

Министерство просвещения РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Глазовский государственный педагогический институт имени В.Г. Короленко»



Утверждена
на заседании ученого совета института

14 апреля 2023 г. протокол № 11

Ректор

подпись

/ Я.А. Чиговская-Назарова /
инициалы, фамилия

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ
ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ**

Уровень основной профессиональной образовательной программы	Магистратура
Направление подготовки	44.04.01 Педагогическое образование
Направленность (профиль)	"Технологии обучения в цифровой образовательной среде"
Форма обучения	Очная
Семестр(ы)	2

1. Цель и задачи изучения дисциплины

1.1. Цель и задачи изучения дисциплины

Цель: Совершенствование компетенций магистров в области информационной безопасности при организации образовательного процесса.

Задачи:

- Формирование навыков осуществления деятельности по организации и руководству работой команды для достижения поставленной цели;
- Совершенствование практических навыков реализации образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде
- Совершенствование навыков соотношения компьютерной преступности и компьютерной этики;
- Совершенствование навыков обеспечения информационной безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными индикаторами достижения компетенций

Код компетенции	УК-3
Формулировка компетенции	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Индикатор достижения компетенции	УК-3.1. Знает: правила командной работы; необходимые условия для эффективной командной работы. УК-3.2. Умеет: планировать командную работу, распределять поручения и делегировать полномочия членам команды; организовывать обсуждение разных идей и мнений; предвидит результаты (последствия) как личных, так и коллективных действий; организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели. УК-3.3. Владеет навыками осуществления деятельности по организации и руководству работой команды для достижения поставленной цели.

Код компетенции	ПК-1
Формулировка компетенции	Способен реализовывать образовательный процесс с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде
Индикатор достижения компетенции	ПК – 1.1. Знает: особенности и возможности применения электронного обучения и дистанционных образовательных технологий в процессе реализации образовательных программ. ПК – 1.2. Умеет: осуществлять планирование образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде. ПК – 1.3. Владеет: практическими навыками реализации образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде.

1.3. Воспитательная работа

Направление воспитательной работы	Типы задач	Формы работы
формирование у обучающихся осознания социальной значимости своей будущей профессии, мотивации к осуществлению профессиональной деятельности	педагогический	участие обучающихся в образовательных интенсивах, как в профессионально ориентированной, так и в социально значимой деятельности
научно-исследовательская работа обучающихся	научно-исследовательский	исследовательская деятельность студентов (публикация статей, выступление с докладом)

1.4. Место дисциплины в структуре образовательной программы

Дисциплина "Основы информационной безопасности в цифровой образовательной среде" относится к части учебного плана, формируемой участниками образовательных отношений.

Требований к предварительной подготовке обучающегося нет. Перечень последующих дисциплин: «Информационно-коммуникационные технологии в профессиональной деятельности», «Методика использования цифровых технологий в учебном процессе».

1.5. Особенности реализации дисциплины

Дисциплина реализуется на русском языке.

2. Объем дисциплины

Вид учебной работы по семестрам	Всего, зачетных единиц	Академ. часы	Из них в форме практической подготовки
Общая трудоемкость дисциплины	4	144	
СЕМЕСТР 2			
Контактная работа с преподавателем:			
Аудиторные занятия (всего)		26	
Занятия лекционного типа		6	
Занятия семинарского типа		-	
Практические занятия		20	
Лабораторные работы		-	
КСР		-	
Самостоятельная работа обучающихся		118	

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Разделы и темы дисциплины Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в академических часах)						
		всего	ауд	лекц	сем	практ	КСР	СРС
Семестр 2								
1.	Государственная политика РФ по информационной безопасности	38	6	2	-	4	-	32
2.	Информационные угрозы	52	14	2	-	12	-	38
3.	Особенности обеспечения информационной безопасности при организации образовательного процесса	38	4	2	-	2	-	34
4.	Защита итогового проекта	16	2	-	-	2	-	14
Всего–по семестр(ам)		144	26	6	-	20	-	118
Итого–по дисциплине		144	26	6	-	20	-	118

3.2. Занятия лекционного типа

СЕМЕСТР 2

Лекция 1.

Тема: Государственная политика РФ по информационной безопасности

Краткая аннотация к лекции.

