

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Байханов Исмаил Баутдинович  
Должность: Ректор  
Дата подписания: 14.07.2023 17:45:29  
Уникальный программный ключ:  
442c337cd125e1d014f62698c9d813e502697764

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**  
**ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«ЧЕЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»**  
**КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ПРЕПОДАВАНИЯ**  
**ИНФОРМАТИКИ**

Утверждаю:  
И.о. зав. каф.: Р.Ю. Исраилов  
  
(подпись)  
Протокол № 8 заседания  
кафедры от 27.04.2023

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**  
**Информационная безопасность**  
(наименование дисциплины (модуля))

**Направление подготовки**  
**44.03.05 Педагогическое образование (с двумя профилями подготовки)**  
(код и направление подготовки)

**Профили подготовки**  
**«Английский язык» и «Информатика»**

**Квалификация**  
**Бакалавр**

**Форма обучения**  
**очно-заочная**

**Год набора 2023**

**Грозный, 2023**

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

## 1.1. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность» (Б1.В.ДВ.04.02) относится к дисциплинам по выбору, части, формируемая участниками образовательных отношений. Дисциплина (модуль) изучается на 5 курсе в 10 семестре.

## 1.2. Цель освоения дисциплины (модуля)

**Целью:** является формирование у студентов принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

## 1.3. Планируемые результаты обучения по дисциплине (модулю)

Достижение цели освоения дисциплины (модуля) обеспечивается через формирование следующих компетенций (*с указанием шифра компетенции*):

Таблица 1

Код и наименование компетенции	Код и наименование индикатора достижения компетенций, которые формирует дисциплина (модуль)	Планируемые результаты обучения
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.	<b>Знает:</b> структуру, состав и дидактические единицы предметной области (преподаваемого предмета). <b>Умеет:</b> осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО <b>Владеет:</b> навыками разработки различных форм учебных занятий, применения методов, приемов и технологий обучения, в том числе информационных

## 1.4. Объем дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 108ч / 3з.е. (академ. часов)

Таблица 2

Вид учебной работы	Количество академ. часов	
	Очно	
<b>4.1. Объем контактной работы обучающихся с преподавателем</b>	<b>72</b>	
<b>4.1.1. аудиторная работа</b>	<b>24</b>	
в том числе:		
лекции	12/6	
практические занятия, семинары, в том числе практическая подготовка	12/6	
лабораторные занятия		
<b>4.1.2. внеаудиторная работа</b>	<b>48</b>	
в том числе:		
индивидуальная работа обучающихся с преподавателем		
курсовое проектирование/работа		
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		
<b>4.2. Объем самостоятельной работы обучающихся</b>		
в том числе часов, выделенных на подготовку к экзамену		

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 2.1. Тематическое планирование дисциплины (модуля):

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоёмкость в акад. часах		Лекции		Практ. занятия		Лаб. занятия		Сам. работа	
		Очно	Заочно	Очно	Заочно	Очно	Заочно	Очно	Заочно	Очно	Заочно
1.	<b>Раздел 1. Виды компьютерной безопасности.</b> Информационная безопасность в системе национальной безопасности. Обеспечение информационной безопасности объектов информационной сферы государства	24		4		4				16	
2.	<b>Раздел 2. Уровни компьютерной безопасности.</b> Общая характеристика компьютерной безопасности. Испытание программного и	24		4		4				16	

	аппаратного уровней компьютерной безопасности.									
3.	<b>Раздел 3. Компьютерные системы.</b> Система физической защиты компьютерных систем. Организация и аудит безопасности компьютерных систем.	24		4		4				16
	<i>Подготовка к экзамену (зачету)</i>	X	X							X X
	Итого:	72		12		12				48

## 1.2. Содержание разделов дисциплины (модуля):

Таблица 4

№ п/п	Наименование темы (раздела) дисциплины	Содержание дисциплины (дидактические единицы) <i>(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования)</i>
1.	<b>Раздел 1. Виды компьютерной безопасности.</b>	Информационная безопасность в системе национальной безопасности. Обеспечение информационной безопасности объектов информационной сферы государства
2.	<b>Раздел 2. Уровни компьютерной безопасности.</b>	Общая характеристика компьютерной безопасности. Испытание программного и аппаратного уровней компьютерной безопасности.
3.	<b>Раздел 3. Компьютерные системы.</b>	Система физической защиты компьютерных систем. Организация и аудит безопасности компьютерных систем.

