

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Минцва Мария Шавитий

Должность: Ректор

Дата подписания: 23.11.2023 09:18:06

Уникальный программный ключ:

236bcc35c296f119d6aafdc22836b21db52dbc07971a86865a5825f9fa4304cc

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»

Первый проректор
И.Г. Гайрабеков



09 2020г.

Рабочая программа

дисциплины

**«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
В УПРАВЛЕНИИ БЖД»**

Направление подготовки

20.03.01 Техносферная безопасность

Профиль

«Пожарная безопасность»

Квалификация

Бакалавр

Грозный – 2020

1. Цель и задачи дисциплины.

Цель дисциплины «Информационные технологии в управлении безопасностью жизнедеятельности» заключается в приобретении студентами знаний об основных понятиях информационных технологий управления; аппаратных и программных средствах систем управления; классификации базовых информационных технологий; типах прикладных информационных технологий; системах управления базами и банками данных; о распределенных базах данных; сетевых технологиях обработки данных; об информационных системах поддержки принятия решений в области безопасности; правовых информационных базах данных; мультимедиа-системах; основных понятиях географических информационных систем.

2. Место дисциплины в структуре образовательной программы.

Изучение дисциплины «Информационные технологии в управлении безопасностью жизнедеятельности» базируется на актуализации междисциплинарных знаний «Экологии», «Физики», «Химии», «Математики» и других дисциплин. Главной составляющей реализации междисциплинарных связей является *актуализация*, в результате которой происходит установление ассоциаций (объединение, связь) между условиями и требованиями междисциплинарной задачи и ранее изученным учебным материалом. Актуализация междисциплинарных связей способствует интериоризации, то есть усвоению междисциплинарных знаний при решении конкретной проблемы комплексной безопасности.

Дисциплина «Информационные технологии в управлении безопасностью жизнедеятельности» относится к вариативной части естественнонаучного цикла. Ей предшествует изучение: физики, математики, химии, экологии.

3. Требования к результатам освоения дисциплины.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

общекультурные:

способность использования основных программных средств, умение пользоваться глобальными информационными ресурсами, владение современными средствами телекоммуникаций, способность использовать навыки работы с информацией из различных источников для решения профессиональных и социальных задач (ОК-12);

общепрофессиональные:

способность учитывать современные тенденции развития техники и технологий в области обеспечения техносферной безопасности, измерительной и

вычислительной техники, информационных технологий в своей профессиональной деятельности (ОПК-1);

профессиональные:

способность ориентироваться в основных проблемах техносферной безопасности (ПК-19);

способность принимать участие в научно-исследовательских разработках по профилю подготовки: систематизировать информацию по теме исследований, принимать участие в экспериментах, обрабатывать полученные данные (ПК-20).

В результате изучения дисциплины студент должен:

знать:

- основные устройства персонального компьютера и оборудование, подключаемое к нему; основное программное обеспечение персонального компьютера;

уметь:

- выполнять действия по сбору, записи, хранению, обработке, выдаче и передачи информации с использованием ПК; использовать программные оболочки и прикладное программное обеспечение для реализации задач, поставленных в других областях знаний;

владеть:

- методами оценки состояния безопасности на производстве и в быту.

4. Объем дисциплины и виды учебной работы

Таблица 1

Вид учебной работы	Всего часов/з.е.		Семестры	
	ОФО	ЗФО	4сем	7сем
			ОФО	ЗФО
Контактная работа (всего)	64/1,7	16/0,4	64/1,7	16/0,4
В том числе:				
Лекции	32/0,8	8/0,2	32/0,8	8/0,2
Практические занятия (ПЗ)	32/0,8	8/0,2	32/0,8	8/0,2
Самостоятельная работа (всего)	80/2,2	128/3,5	80/2,2	128/3,5
В том числе:				
Реферат	20/0,5	46/1,27	20/0,5	46/1,27
Темы для самостоятельного изучения	14/0,3	30/0,8	14/0,3	30/0,8
Подготовка к практическим занятиям	14/0,3	16/0,4	14/0,3	16/0,4
Подготовка к экзамену	36/1	36/1	36/1	36/1
Вид отчетности	Экз	Экз	Экз	Экз
Общая трудоемкость дисциплины	Всего в часах	144	144	144
	Всего в зач. единицах	4	4	4

