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)

Кибербезопасность
(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 «Кибербезопасность» (Б1.В.ДВ.04.01) 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)

Цель: сформировать базовый уровень знаний, умений и владения навыками по обеспечению информационной безопасности информационных систем и информационных ресурсов профессиональной деятельности.

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.	**Знает:** структуру, состав и дидактические единицы предметной области (преподаваемого предмета). **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 72ч / 2з.е. (академ. часов)

Таблица 2

Вид учебной работы	Количество академ. часов	
	Очно	
4.1. Объем контактной работы обучающихся с преподавателем	**72**	
4.1.1. аудиторная работа	**24**	
в том числе:		
лекции	12/6	
практические занятия, семинары, в том числе практическая подготовка	12/6	
лабораторные занятия		
4.1.2. внеаудиторная работа	**48**	
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		
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	Заочно	Очно-заочно	Заочно	Очно-заочно	Заочно	Очно-заочно	Заочно	Очно-заочно	Заочно
1.	**Раздел 1. Введение.** Базовые задачи кибербезопасности в автоматизированных системах. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз. Основы файловой системы Требования к системам защиты информации.	14		2		2				10	
2.	**Раздел 2. Специфика технологии защищенного документооборота. Методологические рекомендации по анализу режимов работы кибернетических систем.**	14		2		2				10	

	Антивирусы и базовая защита электронного документооборота от не санкционированного доступа. Общая характеристика сетей и протоколов передачи данных										
3.	**Раздел 3. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.** Общие требования к паролям симметричное и симметричное шифрование. Основы стеганографии. Электронная подпись. Защита информации средствами стеганографии с помощью прикладного программного обеспечения. Защищенные каналы данных облачные технологии и защищённый документооборота.	22		4		4				14	
4.	**Раздел 4. Киберпреступность и способы её предотвращения** Нормативно-правовые акты и стандарты по основам кибербезопасности. Анализ базовых положений ФЗ "О защите детей от информации,	22		4		4				14	

	причиняющей вред их здоровью и развитию". Преступления в сфере информационных технологий. Анализ примеров практического применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях.										
	Подготовка к экзамену (зачету)	*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) *(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования)*
1.	**Раздел 1. Введение**	Базовые задачи кибербезопасности в автоматизированных системах. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз. Основы файловой системы Требования к системам защиты информации.
2.	**Раздел 2. Специфика технологии защищенного документооборота. Методологические рекомендации по анализу режимов работы кибернетических систем**	Антивирусы и базовая защита электронного документооборота от не санкционированного доступа. Общая характеристика сетей и протоколов передачи данных
3.	**Раздел 3. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты**	Общие требования к паролям симметричное и симметричное шифрование. Основы стеганографии. Электронная подпись. Защита информации средствами стеганографии с помощью прикладного программного обеспечения. Защищенные каналы данных облачные технологии и защищённый документооборота.
4.	**Раздел 4. Киберпреступность и**	Нормативно-правовые акты и стандарты по основам кибербезопасности.

	способы её предотвращения	Анализ базовых положений ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Преступления в сфере информационных технологий. Анализ примеров практического применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях.

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.	**Раздел 1. Введение**	Устный опрос Выполнение практико-ориентированных заданий
2.	**Раздел 2. Специфика технологии защищенного документооборота. Методологические рекомендации по анализу режимов работы кибернетических систем**	Устный опрос. Выполнение практико-ориентированных заданий
3.	**Раздел 3. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты**	Устный опрос Выполнение практико-ориентированных заданий
4.	**Раздел 4. Киберпреступность и способы её предотвращения**	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**	**Количество обучающихся**	**Количество экземпляров в библиотеке университета**	**Режим доступа ЭБС/ электронный носитель (CD,DVD)**	**Обеспеченность обучающихся литературой,**
1	2	3	4	5	6	7
	Основная литература					