Государственная политика РФ в области информационной безопасности. Структура и состав законодательства РФ в информационной сфере. Уровни информационной безопасности. Компьютерная преступность. Компьютерная этика.

Лекция 2.

Тема: Информационные угрозы

Краткая аннотация к лекции.

Информационные угрозы и их источники. Информационные угрозы в сфере образования. Обеспечение информационной безопасности личности.

Лекция 3.

Тема: Особенности обеспечения информационной безопасности при организации образовательного процесса

Краткая аннотация к лекции.

Информационная безопасность обучающихся разных возрастных групп (Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»: обзор статей про информационную продукцию для детей разных возрастных групп; задачи педагогического характера для организации мероприятий по информационной безопасности; примеры, ссылки на интересные материалы; основные показатели, характерные для Интернет-зависимости).

Формирование культуры безопасного взаимодействия в сети Интернет: основы воспитательной работы (мировой уровень цифровой культуры по результатам исследования DCI; понятия информационной грамотности, информационной культуры,

медиаграмотности; секреты информационной безопасности; цели Интернет-общения и правила его организации).

3.3. Занятия семинарского типа

Учебным планом не предусмотрены

3.4. Практические занятия

СЕМЕСТР 2

Практическое занятие 1.

Тема: Нормативно-правовые и теоретические основы информационной безопасности.

Перечень заданий:

1. Подготовка доклада по теме «Основные понятия информационной безопасности» (концепция информационной безопасности; основные понятия: информационная безопасность, защита информации, угроза, утечка, уязвимость, отказ, сбой; виды защищаемой информации; информационная безопасность образовательного учреждения; способы несанкционированного доступа)
2. Подготовка доклада по теме «Нормативно-правовые аспекты защиты информации в образовательных организациях» (Основополагающие документы; обзор законов, указов, актов). Виды защищаемой информации.

Практическое занятие 2.

Тема: Работа с персональными данными

Перечень заданий:

1. Персональные данные (виды персональных данных; понятия субъекта и объекта персональных данных; обработка персональных данных; обязанности оператора персональных данных; принципы обработки персональных данных; ответственность за неправомерное использование персональных данных; полезная информация).
2. Основы государственной политики в области формирования культуры информационной безопасности (Доктрина национальной информационной безопасности, обеспечение свободы и равенства доступа к информации и знаниям, основные направления государственной политики в области формирования культуры информационной безопасности).

Практическое занятие 3.

Тема: Виды угроз информационной безопасности

Перечень заданий:

1. Виды угроз информационной безопасности (понятие угроз информационной безопасности; классификация угроз; угрозы информационной безопасности в образовательной организации; угрозы доступности по компонентам информационных систем; способы несанкционированного доступа).
2. Основные угрозы безопасности (обзор угроз безопасности в настоящее время). Кибербуллинг: понятие, признаки. Примеры программных и технических средств защиты информации.

Практическое занятие 4-5.

Тема: Безопасность общения

Перечень заданий:

1. Общение в социальных сетях и мессенджерах (Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент).

2. С кем безопасно общаться в интернете (Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети).
3. Пароли для аккаунтов социальных сетей (Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей).
4. Безопасный вход в аккаунты (Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта).
5. Настройки конфиденциальности в социальных сетях (Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах).
6. Публикация информации в социальных сетях (Персональные данные. Публикация личной информации).
7. Кибербуллинг (Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга).
8. Публичные аккаунты (Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг).
9. Фишинг (Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах).

Практическое занятие 6-7.

Тема: Безопасность устройств.

Перечень заданий:

1. Что такое вредоносный код (Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов).
2. Распространение вредоносного кода (Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах).
3. Методы защиты от вредоносных программ (Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов).
4. Распространение вредоносного кода для мобильных устройств (Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства).

Практическое занятие 8.

Тема: Безопасность информации

Перечень заданий:

1. Социальная инженерия: распознать и избежать (Приемы социальной инженерии. Правила безопасности при виртуальных контактах).
2. Ложная информация в Интернете (Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы).
3. Безопасность при использовании платежных карт в Интернете (Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов).

4. Беспроводная технология связи (Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях).
5. Резервное копирование данных (Безопасность личной информации. Создание резервных копий на различных устройствах).
6. Обеспечение безопасности облачных технологий (Основные проблемы безопасности облачной инфраструктуры. Средства защиты в виртуальных средах)

Практическое занятие 9.

