

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра безопасности жизнедеятельности

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы


(подпись,

Кривуца З.Ф.
расшифровка подписи)

« 11 » июня 2024 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины (модуля)

**Б1.О.03 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ В
ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ»**

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки

20.04.01 Техносферная безопасность
(код и наименование направления подготовки)

профиль: Промышленная безопасность и охрана труда
(наименование направленности (профиля) образовательной программы)

Квалификация

магистр

Форма обучения

очная

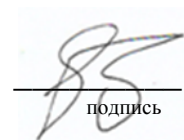
РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск, 2024

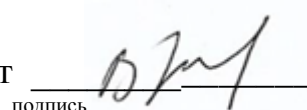
Рабочая программа дисциплины **«Информационные технологии и системы в техносферной безопасности»** составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) _____ по _____ направлению _____ подготовки _____
20.04.01 Техносферная безопасность
код и наименование направления подготовки

Программу составил(и):

Е.Н. Бояров, профессор, доктор педагогических наук, доцент
И.О. Фамилия, должность, ученая степень, ученое звание


подпись

В.В. Моисеев, доцент, кандидат технических наук, доцент
И.О. Фамилия, должность, ученая степень, ученое звание

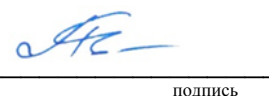

подпись

А.С. Ломов, доцент, кандидат педагогических наук
И.О. Фамилия, должность, ученая степень, ученое звание


подпись

Рабочая программа дисциплины **«Информационные технологии и системы в техносферной безопасности»** утверждена на заседании кафедры безопасности жизнедеятельности протокол № 13 от « 11 » июня 2024 г.

Заведующий кафедрой _____ Абрамова С.В. _____
фамилия, инициалы


подпись

1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля) – формирование у обучающихся представления о назначении и видах информационных систем и технологий в сфере техносферной безопасности, приобретение ими профессиональных теоретических знаний, практических навыков и умений самостоятельной работы использования методов системного анализа, моделирования, прогнозирования и применения современных информационно-вычислительных средств для решения задач, возникающих в условиях техносферы.

Задачи дисциплины (модуля):

- формирование представлений о современных средствах и достижениях информационных технологий в области безопасности;
- формирование профессиональных компетенций в области теоретического и практического использования информационных технологий в сфере обеспечения безопасности;
- освоение основных существующих современных компьютерных и информационных технологий, применяемых в области обеспечения экологической, производственной и промышленной безопасности;
- овладение способностью самостоятельно получать и структурировать знания в области безопасности, используя различные источники информации;
- формирование навыков самостоятельного научного поиска, моделирования, построения прогнозов, творческой постановки задачи и эффективного разрешения проблем в профессиональной деятельности с использованием современных методов и компьютерных технологий.

2. Место дисциплины (модуля) в структуре образовательной программы

Б1.О.03 «Информационные технологии и системы в техносферной безопасности», дисциплина (модуль) относится к базовой части блока 1 «Дисциплины (модули)» учебного плана.

Пререквизиты дисциплины (модуля): дисциплины, обязательные для предварительного изучения дисциплины: Специальная оценка условий труда и профессиональных рисков, Методология и методы научных исследований, Управление техносферной безопасностью на предприятии.

Постреквизиты дисциплины: дисциплины, в которых используется материал данной дисциплины: Мониторинг безопасности в организации, Системный анализ и моделирование в области безопасности.

3. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
УК-1	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выбирать стратегию действий	УК-1.1. знать: – методы критического анализа и оценки проблемных ситуаций на основе системного подхода; – методы решения проблемных ситуаций в научно-технической и производственной профессиональной практике. УК-1.2. уметь: – находить, критически анализировать и выбирать информацию, необходимую для выработки стратегии действий по разрешению проблемной

		<p>ситуации;</p> <ul style="list-style-type: none"> – определять и оценивать практические последствия реализации действий по разрешению проблемной ситуации; – получать новые знания на основе системного подхода; критически анализировать данные по сложным научным проблемам, относящимся к профессиональной области; – осуществлять поиск решений на основе научной методологии. <p>УК-1.3.</p> <p>владеть: – навыками критического анализа проблемных ситуаций на основе системного подхода и определения стратегии действий для достижения поставленной цели;</p> <ul style="list-style-type: none"> – навыками прогностической деятельности, позволяющей выстраивать стратегию исследований и практических решений; навыками эвристического анализа перспективных направлений науки и техники; – навыками стратегического планирования в различных областях профессиональной деятельности
ОПК-1	<p>Способен самостоятельно приобретать, структурировать и применять математические, естественнонаучные, социально-экономические и профессиональные знания в области техносферной безопасности, решать сложные и проблемные вопросы</p>	<p>ОПК-1.1.</p> <p>знать: основные принципы формирования научных знаний (математических, естественнонаучных, социально-экономических, профессиональных) с использованием современных интеллектуальных компьютерных технологий; общие принципы расчета основных систем обеспечения техносферной безопасности.</p> <p>ОПК-1.2.</p> <p>уметь: на практике применять научные знания (математические, естественнонаучные, социально-экономические, профессиональные) для решения вопросов техносферной безопасности; применять методики расчета основных систем обеспечения техносферной безопасности.</p> <p>ОПК-1.3.</p> <p>владеть: навыками решения сложных и проблемных вопросов в сфере техносферной безопасности, в том числе навыками проектирования и расчетов систем обеспечения техносферной безопасности.</p>
ПК-1	<p>Способен самостоятельно выполнять научные исследования в области</p>	<p>ПК-1.1.</p> <p>знать: – спектр научных проблем профессиональной области;</p>