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 3.1. Учебно-методическое обеспечение самостоятельной работы обучающихся

Таблица 5

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1.	<b>Раздел 1. Виды компьютерной безопасности.</b>	Устный опрос Выполнение практико-ориентированных заданий
2.	<b>Раздел 2. Уровни компьютерной безопасности.</b>	Устный опрос. Выполнение практико-ориентированных заданий
3.	<b>Раздел 3. Компьютерные системы.</b>	Устный опрос Выполнение практико-ориентированных заданий

### 3.2 Учебно-методическое и информационное обеспечение программы дисциплины (модуля)

#### 3.2.1. Основная и дополнительная литература

Таблица 6

Виды литературы	Автор, название литературы, город, издательство, год	Количество часов, обеспеченных указанной литературой Аудит./самост.	Количество обучающихся	Количество экземпляров в библиотеке университета	Режим доступа ЭБС/электронный носитель (CD,DVD)	Обеспеченность обучающихся литературой, (5гр./4гр.)x100%)
1	2	3	4	5	6	7
<b>Основная литература</b>						
1	Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. - Санкт-Петербург: Лань, 2021. - 324 с. - ISBN 978-5-8114-6738-9.- Текст: электронный //	108	25		Лань: электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/165837">https://e.lanbook.com/book/165837</a>	100%
2	Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург: Лань, 2022. - 160 с. - ISBN 978-5-8114-4042-9. - Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: <a href="https://e.lanbook.com/book/206285">https://e.lanbook.com/book/206285</a>	100%

3	Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. - 3-е изд., стер. - Санкт-Петербург: Лань, 2021. - 108 с. - ISBN 978-5-8114-8370-9. - Текст: электронный //	108	25		Лань: электронно-библиотечная система. URL: <a href="https://e.lanbook.com/book/175506">https://e.lanbook.com/book/175506</a>	100%
4	Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 4-е изд., стер. - Санкт-Петербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. - Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: <a href="https://e.lanbook.com/book/217445">https://e.lanbook.com/book/217445</a>	100%
<b>Дополнительная литература</b>						
1	Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 3-е изд., стер. - Санкт-Петербург: Лань, 2021. - 124 с. - ISBN 978-5-8114-7970-2.- Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: <a href="https://e.lanbook.com/book/169817">https://e.lanbook.com/book/169817</a>	100%
2	Титова, Л. Н. Информационная безопасность и защита информации: учебно-методическое пособие / Л. Н. Титова. - Уфа: БГПУ имени М. Акмуллы, 2013. - 108 с.- Текст: электронный //	108	25		Лань: электронно-библиотечная система. - URL: <a href="https://e.lanbook.com/book/56704">https://e.lanbook.com/book/56704</a>	100%

3	Фомин, Д. В. Информационная безопасность: учебник / Д. В. Фомин. - Москва: Ай Пи Ар Медиа, 2022. - 222 с. - ISBN 978-5-4497-1548-7. - Текст: электронный //	108	25		Цифровой образовательный ресурс IPR SMART: [сайт]. - URL: <a href="https://www.iprbookshop.ru/118876.html">https://www.iprbookshop.ru/118876.html</a>	100%
---	---	-----	----	--	---	------