1	Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. - Вологда: Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0.- Текст : электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/148383	100%
2	Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: энциклопедия / А. И. Белоус, В. А. Солодуха. - Москва: Техносфера, 2021. - 482 с. - ISBN 978-5-94836-612-8.- Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/181222	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%
	Дополнительная литература					
1	Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя; перевод с английского Д. А. Беликова. - Москва: ДМК Пресс, 2020. - 326 с. - ISBN 978-5-97060-709-1.- Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/131717	100%

2	Кибербезопасность в условиях электронного банкинга: практическое пособие: учебное пособие / А. В. Наваленный, А. Б. Дудка, С. В. Конявская [и др.]; под редакцией П. В. Ревенкова. - Москва: ЦИПСиР, 2020. - 522 с. - ISBN 978-5-907244-61-0.- Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/161659	100%
3	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%

3.2.2. 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

Помещения для осуществления образовательного процесса	Перечень основного оборудования (с указанием кол-ва посадочных мест)	Адрес (местоположение)
Аудитория для проведения лекционных занятий		
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
Аудитории для проведения практических занятий, контроля успеваемости		
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
Помещения для самостоятельной работы		
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.	**Раздел 1. Введение.** Базовые задачи кибербезопасности в автоматизированных системах. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз. Основы файловой системы Требования к системам защиты	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

	информации.			
2.	**Раздел 2. Специфика технологии защищенного документооборота. Методологические рекомендации по анализу режимов работы кибернетических систем.** Антивирусы и базовая защита электронного документооборота от не санкционированного доступа. Общая характеристика сетей и протоколов передачи данных	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.	**Раздел 3. Принципы построения системы кибербезопасности. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем криптографической и стеганографической защиты.** Общие требования к паролям симметричное и симметричное шифрование. Основы стеганографии. Электронная подпись. Защита информации средствами стеганографии с помощью прикладного программного обеспечения. Защищенные каналы данных облачные технологии и защищённый документооборота.	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.	**Раздел 4. Киберпреступность и**	ПК-1. Способен осваивать и	тестирование, практико-	контрольная работа

	способы её предотвращения Нормативно-правовые акты и стандарты по основам кибербезопасности. Анализ базовых положений ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Преступления в сфере информационных технологий. Анализ примеров практического применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях.	использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	ориентированное задание, доклад	

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

1. Всякий раз, когда фотографии, видео или комментарии публикуются в соцсетях, они становятся частью ...

- Вашей оценки;
- **Вашего цифрового следа;**
- Вашей популярности;
- Вашей личности.

2. Когда исчезает информация, размещенная в социальных сетях?

- Когда вы размещаете слишком много информации;
- Через 5 лет;
- Когда вы удаляете информацию;
- **Никогда.**

3. Ограничить круг лиц, которые имеют доступ к информации о вас в социальных сетях

- Очень сложно;
- Невозможно;
- Не имеет смысла;
- **Можно, закрыв свою страницу от посторонних**

4. Стоит ли делиться в соцсетях информацией и фото о том, где и как вы с семьей проводите каникулы?

- Конечно, стоит
- Конечно, не стоит
- Стоит, если вы хотите, чтобы об этом знали все
- **Стоит, но только для ограниченного круга лиц.**

5. Когда вы предоставляете личную информацию в Интернете?

- Всякий раз, когда у вас ее запрашивают;
- Когда вам говорят, что вы выиграли приз;
- Никогда;
- **Когда вы понимаете, зачем нужна информация и как она будет использована.**

6. При регистрации на онлайн-сервис у вас запрашивают персональную информацию. Что вы всегда должны делать? Выберите подходящие варианты ответа.

- Внимательно изучить, какую персональную информацию у вас запрашивают, и решить, готовы ли вы ее предоставить;
- Предоставить всю запрашиваемую персональную информацию;
- Не предоставлять никакой персональной информации;
- **Предоставить только обязательную информацию, если согласны ее предоставить.**

7. Что вы должны сделать, чтобы предотвратить передачу ваших данных другим веб-сайтам или сторонним организациям без вашего разрешения?

