ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«25» мая 2026 г.
Протокол № 2

Рабочая программа дисциплины (модуля)
«Безопасность жизнедеятельности»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Прикладной искусственный интеллект*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2026*

Москва
2026

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Безопасность жизнедеятельности» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по специальности 02.03.01 «Математика и компьютерные науки», профиль «Прикладной искусственный интеллект», утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Безопасность жизнедеятельности» помогает студентам осознать важность профилактики и реагирования на чрезвычайные ситуации, что способствует сохранению здоровья и жизни людей. Кроме того, освоение принципов безопасности жизнедеятельности формирует ответственность за собственные действия и действия окружающих в условиях потенциальных угроз.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки бакалавриата по направлению 02.03.01 «Математика и компьютерные науки», профиль «Прикладной искусственный интеллект» и входит в обязательную часть Блока 1.

Дисциплина (модуль) изучается на 1 курсе во 2 семестре.

Цель изучения дисциплины (модуля): формирование у студентов знаний и навыков, необходимых для обеспечения безопасности человека и общества в различных сферах жизнедеятельности.

Задачи изучения дисциплины (модуля):

создание и поддерживание 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.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

— способы выявления и предупреждения угроз, виды чрезвычайных ситуаций, общие правила и алгоритмы действий в нештатных и чрезвычайных ситуациях;

— способы обеспечения безопасности жизнедеятельности: законодательства и программных документов, видов угроз;

— специфику безопасности в сфере информационных технологий, киберугрозах и защите данных.

уметь:

— находить и правильно оценивать факторы опасности для личности, общества и государства, своевременно и оперативно реагировать на их возникновение;

— обеспечивать безопасность как своих личных данных, так и данных организаций;

— правильно рассчитывать пределы допустимого риска.

владеть:

— способами оказания первой доврачебной помощи при различных поражениях;

— навыками обеспечения безопасности жизнедеятельности.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Код и содержание компетенции	**Индикатор компетенции и перечень планируемых результатов обучения по дисциплине (модулю)**
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	УК-8.1. Знает основные принципы безопасной жизнедеятельности и охраны окружающей среды; нормативные и правовые акты в области экологии и безопасности
	УК-8.2. Умеет оценивать риски и разрабатывать меры по предотвращению чрезвычайных ситуаций; реализовывать стратегии устойчивого развития в повседневной и профессиональной деятельности
	УК-8.3. Имеет практический опыт поддержания безопасных условий жизнедеятельности

3. Тематический план

№ п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Практические занятия			
1	Информационная безопасность	1	2		18	Домашнее задание, тест
2	Кибербезопасность				17	
3	Оказание первой помощи	2	2		17	Домашнее задание, тест
4	Ментальное здоровье				17	
	Зачет					
	Итого:	***3***	***4***		***69***	
Объем дисциплины (модуля) (в ак. ч.)		***76***				
Объем дисциплины (модуля) (в зач. ед.)		***2***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Информационная безопасность	Принципы защиты личных данных. Социальная инженерия и методы противодействия
2	Кибербезопасность	Опасности в сети: фишинг, вирусы, вредоносное ПО. Кибербуллинг и его предотвращение в повседневной жизни
3	Оказание первой помощи	Алгоритм действий при неотложных состояниях. Первая помощь при травмах и кровотечениях. Сердечно-лёгочная реанимация и помощь при остановке дыхания
4	Ментальное здоровье	Стресс: причины, признаки, способы управления. Профилактика эмоционального выгорания. Осознанность и практики заботы о себе

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Белов, С. В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность) : учебник для вузов / С. В. Белов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 636 с. — (Высшее образование). — ISBN 978-5-534-16270-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568495.

2. Резчиков, Е. А. Безопасность жизнедеятельности : учебник для вузов / Е. А. Резчиков, А. В. Рязанцева. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 634 с. — (Высшее образование). — ISBN 978-5-534-20019-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557469.

3. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915.

4. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313.

5. Одинцова, М. А. Психология стресса : учебник и практикум для вузов / М. А. Одинцова, Н. Л. Захарова. — Москва : Издательство Юрайт, 2025. — 291 с. — (Высшее образование). — ISBN 978-5-534-16913-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561139.

Дополнительная литература:

1. О промышленной безопасности опасных производственных объектов: федеральный закон РФ от 21.07.1997 г. No116-ФЗ (ред. с изм. вступающими в силу от 08.12.2020) //Рос.газ.— 1997. — 30 июля.