### 3.2.2. Интернет-ресурсы

1. Цифровой образовательный ресурс «IPR SMART». <https://www.iprbookshop.ru>
2. Образовательная платформа «Юрайт». <https://urait.ru/>
3. Электронно-библиотечная система «Лань». <https://e.lanbook.com/>
4. МЭБ (межвузовская электронная библиотека) НГПУ. <https://icdlib.nspu.ru/>
5. Научная электронная библиотека ELIBRARY.RU. <https://www.elibrary.ru/>
6. СПС «КонсультантПлюс». <http://www.consultant.ru/>  
ОТКРЫТЫЙ РЕСУРС
7. Единое окно доступа к образовательным ресурсам. <http://window.edu.ru/catalog/>
8. Научная электронная библиотека «Киберленинка». <https://cyberleninka.ru/>.

### 3.3. Материально-техническое обеспечение дисциплины

При необходимости для проведения занятий используется аудитория, оборудованная компьютером с доступом к сети Интернет с установленным на нем необходимым программным обеспечением и браузером, проектор (интерактивная доска) для демонстрации презентаций и мультимедийного материала. В соответствии с содержанием практических (лабораторных) занятий при их проведении используется аудитория, рабочие места обучающихся в которой оснащены компьютерной техникой, имеют широкополосный доступ в сеть Интернет и программное обеспечение, соответствующее решаемым задачам.

Для осуществления образовательного процесса по дисциплине необходима следующая материально-техническая база:

Таблица 7

<b>Помещения для осуществления образовательного процесса</b>	<b>Перечень основного оборудования (с указанием кол-ва посадочных мест)</b>	<b>Адрес (местоположение)</b>
<b>Аудитория для проведения лекционных занятий</b>		
5-01	- стандартно оборудованные лекционные аудитории с видеопроектором и настенным экраном - персональный компьютер или ноутбук под управлением MS Windows XP Pro, MS Windows 7, пакет Microsoft Office с возможностью подключения проектора 40 посадочных мест	Чеченская Республика г. Грозный, пр. Х. Исаева, 62. Учебный корпус №1
<b>Аудитории для проведения практических занятий, контроля успеваемости</b>		
5-05	- класс персональных компьютеров под управлением MS Windows XP Pro (Win7), включенных в корпоративную сеть университета 25 посадочных мест	Чеченская Республика г. Грозный, пр. Х. Исаева, 62. Учебный корпус №1
<b>Помещения для самостоятельной работы</b>		
Компьютерный центр	Компьютерная мебель на 52 посадочных мест, 52 компьютеров с выходом в Интернет, системный блок (52 шт.), клавиатура (52 штук), мышь (52 штук)	Чеченская Республика г. Грозный, ул. Субры Кишиевой, № 33

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ / МОДУЛЯ

### 4.1. ХАРАКТЕРИСТИКА ОЦЕНОЧНЫХ СРЕДСТВ

Контроль и оценка результатов освоения дисциплины / модуля осуществляется преподавателем в процессе проведения практических и лабораторных занятий, контрольных работ, а также выполнения обучающимися индивидуальных заданий, проектов, исследований и т.д.

*Таблица 8*

№ п/п	Наименование темы (раздела) с контролируемым содержанием	Код и наименование проверяемых компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1.	<b>Раздел 1. Виды компьютерной безопасности.</b> Информационная безопасность в системе национальной безопасности. Обеспечение информационной безопасности объектов информационной сферы государства	ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	тестирование, практико-ориентированное задание, доклад	контрольная работа



2.	<b>Раздел 2. Уровни компьютерной безопасности.</b> Общая характеристика компьютерной безопасности. Испытание программного и аппаратного уровней компьютерной безопасности.	ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	тестирование, практико-ориентированное задание, доклад	контрольная работа
3.	<b>Раздел 3. Компьютерные системы.</b> Система физической защиты компьютерных систем. Организация и аудит безопасности компьютерных систем.	ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	тестирование, практико-ориентированное задание, доклад	контрольная работа