	техносферной безопасности	<p>– современные методы и средства исследования безопасности человека в современном мире, формирования комфортной среды для деятельности человека в техносфере;</p> <p>– требования к управлению техногенным воздействием, сохранению жизни и здоровья человека за счет использования современных технических средств, методов научного исследования, контроля и прогнозирования;</p> <p>ПК-1.2.</p> <p>уметь: – планировать, обрабатывать, анализировать и обобщать результаты исследования, применять математическое и машинное моделирование, делать построение прогнозов в области техносферной безопасности;</p> <p>– формулировать цели и задачи научных исследований, направленных на повышение безопасности, применять современные методы, системы защиты человека и окружающей среды;</p> <p>– разрабатывать инновационные проекты в области безопасности, их реализовывать и внедрять;</p> <p>– разрабатывать и внедрять в производство рекомендации научно-исследовательских институтов и лабораторий по научной организации охраны труда и промышленной безопасности;</p> <p>ПК-1.3.</p> <p>владеть: навыками самостоятельного выполнения научных исследований в области безопасности, планирования экспериментов, обработки, анализа и обобщения результатов, их прогнозирования и моделирования.</p>
ПК-2	Способен оптимизировать методы и способы обеспечения безопасности человека от воздействия различных негативных факторов в техносфере	<p>ПК-2.1.</p> <p>знать: – принципы, методы, средства и способы обеспечения безопасности человека от воздействия различных негативных факторов в техносфере;</p> <p>– способы определения и прогнозирования зон повышенного техногенного риска и зон повышенного загрязнения;</p> <p>ПК-2.2.</p> <p>уметь: – идентифицировать зоны повышенного техногенного риска и зоны повышенного загрязнения;</p> <p>– выявлять производственные опасности, оценивать риск опасностей, документировать результаты оценки риска опасностей, разрабатывать мероприятия по устранению или снижению риска</p>

		<p>опасностей, контролировать опасности; – обеспечивать безопасность человека от воздействия различных негативных факторов в техносфере; ПК-2.3. владеть: – навыками оптимизации методов и способов обеспечения безопасности человека от воздействия различных негативных факторов в техносфере; – навыками прогнозирования зон повышенного техногенного риска и зон повышенного загрязнения; – навыками экономической оценки эффективности внедряемых инженерно-технических мероприятий по защите от негативных факторов в техносфере, направленных на обеспечение безопасности человека.</p>
--	--	--

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 4 зачетных единиц (144 академических часов).

Очная форма обучения

Вид работы	Трудоемкость, акад. часов	
	2 семестр	всего
Общая трудоемкость	144	144
Контактная работа:	26	26
Лекции (Лек)	10	10
Практические занятия (ПР)	12	12
Лабораторные работы (Лаб)	-	-
Контактная работа в период теоретического обучения (КонтТО) (<i>проведение текущих консультаций и индивидуальная работа со студентами</i>)	4	4
Промежуточная аттестация (зачет, экзамен, зачет с оценкой)	зачет	зачет
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - написание реферата (Р); - написание эссе (Э); - самостоятельное изучение разделов (перечислить); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - подготовка к практическим занятиям; - подготовка к коллоквиумам; - подготовка к промежуточной аттестации и т.п.)	118	118

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

Очная форма обучения

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)					Формы текущего контроля успеваемости, промежуточной аттестации
			контактная				
		семестр	Лекции	Практические занятия	Лабораторные занятия	Самостоятельн ая работа	
1	Раздел 1. Современные информационные системы, компьютерные и информационные технологии в сфере безопасности	2	2	2	0	17	дискуссия, реферативный практическое устный опрос тест, обзор, задание ...
2	Раздел 2. Информационные системы, базы данных и знаний в области обеспечения безопасности	2	2	2	0	17	беседа по вопросам, дискуссия, презентация; практическое задание устный опрос
3	Раздел 3. Системный анализ, математическое моделирование и прогнозирование в сфере безопасности	2	2	4	0	17	беседа по вопросам, дискуссия, презентация; практическое задание устный опрос
4	Раздел 4. Программные продукты, используемые в сфере безопасности природотехнических систем и комплексов, автоматизированные системы оценки и контроля состояния безопасности	2	4	4	0	18	беседа по вопросам, дискуссия, презентация; практическое задание устный опрос
	зачёт	2					итоговая тестовая работа / защита проекта / доклад-презентация и т.п.
	итоги:	2	16	16	0	36	

4.3. Содержание разделов дисциплины

Раздел 1. «Современные информационные системы, компьютерные и информационные технологии в сфере безопасности»

Тема 1. Вводная лекция.

Роль автоматизации в развитии общества. Информационные системы и технологии. Интегрирование процессов в области информационных технологий.

Тема 2. Компьютерные сети. Глобальные компьютерные сети в области безопасности человека и окружающей среды.

Понятие компьютерной сети. Сеть Интернет как источник информации по

проблемам безопасности человека и окружающей среды. Использование сети Интернет как источника обучения в области техносферной безопасности.

Раздел 2. «Информационные системы, базы данных и знаний в области обеспечения безопасности»

Тема 3. Базы и банки данных. Базы данных сети мониторинга техносферной безопасности.

База данных, система управления базами данных, банк данных и компоненты автоматизированного банка данных. Методы мониторинга промышленных объектов. Информационное обеспечение сети мониторинга техносферной безопасности.

Тема 4. Системы электронного документооборота (СЭД) в безопасности: основные понятия, назначение, стандарты и примеры внедрения.

Интеграция СЭД с другими приложениями. Особенности выбора и внедрения СЭД для решения задач в сфере безопасности.

Раздел 3. «Системный анализ, математическое моделирование и прогнозирование в сфере безопасности»

Тема 5. Применение программно-технических средств в решении практических задач обеспечения безопасности природно-технических систем и комплексов.

Преимущества и ограничения применения автоматизированных систем оценки и контроля состояния безопасности. Аппаратные средства реализации информационных процессов в сфере безопасности.

Тема 6. Интеллектуальные системы поддержки принятия решений в области техносферной безопасности.

Экспертные системы. Геоинформационные системы. Моделирование процессов управления. Формирование системы поддержки принятия управленческих решений. Системы на основе искусственного интеллекта.

Раздел 4. «Программные продукты, используемые в сфере безопасности природно-технических систем и комплексов, автоматизированные системы оценки и контроля состояния безопасности»

Тема 7. Основные программные продукты, предназначенные для обеспечения безопасности природно-технических систем и комплексов.

Применение программно-технических средств в решении практических задач обеспечения безопасности природно-технических систем и комплексов. Преимущества и ограничения применения автоматизированных систем оценки и контроля состояния безопасности.

Тема 8. Применение интегрированных пакетов в инженерных расчетах.

Использование специализированного программного обеспечения ТОКСИ+risk для оценки последствий аварий на опасных производственных объектах. Проведение расчетов.

4.4. Темы и планы практических/лабораторных занятий

Тема занятия	Вопросы для обсуждения и другие виды работ
Тема 1. Вводная лекция.	<ol style="list-style-type: none">1. Как автоматизация влияет на современные процессы управления? Проведите исследование, проанализируйте и представьте результаты.2. Какое значение имеют информационные системы в развитии общества? Обсудите в группе и подготовьте совместный отчет.3. В чем состоит роль интеграции процессов в ИТ? Подготовьте презентацию по этой теме.4. Какие преимущества приносит внедрение информационных технологий? Проведите SWOT-анализ преимуществ и недостатков.5. Как автоматизация изменила ключевые отрасли экономики? Проанализируйте конкретные примеры.6. Как ИТ способствуют улучшению безопасности? Подготовьте доклад с практическими примерами.

