Министерство просвещения Российской Федерации
ФГБОУ ВО «Дагестанский государственный педагогический университет им. Р. Гамзатова»

Кафедра безопасности жизнедеятельности

УТВЕРЖДАЮ
И.о. начальника УМУ
«21» 08 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.08 ПРЕДМЕТНО – МЕТОДИЧЕСКИЙ МОДУЛЬ
Б1.О.08.08 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки - 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профили) – «Технология» и «Безопасность жизнедеятельности»
Квалификация выпускника: Бакалавр
Форма обучения – очная (5 лет), заочная (5 лет 6 месяцев)
Год приема – 2024

Форма обучения	Семестр	Трудоемкость	Виды учебной работы					
			Лекции	Практ. занятия	Лабор. занятия	Промежуточный контроль	СРС	Форма аттестации
очная	3	108	18	30			60	Зачет с оценкой
заочная	3	108	4	6			98	Зачет с оценкой

Махачкала, 2024

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель – формирование общепрофессиональных и профессиональных компетенций в области информационной безопасности личности, организации, общества, государства и основных мерах по её обеспечению.

Таблица 1.

Код компетенции	Содержание компетенции	Индикаторы достижения компетенций *(из примерной основной образовательной программы)*
ОПК-1	Способен осуществлять профессиональную деятельность в соответствии с нормативно-правовыми актами в сфере образования и нормами профессиональной этики.	ОПК-1.1. Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно-правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательства о правах ребенка, трудового законодательства. ОПК-1.2. Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности.
ПК-1	Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач.	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета). ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО. ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина **Б1.О.08.08** «Информационная безопасность» относится к обязательной части и модулю **Б1.О.08 «Предметно – методический модуль»** учебного плана по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), профили – «Технология» и «Безопасность жизнедеятельности».

Предшествующими дисциплинами учебного плана являются: Методы и средства проектирования информационных систем управления, Администрирование информационных систем управления.

Дисциплина «Информационная безопасность» является основой для применения полученных теоретических знаний на практике. Дисциплина изучается на 2 курсе в 3 семестре.

3.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЯ)

Дисциплина направлена на формирование следующих компетенций выпускника:
ОПК-1; ПК-1.
В результате изучения дисциплины обучающиеся должны:
Таблица 2.

Код компетенции	Знает	Умеет	Владеет
ОПК-1	нормативно-правовые акты по информационной безопасности в образовании; роль и значение информационной безопасности в образовательном процессе	анализировать и практически использовать нормативно-правовые акты по информационной безопасности в образовании; проводить оценку информации с точки зрения её соответствия нормативно-правовым актам	навыками работы с законодательными и иными нормативно-правовыми актами по информационной безопасности в системе образования; способами предупреждения информационных правонарушений
ПК-1	основы государственной политики обеспечения информационной безопасности; виды и источники опасностей и угроз в сфере информационных процессов и систем; понятия информационной безопасности	защититься от негативного информационного воздействия; принимать решения на основе анализа и оценки информации	методами формирования у учащихся знаний и умений в области информационной безопасности; методами и средствами обеспечения информационной безопасности

4.ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет **3** зачетные единицы (108 академических часа).

Дисциплина изучается в 3 семестре.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица3.

Вид учебной работы	**Трудоёмкость**		
	час.	**В т.ч. по семестрам**	
		№3	
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**	
1. Контактная работа:			
лекции (общее кол-во часов, включая практическую подготовку)	18	18	
практические занятия, семинары и пр. (общее кол-во часов, включая практическую подготовку)	30	30	

лабораторные занятия (общее кол-во часов / включая практическую подготовку)			
курсовое проектирование			
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем			
2. Объем самостоятельной работы обучающихся (СРС)	**60**	**60**	
в том числе часов, выделенных на подготовку к экзамену (зачету)			
Вид промежуточного контроля:	Зачет с оценкой	Зачет с оценкой	

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица4.

Вид учебной работы	**Трудоёмкость**		
	час.	**В т.ч. по семестрам**	
		№3	
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**	
1. Контактная работа:			
лекции (общее кол-во часов, включая практическую подготовку)	4	4	
практические занятия, семинары и пр. (общее кол-во часов, включая практическую подготовку)	6	6	
лабораторные занятия (общее кол-во часов / включая практическую подготовку)			
курсовое проектирование			
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем			
2. Объем самостоятельной работы обучающихся (СРС)	**98**	**98**	
в том числе часов, выделенных на подготовку к экзамену (зачету)			
Вид промежуточного контроля:	Зачет с оценкой	Зачет с оценкой	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
очная форма обучения

Таблица5.