## 4.2. Оценочные средства для проведения текущего контроля успеваемости

### 4.2.1. Наименование оценочного средства: *тест*

*Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.*

#### *Примерные вопросы для тестирования*

Правильный вариант ответа отмечен знаком +

**1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2) Основными источниками угроз информационной безопасности являются все указанное в списке:**

- Хищение жестких дисков, подключение к сети, инсайдерство
- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

**3) Виды информационной безопасности:**

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

**4) Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

**5) Основные объекты информационной безопасности:**

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

**6) Основными рисками информационной безопасности являются:**

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

**7) К основным принципам обеспечения информационной безопасности относятся:**

- + Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

**8) Основными субъектами информационной безопасности являются:**

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

**9) К основным функциям системы безопасности можно отнести все перечисленное:**

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компаний
- Внедрение аутентификации, проверки контактных данных пользователей

**тест 10) Принципом информационной безопасности является принцип недопущения:**

- + Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

**11) Принципом политики информационной безопасности является принцип:**

- + Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

**12) Принципом политики информационной безопасности является принцип:**

- + Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

**13) Принципом политики информационной безопасности является принцип:**

- + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

**14) К основным типам средств воздействия на компьютерную сеть относятся:**

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

**15) Когда получен спам по e-mail с приложенным файлом, следует:**

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

**16) Принцип Кирхгофа:**

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

+ Секретность закрытого сообщения определяется секретностью ключа

**17) ЭЦП – это:**

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

**18) Наиболее распространены угрозы информационной безопасности корпоративной системы:**

- Покупка нелегального ПО

+ Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

**19) Наиболее распространены угрозы информационной безопасности сети:**

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

+ Сбой (отказ) оборудования, нелегальное копирование данных

**тест\_20) Наиболее распространены средства воздействия на сеть офиса:**

- Слабый трафик, информационный обман, вирусы в интернет

+ Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение администрирования, топологии

**21) Утечкой информации в системе называется ситуация, характеризующаяся:**

+ Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

**22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

+ Целостность

- Доступность

- Актуальность

**23) Угроза информационной системе (компьютерной сети) – это:**

+ Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

**24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

- Регламентированной

- Правовой

+ Защищаемой

**25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:**

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

**26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

+ Владелец сети

- Администратор сети

- Пользователь сети

**27) Политика безопасности в системе (сети) – это комплекс:**

- + Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

**28) Наиболее важным при реализации защитных мер политики безопасности является:**

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- + Аудит, анализ уязвимостей, риск-ситуаций

**Критерии оценивания результатов тестирования**

Таблица 9

<b>Уровень освоения</b>	<b>Критерии</b>	<b>Баллы</b>
Максимальный уровень	Выполнены правильно все задания теста (тест зачтен)	2
Средний уровень	Выполнено правильно больше половины заданий (тест зачтен)	1
Минимальный уровень	Выполнено правильно меньше половины заданий (тест не зачтен)	0

**4.2.2. Наименование оценочного средства:** практико-ориентированное задание

Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.

**Примерные практико-ориентированные задания**

1. Законодательство РФ в области информационной безопасности
2. Изучение положений о государственном лицензировании деятельности в области защиты информации
3. Система сертификации средств криптографической защиты информации
4. Изучения положения о сертификации средств вычислительной техники и связи
5. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации
6. Изучение особенностей аттестации помещений по требованиям безопасности информации

**Критерии оценивания результатов выполнения практико-ориентированного задания**

Таблица 10

<b>Уровень освоения</b>	<b>Критерии</b>	<b>Баллы</b>
Максимальный уровень	Задание выполнено правильно: выводы аргументированы, основаны на знании материала, владении категориальным аппаратом	3
Средний уровень	Задание выполнено в целом правильно: но допущены ошибки в аргументации, обнаружено поверхностное владение терминологическим аппаратом	2
Минимальный уровень	Задание выполнено с ошибками в формулировке тезисов и аргументации, обнаружено слабое владение терминологическим аппаратом	1
Минимальный уровень не достигнут	Задание не выполнено или выполнено с серьёзными ошибками	0