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 2

№ п/п	Наименование раздела дисциплины	ОФО			ЗФО		
		Лекц.	Практ зан.	Всего часов	Лекц.	Практ зан.	Всего часов
1	Введение в ИТ	2	2	4	0,5	0,5	1
2	Платформа в ИТ	4	4	8	0,5	0,5	1
3	Технологический процесс обработки информации в ИТ	4	4	8	1	1	2
4	ИТ конечного пользователя	4	4	8	1	1	2
5	Технологии открытых систем	2	2	4	1	1	2
6	ИТ в локальных и корпоративных сетях	4	4	8	1	1	2
7	ИТ в глобальных сетях	4	4	8	1	1	2
8	Прикладные ИТ	4	4	8	1	1	2
9	Защита информации в ИТ	4	4	8	1	1	2

5.2. Лекционные занятия

Таблица 3

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Введение в ИТ	Введение в информационные технологии (ИТ). Роль информатизации в развитии общества. Понятие ИТ. Сравнение информационной и производственной технологий. Свойства ИТ. Эволюционные этапы развития ИТ. Развитие современных ИТ. Новая ИТ. Классификация ИТ.
2	Платформа в ИТ	Моделирование процессов управления . Решение проблемно-ориентированных задач, связанных с управлением безопасностью жизнедеятельности. Накопление, хранение и поиск информации Формирование и поддержка архива данных. Платформа в ИТ. Принцип открытой архитектуры. Совместимость компьютерных платформ. Операционные системы как составная часть платформы. Классификация операционных систем. Сравнительные характеристики компьютерных платформ. Критерии выбора платформы.

		Прикладные решения и средства их разработки. Этапы выбора платформы. Критерии выбора.
3	Технологический процесс обработки информации в ИТ	Характеристика процесса управления безопасностью. Формирование концептуального подхода для управления безопасностью. Технологический процесс обработки информации. Понятие технологического процесса обработки информации. Принципы системотехнического подхода к организации технологического процесса обработки информации. Методика постановки управленческих задач. Использование информационных технологий управления безопасностью жизнедеятельности. Классификация технологического процесса обработки информации. Операции технологического процесса обработки информации, их классификация. Процедуры обработки информации. Взаимосвязь операций и процедур обработки информации. Средства реализации операций обработки информации. Средства формирования, передачи, хранения, поиска и обработки информации. Организация технологического процесса обработки информации. Стандартизация технологического процесса обработки информации. Этапы технологического процесса обработки информации. Взаимосвязь операций технологического процесса.
4	ИТ конечного пользователя	Использование единой системы условных знаков и обозначений в информационных технологиях управления безопасностью. Построение автоматизированных рабочих мест для обеспечения управления безопасностью. Организационные формы обработки информации. Принципы их построения. Понятие автоматизированного рабочего места (АРМ). Виды АРМ. Виды обеспечения АРМ. Автоматизированное рабочее место специалиста по мониторингу ЧС. Электронный офис. Понятие электронного офиса. Функции. Процедуры обработки документов в электронном офисе. Методы и модели формирования управленческих решений. Аппаратные и программные средства. Их характеристика и классификация. Пользовательский интерфейс. Понятие пользовательского интерфейса. Элементы пользовательского интерфейса, их классификация. Направления развития пользовательского интерфейса. Уровни представления данных в ЭВМ: классификация, развитие. Развитие средств взаимодействия с пользователем. Виды пользовательского интерфейса. Критерии качества пользовательского интерфейса.
5	Технологии открытых систем	Методы и модели формирования управленческих решений. Содержание процесса выработки решения. Открытые