2. О пожарной безопасности: федер. закон РФ от 21.12.1994 г. No 69-ФЗ (ред. от 22.12. 2020), (с изм. и доп., вступающими в силу с 02.01.2021) //Рос.газ.. — 1995. — 05 января.

3. О безопасности: федер. закон от 28.12.2010 г. No 390-ФЗ (ред. от 09.11.2020), (с изм. и доп., вступающими в силу с 20.11.2020) // Рос.газ. — 2010. — 29 декабря.

4. О санитарно-эпидемиологическом благополучии населения: федер. закон от 30.03. 1999 г. No 52-ФЗ, (ред. от 13.07.2020, с изм. вступающими в силу с 28.08.2020) // Рос.газ. — 1999. — 06 апреля.

5. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 г. No 197-ФЗ, (ред.от 20.04.2021, с изм. вступающими в силу с 01.05.2021) //Рос.газ. — 2001. — 31 декабря.

6. Кодекс Российской Федерации об административных правонарушениях: федер. закон от 30.12.2001 г. No 195-ФЗ (ред. от 20.04.2021, с изм. вступающими в силу с 01.05.2021) //Рос.газ.. — 2001. — 31 декабря.

7. Об основах охраны здоровья граждан в Российской Федерации: федер. закон от 21.11.2011 г. No 323-ФЗ (ред. от 22.12.2020, с изм. вступающими в силу с 01.01.2021)// Рос.газ. — 2011. — 23 ноября.

8. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: федер. закон от 21.12.1994 г. No 68-ФЗ (ред.с изм. вступающими в силу от 08.12.2020) // Рос.газ. — 1994. — 24 декабря.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

- столами и стульями;
- компьютерной техникой;
- механическими калькуляторами;
- специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1	Катастрофы, стихийные бедствия, аварии, эпидемии. Солнечная и геомагнитная активность. /ежедневный обзор	http://www.disasters.chat.ru
2	Каталог по безопасности жизнедеятельности	http://www.eun.chat.ru
3	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
4	База данных для IT-специалистов	https://habr.com
5	База данных ScienceDirect	https://www.sciencedirect.com
6	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
7	Федеральный портал «Российское образование"	https://www.edu.ru/
8	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
9	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/

10	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Безопасность жизнедеятельности» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекция, семинар, тесты и домашние задания, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций,

поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Участие в семинаре – активная работа студента на семинаре, его ответы на вопросы преподавателя и участие в дискуссии.

Для успешного участия в семинаре студентам рекомендуется заранее ознакомиться с темой обсуждения, прочитать необходимые материалы и подготовить вопросы. Важно активно слушать и вовлекаться в дискуссию, высказывая свои мнения и аргументируя их. При ответах на вопросы преподавателя стоит быть уверенным, четким и логичным, опираясь на изученный материал. Также полезно поддерживать диалог с однокурсниками, чтобы обогатить обсуждение и расширить свои знания.

Домашнее задание – набор заданий по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Тест – особая форма проверки знаний. Проводится после освоения одной или нескольких тем и свидетельствует о качестве понимания основных понятий изучаемого материала. Тестовые задания составлены к ключевым понятиям, основным разделам, важным терминологическим категориям изучаемой дисциплины.

Для подготовки к тесту необходимо знать терминологический аппарат дисциплины, понимать смысл научных категорий и уметь их использовать в профессиональной лексике. Владение понятийным аппаратом, включённым в тестовые задания, позволяет преподавателю быстро проверить уровень понимания студентами важных методологических категорий.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Безопасность жизнедеятельности».

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации

используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	**Пятибалльная оценка**	**Оценка за зачет**	**Общая характеристика результата обучения по дисциплине (модулю)**
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
9	Отлично	Зачтено	
8	Отлично	Зачтено	
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает
4	Удовлетворительно	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	Не зачтено	
1	Не сдан	Не зачтено	

Дисциплина (модуль) «Безопасность жизнедеятельности» оценивается следующим образом:

Активность	Вес	Описание
Тест	100%	Письменные ответы на вопросы по всем темам дисциплины (модуля) за ограниченное время

Для получения зачета нужно решить тест на 70 % и более.

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание: Принципы защиты личных данных. Социальная инженерия и методы противодействия

1. Опишите, что такое личные данные и почему их важно защищать в интернете.
2. Приведите три примера социальной инженерии и объясните, как можно распознать попытку манипуляции.
3. Составьте список из пяти правил безопасного обращения с паролями и объясните их важность.
4. Опишите, какие меры можно предпринять для защиты личных данных в социальных сетях.
5. Проведите небольшой опрос среди знакомых (3-5 человек) о том, как они защищают свои данные, и сделайте выводы.