### **4.2.3. Наименование оценочного средства: доклад/сообщение**

*Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки*

#### **Темы докладов:**

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
9. Система обеспечения информационной безопасности.
10. Обеспечение информационной безопасности Российской Федерации.
11. Понятие информационной войны. Проблемы информационной войны.
12. Информационное оружие и его классификация.
13. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
14. Уровни ведения информационной войны. Информационные операции. Психологические операции.
15. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
16. Основные положения государственной информационной политики Российской Федерации.
17. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
18. Виды защищаемой информации в сфере государственного и муниципального управления.
19. Обеспечение информационной безопасности организации.
20. Характеристика эффективных стандартов по безопасности.
21. Требования к полноте эффективных стандартов по безопасности.
22. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
23. Информация - фактор существования и развития общества.
24. Обеспечение информационной безопасности: содержание и структура понятия.
25. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
26. Обеспечение информационной безопасности Российской Федерации.
27. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
28. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
29. Административный уровень обеспечения информационной безопасности.
30. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
31. Корпоративная нормативная база по защите информации.
32. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).

33. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).
34. Нормативно-методические документы по обеспечению безопасности информации.
35. Управление персоналом на предприятиях и в организациях.
36. Подбор и расстановка кадров.
37. Мотивация добросовестной деятельности сотрудников.
38. Порядок проведения служебных расследований.
39. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.
40. Категорирование объектов информатизации.
41. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
42. Классификация автоматизированных систем в составе объектов вычислительной техники.
43. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.
44. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
45. Правовые основы сертификации и аттестации средств защиты информации.
46. Основные понятия и принципы сертификации.
47. Организация и проведение сертификации.
48. Организация и проведение лицензирования, сертификации и аттестации.
49. Требования к объектам информатизации и необходимость проведения их аттестации. Порядок проведения аттестации объектов информатизации.
50. Права и обязанности органов системы аттестации объектов информатизации.
51. Проведение аттестационных испытаний.
52. Основы организации и обеспечения работ по технической защите информации.
53. Цели и задачи защиты информации.
54. Организация защиты конфиденциальной информации.
55. Концепция безопасности предприятия и ее содержание.
56. Организация работы подразделений (служб) обеспечения информационной безопасности.
57. Организация защиты информации на предприятии.
58. Выявление и классификация угроз.
59. Принципы обеспечения информационной безопасности.
60. Управление информационной безопасностью.
61. Политика безопасности.
62. Разработка и внедрение системы управления информационной безопасности. Обеспечение информационной безопасности организации.
63. Характеристика эффективных стандартов по безопасности.
64. Требования к полноте эффективных стандартов по безопасности.
65. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
66. Информация - фактор существования и развития общества.
67. Обеспечение информационной безопасности: содержание и структура понятия.
68. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
69. Обеспечение информационной безопасности Российской Федерации.
70. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности.
71. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

72. Административный уровень обеспечения информационной безопасности.
73. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
74. Классификация автоматизированных систем в составе объектов вычислительной техники.
75. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.
76. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
77. Правовые основы сертификации и аттестации средств защиты информации.
78. Основные понятия и принципы сертификации.
79. Организация и проведение сертификации.
80. Организация и проведение лицензирования, сертификации и аттестации.
81. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
82. Основные положения государственной информационной политики Российской Федерации.
83. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
84. Виды защищаемой информации в сфере государственного и муниципального управления.
85. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
86. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
87. Административный уровень обеспечения информационной безопасности.