Тема: Методы криптографии.

Перечень заданий:

1. Криптография, Криптоанализ. Основные понятия криптологии.
2. История шифрования. Использование шифрования различными методами.
3. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии.
4. Электронная цифровая подпись.

Практическое занятие 10.

Тема: Антивирусные средства защиты информации.

Перечень заданий:

1. Сканирование
2. Эвристический анализ.
3. Защита итогового проекта по курсу.

3.5. Лабораторные работы

Учебным планом не предусмотрены

3.6. Контроль самостоятельной работы

Учебным планом не предусмотрены

4. Фонд оценочных средств

ФОС включает оценочные средства текущего, промежуточного и поститогового контроля (Приложение 1).

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1. Основная литература

1. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/10677.html> (дата обращения: 11.03.2023).
2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/495922> (дата обращения: 11.03.2023).
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-

0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87995.html> (дата обращения: 11.03.2023).

5.2. Дополнительная литература

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/33430.html> (дата обращения: 11.03.2023).

2. Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. — Москва : Издательство Юрайт, 2022. — 301 с. — (Актуальные монографии). — ISBN 978-5-534-14919-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496939> (дата обращения: 11.03.2023).

3. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/101992.html> (дата обращения: 11.03.2023).

4. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/33857.html> (дата обращения: 11.03.2023).

5. Сологубова, Г. С. Составляющие цифровой трансформации : монография / Г. С. Сологубова. — Москва : Издательство Юрайт, 2022. — 147 с. — (Актуальные монографии). — ISBN 978-5-534-11335-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/494769> (дата обращения: 11.03.2023).

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине

6.1 Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://school-collection.edu.ru/> - Единая коллекция цифровых образовательных ресурсов
2. <http://digital.1september.ru/> - Общероссийский проект "Школа цифрового века"
3. <http://fcior.edu.ru/> - Федеральный центр информационно-образовательных ресурсов

6.2. Перечень необходимых профессиональных баз данных и информационных справочных систем

Электронная библиотечная система «IPR SMART». Режим доступа <http://www.iprbookshop.ru>

электронная библиотечная система «Юрайт». Режим доступа <https://urait.ru>

Электронно-библиотечная система «Лань» (раздел «Сетевая электронная библиотека педагогических вузов»). Режим доступа <https://e.lanbook.com>

Электронно-библиотечная система «Рукопт». Режим доступа: <https://lib.rucont.ru/search>

Межвузовская электронная библиотека. Режим доступа <https://icdlib.nspu.ru/>

Научная электронная библиотека eLIBRARY.RU Режим доступа <https://www.elibrary.ru/defaultx.asp>

Национальная электронная детская библиотека. Режим доступа <https://arch.rgdb.ru/xmlui/>

Национальная электронная библиотека. Режим доступа <https://rusneb.ru>

Президентская библиотека имени Б.Н. Ельцина. Режим доступа <https://www.prilib.ru>

Polpred.com Обзор СМИ. Режим доступа <https://polpred.com>

7. Методические указания и учебно-методическое обеспечение для обучающихся по освоению дисциплины

Дисциплина реализуется в соответствии с указаниями «Методические рекомендации по организации образовательного процесса при освоении дисциплины», размещенными в ЭИОС института (eios.ggpi.org).

Методические рекомендации для работы с инвалидами и лицами с ОВЗ размещены в ЭИОС института (eios.ggpi.org).

8. Материально-техническая база, программное обеспечение, необходимое для осуществления образовательного процесса по дисциплине

Учебный корпус 1, аудитории(я) 219, 232.

Полный перечень материально-технической базы и программного обеспечения размещены в ЭИОС института (eios.ggpi.org).