Домашнее задание: **Опасности в сети: фишинг, вирусы, вредоносное ПО. Кибербуллинг и его предотвращение в повседневной жизни**

1. Объясните, что такое фишинг и приведите пример фишингового письма или сайта.
2. Назовите пять видов вредоносного программного обеспечения и кратко опишите каждый.
3. Опишите, как можно защититься от вирусов и вредоносного ПО на компьютере или смартфоне.
4. Что такое кибербуллинг? Приведите три примера проявления кибербуллинга.
5. Разработайте план действий для человека, ставшего жертвой кибербуллинга.

Домашнее задание: **Стресс: причины, признаки, способы управления. Профилактика эмоционального выгорания. Осознанность и практики заботы о себе**

1. Опишите три основных причины стресса в повседневной жизни подростков или

взрослых.

2. Составьте список из пяти признаков, по которым можно распознать, что человек испытывает стресс.

3. Изучите и опишите три техники управления стрессом, которые можно применять самостоятельно.

4. Что такое эмоциональное выгорание? Приведите примеры ситуаций, которые могут к нему привести.

5. Разработайте личный план заботы о себе на неделю, включающий практики осознанности и снятия стресса.

Примерные задания для теста

1. Что относится к личным данным?
   a) Имя и фамилия
   b) Любая публичная информация
   c) Только номер телефона
   Ответ: a)

2. Что такое социальная инженерия?
   a) Использование технических средств для взлома
   b) Манипуляция людьми с целью получения конфиденциальной информации
   c) Разработка программного обеспечения
   Ответ: b)

3. Какой из способов поможет защитить пароль?
   a) Использовать один и тот же пароль для всех сайтов
   b) Хранить пароль в блокноте на рабочем столе
   c) Использовать сложный и уникальный пароль для каждого сайта
   Ответ: c)

4. Что НЕ является признаком попытки социальной инженерии?
   a) Просьба срочно сообщить пароль
   b) Официальное письмо от банка с просьбой подтвердить данные
   c) Получение письма от знакомого с обычным вопросом
   Ответ: c)

5. Как лучше всего защитить личные данные в социальных сетях?
   a) Открыть профиль для всех
   b) Ограничить доступ к личной информации
   c) Использовать простые пароли
   Ответ: b)

6. Что такое фишинг?
   a) Вирус, который повреждает файлы
   b) Попытка получить личные данные через поддельные сайты или письма
   c) Программа для защиты компьютера
   Ответ: b)

7. Какой из перечисленных видов ПО является вредоносным?
   a) Антивирус
   b) Троян
   c) Операционная система
   Ответ: b)

8. Что поможет защитить устройство от вирусов?
   a) Установка антивируса и обновление системы
   b) Открытие всех вложений в письмах

c) Использование одного пароля для всех сайтов
Ответ: a)

9. Что такое кибербуллинг?
   a) Защита в интернете
   b) Преследование и травля в сети
   c) Создание сайтов
   Ответ: b)

10. Как поступить, если вы стали жертвой кибербуллинга?
    a) Игнорировать ситуацию
    b) Сообщить взрослым и заблокировать обидчика
    c) Отвечать обидчику в том же стиле
    Ответ: b)

11. Что является первым действием при обнаружении пострадавшего без сознания?
    a) Положить пострадавшего на живот
    b) Проверить реакцию и дыхание
    c) Немедленно начинать массаж сердца
    Ответ: b)

12. При сильном кровотечении необходимо:
    a) Поднять пострадавшего и дать воду
    b) Наложить жгут или давящую повязку выше раны
    c) Оставить рану открытой для воздуха
    Ответ: b)

13. Что из перечисленного входит в алгоритм сердечно-лёгочной реанимации (СЛР)?
    a) Проверка сознания, вызов помощи, искусственное дыхание, массаж сердца
    b) Питьё воды и отдых
    c) Наложение шины
    Ответ: a)

14. Как правильно выполнять искусственное дыхание?
    a) Сделать глубокий вдох и дуть в рот пострадавшего, закрыв нос
    b) Дуть в нос пострадавшего
    c) Не дышать, только делать массаж сердца
    Ответ: a)

15. Что делать при подозрении на перелом?
    a) Пытаться самостоятельно вправить кость
    b) Зафиксировать конечность и вызвать скорую помощь
    c) Игнорировать и продолжить движение
    Ответ: b)