- Отказаться предоставлять информацию;
- **Внимательно ознакомиться с политикой конфиденциальности;**
- Использовать пароль;
- Использовать вымышленное имя.

8. Кто несет ответственность за безопасность вашей информации в интернете?

- Интернет;
- Веб-сайты, которые вы посещаете;
- Социальные сети, на которые вы подписаны;
- **Вы.**

9. Что из перечисленного может представлять угрозу вашей безопасности в интернете?

- Вредоносные программы, например, вирусы, троянские или шпионские программы;
- Поддельные веб-сайты или электронные письма и сообщения, используемые мошенниками для сбора вашей конфиденциальной информации обманным путем;
- Взлом сервера;
- **Все перечисленное.**

10. Чем опасно вредоносное ПО?

- Несанкционированный сбор конфиденциальной информации;
- Переадресация платежей;
- Вымогательство;
- **Все перечисленное.**

11. Социальная инженерия - это

- **Манипулирование людьми с целью несанкционированного доступа к конфиденциальной информации;**
- Защита людей от несанкционированного доступа к конфиденциальной информации;
- Помощь людям в защите от любых киберугроз;
- Ничего из перечисленного.

12. Как называют программы, которые могут нанести ущерб вашему устройству?
- Социальная инженерия;
- Проблемное ПО;
- **Вредоносное ПО;**
- Гиперссылки.

13. Фишинг – это термин
- относящийся к рыбалке;
- относящийся к озеру данных;
- **относящийся к интернет-мошенничеству;**
- Другое_____.

14. Вишинг – это
- Ошибочное написание термина “фишинг”;
- То же, что фишинг;
- **Телефонное мошенничество;**
- Другое_____.

15. Фарминг – это
- Современные методы ведения фермерского хозяйства;
- **Кража персональных данных путем перенаправления пользователей на поддельные веб-сайты;**
- Вирус;
- Другое_____.

16. Каков уровень риска, связанный с открытием вложения, полученного по электронной почты от незнакомого отправителя?
- Низкий;
- **Высокий;**
- Умеренный;
- Другое_____.

17. Что из перечисленного может быть попыткой атаки на вашу безопасность в интернете?
- Сообщение от неизвестного вам отправителя по электронной почте или в социальных сетях;
- Неожиданные сообщения со странными просьбами от членов семьи или друзей;
- Сообщение о выигрыше в лотерее;
- **Все перечисленное.**

18. Чего вы не сделаете, получив неожиданное письмо или сообщение, в котором вам предлагается перейти по ссылке, чтобы обновить или подтвердить информацию для вашего аккаунта в соцсети:

- **Перейдете по ссылке;**
- Проигнорируете письмо;
- Отправите письмо в спам;
- Войдете в свой аккаунт на официальном сайте социальной сети.

19. Кому из следующих людей, связавшихся с вами по телефону, чтобы получить информацию о вашем ПИН-коде, логине, пароле или номере банковской карты, вы должны предоставить запрашиваемую информацию?

- Менеджеру банка;
- Эксперту по безопасности;
- Администратору социальной сети;
- **Никому.**

20. Чего вы не сделаете, если абонент, представившийся представителем какой-либо организации, просит уточнить или обновить ваши личные данные и для убедительности предлагает вам перезвонить по указанному номеру.

- Сразу перезвоните по указанному номеру;
- **Подождете не менее пяти минут, прежде чем перезвонить по указанному номеру;**
- Используете для звонка по указанному номеру другую линию;
- Позвоните по номеру, который найдете на официальном сайте организации.

21. Форма кражи личных данных и денег пользователя с помошью поддельного интернет-магазина, - это:

- Вишинг;
- Фишинг;
- **Фарминг;**
- Ничего из перечисленного.

22. С чего начинается адрес надежного сайта?

- http://;
- **https://;**
- https:\\;
- http//.