№ п/п	**Наименование темы (раздела) дисциплины (модуля)**	**Общая трудоёмкость в акад.часах**	**Трудоёмкость по видам учебных занятий (в акад.часах)**			
			Лек/ пр.подг.	**Лаб / пр.подг.**	**Пр/ пр.подг.**	**СР**
1	Информация и информационная безопасность в современном мире		6		10	12
2	Обеспечение информационной безопасности РФ		6		10	24
3	Информационная безопасность человека		6		10	24
6	*Подготовка к экзамену (зачету)*					

7	Итого:	108	18		30	60

заочная форма обучения

Таблица6.

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоёмкость в акад.часах	Трудоёмкость по видам учебных занятий (в акад.часах)			
			Лек/ пр.подг.	Лаб / пр.подг.	Пр/ пр.подг.	СР
1	Информация и информационная безопасность в современном мире		2		2	26
2	Обеспечение информационной безопасности РФ		2		2	34
3	Информационная безопасность человека				2	38
6	*Подготовка к зачету (экзамену)*					
7	Итого:	108	4		6	98

5.1. Содержание разделов дисциплины (модуля)

Тема 1. Информация и информационная безопасность в современном мире

Понятие информации и информационной безопасности. Окружающая среда как источник информации. Восприятие информации человеком. Роль информации в развитии общества. Понятие информационного общества. Образование в информационном обществе.

Тема 2. Обеспечение информационной безопасности РФ

Информация как объект правового регулирования. Информационная безопасность РФ. Правовое обеспечение информационной безопасности РФ. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 5 декабря 2016 г. № 646). Защита государственной тайны. Конфиденциальная информация и её защита. Защита интеллектуальной собственности. Служебная тайна. Коммерческая тайна. Профессиональная тайна. Информационная война. Психологическая война.

Тема 3. Информационная безопасность человека

Концепция информационной безопасности детей. ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Неприкосновенность частной жизни граждан. Персональные данные и их защита. Технологии идентификации человека. Применение паролей в механизме аутентификации человека. Влияние средств массовой информации на человека. Влияние рекламы на человека.

Цифровая зависимость. Правила кибергигиены. Деструктивные течения и деятельность в Интернете и их профилактика. Опасный и запрещенный контент в Интернете и его признаки. Правила цифрового поведения, необходимого для предотвращения рисков и угроз при использовании Интернета (кибербуллинга, вербовки в различные организации и группы). Принятие решений в повседневной жизни и в чрезвычайных ситуациях. Информационные и компьютерные преступления.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Таблица7.

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1	Информация и информационная безопасность в современном мире	Изучение литературы Подготовка конспекта. Тематическое собеседование, опрос; анализ и обсуждение проблемных вопросов, докладов, дополнений.
2	Обеспечение информационной безопасности РФ	Изучение литературы Составление доклада. Анализ и обсуждение проблемных вопросов, докладов и дополнений
3	Информационная безопасность человека	Тематическое собеседование, опрос; анализ и обсуждение проблемных вопросов, докладов, дополнений.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

7.1. Оценочные материалы для проведения текущего контроля успеваемости

Указывается перечень компетенций в процессе освоения образовательной программы.

Таблица8.

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Средства текущего контроля успеваемости	Перечень компетенций
1	Тема 1. Информация и информационная безопасность в современном мире	**1. Защита презентации.** *Примерные темы презентаций:* - Окружающая среда как источник информации - Роль информации в развитии общества - Образование в информационном обществе 2**. Устный опрос.** *Примерные вопросы:* - Покажите на примерах значение информации в развитии общества - Что такое информационное общество? - Что такое информационное неравенство людей в информационной среде? Каковы его причины?	ОПК-1,ПК-1
2	Тема 2. Обеспечение информационной безопасности РФ	**1. Защита презентации.** *Примерные темы презентаций:* - Понятие информационной войны - Психологическая война в истории человечества - Доктрина информационной безопасности РФ 2**. Устный опрос.** *Примерные вопросы:* - Покажите на примерах значение информационной безопасности в обеспечении национальной безопасности	ОПК-1,ПК-1

		государства - Какие нормативно-правовые акты обеспечивают информационную безопасность на территории РФ? - Покажите на примерах значение информации в условиях войны - Каковы цели и задачи информационной войны в мирное и в военное время?	
3	Тема 3. Информационная безопасность человека	**1. Защита презентации.** *Примерные темы презентаций:* - Персональные данные и их защита. - Влияние средств массовой информации на человека - Интернет и безопасность человека. 2**. Устный опрос.** *Примерные вопросы:* - Какие методы биометрической идентификации человека вам известны? Насколько они могут быть точны? - Почему защита информации о частной жизни граждан стала проблемой в наше время? - Почему в обеспечении защиты информации человек является «самым слабым звеном»? - Перечислите способы защиты человека от негативного влияния информации. *3.* **Практические задания.** *Примерные задания* - разработать правила по безопасному пользованию банковской картой; - разработать памятку по правилам размещения контента в Интернете; - разработать схему-памятку по выходу из деструктивного течения (группы).	ОПК-1,ПК-1

В университете БРС применяется при реализации всех дисциплин (в том числе при оценивании курсовых работ (проектов)) и практик, установленных учебными планами ОП ВО.