16. Что может быть причиной стресса?
    a) Постоянный отдых
    b) Учёба, конфликты, перегрузки
    c) Полноценный сон
    Ответ: b)

17. Какой из признаков может указывать на стресс?
    a) Улучшение аппетита
    b) Раздражительность и усталость
    c) Повышенная энергия
    Ответ: b)

18. Какая техника помогает управлять стрессом?
    a) Глубокое дыхание и медитация
    b) Прокрастинация
    c) Игнорирование проблем
    Ответ: a)

19. Что такое эмоциональное выгорание?
    a) Полное отсутствие эмоций
    b) Состояние хронической усталости и снижения мотивации
    c) Радость и вдохновение
    Ответ: b)

20. Какая практика способствует заботе о себе?
    a) Регулярный сон, физическая активность, хобби
    b) Игнорирование своих потребностей
    c) Постоянная работа без отдыха
    Ответ: a)

21. Назовите три способа защиты личных данных в интернете.
    Ответ: Использование сложных паролей, двухфакторная аутентификация, ограничение доступа к информации.

22. Что делать при получении подозрительного письма с просьбой ввести пароль?
    Ответ: Не вводить пароль, проверить источник, удалить письмо.

23. Какие признаки указывают на фишинговый сайт?
    Ответ: Подозрительный URL, ошибки в тексте, просьба срочно ввести личные данные.

24. Как можно предотвратить заражение компьютера вирусом?
    Ответ: Устанавливать антивирус, не открывать подозрительные файлы, обновлять ПО.

25. Какие действия входят в алгоритм СЛР?
    Ответ: Проверка сознания, вызов скорой, искусственное дыхание, массаж сердца.

26. Что делать при сильном кровотечении?
    Ответ: Наложить жгут или давящую повязку, вызвать скорую помощь.

27. Назовите три причины стресса.
    Ответ: Учёба, конфликты, перегрузки.

28. Как распознать эмоциональное выгорание?
    Ответ: Хроническая усталость, снижение мотивации, апатия.

29. Какие практики помогают снизить стресс?
    Ответ: Медитация, физические упражнения, правильный сон.

30. Что делать, если вы стали жертвой кибербуллинга?
    Ответ: Сообщить в службу безопасности, заблокировать обидчика, не отвечать агрессией.

Примерные задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Установленные правила и стандарты, направленные на обеспечение сохранения и укрепления здоровья людей, предотвращение заболеваний и создание безопасных условий окружающей среды.	Санитарные нормы/санитарные нормы/СанПиН/СанПиНы/санпины/санпин/ Санпин/Санпины	УК-8
2.	Это метод защиты данных, который требует использования двух различных способов для подтверждения вашей личности при входе в систему. *Ответ запишите в виде словосочетания*	Двухфакторная аутентификация/ двухфакторная аутентификация	УК-8
3.	Определите, какой закон закрепляет правовые основы обеспечения безопасности личности, общества и государства: А) Федеральный закон «Об обороне»; Б) Федеральный закон «О гражданской обороне»; В) Закон Российской Федерации «О безопасности».	В	УК-8
4.	К какому виду чрезвычайных событий относятся землетрясения? А) геофизическому; Б) метеорологическому; В) гидрологическому; Г) геологическому	В	УК-8
5.	... микроклиматические условия установлены по критериям теплового и функционального состояния организма	Оптимальные/оптимальные	УК-8
6.	Вид процесса, при котором деятельность человека происходит по заранее известным правилам, инструкциям, алгоритмам действий, жесткому технологическому графику и т.п.:	Детерминированный/ детерминированный	УК-8
7.	Горный поток, состоящий из смеси воды и рыхлообломочной горной породы, называется:	Селем/ селем/ Сель/сель	УК-8
8.	Правила безопасности, определяющие требования безопасности, являющиеся специфическими для той или иной отрасли экономики страны	Отраслевые/ отраслевые	УК-8
9.	Основными источниками угроз информационной безопасности являются все указанное в списке: А. Хищение жестких дисков, подключение к сети, инсайдерство Б. Перехват данных, хищение данных, изменение архитектуры системы В. Хищение данных, подкуп системных администраторов, нарушение регламента работы	Б	УК-8

10.	К основным типам средств воздействия на компьютерную сеть относится: А. Компьютерный сбой Б. Логические закладки («мины») В. Аварийное отключение питания	Б	УК-8
11.	Угроза информационной системе (компьютерной сети) – это …. событие	Вероятное/вероятное	УК-8
12.	Окончательно, ответственность за защищенность данных в компьютерной сети несет:	Владелец/владелец	УК-8