	<p>7. Какие виды информационных систем наиболее важны в современном мире? Составьте сравнительную таблицу.</p> <p>8. Как изменяются технологии по мере развития общества? Напишите эссе, опираясь на исторические данные.</p> <p>9. Какую роль играет автоматизация в повседневной жизни? Организуйте дебаты в классе.</p> <p>10. Какие факторы влияют на интеграцию ИТ в сфере безопасности? Подготовьте аналитическую статью.</p>
Тема 2. Компьютерные сети. Глобальные компьютерные сети в области безопасности человека и окружающей среды.	<p>1. Какие ключевые компоненты включает компьютерная сеть? Составьте схему и объясните ее работу.</p> <p>2. Как Интернет влияет на безопасность человека и окружающей среды? Обсудите и представьте доклад.</p> <p>3. В чем заключается роль Интернета в обучении в области безопасности? Проведите мини-исследование и сделайте презентацию.</p> <p>4. Какие угрозы существуют при использовании глобальных сетей? Проведите анализ угроз и представьте отчет.</p> <p>5. Как глобальные сети могут быть использованы для улучшения безопасности? Составьте сценарий решения одной из проблем.</p> <p>6. Какие меры предосторожности нужно соблюдать при работе в глобальных сетях? Проведите групповую работу и представьте рекомендации.</p> <p>7. Как развивается Интернет как источник информации? Напишите эссе на эту тему.</p> <p>8. Какие технологии способствуют повышению безопасности в глобальных сетях? Подготовьте доклад с примерами.</p> <p>9. Как можно интегрировать Интернет в систему безопасности компании? Проведите исследование и сделайте презентацию.</p> <p>10. Каковы основные принципы защиты данных в глобальных сетях? Составьте инструкцию по защите данных.</p>
Тема 3. Базы и банки данных. Базы данных сети мониторинга техносферной безопасности.	<p>1. Какие различия между базой данных и банком данных? Проведите сравнительный анализ.</p> <p>2. Какие компоненты входят в автоматизированный банк данных? Составьте схему с пояснением.</p> <p>3. Как используется система управления базами данных для мониторинга безопасности? Напишите реферат на эту тему.</p> <p>4. Какие методы мониторинга применяются на промышленных объектах? Проанализируйте конкретные примеры.</p> <p>5. Как осуществляется информационное обеспечение сети мониторинга? Подготовьте презентацию.</p> <p>6. Какие типы баз данных наиболее важны для обеспечения безопасности? Составьте сравнительную таблицу.</p> <p>7. Какова роль автоматизированных систем в контроле за безопасностью? Проведите исследование с практическими примерами.</p> <p>8. Как данные из банка данных могут помочь в управлении рисками? Напишите доклад по этой теме.</p> <p>9. Какие стандарты используются в системах управления базами данных? Подготовьте аналитический обзор.</p> <p>10. Как развивается технология управления базами данных? Напишите эссе, опираясь на современные тренды.</p>
Тема 4. Системы электронного документооборота (СЭД) в безопасности:	<p>1. Что такое СЭД и какие функции она выполняет? Подготовьте доклад с примерами внедрения.</p> <p>2. Какие стандарты используются при внедрении СЭД в сфере безопасности? Проведите исследование и представьте</p>

<p>основные понятия, назначение, стандарты и примеры внедрения.</p>	<p>результаты.</p> <p>3. Как СЭД интегрируется с другими системами? Составьте схему и поясните ее работу.</p> <p>4. Какие примеры успешного внедрения СЭД можно привести? Проанализируйте конкретные кейсы.</p> <p>5. Какие преимущества предоставляет использование СЭД в области безопасности? Проведите SWOT-анализ.</p> <p>6. Какие сложности могут возникнуть при внедрении СЭД? Подготовьте аналитическую статью с рекомендациями.</p> <p>7. Как СЭД помогает улучшить процесс управления документами? Напишите эссе на эту тему.</p> <p>8. Какие перспективы развития СЭД в будущем? Подготовьте презентацию с прогнозами.</p> <p>9. Как интеграция СЭД может повлиять на общую безопасность компании? Проведите исследование с примерами.</p> <p>10. Какие требования к защите данных необходимо учитывать при внедрении СЭД? Составьте инструкцию по защите данных.</p>
<p>Тема 5. Применение программно-технических средств в решении практических задач обеспечения безопасности природно-технических систем и комплексов.</p>	<p>1. Какие программно-технические средства применяются для мониторинга безопасности? Проведите исследование и представьте отчет.</p> <p>2. В чем заключаются основные преимущества автоматизированных систем оценки состояния безопасности? Подготовьте аналитический доклад.</p> <p>3. Какие ограничения существуют при использовании автоматизированных систем в сфере безопасности? Проведите групповой анализ и представьте презентацию.</p> <p>4. Как применяются аппаратные средства в информационных процессах безопасности? Проанализируйте конкретные примеры.</p> <p>5. Какие задачи решаются с помощью автоматизированных систем безопасности на промышленных объектах? Напишите доклад с практическими примерами.</p> <p>6. Какие программные продукты применяются для оценки состояния природно-технических комплексов? Проведите исследование и подготовьте презентацию.</p> <p>7. Какие технологии позволяют повысить точность оценки состояния безопасности? Напишите статью на эту тему.</p> <p>8. Какие примеры успешного применения программно-технических средств можно привести? Проанализируйте конкретные кейсы.</p> <p>9. Как автоматизированные системы контроля безопасности помогают предотвращать аварии? Подготовьте сценарий аварийной ситуации и решение с использованием систем.</p> <p>10. Какие нормативные документы регламентируют использование программно-технических средств в сфере безопасности? Проведите анализ стандартов и представьте результаты.</p>
<p>Тема 6. Интеллектуальные системы поддержки принятия решений в области техносферной безопасности.</p>	<p>1. Что такое интеллектуальная система поддержки принятия решений? Подготовьте доклад с примерами использования.</p> <p>2. Как экспертные системы помогают в принятии решений в области безопасности? Напишите исследовательскую работу.</p> <p>3. Какие задачи решают геоинформационные системы (ГИС) в сфере безопасности? Проведите исследование и сделайте презентацию.</p> <p>4. Как моделирование процессов управления помогает улучшить безопасность? Подготовьте аналитический отчет.</p>