Оценка обучающегося по дисциплине в БРС формируется из:

- баллов, полученных при проведении текущего контроля успеваемости;
- баллов, полученных на промежуточной аттестации.

Баллы, полученные обучающимся при проведении текущего контроля успеваемости, представляют собой сумму баллов, полученных по контрольным точкам, а также дополнительных и премиальных баллов.

Результаты текущего контроля успеваемости фиксируются в единых для всего университета контрольных срезах, устанавливаемые после определенного периода обучения.

Для очной формы обучения устанавливаются 2 контрольных среза в каждом семестре. Для заочной – по результатам итогового контроля освоения дисциплины.

По каждому контрольному срезу обучающемуся начисляются баллы за:

- посещаемость в оцениваемый период (20%);
- результаты обучения по (80%):

а) освоенным за оцениваемый период разделам и (или) темам (очная форма обучения);

б) дисциплине (очно-заочная и заочная форма обучения).

По дисциплине обучающемуся могут быть начислены:

- дополнительные баллы;
- премиальные баллы.

Перевод оценок из пятибалльной системы оценивания в 100-балльную по дисциплинам и практикам, а также оценок обучающихся, переведенных в университет из других организаций, осуществляющих образовательную деятельность, в которых БРС не применялась, и в других подобных случаях осуществляется следующим образом:

- «отлично» - 85-100 баллов;
- «хорошо» - 70-84 баллов;
- «удовлетворительно» - 51-69 баллов;
- «зачтено» - 51 балл.

Максимальное количество баллов обучающегося по одной дисциплине (включая баллы, полученные при проведении текущего контроля успеваемости, и баллы, полученные на промежуточной аттестации) составляет 100 баллов.

Если средний рейтинговый балл студента по дисциплине гарантирует ему положительную оценку, в соответствии со шкалой оценок, то преподаватель обязан при желании студента выставить соответствующую оценку без итогового контроля, проставив полученный им средний рейтинговый балл.

Студент может повысить свой рейтинговый балл, проходя итоговый контроль, но при этом весомость набранного в ходе текущего контроля среднего рейтингового балла составляет: 0,5 (50%).

По дисциплине с итоговым контролем – «зачет» студент допускается к сдаче зачета только в том случае, если его средний рейтинговый бал по итогам срезов составляет 30 и выше. В противном случае он автоматически получает – «незачтено». Если его средний рейтинговый балл по итогам срезов составляет 51 и выше, он автоматически получает – «зачтено».

В случаях, когда студент желает повысить свой рейтинговый балл и принимает решение участвовать в промежуточной аттестации, то весомость среднего рейтинговых баллов, полученных при проведении текущего контроля успеваемости и полученных на промежуточной аттестации составляет: 0,5 (50%) и 0,5 (50%).

При проведении текущего контроля успеваемости преподаватель может учесть дополнительные баллы в качестве премиальных баллов, начисляемых обучающемуся:

- определения дополнительных баллов по научно-исследовательской деятельности

Показатель	**Баллы**
Публикация статьи в журнале, сборнике трудов российской, региональной, вузовской конференции	От 5 до 10
Публикация тезисов статьи в сборнике трудов российской, региональной, вузовской конференции, депонирование статьи	От 5 до 10
Доклады на конференциях: внутривузовских, межвузовских, всероссийских и международных	От 5 до 10
Участие в конкурсах грантов: внутривузовский, региональный, всероссийский и международный	От 10 до 15
Участие в конкурсах НИРС: внутривузовский, региональный, всерос-	От 5 до 10

сийский и международный	
Участие в изготовлении демонстрационных материалов, наглядных и учебно-методических пособий и т.д.	От 5 до 10
Получение патента, свидетельства на охрану интеллектуальной собственности	От 10 до 15
Участие в вузовской, межвузовской, всероссийской олимпиадах	От 5 до 10
Внедрение результатов исследований в учебный, производственный процесс	От 5 до 10

Показатель	**Баллы**
Участие в организационной структуре факультета: староста группы, курса, профорг студентов факультета и т.д.	От 10 до 15
Организация разовых общественных акций на факультете, в университете и т.д.	От 10 до 15
Участие в культурно-массовых мероприятиях на факультете, в университете и т.д.	От 10 до 15
Участие в вузовских спортивных, организационно-воспитательных мероприятиях	От 10 до 15
Участие в городских, областных спортивных, организационно-воспитательных мероприятиях	От 10 до 15
Участие в российских, международных спортивных, организационно-воспитательных мероприятиях	От 10 до 20

Весомость среднего рейтингового балла и баллов, полученных на пересдаче, составляет соответственно: 0,3 (30%) и 0,7 (70%).