9. Рейтинг-план успеваемости по дисциплине

Дисциплина /семестры	Объем аудиторной работы				Виды текущей аттестационной аудиторной и внеаудиторной работы	Максимальное (норматив) количество баллов	Поощрение	Штрафы	Итоговая форма отчета (мин. балл)
	лк	Сем/ пр	лаб	КСР					
Основы информационной безопасности в цифровой образовательной среде / 2	6	- / 20	-	-	1. Контроль посещаемости лекций 2. Работа на практических занятиях <u>Формы контрольных мероприятий</u> 1. Контрольная работа 2. Тест <u>Компенсационные мероприятия</u> 1. Письменный реферат по темам практических занятий	6 50 (5*10) 5 5 1	+1 балл за дополнения; +3 балла за подготовку дополнительного дидактического материала	- 2 балла за пропуск занятия по неуважительной причине	Программа освоена, обучающийся допущен до экзамена по модулю, если набрано более 50% баллов
ИТОГО						66 (без компенсации)			

Лист регистрации изменений и дополнений к РПД
(фиксируются изменения и дополнения перед началом учебного года,
при необходимости внесения изменений на следующий год –
оформляется новый лист изменений)

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой	Дата, номер протокола заседания совета факультета. Подпись декана факультета
1.			
2.			
3.			
4.			
5.			
6.			

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

1 Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации и поститогового контроля по дисциплине

1.1. Настоящий Фонд оценочных средств (ФОС) по дисциплине «Основы информационной безопасности в цифровой образовательной среде» является неотъемлемым приложением к рабочей программе дисциплины «Основы информационной безопасности в цифровой образовательной среде» (РПД). На данный ФОС распространяются все реквизиты утверждения, представленные в РПД по данной дисциплине.

1.2. Оценивание всех видов контроля (текущего, промежуточного, поститогового) осуществляется по 5-балльной шкале.

1.3. Результаты оценивания текущего контроля учитываются в рейтинге.

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными индикаторами достижения компетенций

Код компетенции	УК-3
Формулировка компетенции	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Индикатор достижения компетенции	УК-3.1. Знает: правила командной работы; необходимые условия для эффективной командной работы. УК-3.2. Умеет: планировать командную работу, распределять поручения и делегировать полномочия членам команды; организовывать обсуждение разных идей и мнений; предвидит результаты (последствия) как личных, так и коллективных действий; организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели. УК-3.3. Владеет навыками осуществления деятельности по организации и руководству работой команды для достижения поставленной цели.

Код компетенции	ПК-1
Формулировка компетенции	Способен реализовывать образовательный процесс с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде
Индикатор достижения компетенции	ПК – 1.1. Знает: особенности и возможности применения электронного обучения и дистанционных образовательных технологий в процессе реализации образовательных программ. ПК – 1.2. Умеет: осуществлять планирование образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде.

	ПК – 1.3. Владеет: практическими навыками реализации образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде.
--	--

3 Содержание оценочных средств текущего контроля и критерии их оценивания

3.1 Текущий контроль осуществляется преподавателем дисциплины при проведении занятий в следующих формах: тестирование, контрольная работа.

3.2 Формы текущего контроля и критерии их оценивания

Форма контроля 1 - Типовые тестовые задания

Типовой тест

Проверяемые компетенции и индикаторы достижения компетенций: УК-3: УК-3.1, УК-3.2, УК-3.3; ПК-1: ПК – 1.1, ПК – 1.2, ПК – 1.3.

Время выполнения заданий: 45 минут

Критерии оценивания:

- верные ответы на 90% - 100% вопросов – «отлично»;
- верные ответы на 70% - 89% вопросов – «хорошо»;
- верные ответы на 50% - 69% вопросов – «удовлетворительно»;
- меньше 50% ответов на вопросы – «неудовлетворительно».

1. Совокупность методов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, обработку, хранение, распределение и отображение информации с целью снижения трудоемкости процессов использования информационных ресурсов - это...
 - а) информационная технология;
 - б) информационная система;
 - в) информатика;
 - г) кибернетика.
2. Кто является основным ответственным за определение уровня классификации информации?
 - а) Руководитель среднего звена
 - б) Высшее руководство
 - в) Владелец
 - г) Пользователь
3. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
 - а) Сотрудники
 - б) Хакеры
 - в) Атакующие
 - г) Контрагенты (лица, работающие по договору)
4. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
 - а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

