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 и защита информации

(наименование дисциплины (модуля))

Направление подготовки

44.03.05 Педагогическое образование (с двумя профилями подготовки)

(код и направление подготовки)

Профиль(и) подготовки

«Математика» и «Информатика»

Квалификация

Бакалавр

Форма обучения

Очная, заочная

Год набора
2023

Грозный, 2023

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ
Информационная безопасность и защита информации

1.1. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к предметно-методическому модулю по профилю Информатика (Б1.О.08.14. Дисциплина (модуль) изучается на 5 курсе в 9 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 ПК-1; ПК-1.1, ПК-1.2:

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.** **ПК-1.2.**	Знает: Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета). Умеет: Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО. Владеет: 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 .72/2. з.е. (академ. часов)

Таблица 2

Вид учебной работы	Количество академ. часов	
	Очно	**Заочно**
4.1. Объем контактной работы обучающихся с преподавателем	**72**	**72**
4.1.1. аудиторная работа		
в том числе:	6	4
лекции	12	8
практические занятия, семинары, в том числе практическая подготовка	*18/8*	*18/8*
лабораторные занятия		
4.1.2. внеаудиторная работа	**36**	**36**

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		
4.2. Объем самостоятельной работы обучающихся	54	56
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		Трудоёмкость по видам учебных занятий (в акад.часах)							
				Лекции		Практ. занятия		Лаб. занятия		Сам. работа	
		Очно	Заочн.	Очно	Заочн.	Очно	Заочн.	Очно	Заочн.	Очно	Заочн.
1.	Основные понятия «информационной безопасности».	14	14	2	2	*2*	2			10	10
2.	Правовые основы информационной безопасности и защиты персональных данных.	14	12	2	2	2				10	10
3.	Программные средства защиты информации.	22	12	2		4	2			16	10
4	Технические средства защиты и комплексное обеспечение информационной безопасности.	14	14			4	4			10	10
5	Элементы криптографии.									8	16
	Курсовое проектирование/работа	*X*	*X*							*X*	*X*
	Подготовка к экзамену (зачету)	*X*	*X*							*X*	*X*
	Итого:	72		6	4	12	8			54	56

2.2. Содержание разделов дисциплины (модуля):

Таблица 4

№ п/п	Наименование темы (раздела) дисциплины	Содержание дисциплины (дидактические единицы) *(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования)*
1 1	Основные понятия «информационной	Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная

2	Правовые основы информационной безопасности и защиты персональных данных.	Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.
3	Программные средства защиты информации.	Компьютерные вирусы и антивирусная защита. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства
4	Технические средства защиты и комплексное обеспечение информационной безопасности.	Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы
2	Элементы криптографии.	Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.

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.	Основные понятия «информационной безопасности».	Подготовка докладов
2.	Правовые основы информационной безопасности и защиты персональных данных.	Подготовка реферата
3.	Программные средства защиты информации.	Подготовка доклада
4.	Технические средства защиты и комплексное обеспечение информационной безопасности.	Подготовка доклада
5.	Элементы криптографии.	Выполнение практической работы

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 библиотеке в университета	Режим доступа ЭБС/ электронный носитель (CD,DVD)	Обеспеченность обучающихся литературой, (5гр./4гр.)х100%))
1	2	3	4	5	6	7
	Основная литература					
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: https://e.lanbook.com/book/165837	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: https://e.lanbook.com/book/206285	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: https://e.lanbook.com/book/175506	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: https://e.lanbook.com/book/217445	100%
	Дополнительная литература					
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: https://e.lanbook.com/book/169817	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: https://e.lanbook.com/book/56704	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: https://www.iprbookshop.ru/118876.html	100%

3.2.2. Интернет-ресурсы

1. Электронно-библиотечная система IPRbooks (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
6. (https://www.elibrary.ru/)
7. СПС «КонсультантПлюс» (http://www.consultant.ru/)