23. Сайт с адресом, начинающимся с http: // и всплывающим окном, куда вам предлагается ввести личную информацию, кажется вам …

- Надежным;
- Безопасным;
- **Подозрительным;**
- Обычным.

24. Пароль - отличное средство киберзащиты. Если это надежный пароль. Что из перечисленного является ключевым компонентом надежного пароля?

- Его легко запомнить владельцу;
- **Это случайная комбинация из 8 и более прописных и строчных букв, цифр и символов;**

- Его трудно угадать посторонним;
- Все перечисленное.

25. Что НЕ является советом по созданию надежного пароля?
- Использовать личную информацию, например, имя или день рождения;
- Использовать последовательность букв или цифр;
- Использовать один и тот же пароль для всех учетных записей;
- **Все перечисленное.**

26. Как вы можете усилить защиту своего аккаунта? Выберите все подходящие варианты
- **Использовать надежный пароль;**
- **Использовать двухфакторную аутентификацию;**
- Никогда не менять надежный пароль;
- Использовать один и тот же пароль для всех аккаунтов.

27. Чего следует избегать, когда вы подключены к публичной Wi-Fi-сети?
- Входа в платежную систему;
- Подключения к любым финансовым сервисам;
- Интернет-покупок;
- **Всего перечисленного.**

28. Публичные зарядные станции с USB для мобильных устройств… Выберите подходящие варианты ответа.
- **Могут использоваться для сбора и передачи данных с заряжаемого устройства;**
- **Несут риски заражения заряжаемого устройства вирусами;**
- Лучше и надежнее внешнего аккумулятора;
- Удобнее зарядки от обычной розетки.

29. Что из перечисленного лучше всего защитит вас от кибератак?
- Регулярное обновление всего ПО;
- Регулярное обновление антивируса;
- Осторожное отношение к любым письмам со ссылками и вложениями, особенно неожиданным;
- **Все перечисленное.**

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: практико-ориентированное задание

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

Примерные практико-ориентированные задания

1. Раскрыть базовые задачи кибербезопасности в автоматизированных системах.
2. Описать свойства информации как объекта защиты от киберугроз.
3. Описать антивирусы и базовая защита электронного документооборота от не санкционированного доступа.
4. Раскрыть основы стеганографии.
5. Рассмотреть электронную подпись.
6. Рассмотреть защищенные каналы данных облачных технологий.
7. Изучить и рассмотреть нормативно-правовые акты и стандарты по основам кибербезопасности.
8. Проанализировать базовые положения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".
9. Рассмотреть преступления, совершаемые в сфере информационных технологий.
10. Проанализировать примеры практического применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях.

Критерии оценивания результатов выполнения практико-ориентированного задания

Таблица 10

Уровень освоения	***Критерии***	***Баллы***
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: ***контрольная работа***

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

Примерное задание для контрольной работы:

1. Европейская Конвенция по борьбе с киберпреступностью. Виды и составы компьютерных преступлений.
2. Директивы и регламенты ЕС по противодействию киберпреступности.
3. Защита государственной тайны в США.
4. Защита государственной тайны в европейских странах (Великобритания, Германия, Франция).
5. Защита государственной тайны в странах Азии и Дальнего Востока.
6. Национальное законодательство США по противодействию компьютерным преступлениям. Правовые основы информационной безопасности. Законодательство в области компьютерных преступлений. Расследование компьютерных преступлений. Состав и основные направления деятельности органов защиты информации.
7. Национальные законодательства стран ЕС по противодействию компьютерным преступлениям. Правовые основы информационной безопасности. Законодательство в области компьютерных преступлений. Расследование компьютерных преступлений. Состав и основные направления деятельности органов защиты информации.

8. Национальные законодательства стран Азии и Дальнего Востока (КНР, Япония, Индия, Сингапур) по противодействию компьютерным преступлениям. Правовые основы информационной безопасности. Законодательство в области компьютерных преступлений. Расследование компьютерных преступлений. Состав и основные направления деятельности органов защиты информации.