	<p>5. Какие технологии лежат в основе современных интеллектуальных систем поддержки решений? Проанализируйте и представьте результаты в виде доклада.</p> <p>6. Как использование ГИС помогает в прогнозировании аварий и чрезвычайных ситуаций? Напишите статью с примерами.</p> <p>7. Какие преимущества дает использование экспертных систем для оценки рисков? Проведите исследование с анализом данных.</p> <p>8. Как интеллектуальные системы могут быть интегрированы в систему управления предприятия? Подготовьте сценарий интеграции.</p> <p>9. Какие примеры успешного использования ГИС в области безопасности существуют? Проанализируйте конкретные примеры.</p> <p>10. Какие перспективы развития интеллектуальных систем поддержки принятия решений можно ожидать? Напишите прогноз на ближайшие 5 лет.</p>
Тема 7. Основные программные продукты, предназначенные для обеспечения безопасности природно-технических систем и комплексов.	<p>1. Какие программные продукты используются для обеспечения безопасности природно-технических систем? Подготовьте обзор с примерами.</p> <p>2. Какие задачи решают автоматизированные системы в сфере безопасности? Проанализируйте на примере конкретных программных решений.</p> <p>3. Какие преимущества имеют специализированные программные продукты перед универсальными? Подготовьте сравнительную таблицу.</p> <p>4. Как программно-технические средства могут снизить риски на производстве? Проведите исследование и представьте доклад.</p> <p>5. Как автоматизированные системы могут помочь в решении задач экологической безопасности? Напишите аналитическую статью.</p> <p>6. Какие примеры успешного использования программных продуктов для обеспечения безопасности можно привести? Подготовьте презентацию.</p> <p>7. Как осуществляется оценка последствий аварий с помощью специализированного ПО? Проведите практическое задание на основе выбранного ПО.</p> <p>8. Какие ограничения существуют при использовании автоматизированных систем безопасности? Проведите групповой анализ и представьте результаты.</p> <p>9. Как можно интегрировать программные продукты для безопасности в систему управления предприятием? Подготовьте проект интеграции.</p> <p>10. Каковы ключевые тенденции в развитии программных продуктов для обеспечения безопасности? Напишите исследовательский прогноз.</p>
Тема 8. Применение интегрированных пакетов в инженерных расчетах.	<p>1. Какие интегрированные пакеты применяются для инженерных расчетов в сфере безопасности? Подготовьте обзор программного обеспечения.</p> <p>2. Как программное обеспечение ТОКСИ+risk используется для оценки последствий аварий? Проведите исследование и представьте его результаты.</p> <p>3. Как интегрированные пакеты помогают в проведении расчетов безопасности? Проведите практическую работу с примером расчета.</p> <p>4. Какие задачи решаются с помощью интегрированных</p>

	<p>инженерных пакетов? Подготовьте доклад с примерами.</p> <p>5. Какие преимущества имеют специализированные программы для инженерных расчетов перед общими программными решениями? Проведите сравнительный анализ.</p> <p>6. Какие примеры успешного использования интегрированных пакетов для расчетов в безопасности можно привести? Подготовьте аналитический отчет.</p> <p>7. Как интегрированные пакеты способствуют улучшению прогнозирования аварийных ситуаций? Проведите исследование с практическими примерами.</p> <p>8. Какие нормативные требования предъявляются к использованию программного обеспечения для инженерных расчетов в сфере безопасности? Проведите анализ стандартов.</p> <p>9. Каковы ограничения применения интегрированных пакетов для расчетов в техносферной безопасности? Напишите аналитическую статью.</p> <p>10. Как развиваются технологии инженерных расчетов в области безопасности? Подготовьте исследовательскую статью с прогнозами.</p>
--	---

4.5. Примерная тематика курсовых проектов (курсовых работ)

не планировалось

5. Темы дисциплины (модуля) для самостоятельного изучения

Вопросы для самоконтроля: не представлено

6. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине **«Информационные технологии и системы в техносферной безопасности»** используются различные образовательные технологии:

1. Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

2. Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений, обеспечивающих возможность качественно выполнять профессиональную деятельность.

3. Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения.

Используются виды проблемного обучения: освещение основных вопросов дисциплины на лекциях, учебные дискуссии, коллективная мыслительная деятельность в группах при выполнении групповых заданий, решение ситуационных задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель лишь создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

4. Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в

учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при сдаче коллоквиумов, при выполнении домашних индивидуальных заданий.

Для целенаправленного и эффективного формирования запланированных компетенций у обучающихся, выбраны следующие сочетания форм организации учебного процесса и методов активизации образовательной деятельности.

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Современные информационные системы, компьютерные и информационные технологии в сфере безопасности	Лекция 1 Семинар 1 Самостоятельная работа	ИКТ с использованием видеоматериалов Развернутая беседа с обсуждением доклада Консультирование и проверка домашних заданий посредством электронной почты
2.	Информационные системы, базы данных и знаний в области обеспечения безопасности	Лекция 2 Семинар 2 Самостоятельная работа	ИКТ с использованием видеоматериалов Развернутая беседа с обсуждением доклада Консультирование и проверка домашних заданий посредством электронной почты
3.	Системный анализ, математическое моделирование и прогнозирование в сфере безопасности	Лекция 3 Семинар 3,4. Самостоятельная работа	ИКТ с использованием видеоматериалов Развернутая беседа с обсуждением доклада Консультирование и проверка домашних заданий посредством электронной почты
4.	Программные продукты, используемые в сфере безопасности природно-технических систем и комплексов	Лекция 4,5 Семинар 5,6 Самостоятельная работа	ИКТ с использованием видеоматериалов Развернутая беседа с обсуждением доклада Консультирование и проверка домашних заданий посредством электронной почты

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Текущая самостоятельная работа (СРС)

Текущая самостоятельная работа по дисциплине «Информационные технологии и системы в техносферной безопасности», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- изучение тем, вынесенных на самостоятельную проработку;
- подготовка к практическим занятиям;
- выполнение домашних индивидуальных заданий;
- подготовка к практическим занятиям;
- подготовка к самостоятельным и контрольным работам;
- подготовка к зачету.

7.2. Темы индивидуальных домашних заданий: долгосрочное задание (подготовка доклада) по два студента на тему:

1. Роль автоматизации в повышении уровня безопасности на промышленных объектах.

Подготовьте доклад с анализом конкретных примеров внедрения автоматизации на производственных площадках.

2. Влияние глобальных компьютерных сетей на обеспечение безопасности информационных систем.

Исследуйте, как глобальные сети способствуют развитию и защите информационных систем.