		<p>системы. Основные понятия открытых систем. Свойства открытых систем. Стандарты ИТ. История развития технологии открытых систем. Эталонная модель взаимодействия открытых систем. Принципы разработки сетевых уровней. Технология передачи информации в модели взаимодействия открытых систем.</p> <p>Характеристика уровней модели взаимодействия открытых систем. Уровни эталонной модели взаимодействия открытых систем. Назначение и основные функции уровней эталонной модели. Характеристика уровней эталонной модели.</p>
6	ИТ в локальных и корпоративных сетях	<p>Распределенная обработка данных. Преимущества распределенной обработки данных. Локальная и распределенная базы данных. Технология «клиент-сервер»: понятие, компоненты, модели реализации.</p> <p>Информационные хранилища (ИХ). Корпоративные системы. Понятие информационного хранилища. Внутренние и внешние базы. Сравнение ИХ и баз данных. Технология помещения данных в ИХ. Свойства данных в ИХ. Виды ИХ. Функции технологии обеспечения групповой работы. Объекты системы групповой работы. Понятие корпоративной информационной системы. Структура корпоративной сети. Особенности операционных систем.</p>
7	ИТ в глобальных сетях	<p>Глобальная сеть Internet. Электронная почта. Телеконференции. Понятие Internet. История развития. Структура и услуги Internet. Использование сети Internet как источника информации по проблемам безопасности жизнедеятельности. Понятие и функции электронной почты. Понятие, виды и жизненный цикл телеконференции.</p> <p>Гипертекстовые технологии. Технологии мультимедиа. Понятие гипертекстовой технологии. Структурные элементы гипертекста. Виды навигаций по гипертекстовому документу. Понятие и компоненты мультимедийных технологий. Географические информационные системы (ГИС). История развития ГИС. Основные понятия ГИС. Принципы и функции ГИС. Компоненты. Системы координат. Проекция. Модели представления данных. Организация работы, сравнительные характеристики наиболее распространенных геоинформационных систем: ArcGIS, ИнГео, MapInfo, Панорама и других. Преимущества и недостатки. Применение ГИС для мониторинга и прогнозирования чрезвычайных ситуаций. ГИС автомобильных дорог IndorInfo/Road. Использование ГИС для повышения эффективности управления сетями газоснабжения, водоканалами и другим.</p>
8	Прикладные ИТ	<p>Системы поддержки принятия решений. Ситуационные центры. Понятие и виды систем поддержки принятия</p>

		<p>решений. Ситуационный центр. Планирование и управление чрезвычайными ситуациями на примере системы Федерального Агентства по Управлению Чрезвычайными Ситуациями (ФЕМА) и системы Центра интеграции технологий (Genoa). Ситуационный центр Министерства природных ресурсов России. Серия программных комплексов «Кедр». Экологический программный комплекс «РОСА». Система теплотехнических расчетов «Источник».</p> <p>Прикладные ИТ в государственном управлении. Задачи государственного управления, реализуемые с применением ИТ. Организация работы ИТ управления. Принципы создания и использования информационно-аналитических систем. Экспертно-аналитические услуги. Особенности электронного правительства. Автоматизированная информационно – управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций. Функции АИУС РСЧС. Функциональная схема, состав, режимы работы. Используемые ИТ, информационное обеспечение АИУС РСЧС. Система управления риском. Понятие системы управления риском. Структура. Информационное обеспечение. Типовая процедура анализа риска. Системы мониторинга. Структурированная система мониторинга и управления инженерными системами зданий и сооружений (СМИС): понятие, объекты управления, компоненты СМИС, задачи СМИС. Общие технические требования к СМИС. Порядок создания СМИС. Концепция федеральной системы мониторинга критически важных объектов: понятие, цели, задачи, функции. Состав и структура системы мониторинга критически важных объектов, принципы создания. Автоматизированная система обеспечения градостроительной деятельности «Мониторинг».</p>
9	<p align="center">Защита информации в ИТ</p>	<p>Защита информации в информационных технологиях управления безопасностью. Разработка системы защиты данных в информационных технологиях. Понятие и классификация угроз безопасности информации в ИТ. Характеристика субъектов, реализующих угрозы безопасности информации в ИТ. Основные принципы создания базовой системы защиты информации в ИТ. Методы, средства и механизмы обеспечения безопасности информации в ИТ. Меры и способы защиты, используемые в ИТ. Понятие и виды вредоносных программ. Виды компьютерных вирусов, их классификация. Организация защиты ресурсов ИТ от компьютерных вирусов.</p>