3.3. Материально-техническое обеспечение дисциплины

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

Таблица 7

Помещения для осуществления образовательного процесса	**Перечень основного оборудования (с указанием кол-ва посадочных мест)**	**Адрес (местоположение)**
Аудитория для проведения лекционных занятий		
Лекционная аудитория	видеопроектор, экран настенный, компьютер/ноутбук	Ул.Ляпидевского, 33
Аудитории для проведения практических занятий, контроля успеваемости		
Аудитории для проведения практических занятий	видеопроектор, экран настенный, компьютер/ноутбук	Ул.Ляпидевского, 33
Помещения для самостоятельной работы		
Компьютерно-библиотечный центр	Учебники, компьютер	Ул. Киевская, 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.	Основные понятия	ПК-1		
2.	Правовые основы	ПК-1.1		
3	Программные средства защиты	ПК-1.2		
	Курсовая работа (проект)			
	Учебная практика			
	Производственная практика			

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 относится:

+ 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-компании

- 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 относится:

- 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 парке «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 нелицензионного 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, характеризуемая:

+ 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 перечисленное 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

Уровень освоения	***Критерии***	***Баллы***
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: *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.

Критерии и шкалы оценивания доклада/сообщения (в форме презентации):

Таблица 11

Уровень освоения	*Критерии*	*Баллы*
Максимальный уровень	*– продемонстрировано умение выступать перед аудиторией;* *– содержание выступления даёт полную информацию о теме;* *– продемонстрировано умение выделять ключевые идеи;* *– умение самостоятельно делать выводы, использовать актуальную научную литературу;* *– высокая степень информативности, компактность слайдов*	*3*
Средний уровень	*– продемонстрирована общая ориентация в материале;* *– достаточно полная информация о теме;* *– продемонстрировано умение выделять ключевые идеи, но нет самостоятельных выводов;* *– невысокая степень информативности слайдов;* *– ошибки в структуре доклада;* *– недостаточное использование научной литературы*	*2*
Минимальный уровень	*– продемонстрирована слабая (с фактическими ошибками) ориентация в материале;* *– ошибки в структуре доклада;* *– научная литература не привлечена*	*1*
Минимальный уровень не достигнут	*– выступление не содержит достаточной информации по теме;* *– продемонстрировано неумение выделять ключевые идеи;* *– неумение самостоятельно делать выводы, использовать актуальную научную литературу.*	*0*

4.3. Оценочные средства для промежуточной аттестации

Представлено в приложении №1.

Автор(ы) рабочей программы дисциплины (модуля):

Преподаватель: _____ Ибрагимова М.С..

СОГЛАСОВАНО _____ Арсагираева Т.А.
Директор библиотеки

Приложение 1

Оценочные средства
для проведения промежуточной аттестации по дисциплине
_____Информационная безопасность и защита информации_____
Направление подготовки
44.03.05 - ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ
(с двумя профилями подготовки)
Профили подготовки __Математика и Информатика_____
Форма обучения: очная и 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. Роль информации в современном мире. Понятие о защищаемой информации.
2. Теория информационной безопасности. Основные направления.
3. Обеспечение ИБ и направления защиты.
4. Требования к системе и политике ИБ.
5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
6. Доктрина информационной безопасности РФ.
7. Защита государственной тайны в РФ.
8. Защита коммерческой тайны в РФ.
9. Защита персональных данных в РФ.
10. Защита служебной и профессиональной тайны в РФ.
11. Процедуры сертификации и аттестации в РФ.
12. Понятие о защищаемой информации. Свойства информации.
13. Угрозы информации. Классификация угроз.
14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.
15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз.
16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.
17. Источники угроз. Классификация источников угроз.
18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.
19. Понятие электронной подписи.
20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия.
21. Организация внутри объектового режима предприятия. Организация охраны.
22. Криптографические меры обеспечения информационной безопасности. Классификация криптографических алгоритмов.
23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.
24. Программно-аппаратные защиты информации. Антивирусные средства, их

функции и назначения.