Если студент после пересдачи не получил положительной оценки, то он в установленные вузом сроки идет на комиссионную пересдачу дисциплины.

Весомость среднего балла, полученного при комиссионной сдаче, составляет, соответственно 0 (0%) и 1 (100%), а баллы, полученные при повторной сдаче – аннулируются.

Студент, пропустивший текущий контроль по уважительной причине (болезнь или иные причины, подтвержденные документально), должен его пройти до сдачи следующего промежуточного контроля по дисциплине. Для этого с разрешения декана факультета, директора института формируется индивидуальная балльно-рейтинговая ведомость.

Итоговая оценка по результатам освоения дисциплины выставляется по 5-балльной шкале или в зачетном формате (в соответствии с формой промежуточной аттестации по дисциплине, установленной учебным планом).

Итоговая оценка заносится в экзаменационную (зачетную) ведомость и зачетную книжку студента.

Итоговый государственный экзамен по специальности оценивается по 100 – балльной шкале.

Правила перевода оценок из 100-балльной системы в пятибалльную систему приведены в таблице 1.

Форма промежуточной аттестации	**Отрицательная оценка**	**Положительные оценки**		
Зачет	**Не зачтено (менее 50 баллов)**	**Зачтено (более 50 баллов)**		
Курсовая работа Зачет с оценкой	Неудовлетворительно (менее 50 баллов)	**Удовлетворительно** (51-69 баллов)	**Хорошо** (70-84 баллов)	**Отлично** (8 5 - 1 0 0 баллов)

7.2. Оценочные материалы для проведения промежуточной аттестации

1. Семестр – 3; форма аттестации – зачет с оценкой.

Вопросы по учебной дисциплине (модулю) для промежуточной аттестации обучающихся (зачет с оценкой)

Понятие об информации. Роль информации в развитии общества.

Понятия информационной безопасности. Цели и задачи информационной безопасности.

Виды и источники опасностей и угроз в сфере информационных процессов и систем.

Информационная безопасность в системе национальной безопасности государства.

Государственная система защиты информации.

Информационная безопасность РФ в условиях глобализации.

Российское законодательство в области информационной безопасности.

Правовая защита интеллектуальной собственности.

Международное право в сфере защиты информации.

Информационно-психологические операции в войнах и вооруженных конфликтах прошлого.

Информационное противоборство в современной войне.

Информационная война и ее особенности.

Цели и задачи информационной войны в мирное и военное время.

Виды информационного оружия и его особенности.

Методы и средства современной информационной войны.

Глобальная информатизация общества и ее последствия.

Информационное общество

Информационное неравенство людей в информационной среде.

Проблема защиты информации о частной жизни граждан.

Информационные технологии и здоровье человека.

Информационный стресс. Компьютерная зависимость.

Информационное воздействие окружающей среды на человека как фактор деструктивного и агрессивного поведения.

Влияние средств массовой информации на человека.

Восприятие рекламной информации и формирование поведения потребителей.

Способы защиты человека от негативного влияния информации.

Цифровая зависимость.

Правила кибергигиены.

Информационная преступность (компьютерные преступления).

Методы и средства защиты обычной и электронной информации.

Информационная безопасность в сети Internet.

Информационная изоляция человека в ЧС.

Возникновение и распространение слухов в ЧС.

Сбор, анализ и оценка информации для принятия решения в ЧС.

Этапы принятия и реализации решения.

Особенности индивидуального принятия решений в ЧС.

Особенности группового принятия решений в ЧС.

Примеры тестовых заданий для оценки качества освоения дисциплины (модуля)

1.Под информационной безопасностью понимается …

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре.

б) программный продукт и базы данных должны быть должны быть защищены по нескольким направлениям от воздействия.

в) нет правильного ответа.

2. Защита информации – это …

а) комплекс мероприятий, направленных на обеспечение информационной безопасности.

б) процесс разработки структуры базы данных в соответствии с требованиями пользователей.

в) небольшая программа для выполнения определенной задачи.

3. От чего зависит информационная безопасность?

а) от компьютеров

б) от поддерживающей инфраструктуры

в) от информации.

4. Основные составляющие информационной безопасности:

а) целостность

б) достоверность

в) конфиденциальность

5. Доступность – это …

а) возможность за приемлемое время получить требуемую информационную услугу

б) логическая независимость

в) нет правильного ответа

6. Целостность – это …

а) целостность информации

б) непротиворечивость информации

в) защищенность от разрушения

7. Конфиденциальность – это …

а) защита от несанкционированного доступа к информации

б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

в) все ответы правильные.

8. Угроза – это …

а) потенциальная возможность определенным образом нарушить информационную безопасность;

б) система программных, языковых, организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.

