяются по следующей формуле:

Балл (>50%) = (Макс. Балл) (%отв/100%) [Балл], где %отв – правильные ответы в процентах, 50% - допустимое значение правильных ответов, при котором итоговый рейтинг-контроль полагают успешным, Макс. Балл равен от 3 до 4 в зависимости от тестового задания.

6 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Самостоятельная работа студентов (СРС) направлена на закрепление и углубление освоения учебного материала, развитие практических умений. СРС включает следующие виды самостоятельной работы студентов:

- самостоятельное изучение материала по учебникам и другим источникам;
- тестирование по дисциплине;
- обзор литературы;
- проработка тем (вопросов), вынесенных на самостоятельное изучение;
- конспектирование учебной литературы;
- подготовка докладов;
- подготовка презентаций;
- подготовка к аудиторным занятиям;
- подготовка к сдаче зачета.

Контроль результатов внеаудиторной самостоятельной работы студентов осуществляется в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, проходит в письменной форме.

Критериями оценки результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умение студента использовать теоретические знания при выполнении практических, творческих заданий;
- обоснованность и четкость изложения ответа.

Перечень контрольных вопросов и заданий для самостоятельной работы студентов хранится на кафедре.

Для СРС рекомендуется использовать источники, приведенные в п. 7.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1 Основная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров
1	Информационная безопасность сетей и систем : учеб. пособие / В. И. Аверченков, В. Т. Еременко, Е. А. Зайченко. – Могилев : Белорус.-Рос. ун-т, 2020. – 212с	Рек. УМО по образованию в обл. информатики и радиоэлектроники в качестве учеб. пособия	66

7.2 Дополнительная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров
1	Петренко В. И. Защита персональных данных в информационных системах. Практикум : учеб, пособие / В. И. Петренко, И. В.Мандрица. – 3-е изд., стер. – СПб. ; М. ; Краснодар Лань, 2021. – 108с. : ил.	-	5

7.3 Перечень ресурсов сети Интернет по изучаемой дисциплине

1. Курсы на платформе Coursera по кибербезопасности и информационным технологиям.

2. Специализированные учебные материалы на сайте Cybersecurity and Infrastructure Security Agency (CISA).

3. Статьи и руководства на сайте OWASP (Open Web Application Security Project) по вопросам безопасности веб-приложений.

4. Вебинары и обучающие материалы от компании Kaspersky Lab, специализирующейся на кибербезопасности.

5. Ресурсы и материалы от SANS Institute, организации, занимающейся разработкой стандартов в области информационной безопасности.

6. Учебные материалы и курсы по кибербезопасности от компании Cisco.

7. Блог и статьи от The Electronic Frontier Foundation (EFF) по вопросам цифровых прав и информационной безопасности.

8. Материалы по кибербезопасности от Интерпола и других международных организаций.

9. Образовательные видеоролики и статьи от InfoSec Institute по тематике техносферной безопасности.

10. Книги и учебные пособия по информационным технологиям в сфере обеспечения безопасности, представленные на платформе Amazon.

7.4 Перечень наглядных и других пособий, методических рекомендаций по проведению учебных занятий, а также методических материалов к используемым в образовательном процессе техническим средствам

7.4.1 Методические рекомендации

1. Информационные технологии в сфере обеспечения техносферной безопасности [Электронный ресурс] : метод. рек. к лабораторным работам для студентов / сост. А. И. Якимов. – Могилев : Белорус.-Рос. ун-т, 2023.

7.4.2 Информационные технологии

Мультимедийные презентации по лекционному курсу:

Тема 1:

Введение в геоинформационные системы.

Тема 2:

Основы криптографии и защиты информации.

Тема 3:

Защита компьютерных сетей и информационных систем.

Тема 4:

Анализ и управление рисками в информационных технологиях.

Тема 5:

Этика и правовые аспекты в информационной безопасности.

Тема 6:

Методы и технологии идентификации и аутентификации.

Тема 7:

Технологии обнаружения и предотвращения атак.

Тема 8:

Управление информационной безопасностью в организациях.

7.4.3 Перечень программного обеспечения, используемого в образовательном процессе

1. MicrosoftOfficeProfessionalPlus2019 – текстовый процессор (Лицензия 74280727 от 17.01.2020 г.) (практические работы):

Л.р. № 1. Основы геоинформационных систем.

Л.р. № 2. Криптография и защита информации.

Л.р. № 3. Сетевая безопасность.

Л.р. № 4. Анализ угроз и рисков в сфере техносферной безопасности..
Л.р. № 5. Этические аспекты информационной безопасности.
Л.р. № 6. Аутентификация и контроль доступа.
Л.р. № 7. Безопасность веб-приложений.
Л.р. № 8. Мониторинг и аудит информационной безопасности.

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины содержится в паспорте лаборатории «Компьютерный класс кафедры АСУ», рег. № ПУЛ-4.416/2/-23.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ

(наименование дисциплины)

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Направление подготовки 20.03.01 Техносферная безопасность

Направленность (профиль) Охрана труда

	Форма обучения
	Очная (дневная)
Курс	3
Семестр	6
Лекции, часы	34
Лабораторные работы, часы	34
Зачёт, семестр	6
Контактная работа по учебным занятиям, часы	68
Самостоятельная работа, часы	40
Всего часов / зачетных единиц	108 / 3

1 Цель учебной дисциплины.

Формирование у студентов осознанного отношения к безопасности информационных технологий и развитие навыков применения безопасных практик в сфере техносферы.

2 Планируемые результаты изучения дисциплины.

В результате освоения учебной дисциплины студент должен

знать: основные принципы и методы обеспечения безопасности информационных технологий в сфере техносферы; основные нормативные и правовые акты, регулирующие обеспечение безопасности информационных технологий в сфере техносферы; проблемы и угрозы, связанные с использованием информационных технологий, а также основные пути их предотвращения и минимизации;

уметь: разрабатывать и применять стратегии и политики безопасности информационных систем в сфере техносферы; реагировать на инциденты безопасности и проводить расследование инцидентов в сфере техносферы;

владеть: методами анализа и оценки уязвимостей информационных систем, а также методами контроля и мониторинга безопасности; навыками установки, настройки и обслуживания систем безопасности информационных технологий; навыками работы с современными информационными технологиями и средствами защиты информации.

3. Требования к освоению учебной дисциплины.

Освоение данной учебной дисциплины должно обеспечивать формирование следующих компетенций: УК-8 - Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов, ПК-9 - Способен ориентироваться в основных проблемах техносферной безопасности.

4. Образовательные технологии.

Мультимедиа, с использованием ЭВМ.