#### **4.2.4. Наименование оценочного средства: контрольная работа**

*Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.*

#### ***Примерное задание для контрольной работы:***

- ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ
- ИСТОРИЯ И СОВРЕМЕННЫЕ ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
- КЛАССИФИКАЦИЯ ВИРУСОВ И ВРЕДОНОСНЫХ ПРОГРАММ
- КОНТРОЛЬНАЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВАРИАНТ
- МЕТОДЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

#### ***Критерии оценивания результатов контрольной работы***

*Таблица 12*

<b><i>Балл (интервал баллов)</i></b>	<b><i>Уровень освоения</i></b>	<b><i>Критерии оценивания уровня освоения компетенций*</i></b>
<i>10</i>	<i>Максимальный уровень (интервал)</i>	<i>Контрольная работа оформлена в соответствии с предъявляемыми требованиями, содержит 1-2 мелких ошибки; ответы студента правильные, четкие, содержат 1-2 неточности</i>
<i>[6-8]</i>	<i>Средний уровень (интервал)</i>	<i>Контрольная работа содержит одну принципиальную или 3 или более недочетов; ответы студента правильные, но их</i>


		<i>формулирование затруднено и требует наводящих вопросов от преподавателя</i>
<i>[3-5]</i>	<i>Минимальный уровень (интервал)</i>	<i>Контрольная работа оформлена в соответствии с предъявляемыми требованиями, неполное раскрытие темы в теоретической части и/или в практической части контрольной работы; ответы студенты формально правильны, но поверхностны, плохо сформулированы, содержат более одной принципиальной ошибки</i>
<i>Менее 3</i>	<i>Минимальный уровень (интервал) не достигнут.</i>	<i>Контрольная работа содержит более одной принципиальной ошибки моделей решения задачи; контрольная работа оформлена не в соответствии с предъявляемыми требованиями; ответы студента путанные, нечеткие, содержат множество ошибок, или ответов нет совсем; несоответствие варианту.</i>

### **4.3. Оценочные средства для промежуточной аттестации**


Представлено в приложении №1.

#### **Автор(ы) рабочей программы дисциплины (модуля):**

доцент кафедры ИТ и МПИ,  
кан. пед. наук, доцент

  
Абдуллаев Д.А.  
(подпись)

СОГЛАСОВАНО:  
Директор библиотеки

  
Арсагериева Т.А.  
(подпись)



**Оценочные средства  
для проведения промежуточной аттестации по дисциплине  
Информационная безопасность**

**Направление подготовки  
44.03.05 - ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ  
(с двумя профилями подготовки)**

**Профили подготовки «Английский язык» и «Информатика»**

**Форма обучения:** очно-заочная

**Год приема:** 2023

**1. Характеристика оценочной процедуры:**

Семестр - 10

Форма аттестации – зачет

**2. Оценочные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности**

**2.1. Вопросы для промежуточной аттестации по дисциплине:**

1. Информационная безопасность в системе национальной безопасности.
2. Обеспечение информационной безопасности объектов информационной сферы государства
3. Общая характеристика компьютерной безопасности.
4. Испытание программного и аппаратного уровней компьютерной безопасности.
5. Система физической защиты компьютерных систем.
6. Организация и аудит безопасности компьютерных систем.

**2.2. Структура экзаменационного билета (примерная):**

**3. Критерии и шкала оценивания устного ответа обучающегося на экзамене (зачете)**

**Максимальное количество баллов на экзамене (зачете) – 30, из них:**

1. Ответ на первый вопрос, содержащийся в билете – 15 баллов.
2. Ответ на второй вопрос, содержащийся в билете – 15 баллов.

*Таблица 13*

№ n/n	Характеристика ответа	Баллы
1.	Если ответ студента показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа	<b>13-15</b>
2.	Если студент показывает знание узловых проблем программы и	<b>10-12</b>

	основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа	
3	Если студент показывает фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ	<b>7-9</b>
4.	Если студент показывает незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе	<b>6 и менее</b>

### Расчет итоговой рейтинговой оценки

Таблица 14

До 50 баллов включительно	«неудовлетворительно»
От 51 до 70 баллов	«удовлетворительно»
От 71 до 85 баллов	«хорошо»
От 86 до 100 баллов	«отлично»