25. Особенности защиты беспроводных и мобильных подключений.
26. Симметричное и ассиметричное шифрование.
27. Принципы симметричного шифрования.
28. Односторонние функции и их применение.
29. Простейшие методы ассиметричного шифрования.
30. Метод RSA.
31. Электронная подпись и ее применение.

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

№ п/п	Характеристика ответа	Баллы
1.	Ответил на все вопросы	**13-15**
2.	Не достаточно ответил на вопросы	**10-12**
3	Ответил на один вопрос	**7-9**
4.	Плохо ответил на вопрос	**6 и менее**

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»**
	86-100	**71-85**	**51-70**	**Менее 51**
	«зачтено»			**«не зачтено»**
Код и наименование формируемой компетенции				
ПК-1.1	Знает: структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	Не знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).
	Умеет: осуществлять отбор учебного содержания для его реализации в различных формах обучения в	Умеет осуществлять отбор учебного содержания для его реализации в различных	Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС	Не умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС

	соответствии с требованиями ФГОС ОО.	формах обучения в соответствии с требованиями ФГОС ОО.	ОО.	ОО.
	Владеет навыками разработки различных форм учебных занятий, применения методов, приемов и технологий обучения, в том числе информационных	Владеет навыками разработки различных форм учебных занятий, применения методов, приемов и технологий обучения, в том числе информационных	Владеет навыками разработки различных форм учебных занятий, применения методов, приемов и технологий обучения, в том числе информационных	Не владеет навыками разработки различных форм учебных занятий, применения методов, приемов и технологий обучения, в том числе информационных
….				

5. Рейтинг-план изучения дисциплины

Таблица 16

I	**БАЗОВАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**		
Виды контроля	**Контрольные мероприятия**	**Мин. кол-во баллов на занятиях**	**Макс. кол-во баллов на занятиях**
Текущий контроль № 1	Тема № 1-2 Теория множеств.	0	10
Текущий контроль № 2	Тема № 3. Алгоритмы на графах	0	10
	Тема № 4. Математическая логика		
Рубежный контроль: контрольная работа №1 (Темы 1-4)		0	10
Текущий контроль №3	Тема 5.Логические операции	0	10
	Тема 6. Таблица истинности		
	Тема 7. Интерпитация формул в логике высказываний		
Текущий контроль №4	Тема 8. Логическое следование	0	10
	Тема 9. Идея метода резолюции		
Рубежный контроль: контрольная работа №2 (Темы 5-9)		0	10
Допуск к промежуточной аттестации		**Мин 36**	
II	**ДОПОЛНИТЕЛЬНАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**	**Мин.**	**Макс.**
1	**Поощрительные баллы**	**0-10**	**10**
	Подготовка доклада с презентацией по дисциплине	0-1	1
	Посещаемость лекций (100%)	0-2	2
	Участие в работе круглого стола, студенческой конференции	0-2	2
	Соц.-личностный рейтинг	0-3	3
	Участие в общественной, культурно-массовой и спортивной работе	0-2	2

2	**Штрафные баллы**		**0-3**	**3**
	Пропуск учебных лекций	за пропуск лекции снимается балльная стоимость лекции (2:8=0,25)	0,25 x N (N – количество пропущенных лекций	
	Несвоевременное выполнение контрольной (аттестационной) работы №1	минус 5% от максимального балла	- 0,5	
	Несвоевременное выполнение контрольной (аттестационной) работы №2	минус 5% от максимального балла	- 0,5	
III	**ИТОГОВЫЙ КОНТРОЛЬ**		**0-30**	**30**
Форма итогового контроля:	Зачет (экзамен)		0-30	**30**
ИТОГО БАЛЛОВ ЗА СЕМЕСТР:			**0-100**	

Приложение 2

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ
Информационная безопасность и защита информации
(наименование дисциплины / модуля)
Направление подготовки 44.03.05. Педагогическое образование с двумя профилями подготовки)
Профили Математика и Информатика
(год набора 2023, форма обучения очная, заочная)
на 2023 2024 учебный год

В рабочую программу дисциплины / модуля вносятся следующие изменения:

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