9. Атака – это …

а) попытка реализации угрозы;

б) потенциальная возможность определенным образом нарушить информационную безопасность;

в) программы, предназначенные для поиска необходимых программ.

10. Источник угрозы – это …

а) потенциальный злоумышленник;

б) злоумышленник;

в) нет правильного ответа.

11. Окно опасности – это …

а) промежуток времени от момента, когда появляется возможность слабого места и до момента, когда пробел ликвидируется;

б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области;

в) формализованный язык для описания задач алгоритма решения пользователя на компьютере.

12. По каким критериям можно классифицировать угроза …

а) по спектру И.Б.;

б) по способу осуществления;

в) по компонентам И.С.

Комплект заданий для промежуточной аттестации обучающихся (экзамен/зачет)

Вариант 1.

Задание 1

1. По уровню обеспеченной защиты все системы делят:

а) сильной защиты;

б) особой защиты;

в) слабой защиты.

2. Правовое обеспечение безопасности информации – это …

а) совокупность законодательных актов, нормативно – правовых документов, руководств, требований, которые обязательны в системе защиты информации;

б) система программных, языковых, организационных и технических средств, предназначенных для накопления и коллективного использования данных;

в) нет правильного ответа.

3. Правовое обеспечение безопасности информации делится…

а) международно – правовые нормы;

б) национально – правовые нормы;

в) все ответы правильные.

4. Информацию с ограниченным доступом делят на…

а) государственную тайну;

б) конфиденциальную информацию;

в) достоверную информацию.

5. Что относится к государственной тайне?

а) сведения защищаемые государством в области военной, экономической деятельности;

б) документированная информация;

в) нет правильного ответа.

Вариант 1.

Задание 2. Ситуационные задачи

Задача № 1.

Вы – сотрудник образовательного учреждения. Есть большое количество информации о студентах и их данных.

1. Перечислите возможные способы обеспечения целостности и предотвращения уничтожения данных.

2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Ответ:

Резервное копирование, архивирование.

В случае резервного копирования речь идет о кратко – или среднесрочном дополнительном хранении данных, которые еще могут понадобиться пользователям в их работе. Если, например, в результате повреждения жесткого диска или по иным причинам текущие данные теряются, их удастся быстро восстановить. Так можно эффективно защитить данные от разного рода случайностей. Время хранения резервных копий устанавливается не слишком продолжительное.

Вариант 2

Задание 1

1. Вредоносная программа – это …

а) программа, специально разработанная для нарушения нормального функционирования систем;

б) упорядочение абстракций, расположение их по уровням;

в) процесс разделения элементов абстракции, которые образуют ее структуру и поведение.

2. Основополагающие документы для обеспечения безопасности внутри организации:

а) трудовой договор сотрудников;

б) должностные обязанности руководителей;

в) коллективный договор.

3.Какие средства используются на инженерных и технических мероприятиях в защите информации:

а) аппаратные;

б) криптографические;

в) физические.

4. Основным источником угроз информационной безопасности являются

а) хищение жестких дисков, подключение к сети;

б) перехват данных, хищение данных, изменение архитектуры системы;

в) хищение данных, подкуп системных администраторов, нарушение регламента работы.

5. Основные объекты информационной безопасности:

а) компьютерные сети, базы данных;

б) информационные системы, психологическое состояние пользователей;

в) бизнес – ориентированные, коммерческие системы.

Вариант 2

Задание 2. Ситуационные задачи

Задача № 1.

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

Какие правила обеспечения информационной безопасности нарушены?

Какие символы должны быть использованы при записи пароля?

Ответ к задаче:

1.Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера телефонов, автомобилей и другие пароли, которые можно угадать.

2. в качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность ее угадывания. Пароль должен легко запоминаться.

3. Перечень компетенций и индикаторов их достижения, описание критериев оценивания компетенций представляются в таблице.

Таблица10.

Код и наименование компетенции и для ОП ВО, индикаторы достижения компе-	**Шкала оценивания**			
	«отлично»	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**