Критерии оценивания результатов контрольной работы

Таблица 12

Балл (интервал баллов)	***Уровень освоения***	***Критерии оценивания уровня освоения компетенций****
10	*Максимальный уровень (интервал)*	*Контрольная работа оформлена в соответствии с предъявляемыми требованиями, содержит 1-2 мелких ошибки; ответы студента правильные, четкие, содержат 1-2 неточности*
[6-8]	*Средний уровень (интервал)*	*Контрольная работа содержит одну принципиальную или 3 или более недочетов; ответы студента правильные, но их формулирование затруднено и требует наводящих вопросов от преподавателя*
[3-5]	*Минимальный уровень (интервал)*	*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*
Менее 3	*Минимальный уровень (интервал) не достигнут.*	*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.*

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)

Приложение 1

Оценочные средства
для проведения промежуточной аттестации по дисциплине
Кибербезопасность
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. Базовые задачи кибербезопасности в автоматизированных системах.
2. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз.
3. Основы файловой системы. Требования к системам защиты информации.
4. Антивирусы и базовая защита электронного документооборота от не санкционированного доступа.
5. Общая характеристика сетей и протоколов передачи данных
6. Общие требования к паролям симметричное и симметричное шифрование.
7. Основы стеганографии.
8. Электронная подпись.
9. Защита информации средствами стеганографии с помощью прикладного программного обеспечения.
10. Защищенные каналы данных облачные технологии и защищённый документооборота.
11. Нормативно-правовые акты и стандарты по основам кибербезопасности.
12. Анализ базовых положений ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".
13. Преступления в сфере информационных технологий.
14. Анализ примеров практического применения ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в образовательных учреждениях.

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

№ п/п	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	**13-15**
2.	Если студент показывает знание узловых проблем программы и 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	**10-12**
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	**7-9**
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	**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»**
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).	*Критерий* 1 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 1 Знает материал в запланированном объёме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 1 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 1 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
	Критерий 2 Раскрывает структуру и состав изучаемых разделов информатики,	*Критерий 2* Раскрывает структуру и состав некоторых	*Критерий 2* Фрагментарно описывает структуру и состав изучаемых	*Критерий 2* Не знает структуру и содержание изучаемых разделов информатики.

	демонстрирует сформированные системные знания. Успешно справляется с решением всех поставленных математических задач	изучаемых разделов информатики. При решении предметных задач допускает единичные ошибки	разделов информатики. Допускает множественные ошибки при решении предметных задач	Не справляется с решением предложенных предметных задач
	Критерий 3 Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости. Обладает диапазоном практических умений, требуемых для решения определенных проблем в нестандартной ситуации.	*Критерий 3* Знает основные понятия и ключевые факты в пределах изучаемой области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области.	*Критерий 3* Обладает базовыми общими знаниями и основными умениями, требуемыми для выполнения простых задач	*Критерий 3* Неспособен самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.
ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	*Критерий* 1 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 1 Знает материал в запланированном объёме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 1 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 1 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.
	Критерий 2 Самостоятельно анализирует теоретический материал, умеет применять теоретическую базу при выполнении практических заданий, предлагает собственный метод решения.	*Критерий* 2 Правильно применяет теоретическую базу при выполнении практических заданий.	*Критерий* 2 Способен решать задачи по заданному алгоритму. Испытывает затруднения при анализе теоретического материала и его применении на практике.	*Критерий* 2 Не может установить связь теории с практикой. Не может проанализировать теоретический материал и обосновать его использование на практике.
	Критерий 3 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	Критерий 3 Способен отбирать материал в зависимости от уровня сложности, но допускает неточности в в применении учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	Критерий 3 Испытывает затруднения в отборе материала, связанные с логикой изложения и с применением учебного материала в различных формах обучения в соответствии с требованиями ФГОС ОО	Не умеет соотносить содержание изучаемых дисциплин с содержанием школьного курса информатики

Приложение 2

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ
Кибербезопасность
(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:

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