3. Информационные технологии в прогнозировании и предотвращении чрезвычайных ситуаций.

Подготовьте обзор существующих технологий и их возможностей в сфере прогнозирования рисков.

4. Использование геоинформационных систем для повышения техносферной безопасности.

Проанализируйте примеры использования ГИС в управлении безопасностью территорий.

5. Интеллектуальные системы поддержки принятия решений в управлении техносферной безопасностью.

Исследуйте внедрение и практическое применение таких систем в различных отраслях.

6. Современные базы данных для мониторинга техносферной безопасности: примеры и перспективы.

Составьте обзор современных решений для мониторинга безопасности и их внедрения.

7. Системы электронного документооборота (СЭД) в обеспечении безопасности: примеры и эффективность.

Оцените преимущества внедрения СЭД в компаниях, ориентированных на безопасность.

8. Автоматизированные системы контроля и оценки состояния природно-технических систем.

Проведите анализ возможностей и ограничений таких систем на реальных примерах.

9. Программно-технические средства для оценки последствий аварий на опасных производственных объектах.

Исследуйте применение специализированного ПО для анализа и предотвращения последствий аварий.

10. Роль математического моделирования в управлении рисками и прогнозировании аварий.

Оцените значимость и возможности математических моделей в управлении аварийными ситуациями.

11. Использование Интернет-технологий для обучения и повышения осведомленности в области техносферной безопасности.

Проанализируйте различные платформы и интернет-ресурсы, используемые для обучения в данной сфере.

12. Интеграция информационных систем в управление техносферной безопасностью.

Исследуйте преимущества интеграции различных информационных систем для повышения уровня безопасности.

13. Разработка систем поддержки принятия управленческих решений в условиях чрезвычайных ситуаций.

Оцените существующие решения и предложите рекомендации по их улучшению.

14. Использование автоматизированных систем для мониторинга состояния окружающей среды и экологической безопасности.

Проанализируйте возможности использования автоматизированных систем в этой сфере.

15. Внедрение искусственного интеллекта в системы управления безопасностью

на промышленных предприятиях.

Исследуйте примеры использования ИИ для повышения безопасности на промышленных объектах.

16. Программные продукты для анализа аварийных ситуаций: особенности применения и перспективы развития.

Составьте обзор современных программных решений для анализа и моделирования аварий.

17. Роль больших данных (Big Data) в управлении техносферной безопасностью.

Проанализируйте, как использование больших данных помогает в управлении рисками и прогнозировании чрезвычайных ситуаций.

18. Интегрированные системы мониторинга и их роль в предотвращении промышленных аварий.

Исследуйте примеры внедрения интегрированных систем и их влияние на снижение аварийности.

19. Обеспечение информационной безопасности в условиях цифровой трансформации предприятий.

Проанализируйте, как цифровая трансформация влияет на риски в области информационной безопасности и методы их снижения.

20. Использование программно-аппаратных средств для обеспечения безопасности в энергетической отрасли.

Исследуйте, как программно-аппаратные средства применяются для повышения безопасности на энергетических объектах.

7.3. Контроль самостоятельной работы:

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя. Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

Темы рефератов и докладов:

1. История развития информационных технологий и их влияние на безопасность общества.

2. Роль автоматизированных систем в управлении безопасностью промышленных объектов.

3. Современные подходы к защите информации в глобальных компьютерных сетях.

4. Использование искусственного интеллекта в системах мониторинга техносферной безопасности.

5. Геоинформационные системы и их роль в управлении чрезвычайными ситуациями.

6. Технологии больших данных (Big Data) в управлении техносферной безопасностью.

7. Программные продукты для оценки последствий техногенных аварий.

8. Интеллектуальные системы поддержки принятия решений в условиях чрезвычайных ситуаций.

9. Современные подходы к кибербезопасности на промышленных объектах.

10. Системы электронного документооборота (СЭД) в сфере безопасности: преимущества и вызовы.

11. Использование облачных технологий для обеспечения информационной

безопасности.

12. Роль Интернет-технологий в образовании и повышении осведомленности о техносферной безопасности.
13. Автоматизация процессов контроля и оценки состояния промышленных объектов.
14. Экспертные системы в управлении рисками на опасных производственных объектах.
15. Математическое моделирование аварий и чрезвычайных ситуаций.
16. Влияние цифровой трансформации на безопасность корпоративных информационных систем.
17. Интеграция систем мониторинга для управления безопасностью природно-технических комплексов.
18. Обеспечение информационной безопасности в эпоху цифровой экономики.
19. Применение виртуальной и дополненной реальности для обучения в сфере безопасности.
20. Технологии предотвращения и ликвидации последствий аварий на опасных производственных объектах.

7.4. Вопросы к зачету по дисциплине «Информационные технологии и системы в техносферной безопасности»:

1. Основные этапы развития информационных технологий и их влияние на безопасность.
2. Роль автоматизированных систем в управлении безопасностью промышленных объектов.
3. Ключевые компоненты компьютерных сетей и их значение для обеспечения безопасности.
4. Система управления базами данных (СУБД) и ее применение в мониторинге безопасности.
5. Геоинформационные системы (ГИС) для повышения безопасности природно-технических систем.
6. Преимущества автоматизированных систем мониторинга техносферной безопасности.
7. Функции системы электронного документооборота (СЭД) в обеспечении безопасности.
8. Математическое моделирование для прогнозирования аварий и управления рисками.
9. Программные продукты для оценки последствий аварий на опасных производственных объектах.
10. Интеллектуальные системы поддержки принятия решений в управлении безопасностью.
11. Основные угрозы кибербезопасности в глобальных сетях.
12. Подходы к обеспечению информационной безопасности в условиях цифровой экономики.
13. Задачи больших данных (Big Data) в управлении техносферной безопасностью.
14. Методы защиты информации в сетях Интернет.
15. Технологии мониторинга состояния окружающей среды.
16. Программно-технические средства контроля безопасности на предприятиях.
17. Преимущества интеграции информационных систем для повышения уровня безопасности.
18. Экспертные системы и их использование для управления рисками.
19. Использование виртуальной реальности для обучения в сфере безопасности.
20. Нормативные акты, регулирующие использование автоматизированных систем оценки безопасности.
21. Применение интернет-технологий для обучения и повышения осведомленности в техносферной безопасности.