- б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
 - в) Улучшить контроль за безопасностью этой информации
 - г) Снизить уровень классификации этой информации
5. Что самое главное должно продумать руководство при классификации данных?
- а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
 - б) Необходимый уровень доступности, целостности и конфиденциальности
 - в) Оценить уровень риска и отменить контрмеры
 - г) Управление доступом, которое должно защищать данные
6. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
- а) Владельцы данных
 - б) Пользователи
 - в) Администраторы
 - г) Руководство
7. Основные объекты информационной безопасности:
- а) Компьютерные сети, базы данных
 - б) Технические средства ПК
 - в) Физическое состояние пользователей
 - г) Психологическое состояние пользователей
8. Основными рисками информационной безопасности являются:
- а) Искажение, уменьшение объема, перекодировка информации
 - б) Выведение из строя оборудования сети
 - в) Потеря, искажение, утечка информации
 - г) Техническое вмешательство
9. Угроза информационной системе (компьютерной сети) – это:
- а) Вероятное событие
 - б) Детерминированное (всегда определенное) событие
 - в) Событие, происходящее периодически
 - г) Событие, происходящее один раз в год
10. Утечкой информации в системе называется ситуация, характеризующаяся:
- а) Потерей данных в системе
 - б) Изменением формы информации
 - в) Изменением содержания информации
 - г) Изменением вида информации
11. Установите соответствие между понятием защиты информации и его описанием:
- | Название | Описание |
|-----------------------------------|--|
| 1 Эффективность защиты информации | а) Степень соответствия результатов защиты информации поставленной цели |
| 2 Защита информации от утечки | б) деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к ней и от получения защищаемой информации злоумышленниками. |

- | | | | |
|---|---|----|--|
| 3 | Санкционированный доступ к информации | в) | это доступ к информации, не нарушающий установленных правил разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы |
| 4 | Несанкционированный доступ к информации | г) | характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. |

12. Соотнесите понятие с определением:

- | Понятие | Определение |
|---|--|
| 1 Несанкционированный доступ к информации | а) характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа.. |
| 2 Идентификация субъекта | б) это процедура распознавания субъекта по его идентификатору; выполняется при попытке субъекта войти в систему (сеть) |
| 3 Аутентификация субъекта | в) это проверка подлинности субъекта с данным идентификатором. Процедура устанавливает, является ли субъект именно тем, кем он себя объявил. |
| 4 Авторизация субъекта | г) это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети) |

Ключ к тесту:

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
а	в	а	в	б	г	а	в	а	а	1-а 2-б 3-в 4-г	1-а 2-б 3-в 4-г

Форма контроля 2 –Типовая контрольная работа

Типовая контрольная работа.

Проверяемые компетенции и индикаторы достижения компетенций: УК-3: УК-3.1, УК-3.2, УК-3.3; ПК-1: ПК – 1.1, ПК – 1.2, ПК – 1.3.

Время выполнения заданий: 45 минут

Критерии оценивания:

Обучающимся предлагается решить серию из трех заданий на компьютере.

Для получения оценки «удовлетворительно» предлагается выполнить одно задание.

Для получения оценки «хорошо» предлагается выполнить два задания.

Для получения оценки «отлично» предлагается выполнить все задания.

Практическое задание (выполняется на компьютере):

Укажите признаки, по которым можно понять, что компьютер стал жертвой вирусной атаки.

Ключ к практическому заданию.

В результате выполнения задания необходимо учесть один, два, три признака из ниже перечисленных.