5.3. Лабораторные занятия (не предусмотрены)

5.4. Практические занятия (семинары)

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Раздел 1. Введение в ИТ.	Эволюционные этапы развития ИТ.
2	Раздел 2. Платформа в ИТ.	Накопление, хранение и поиск информации Формирование и поддержка архива данных Уровни представления данных в ЭВМ: классификация, развитие.
3	Раздел 3. Технологический процесс обработки информации в ИТ.	Методика постановки управленческих задач Использование информационных технологий управления безопасностью жизнедеятельности Классификация технологического процесса обработки информации. Назначение и основные функции уровней эталонной модели.
4	Раздел 4. ИТ конечного пользователя.	Структура корпоративной сети. Особенности операционных систем. Методы и модели формирования управленческих решений .
5	Раздел 5. Технологии открытых систем.	Эталонная модель взаимодействия открытых систем. Виды навигаций по гипертекстовому документу.
6	Раздел 6. ИТ в локальных и корпоративных сетях.	Функции технологии обеспечения групповой работы. Объекты системы групповой работы.
7	Раздел 7. ИТ в глобальных сетях.	Общие технические требования к СМИС. Порядок создания СМИС.
8	Раздел 8. Прикладные ИТ.	Меры и способы защиты, используемые в ИТ.
9	Раздел 9. Защита информации в ИТ.	Понятие и виды вредоносных программ.

6. Самостоятельная работа студентов по дисциплине

Темы, выносимые для самостоятельного изучения.

1. Классификация этапов развития ИТ.

2. Этапы развития операционных систем. Перспективы развития операционных систем.
3. Графическое изображение технологического процесса.
4. Программное обеспечение АРМ.
5. Принципы построения пользовательского интерфейса.
6. История развития технологии открытых систем.
7. Топология локальной вычислительной сети.
8. Сравнительные характеристики моделей технологии «клиент-сервер».
9. Технология видеоконференций: средства, схема организации, технология проведения.
10. Применение гипертекстовых технологий в глобальных сетях.
11. Специальные ГИС для мониторинга и прогнозирования чрезвычайных ситуаций.
12. Сценарии развития чрезвычайных ситуаций системы Центра интеграции технологий. Другие примеры систем поддержки принятия решений.
13. Функциональная схема АИУС РСЧС.
14. Типовая процедура анализа риска.

Темы рефератов

1. Развитие информационных технологий
2. Системы управления базами данных
3. Информационные системы и их виды
4. Прикладные программные обеспечения трудового профиля (АРМот и Аттестация)
5. Прикладные программные обеспечения экологического профиля (УПРЗА «Эколог», Интеграл.)
6. Web - браузеры. Сравнительный анализ.
7. Мультимедийные технологии
8. Прикладные программные обеспечения, предназначенные для МЧС
9. Конверторы форматов
10. Программное и аппаратное обеспечение персонального компьютера.

Методические рекомендации студентам по выполнению реферата.

Данный вид работы – определенный итог самостоятельной учебы студента в области расследования и экспертизы пожаров.

Реферат выполняется по личной инициативе студента или по рекомендации преподавателя. Его тема определяется в порядке, установленном, руководителем занятий.

Обязательно необходимо получить у преподавателя консультацию о порядке написания работы и требованиях к ней.