22. Меры предосторожности в глобальных компьютерных сетях для обеспечения безопасности.
23. Влияние цифровой трансформации на управление информационной безопасностью предприятий.
24. Методы предотвращения аварий на опасных производственных объектах.
25. Развитие технологий управления базами данных в сфере безопасности.
26. Особенности использования облачных технологий для защиты данных.
27. Программно-аппаратные средства для мониторинга безопасности на энергетических объектах.
28. Перспективы развития интеллектуальных систем поддержки принятия решений в техносферной безопасности.
29. Автоматизированные системы в управлении чрезвычайными ситуациями на производстве.
30. Применение искусственного интеллекта в системах безопасности.

7.5. Тематика заданий для самостоятельной работы студентов

Раздел 1: Современные информационные системы, компьютерные и информационные технологии в сфере безопасности

1. Исследование роли автоматизированных систем в управлении безопасностью на производственных объектах.
2. Подготовка отчета о применении информационных систем для повышения безопасности в организациях.
3. Изучение методов защиты информации в глобальных компьютерных сетях.
4. Разработка проекта по интеграции информационных технологий в систему управления безопасностью.
5. Анализ преимуществ облачных технологий для обеспечения информационной безопасности.
6. Сравнение различных систем мониторинга безопасности, основанных на современных ИТ-решениях.
7. Разработка презентации о применении информационных технологий для предотвращения киберугроз.
8. Проведение исследования о роли Интернета вещей (IoT) в повышении безопасности объектов.
9. Подготовка обзора существующих стандартов в области информационных технологий для безопасности.
10. Разработка сценария применения ИТ-систем для управления безопасностью в реальных условиях.

Раздел 2: Информационные системы, базы данных и знаний в области обеспечения безопасности

1. Исследование роли баз данных для мониторинга безопасности промышленных объектов.
2. Подготовка доклада о применении систем управления базами данных (СУБД) для обеспечения безопасности.
3. Сравнительный анализ различных типов баз данных и их применение для мониторинга рисков.
4. Разработка модели базы данных для системы мониторинга техносферной безопасности.
5. Анализ методов управления большими данными в сфере безопасности.
6. Исследование особенностей автоматизированных банков данных и их роли в обеспечении безопасности.
7. Изучение применения систем управления базами данных для прогнозирования аварийных ситуаций.
8. Разработка сценария по использованию баз данных в системах техносферной безопасности.

9. Подготовка обзора существующих программных продуктов для создания баз данных в сфере безопасности.

10. Исследование перспектив развития баз данных для повышения уровня безопасности.

Раздел 3: Системный анализ, математическое моделирование и прогнозирование в сфере безопасности

1. Разработка математической модели для оценки рисков аварий на опасных производственных объектах.

2. Исследование применения системного анализа для прогнозирования техногенных аварий.

3. Подготовка доклада о методах математического моделирования процессов управления безопасностью.

4. Разработка проекта по применению системного анализа для мониторинга техносферных объектов.

5. Анализ использования геоинформационных систем (ГИС) для оценки состояния безопасности.

6. Изучение методов прогнозирования последствий аварий с применением математических моделей.

7. Разработка сценария использования системного анализа в управлении рисками предприятия.

8. Подготовка отчета о примерах успешного применения математического моделирования в безопасности.

9. Изучение технологий, применяемых для моделирования и анализа аварийных ситуаций.

10. Проведение анализа различных подходов к прогнозированию и их эффективности в обеспечении безопасности.

Раздел 4: Программные продукты, используемые в сфере безопасности природно-технических систем и комплексов, автоматизированные системы оценки и контроля состояния безопасности

1. Подготовка обзора существующих программных продуктов для оценки состояния природно-технических систем.

2. Исследование программно-технических средств для мониторинга состояния безопасности на опасных объектах.

3. Сравнение различных автоматизированных систем оценки и контроля состояния безопасности на предприятиях.

4. Разработка проекта по внедрению автоматизированной системы мониторинга на производстве.

5. Анализ возможностей использования программных продуктов для прогнозирования аварий на промышленных объектах.

6. Изучение программных решений для оценки рисков и последствий техногенных катастроф.

7. Разработка сценария применения программного обеспечения для предотвращения аварийных ситуаций.

8. Подготовка презентации о ключевых функциях автоматизированных систем контроля состояния безопасности.

9. Анализ преимуществ и недостатков существующих автоматизированных систем оценки техносферных рисков.

10. Исследование перспектив развития программного обеспечения для контроля и управления безопасностью природно-технических комплексов.

Вариант тестового задания

1. Какая основная задача интеграции информационных систем в обеспечении безопасности?

а) Упрощение процессов хранения данных

б) Повышение эффективности управления рисками и угрозами

- в) Оптимизация маркетинговых стратегий
 - г) Снижение затрат на информационные технологии
2. Каковы основные преимущества использования больших данных (Big Data) в области безопасности?
- а) Сокращение времени на обработку инцидентов
 - б) Улучшение прогноза рисков и повышение точности анализа угроз
 - в) Автоматизация процессов управления данными
 - г) Повышение скорости передачи данных в сетях
3. Какие методы наиболее часто используются для обеспечения кибербезопасности?
- а) Методы анализа угроз и шифрование
 - б) Визуализация данных и машинное обучение
 - в) Виртуальная реальность и блокчейн
 - г) Автоматизация документооборота и управление проектами
4. Какую роль играют геоинформационные системы (ГИС) в управлении техносферной безопасностью?
- а) Мониторинг экологических параметров и пространственное моделирование
 - б) Управление финансами на предприятиях
 - в) Анализ бизнес-процессов и оптимизация цепочек поставок
 - г) Управление документооборотом в компаниях
5. Какие системы лучше всего подходят для управления аварийными ситуациями на опасных производственных объектах?
- а) Автоматизированные системы управления предприятием (ERP)
 - б) Интеллектуальные системы поддержки принятия решений (СППР)
 - в) CRM-системы для работы с клиентами
 - г) Системы управления проектами (PMS)
6. Какие ключевые компоненты включает система управления базами данных (СУБД) в сфере безопасности?
- а) Ядро СУБД, хранилище данных, клиентские приложения
 - б) Сеть Интернет, сервисы мониторинга, защитные экраны
 - в) Маркетинговая стратегия, корпоративные структуры, процессы аудита
 - г) Физическая инфраструктура, локальные сети, операционные системы
7. Каковы основные подходы к прогнозированию чрезвычайных ситуаций с использованием математических моделей?
- а) Моделирование на основе исторических данных и вероятностный анализ
 - б) Машинное обучение и нейронные сети
 - в) Визуализация данных и анализ рынка
 - г) Креативное мышление и интуитивное моделирование
8. Какие ограничения могут возникнуть при внедрении автоматизированных систем мониторинга безопасности?
- а) Высокие затраты на первоначальную настройку и интеграцию
 - б) Ограниченные возможности для визуализации данных
 - в) Отсутствие необходимости в обучении персонала
 - г) Упрощенная передача данных между подразделениями
9. Как искусственный интеллект может применяться в управлении техносферной безопасностью?
- а) Для разработки маркетинговых стратегий и анализа потребительских данных
 - б) Для мониторинга и анализа данных о потенциальных угрозах и рисках
 - в) Для создания финансовых отчетов и бухгалтерского учета
 - г) Для повышения скорости передачи данных в сетевых системах
10. Что такое риск-ориентированный подход в управлении безопасностью?
- а) Управление инцидентами и аварийными ситуациями на основе прогнозируемых рисков
 - б) Автоматизация всех процессов управления на предприятии
 - в) Организация документооборота с минимальным вмешательством человека