### 4. Уровни сформированности компетенций по итогам освоения дисциплины (модуля)

Таблица 15

Индикаторы достижения компетенции (ИДК)	Уровни сформированности компетенций			
	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»
	<b>86-100</b>	<b>71-85</b>	<b>51-70</b>	<b>Менее 51</b>
	<b>«зачтено»</b>			<b>«не зачтено»</b>
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).	<i>Критерий 1</i> Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	<i>Критерий 1</i> Знает материал в запланированном объеме. Ответ достаточно полный, но не отражает некоторые аспекты.	<i>Критерий 1</i> Допускает неточности в формулировках. Знает только основной материал.	<i>Критерий 1</i> Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
	<i>Критерий 2</i> Раскрывает структуру и состав изучаемых разделов информатики, демонстрирует сформированные системные знания. Успешно справляется с решением всех поставленных математических задач	<i>Критерий 2</i> Раскрывает структуру и состав некоторых изучаемых разделов информатики. При решении предметных задач допускает единичные ошибки	<i>Критерий 2</i> Фрагментарно описывает структуру и состав изучаемых разделов информатики. Допускает множественные ошибки при решении предметных задач	<i>Критерий 2</i> Не знает структуру и содержание изучаемых разделов информатики. Не справляется с решением предложенных предметных задач
	<i>Критерий 3</i> Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием	<i>Критерий 3</i> Знает основные понятия и ключевые факты в пределах изучаемой	<i>Критерий 3</i> Обладает базовыми общими знаниями и основными умениями, требуемыми для	<i>Критерий 3</i> Неспособен самостоятельно продемонстрировать наличие знаний при

		<p>границ применимости. Обладает диапазоном практических умений, требуемых для решения определенных проблем в нестандартной ситуации.</p>	<p>области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области.</p>	<p>выполнения простых задач</p>	<p>решении заданий, которые были представлены преподавателем вместе с образцом их решения.</p>
<p>ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.</p>	<p><i>Критерий 1</i> Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ</p>	<p><i>Критерий 1</i> Знает материал в запланированном объеме. Ответ достаточно полный, но не отражает некоторые аспекты.</p>	<p><i>Критерий 1</i> Допускает неточности в формулировках. Знает только основной материал.</p>	<p><i>Критерий 1</i> Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.</p>	
	<p><i>Критерий 2</i> Самостоятельно анализирует теоретический материал, умеет применять теоретическую базу при выполнении практических заданий, предлагает собственный метод решения.</p>	<p><i>Критерий 2</i> Правильно применяет теоретическую базу при выполнении практических заданий.</p>	<p><i>Критерий 2</i> Способен решать задачи по заданному алгоритму. Испытывает затруднения при анализе теоретического материала и его применении на практике.</p>	<p><i>Критерий 2</i> Не может установить связь теории с практикой. Не может проанализировать теоретический материал и обосновать его использование на практике.</p>	
	<p><i>Критерий 3</i> Умеет отбирать материал в зависимости от уровня сложности и логики изложения; умеет применять учебный материал в различных формах обучения в соответствии с требованиями ФГОС ОО</p>	<p><i>Критерий 3</i> Способен отбирать материал в зависимости от уровня сложности, но допускает неточности в применении учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО</p>	<p><i>Критерий 3</i> Испытывает затруднения в отборе материала, связанные с логикой изложения и с применением учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО</p>	<p>Не умеет соотносить содержание изучаемых дисциплин с содержанием школьного курса информатики</p>	

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ  
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ  
Информационная безопасность**

(наименование дисциплины / модуля)

Направление подготовки 44.03.05 Педагогическое образование  
(с двумя профилями подготовки)

Профили «Английский язык» и «Информатика»

(год набора 2023, форма обучения очно-заочная)

на 2023 / 2024 учебный год

В рабочую программу дисциплины / модуля вносятся следующие изменения:

№ п/п	Раздел рабочей программы (пункт)	Краткая характеристика вносимых изменений	Основание для внесения изменений