При выполнении реферата важно использовать материалы периодической печати, особенно научно-практической и специальной литературы. В тексте работы по установленным стандартам должны быть даны сноски на факты, примеры, цитаты, взятые из печати и из научных работ.

Реферат выполняется, представляется преподавателю для проверки и защиты не позднее, чем за один месяц до завершения семестра. Защита реферата может проходить на семинарских занятиях или в часы индивидуальных занятий преподавателя со студентами.

Работа над рефератом, который является продолжением углубленного изучения темы контрольной работы, должна отвечать ряду правил и требований.

Правило I.

Требования к структуре и оформлению реферата.

Титульный лист. На нем должны быть: наименование ведомства, вуза и кафедры, фамилия, инициалы студента, шифр, а так же тема работы.

Первый лист должен давать представление о структуре и содержании реферата. На нем оформляется план работы (вступление, первый, второй, третий вопросы, заключение, список использованной литературы).

Литература, таблицы, схемы, рисунки, графики, представленные в работе, оформляются в соответствии с установленными требованиями.

Реферат, как правило, разрабатывается на листе форматом А4. Размеры полей: правое – 3 см., левое – 1,5 см., верхнее и нижнее по 2 см.

Шрифт - Times New Roman, размер – 14, интервал – 1,5; отступ – 1,27.

Общий объем работы – 10 – 11 страниц, без учета титульного и первого листа.

Правило 2.

Реферат должен состоять из следующих частей:

План (он же - оглавление работы), определяющий основные разделы реферата и указание страниц, которыми раздел начинается.

Первая строка плана - введение, занимающее 1/2 страницу текста. Во введении автор четко определяет предмет своего исследования, кратко обосновывает важность и актуальность рассматриваемой проблемы, указывает, чем конкретно эта проблема представляет интерес лично для него.

Далее цифрами 1, 2, 3 обозначаются первый, второй и третий вопросы основной части реферата, на которые автор, сообразуясь с логикой изложения темы, разбивает ее содержание с обязательным указанием страниц.

Названия вопросов обязательно должны присутствовать в тексте работы.

В заключение работы, занимающем 1/2 страницы, должны быть ясно и четко сформулированы те выводы, к которым автор пришел в результате самостоятельно проведенного исследования проблемы.

Последняя часть - список литературы. В алфавитном порядке дается список использованных источников и литературы, при этом, если это какой-либо документ, сборник документов или монография, написанная коллективом авторов, надо указать название книги (документа), место издания, издательство, год издания и ее общий объем в страницах; если это авторская работа, начинать надо с фамилии автора, затем следует название статьи (книги), далее - место издания, издательство, год издания и общий объем работы в страницах; при использовании статьи, взятой из журнала или газеты, указывается фамилия автора, название статьи, название журнала (газеты, брошюры и т.п.), год издания, номер выпуска и страницы, на которых в журнале располагается статья.

Защита реферата - устное изложение сути проделанной вами работы в течение 15-20 мин, когда вы подчеркиваете важность, актуальность и интерес выбранной темы, излагаете самое главное, самое интересное в содержании и выводы.

Успешная защита реферата является условием допуска обучающегося к установленной форме контроля, а также, по согласованию с руководством кафедры,

ее итоги преподаватель может использовать для определения оценки знаний студента по дисциплине, если он не имеет задолженностей по семинарским занятиям.

Учебно-методическое обеспечение самостоятельной работы студента

1. Мастрюков Б.С. Безопасность в чрезвычайных ситуациях в природно-техногенной сфере. Прогнозирование последствий. Учебное пособие для студ. высш. проф. образования. – М.: изд.центр «Академия». 2011 – 368с.
2. Каракеян В.И. Безопасность жизнедеятельности. – М.: изд. Юрайт. 2012 – 456с.
3. Белов С.В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность) 4-е изд. – М.: изд. Юрайт. 2013 – 682с.
4. Еремин В.Г., Сафронов В.В., Схиртладзе А.Г., Харламов Г.А. Безопасность жизнедеятельности в энергетике/ – М.: изд. центр «Академия». 2010 – 400с.