- г) Повышение рентабельности за счет оптимизации бизнес-процессов
11. Какие технологии наиболее эффективны для защиты информации в сетях?
(Выберите два правильных варианта)
- а) Шифрование данных
 - б) Виртуальная реальность
 - в) Блокчейн
 - г) Программные решения для анализа продаж
12. Какие элементы входят в состав системы интеллектуальной поддержки принятия решений?
(Выберите два правильных варианта)
- а) Модуль сбора данных
 - б) Модуль управления финансовыми транзакциями
 - в) База знаний
 - г) Маркетинговый блок
13. Какие методы используются для анализа угроз в системах информационной безопасности?
(Выберите три правильных варианта)
- а) Оценка уязвимостей
 - б) Мониторинг данных в реальном времени
 - в) Создание отчетов о продажах
 - г) Поведенческий анализ
14. Какие программные продукты применяются для моделирования чрезвычайных ситуаций?
(Выберите два правильных варианта)
- а) ТОКСИ+risk
 - б) Microsoft Excel
 - в) ArcGIS
 - г) Google Docs
15. Какие факторы влияют на выбор программного обеспечения для управления безопасностью?
(Выберите три правильных варианта)
- а) Стоимость внедрения и обслуживания
 - б) Возможности интеграции с другими системами
 - в) Удобство интерфейса для пользователя
 - г) Способности для автоматизации бизнес-процессов
16. Программные продукты для оценки последствий аварий на предприятиях предназначены только для использования в реальном времени.
- а) Да
 - б) Нет
17. Математическое моделирование используется для прогнозирования рисков в системе управления безопасностью.
- а) Да
 - б) Нет
18. Интеллектуальные системы поддержки принятия решений не могут использовать данные из геоинформационных систем (ГИС).
- а) Да
 - б) Нет
19. Какие риски может помочь предотвратить интеграция автоматизированных систем контроля состояния безопасности?
- а) Финансовые риски
 - б) Экологические риски
 - в) Риски отказа оборудования и аварийных ситуаций
 - г) Риски кадрового дефицита
20. Что является основной функцией баз данных в системе мониторинга техносферной безопасности?

- а) Управление финансовыми потоками
- б) Сбор, хранение и обработка данных о состоянии объектов
- в) Оптимизация производства
- г) Разработка рекламных стратегий

8. Система оценивания планируемых результатов обучения

Контроль за академической успеваемостью студента на протяжении всего периода обучения в СахГУ строится на основе балльно-рейтинговой системы оценки знаний, умений и навыков студента. При успешном овладении учебной дисциплиной студент получает определенное количество баллов. Баллы, заработанные студентом по каждой учебной дисциплине, суммируются и образуют рейтинг студента на любом этапе обучения в университете.

Оценка качества освоения основной профессиональной образовательной программы включает текущий контроль успеваемости (контрольную проверку по темам учебной дисциплины) студента, промежуточную аттестацию по учебной дисциплине и итоговую государственную аттестацию выпускника.

Аттестация по учебной дисциплине проводится в форме экзамена / зачета.

100 баллов – это максимальное количество баллов, которое может заработать студент за семестр. В связи с этим устанавливается минимальное и максимальное количество баллов, которое может быть заработано студентом.

Самостоятельная работа студента	Кол-во баллов минимум	Кол-во баллов максимум
Тестовый контроль	4	20
Реферат, эссе	2	5
Решение казусов или другой вид работы студентов	20	40
Опрос	26	50
Итого	52	100

Максимальное количество баллов за семестр – 100 баллов. При этом:

- менее 52 баллов – неудовлетворительно / не зачтено;
- 52–69 баллов – удовлетворительно;
- 70–84 балла – хорошо;
- 85–100 баллов – отлично.

Зачет определяется на основе суммы баллов, полученных по всем разделам по результатам самостоятельной работы при условии, что студент по каждому виду набрал количество баллов не менее зачетного минимума. Студент получает оценку за экзамен, если сумма баллов составит 52 и более.

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

Белов П.Г. Системный анализ и моделирование опасных процессов в техносфере
https://www.studmed.ru/belov-pg-sistemnyy-analiz-i-modelirovanie-opasnyh-processov-v-tehnosfere_c9bfaa27883.html

Гаврилин И. И. Информационные технологии в техносферной безопасности : метод. рекомендации по организации самостоятельной работы / И. И. Гаврилин, С. О. Белинский. – Екатеринбург : УрГУПС, 2016. – 41, [3] с.

Конопелько Л.А., Растоскуев В.В., Кустикова М.А., Банарь С.А., Быковская Е.А., Маюрова А.С. Математическое моделирование в техносферной безопасности: [Учебно-методическое пособие] / Рецензент: Пинчук О.А. - Санкт-Петербург: Университет ИТМО, 2018. - 65 с.

Балюк А.А. Системный анализ и моделирование процессов в техносфере https://www.studmed.ru/balyuk-a-a-sistemnyy-analiz-i-modelirovanie-processov-v-tehnosfere_8fb6c6d4a2c.html

Северцев Н.А., Дедков В.К. Системный анализ и моделирование безопасности. Учеб. пособие. – М.: Высшая школа, 2006. – 462 с. – https://www.studmed.ru/severcev-na-dedkov-vk-sistemnyy-analiz-i-modelirovanie-bezopasnosti_a145b435aff.html

Аварии и катастрофы: предупреждение и ликвидация последствий / В.А. Котляревский и др. – М.: Ассоциация, 1995. – 320 с.

Белов П. Г. Моделирование опасных процессов в техносфере. – М.: Изд-во АГЗ МЧС, 1999. – 124 с.

Белов П. Г. Теоретические основы системной инженерии безопасности. – М.: ГПНТБ «Безопасность», 1996 – 426 с.