тенции (ИДК)				
Компетенция (шифр и индикаторы) ОПК-1, ОПК-1.1, ОПК-1.2.ПК-1,	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам промежуточной аттестации обнаружил системные знания по всем разделам программы дисциплины, продемонстрировал способность к их самостоятельному пополнению, в том числе в рамках учебно-исследовательской и научно-исследовательской деятельности	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам промежуточной аттестации обнаружил системные знания по всем разделам программы дисциплины, продемонстрировал способность к их самостоятельному пополнению в процессе учебной деятельности, за исключением учебно-исследовательской и научно-исследовательской деятельности	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам промежуточной аттестации обнаружил фрагментарные знания по всем разделам программы дисциплины	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам промежуточной аттестации обнаружил отсутствие знаний по основным разделам программы дисциплины;
ПК-1.1, ПК-1.2, ПК-1.3.	представил результаты выполнения всех заданий для самостоятельной работы полностью и качественно, на творческом уровне, выразил личностную значимость деятельности	представил результаты выполнения всех заданий для самостоятельной работы, но на репродуктивном уровне	представил результаты выполнения более 70 % всех заданий для самостоятельной работы	выполнил менее 50% предусмотренных рабочей программой дисциплины задания для самостоятельной работы
	при устном ответе высказал самостоятельное суждение на основе исследования теоретических источни-	при устном ответе высказал самостоятельное суждение на основе исследования тео-	при устном ответе высказал репродуктивное суждение по предлагаемому вопросу из теоретических источников, не	при устном ответе допустил фактические ошибки в использовании научной терминологии и

	ков, логично и аргументированно изложил материал, связал теорию с практикой посредством иллюстрирующих примеров, свободно ответил на дополнительные вопросы	ретических источников, логично и аргументированно изложил материал, испытывал затруднение связать теорию с практикой посредством иллюстрирующих примеров, ответить на дополнительные вопросы	смог связать теорию с практикой (не привел примеров), в ответе на дополнительные вопросы испытывал затруднение	изложении учебного содержания, сделал ложные выводы

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Таблица11.

№ п/п	Наименование литературы	Местонахождение	Кол. экземпляров
Основная литература			
1	Бабаш, А.В. Информационная безопасность: Лабораторный практикум/ А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с.	Библиотека ДГПУ	7
2	Бабаш, А.В. Информационная безопасность: Лабораторный практикум: Учебное пособие/А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с.	Библиотека ДГПУ	25
3	Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб.пособие для студ.высш.учеб.заведений / П.Б.Хорев. — М.: Академия, 2005. — 256с.	Библиотека ДГПУ	5
4	Авдошин, Сергей Михайлович. Криптоанализ : современное состояние и перспективы развития / С. М. Авдошин, А. А. Савельева. — М.: Новые технологии, 2007. — 32 с.	Библиотека ДГПУ	5
5	Колин, Константин Константинович. Гуманитарные проблемы информационной безопасности / К. К. Колин. — М.: Новые технологии, 2007. — 32 с.	Библиотека ДГПУ	3
6	Калинин, Илья Александрович. Элективный курс "Основы информационной безопасности при работе в телекоммуникационных сетях" / И. А. Калинин, Н. Н. Самылкина. — М.: Чистые пруды, 2007. — 32 с.	Библиотека ДГПУ	5
Дополнительная литература			
1	Основы организационного обеспечения информационной безопасности объектов информатизации: учеб.пособие / С.Н.Семкин [и др.]. — М.: Гелиос АРВ, 2005. — 192с.	Библиотека ДГПУ	5

2	Гафнер В.В. Информационная безопасность: Учебное пособие. Рн/Д: Феникс, 2010. – 324 с.	Библиотека ДГПУ	8
3	Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие:- Ст. Оскол:ТНТ,2010. – 384 с.	Библиотека ДГПУ	3
4	Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: монография / Л.Л. Ефимова, С.А. Кочерга.-М.:ЮНИТИ, 2013.- 239 с.	Библиотека ДГПУ	Электронный читальный зал
5	Кузнецова А.В. Искусственный интелект и информационная безопасность общества/ А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.	Библиотека ДГПУ	Электронный читальный зал
6	Семененко В.А. Информационная безопасность: Учебное пособие. –М.: МГИУ, 2011. -277 с.	Библиотека ДГПУ	5
7	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие.- М.: Форум, 2018.- 256 с.	Библиотека ДГПУ	5
8	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие.- М.:ИД Форум, НИЦ Инфра-М, 2013.- 416 с.	Библиотека ДГПУ	5
9	Мельников Д.А. Информационная безопасность открытых систем: учебник. – М.: Флинта, 2013. – 448 с.	Библиотека ДГПУ	5
10	Халимбекова А.М., Магомедов Р.В., Абдуразаков Ш.М. Учебно-методический комплекс «Безопасность жизнедеятельности» – Махачкала: 2013. – 176 с.	Библиотека ДГПУ	5
11	Омаров М.М., Омарова М.М-г. Безопасность жизнедеятельности. Учебное пособие для вузов. Махачкала: ДГПУ, 2016. – 359 с.	Библиотека ДГПУ	5
12	Омаров М.М. Безопасность жизнедеятельности. (учебно-методическое пособие) второе издание. Махачкала: ДГПУ, 2017. – 227 с.	Библиотека ДГПУ	2
13	Малюк А.А. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 147 с.	Библиотека ДГПУ	4
14	Ярочкин В.И. Информационная безопасность: Учебник для вузов. – М.: Академический проспект, 2008.- 544 с.	Библиотека ДГПУ	1
15	Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. С.-П.,2004.-384 с.	Библиотека ДГПУ	2