7. Оценочные средства

7.1. Вопросы для текущего контроля

1. Классификация ИТ. Классификация операционных систем.
2. Уровни представления данных в ЭВМ: классификация, развитие.
3. Классификация технологического процесса обработки информации.
Назначение и основные функции уровней эталонной модели.
4. Структура корпоративной сети. Особенности операционных систем.
5. Виды навигаций по гипертекстовому документу.
6. Понятие и компоненты мультимедийных технологий.
7. Общие технические требования к СМИС. Порядок создания СМИС.
8. Меры и способы защиты, используемые в ИТ.
9. Понятие и виды вредоносных программ.

7.2. Вопросы к первой рубежной аттестации

1. Введение в информационные технологии (ИТ).
2. Понятие ИТ.
3. Платформа в ИТ.
4. Понятие платформы.
5. Технологический процесс обработки информации.
6. Понятие технологического процесса обработки информации.

7. Классификация технологического процесса обработки информации.
8. Операции технологического процесса обработки информации, их классификация.
9. Этапы технологического процесса обработки информации.
10. Взаимосвязь операций технологического процесса.
11. Автоматизированное рабочее место.
12. Организационные формы обработки информации.
13. Открытые системы. Основные понятия открытых систем.
14. Свойства открытых систем. Стандарты ИТ.

7.2. Вопросы ко второй рубежной аттестации

1. Понятие компьютерных сетей.
2. Информационные хранилища (ИХ). Корпоративные системы.
3. Понятие информационного хранилища.
4. Глобальная сеть Internet. Электронная почта. Телеконференции.
5. Понятие Internet. История развития.
6. Применение ГИС для мониторинга и прогнозирования чрезвычайных ситуаций. ГИС автомобильных дорог IndorInfo/Road.
7. Ситуационные центры. Понятие и виды систем поддержки принятия решений.
8. Планирование и управление чрезвычайными ситуациями на примере системы Федерального Агентства по Управлению Чрезвычайными Ситуациями (FEMA) и системы Центра интеграции технологий (Genoa).
9. Ситуационный центр Министерства природных ресурсов России.
10. Серия программных комплексов «Кедр».
11. Экологический программный комплекс «РОСА».
12. Система теплотехнических расчетов «Источник».
13. Автоматизированная информационно – управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций. Функции АИУС РСЧС.
14. Система управления риском.
15. Системы мониторинга.

16. Понятие и классификация угроз безопасности информации в ИТ.

7.3. Вопросы к экзамену

1. Введение в информационные технологии (ИТ).
2. Понятие ИТ.
3. Платформа в ИТ.
4. Понятие платформы.
5. Технологический процесс обработки информации.
6. Понятие технологического процесса обработки информации.
7. Классификация технологического процесса обработки информации.
8. Операции технологического процесса обработки информации, их классификация.
9. Этапы технологического процесса обработки информации.
10. Взаимосвязь операций технологического процесса.
11. Автоматизированное рабочее место.
12. Организационные формы обработки информации.
13. Открытые системы. Основные понятия открытых систем.
14. Свойства открытых систем. Стандарты ИТ.
15. Понятие компьютерных сетей.
16. Информационные хранилища (ИХ). Корпоративные системы.
17. Понятие информационного хранилища.
18. Глобальная сеть Internet. Электронная почта. Телеконференции.
19. Понятие Internet. История развития.
20. Применение ГИС для мониторинга и прогнозирования чрезвычайных ситуаций. ГИС автомобильных дорог IndorInfo/Road.
21. Ситуационные центры. Понятие и виды систем поддержки принятия решений.
22. Планирование и управление чрезвычайными ситуациями на примере системы Федерального Агентства по Управлению Чрезвычайными Ситуациями (ФЕМА) и системы Центра интеграции технологий (Genoa).
23. Ситуационный центр Министерства природных ресурсов России.
24. Серия программных комплексов «Кедр».