Браун Д.Б. Анализ и разработка систем обеспечения техники безопасности: Пер. с англ. – М.: Машиностроение, 1979. – 359 с.

Введение в математическое моделирование / Под ред. П. В.Трусова. М.: Интермет инжиниринг, 2000. — 336 с. 4

Вентцель Е. С. Исследование операций. Задачи, принципы, методология. – М.: Наука, 1980. – 208 с.

Гайкович А.И. Основы теории проектирования сложных технических систем. 2001. 432 с.

Научно-методические аспекты анализа аварийного риска // В. Г. Горский, Г.А. Моткин, В.А. Петрунин, Г.Ф. Терещенко и Др. – М.: Экономика и информатика, 2002. – 320 с.

ГОСТ 11.005-74. Правила определения оценок и доверительных границ для параметров экспоненциального распределения и распределения Пуассона. – М.: Изд-во стандартов, 1974. с.

Губинский А. И. Надежность и качество функционирования эргатических систем. Наука, 1982. – 270 с.

Дюбуа Д., Прад А. Теория возможностей // Приложения к представлению знаний в информатике: Пер. с франц. – М.: Радио и связь, 1990. – 288 с.

Рахимова, Н. Н. Управление рисками, системный анализ и моделирование : учебное пособие / Н. Н. Рахимова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016. — 191 с. — ISBN 978-5-7410-1538-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/69961.html>

Алексеев, В. Б. Основы системного анализа : учебное пособие / В. Б. Алексеев, В. А. Красавина. — Москва : Российский университет дружбы народов, 2010. — 172 с. — ISBN 978-5-209-03521-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/11398.html>

9.2. Дополнительная литература

Волкова В.Н. Структуризация целей в системе управления высшей школы: – СПб.: Изд-во СПбГГУ, 2000. 80 с.

Волкова В.Н. Из истории теории систем и системного анализа. – СПб.: Изд-во СПбГПУ. 2001. 260 с.

Волкова В.Н. Теория систем: и системный анализ: Методики и автоматизированные процедуры для реструктуризации систем управления. – СПб.: Изд-во Политехнического ун-та, 2005. – 72 с.

Щербаков, Ю.С. Информационные технологии в управлении безопасностью жизнедеятельности: учеб. пособие / Ю.С. Щербаков. – Новосибирск: СГГА, 2009. – 113 с.

Леонова Н.А. Математические модели физических явлений в техносферной безопасности [Электронный ресурс]: учебное пособие для реализации программ высшего образования по направлению подготовки магистров 20.04.01 "Техносферная безопасность" / Н. А. Леонова, М. Р. Бортковская; Санкт-Петербургский политехнический университет Петра Великого. — Электрон. текстовые дан. (1 файл : 3,15 Мб). — Санкт-Петербург: Изд-во Политехн. ун-та, 2016 (Санкт-Петербург, 2017).

Информационные ресурсы:

1. Система и системность: основные понятия. – URL: <http://dit.isuct.ru/ivt/books/IS/IS5/glava2.htm>
2. Предмет системного анализа. – URL: <http://victor-safronov.narod.ru/systems-analysis/lectures/kaziev/00.html>
3. Основные понятия моделирования. – URL: <http://bigc.ru/theory/books/kvisam/glava4.php>
4. Белов П.Г. Моделирование опасных процессов в техносфере. – URL: <http://www.studfiles.ru/dir/cat19/subj44/file8518.html>
5. Структура системного анализа. – URL: http://www.psychologos.ru/images/sistemn_1390804912.jpg
6. Системный анализ проблем. – URL: <http://victor-safronov.narod.ru/systems-analysis/lectures/rodionov/07-01.jpg>

9.3. Периодические издания (при необходимости)

9.4. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),
14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
15. Visual Studio Professional
16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление)

9.5. Профессиональные базы данных и информационные справочные системы современных информационных технологий (обязательно!)

Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)

Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>) и т.д.

Федеральный портал «Российское образование» <https://edu.ru/>. Режим доступа: индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет.

Официальная электронная учебно-методическая библиотека для общего и

профессионального образования – <http://www.window.edu.ru>

Российский общеобразовательный портал – <http://www.school.edu>

Федеральный портал «Российское образование» – <http://www.edu.ru/>

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

Для слепых и слабовидящих:

для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

– акустический усилитель и колонки;

Для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

1. Специализированные аудитории с наличием мультимедийного комплекса (компьютерная техника, мультимедийный проектор, экран, видео-, аудиоаппаратура).

2. Аудитории с наличием тематических стендов и технической аппаратуры.

Для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы используются учебные аудитории, отвечающие противопожарным правилам и нормам, обеспечивающих проведение всех видов деятельности обучающихся при освоении дисциплины, а также помещения для хранения и профилактического обслуживания учебного оборудования.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения (мультимедийными комплексами), служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду вуза.

К рабочей программе прилагаются:

Приложение 1 - Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю) *(разрабатывается в виде отдельного документа);*

Приложение 2 - Методические указания для обучающихся по освоению дисциплины (модуля).

(Методические указания для обучающихся по освоению дисциплины (модуля) могут быть представлены в виде изданных печатным и (или) электронным способом методических разработок со ссылкой на адрес электронного ресурса в виде рекомендаций обучающимся по изучению разделов и тем дисциплины (модуля) указанием глав, разделов, параграфов, задач, заданий, тестов и т.п. из рекомендованного списка литературы.)

УТВЕРЖДЕНО
Протокол заседания кафедры
№ _____ от _____

ЛИСТ ИЗМЕНЕНИЙ

(Изменения и дополнения в РПД вносятся ежегодно и оформляются в данной форме. Изменения вносятся заменой отдельных листов (старый лист при этом цветным маркером перечеркивается, а новый лист с изменением степлером прикалывается к рабочей программе (хранится на кафедре), в электронной форме РПД должна быть актуализированной всегда, т.е. с внесенными изменениями.

При наличии большого количества изменений и поправок, затрудняющих понимание, возникших в связи с изменением нормативной базы ВО и другим причинам, проводится полный пересмотр РПД (т.е. выпускается новая РПД), которая проходит все стадии проверки и утверждения).

в рабочей программе (модуле) дисциплины _____
(название дисциплины)
по направлению подготовки (специальности) _____

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)

- 1.1.;
- 1.2.;
- ...
- 1.9.

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)

- 2.1.;
- 2.2.;
- ...
- 2.9.

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)

- 3.1.;
- 3.2.;
- ...
- 3.9.

Составитель
дата

подпись

расшифровка подписи

Зав. кафедрой

подпись

расшифровка подписи