8.3. Перечень Интернет-ресурсов, необходимых для освоения дисциплины (модуля)

Учебные издания, доступные через ЭБС

1. BiblioclubURL: http://www.biblioclub.ru/book/57583/
2. Biblioclub URL: http://www.biblioclub.ru/book/42808/
3. Biblioclub URL: http://www.biblioclub.ru/book/116766/
4. Biblioclub URL: http://www.biblioclub.ru/book/116583/
5. Biblioclub URL: http://www.biblioclub.ru/book/56296/
6. Biblioclub URL: http://www.biblioclub.ru/book/117529/
7. http://bibHodub.ru/index.php?page=book&id=271507
8. http://bibliodub.ru/mdex.php?page=book&id=271593
9. http://www.consultant.ru/document/cons doc LAW 169811/

10. URL: http://bibliodub.ru/mdex.php?page=book&id=235824

11. http://bibHodub.ru/index.php?page=book&id=271507

Для освоения дисциплины «Информационная безопасность» рекомендуется пользоваться следующими ресурсами: http://www.mchs.gov.ru/library - сайт МЧС РФ, библиотека. http://gz-journal.ru/ - журнал «Гражданская защита». http://www.school-obz.org/ - журнал «Основы безопасности жизнедеятельности».

8.4. Перечень информационных технологий и программного обеспечения

Для осуществления образовательного процесса по дисциплине необходимо использование следующего лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Реализация дисциплины требует наличия учебной аудитории, компьютерного класса, оборудованного рабочими местами для выполнения учебных работ с использованием стандартных пакетов программ.

Оборудование учебного кабинета: комплект образовательных стандартов, учебных программ по основам безопасности жизнедеятельности, электронные учебники по основам безопасности жизнедеятельности.

Технические средства обучения: компьютер, мультимедийный проектор.

Электронные ресурсы (видео уроки):

«Защита целостности информации при хранении».

«Построение систем защиты от угрозы».

«Единые критерии безопасности информационных технологий».

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Внеаудиторная самостоятельная работа студентов – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа студента предполагает изучение части тем, подготовку докладов, сообщений по курсу «Информационная безопасность». Студентами самостоятельно рассматриваются предлагаемые преподавателем вопросы к практи-

ческим занятиям, разрабатываются сценарии дискуссий и альтернативных выступлений. Данные виды учебной деятельности предполагают формирование умений работы с законодательной базой, нормативными документами, научной, учебной,

ответа на зачете или экзамене, методической литературой, которые приобретаются студентами в процессе анализа и систематизации материала по заданным темам.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Требования, предъявляемые к самостоятельной работе студентов.

Лекционные занятия

Главным звеном в обучении является вузовская лекция, цель которой – формирование ориентировочной основы для последующего усвоения студентами учебного материала. Назначение лекции – это подготовка студентов к самостоятельной работе с литературой.

В ходе лекционного курса проводится изложение современных научных материалов, освещение главных проблем информационной безопасности; развитие системно-ориентированного взгляда на сложные вопросы вероятностной оценки и прогнозирования событий опасного типа с целью управления рисками в информационно – социальных и информационно - экономических системах.

Студенту необходимо конспектировать лекционный материал. При этом желательно оставлять поля для различных заметок. Нет необходимости записывать каждое слово преподавателя, т.е. записи должны быть избирательными. Рекомендуется полностью записывать только определения.

При конспектировании лекции необходимо применять сокращение слов, по возможности использовать аббревиатуру, на полях указать, что означает то или иное сокращение. Например, т.е.- то есть, т.к. – так как, ПДК - предельно допустимые концентрации, БЖД – безопасность жизнедеятельности и т.д. Или же в конце тетради можно вести словарь сокращений и новых терминов.

Если лекция сопровождается рисунками, схемами, сделанные преподавателем на доске студент обязательно должен у себя в тетради их зарисовывать, так как наглядность улучает усвояемость читаемого материала.

Если у студента возникают вопросы по читаемой лекции, ему необходимо записать их на полях и в конце лекции обратится за разъяснениями к преподавателю.

Практические занятия

Практические занятия по дисциплине «Информационная безопасность» проводятся с целью расширенного изучения безопасности в информационной среде человека; детального раскрытия информационной безопасности и более углубленного изучения источников, причин, классификации информационной опасности.

Необходимо выработать простейшие навыки безопасного поведения, уметь реально оценить опасность, дать прогноз, т.е. выработать навыки профессиональной деятельности.

Посещение практического занятия – это необходимое условие допуска студента к сдаче зачета. В случае пропуска занятий по уважительной причине его необходимо отработать.