25. Экологический программный комплекс «РОСА».
26. Система теплотехнических расчетов «Источник».
27. Автоматизированная информационно – управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций. Функции АИУС РСЧС.
28. Система управления риском.
29. Системы мониторинга.
30. Понятие и классификация угроз безопасности информации в ИТ.

ФОС к первой рубежной аттестации

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова
Карточка №1

Дисциплина: ИТ в управлении БЖД

ИНГ Группа _____

1. Взаимосвязь операций технологического процесса.
2. Автоматизированное рабочее место.

ФОС ко второй рубежной аттестации

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

Карточка №1

Дисциплина: ИТ в управлении БЖД

ИНГ Группа _____

1. Ситуационные центры. Понятие и виды систем поддержки принятия решений.

2. Планирование и управление чрезвычайными ситуациями на примере системы Федерального Агентства по Управлению Чрезвычайными Ситуациями (ФЕМА) и системы Центра интеграции технологий (Genoa).

ФОС к экзамену

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
имени академика М.Д. Миллионщикова

БИЛЕТ № 1

Дисциплина: Информационные технологии в управлении БЖД
ИНГ Группа:

1. Введение в информационные технологии (ИТ).
2. Платформа в ИТ.
3. Технологический процесс обработки информации.

УТВЕРЖДАЮ:

« ____ » _____ 20 ____ г.

Зав. кафедрой _____

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Газаров Р.А., Эржапова Р.С., Таймасханов Х.Э., Хасиханов М.С., Эржапова Р.С. Безопасность жизнедеятельности: Учебное пособие,- Пятигорск : изд-во АИТОНК, 2009-321с.
2. Эржапова Р.С., Хасиханов М.С., Расуев Б.Х., Хаджимуратова З.С. Основы безопасности жизнедеятельности: Учебное пособие,- Грозный: изд-во ЧГУ, 2013- 175с.
3. Белов С.В., Ильницкая А.В., Козьяков А.Ф. Безопасность жизнедеятельности: Учебник для вузов. 4-е изд.,испр. и доп -М.: В.шк.,2009.-606с.

4. Бадагуев Б.Т. Документация по охране труда в организации: Альфа-Пресс, 2010г.
5. Фадеев Ю.Л., Родин Д.А. «Безопасность труда в строительстве».: М: Альфа-Пресс, 2008. - 192с.

б) дополнительная литература:

1. Кукин П.П. «Безопасность жизнедеятельности»: 5-е изд. Стер. М.: Высш. шк., 2009. – 335с.
2. Акимов В.А., Воробьев Ю.Л., Фанеев М.И. «Безопасность жизнедеятельности. Безопасность в чрезвычайных ситуациях природного и техногенного характера» Учеб. пособие 3-е изд., испр. – Н: Высш. шк, 2008.- 592с.

в) интернет - ресурсы:

В качестве дополнительного источника информационных ресурсов по изучению курса «БЖД» рекомендуются Интернет – сайты:

- Электронная школа безопасности жизнедеятельности.

<http://www.mos-uk1.ru/func.php?cab=o>

- Основы безопасности жизнедеятельности. Методика и опыт.

<http://pedsovet.org/forum/index.php?showtopic>

- Портал МЧС России. Новости. Прогнозы, Сводка ЧС. Полезная информация.

Статистика. Материалы СМИ. http://www.referatec.com/referat_32768_str_7.html

9. Материально-техническое обеспечение дисциплины

программное и коммуникационное обеспечение:

1. Электронный конспект лекций.
2. Комплект демонстрационных материалов.

Составитель:

Доцент кафедры «БЖД»



/Тагирова П.Р./

СОГЛАСОВАНО:

Зав. выпускающей каф. «БЖД»



/Хасиханов М.С./

Директор ДУМР



/Магомаева М.А./