Задание к практическим занятиям необходимо получить у преподавателя за 5-6 дней для подготовки к нему. За это время рекомендуется просмотреть все вопросы и литературу к ним. При необходимости законспектировать тот или иной вопрос в тетради.

Если преподавать рекомендовал подготовку докладов, рефератов для обсуждения их на занятии необходимо заранее подготовить материал, изучить его, выделить основные положения, сделать собственные выводы.

При этом остальные студенты не должны оставаться пассивными слушателями, а активно участвовать в обсуждении, т.е. доклад предполагает обмен мнениями участников практического занятия. Здесь реализуется принцип совместной деятельности, сотворчества.

Таким образом, студент должен вести активную познавательную работу. Важно научиться включать новую информацию в систему уже имеющихся знаний, уметь анализировать прочитанное и услышанное, т.е. творчески подходить к освоению новых знаний.

Для подготовки к практическим занятиям студенту необходимо иметь конспект лекций, план соответствующую литературу.

Если студент готовит реферат или доклад, то он может использовать литературу из списка дополнительной, газеты, журналы, Интернет, при этом не рекомендуется сплошное списывание глав из учебников. Студент должен научиться работать с несколькими источниками, уметь отобрать необходимый ему материал, максимально его синтезировать и изложить в соответствии с темой.

При проведении текущих аттестаций преподаватель проводит тестирование по пройденным темам курса. Студентам предоставляются индивидуальные тестовые задания, содержащие не менее 60 вопросов. На каждый вопрос имеется несколько (не менее 4) вариантов ответа и необходимо найти правильный, если в вопросе 2 и более правильных ответов преподаватель должен это указать. Время тестирования 60 минут.

При подготовке к сдаче зачета студенту достаточно иметь конспект лекций, тетрадь для практических занятий и учебно-методическое пособие в виде развернутого курса лекций или словаря – справочника по дисциплине «Информационная безопасность». Перечень зачетных вопросов можно взять у преподавателя в начале «семестра, и при необходимости консультироваться по непонятным вопросам.

При выполнении реферативной работы необходимо учитывать, что ее минимальный объем должен быть не менее 10 страниц машинописного текста, включающих план изложения темы, ее содержания со ссылками на использованную литературу, выводы и библиографию, составленную в алфавитном порядке с учетом современных требований.

Содержание работы должно быть научным, теоретические положения систематизированы и сведены к четким и логичным выводам, раскрыта практическая значимость изучаемого вопроса, отражена связь с будущей профессией и собственное отношение к наиболее волнующим моментам.

Самостоятельная работа позволяет через систему усложняющихся заданий лучше усвоить курс «Информационная безопасность»

11. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Под специальными условиями для получения образования обучающихся с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития таких студентов, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания вуза и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающихся с ограниченными возможностями здоровья.

Обучение в рамках учебной дисциплины обучающихся с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта института в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электроном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию института.

2) для лиц с ограниченными возможностями здоровья по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ограниченными возможностями адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины профессорско-преподавательскому составу рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ограниченными возможностями здоровья в установлении полноценных межличностных отношений с другими обучающихся, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ограниченными возможностями здоровья устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и другое). При необходимости предоставляется дополнительное время для подготовки

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ):
Б1.О.08 ПРЕДМЕТНО-МЕТОДИЧЕСКИЙ МОДУЛЬ
Б1.О.08.08 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Цель освоения дисциплины (модуля):

Цель – формирование общепрофессиональных и профессиональных компетенций в области информационной безопасности личности, организации, общества, государства и основных мерах по её обеспечению.

Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.08.08 «Информационная безопасность» относится к обязательной части и модулю Б1.О.08 «Предметно – методический модуль» учебного плана по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), профили «Технология» и «Безопасность жизнедеятельности».

Предшествующими дисциплинами учебного плана являются: Методы и средства проектирования информационных систем управления, Администрирование информационных систем управления.

Дисциплина «Информационная безопасность» является основой для применения полученных теоретических знаний на практике. Дисциплина изучается на 2 курсе в 3 семестре.

Требования к результатам освоения дисциплины(модуля):

Перечисляются код и наименование компетенций, индикаторы достижения компетенций

ОПК-1 Способен осуществлять профессиональную деятельность в соответствии с нормативно-правовыми актами в сфере образования и нормами профессиональной этики.

ПК-1 Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных.

Общая трудоемкость дисциплины (модуля) составляет 3 зачетные единицы (108 часов).

Семестр: 3

Основные разделы дисциплины (модуля):

Тема 1. Информация и информационная безопасность в современном мире

Тема 2. Обеспечение информационной безопасности РФ

Тема 3. Информационная безопасность человека.

Формы текущего контроля успеваемости и промежуточной аттестации: зачет с оценкой.

Автор: Исаева М.М. – к. п. н., доцент кафедры безопасности жизнедеятельности