1. **Проблемы в работе компьютера.** Резкое уменьшение производительности, которое нельзя объяснить очевидными причинами, может быть признаком того, что в устройстве поселился вирус. И, вероятно, для совершения своих преступных действий он использует дополнительные мощности. Участвовавшие внезапные отключения и частая перезагрузка устройства — тоже повод насторожиться, ведь иногда это означает, что вирус пытается взять ПК под контроль и дестабилизирует систему. Более того, случается и так, что компьютер как будто бы начинает жить своей жизнью: программы запускаются сами, спящий режим вдруг прекращается, а курсор на экране движется независимо от движений мыши.
2. **Проблемы с системой.** Новые программы на компьютере, которые вы не устанавливали и происхождение которых не можете установить — признак вмешательства в работу устройства. Особенно если у него только один пользователь. Готовьтесь к тому, что на самом деле чужого ПО больше, чем кажется: взломщики, обнаруживая лазейку в защите и устанавливая основную часть своих файлов, могут продолжить загрузку вредоносных программ, постепенно укореняясь в компьютере и изменяя системные настройки. Впрочем, вы сами можете спровоцировать вмешательство в настройки компьютера, если, например, вы выдали лишние разрешения непроверенным программам, которые решили установить на ПК. Это чревато самыми разными последствиями, например, если вредоносная программа получит доступ к камере и к микрофону, она сможет с помощью этого фиксировать вашу конфиденциальную информацию.
3. **Проблемы с аккаунтами и настройками браузеров.** Если в вашем браузере неожиданно появились новые закладки с неизвестными вам сайтами или новые расширения, а при его использовании происходит перенаправление с нужных сайтов на сомнительные ресурсы, то признаки заражения налицо. То же касается и изменения домашней страницы в браузере. Неудачные попытки зайти в аккаунты со своими логином и паролем тоже должны навести на мысль, что компьютер поражен вирусом. Нередко вредоносные программы захватывают аккаунты пользователей, чтобы от их имени начинать рассылать спам письмами по электронной почте или сообщениями в соцсетях. Рассылку писем от вашего имени вы можете поначалу и не заметить, поэтому проверяйте не только входящие письма в свой ящике, но и отправленные.
4. **Проблемы с антивирусом.** Антивирусная программа самопроизвольно отключается или не позволяет провести сканирование компьютера? Тогда не исключено, что она была взломана и теперь контролируется вирусом. Такое может происходить, если вы вовремя не обновили антивирусные базы или установили вредоносное приложение из непроверенного источника. Этим пользуются хакеры, чтобы сначала вывести из строя защиту, а затем получить доступ к файлам и пробраться в систему.

3.3 Методические указания по проведению процедуры текущего контроля

1. Текущий контроль проводится на протяжении всего семестра.
2. Сбор, обработка и оценивание результатов текущего контроля проводятся преподавателем, ведущим дисциплину.
3. Предъявление результатов оценивания осуществляется в течение недели после проведения контрольного мероприятия.
4. Результаты текущего контроля учитываются в рейтинге по дисциплине.

5. Все материалы, полученные от обучающихся в ходе текущего контроля (контрольная работа, диктант, тест, организация дискуссии, круглого стола, доклад, реферат, отчет по лабораторной работе, отчет по педагогической практике и т.п.), должны храниться в течение текущего семестра на кафедрах.
6. Считать, что положительные результаты текущего контроля свидетельствуют об успешном процессе формирования указанных компетенций и индикаторов достижения компетенций (этапов формирования компетенций).

4 Содержание оценочных средств промежуточной аттестации и критерии их оценивания

4.1 Промежуточная аттестация проводится в виде: экзамена по модулю

4.2. Содержание оценочного средства

Проверяемые компетенции и индикаторы достижения компетенций: УК-3: УК-3.1, УК-3.2, УК-3.3; ПК-1: ПК – 1.1, ПК – 1.2, ПК – 1.3.

Примерные вопросы для экзамена по модулю

1. Нормативно-правовые и теоретические основы информационной безопасности
2. Виды угроз информационной безопасности
3. Особенности обеспечения информационной безопасности при организации образовательного процесса
4. Работа с персональными данными
5. Безопасность общения
6. Безопасность устройств
7. Безопасность информации
8. Методы криптографии
9. Антивирусные средства защиты информации
10. Вредоносные программы и защита от них.

4.3 Критерии оценивания

Оценка за экзамен выставляется с учетом рейтинга. Если обучающийся набрал недостаточное количество баллов или хочет повысить оценку, то обучающийся сдает экзамен.

Шкала оценивания для экзамена:

Уровни освоения индикаторов в достижении компетенций	Содержательное описание уровня	Основные признаки выделения уровня	Академическая оценка	% освоения (рейтинговая оценка)
Повышенный (высокий)	Творческая деятельность	Включает нижестоящий уровень. Умение самостоятельно принимать решение, решать проблему/задачу теоретического или прикладного характера на основе изученных методов, приемов, технологий.	Отлично	90-100

Базовый	Продуктивная деятельность	Включает нижестоящий уровень. Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	Хорошо	70-89
Удовлетворительный	Репродуктивная деятельность	Изложение в пределах задач курса теоретического и практического материала	Удовлетворительно	50-69
Недостаточный	Отсутствие признаков удовлетворительного уровня		Неудовлетворительно	менее 50

4.4 Методические указания по проведению процедуры промежуточной аттестации

1. Сроки проведения процедуры оценивания: по расписанию экзамена по модулю. Если обучающийся по результатам рейтинговой системы не набирает нужное количество баллов или желает повысить оценку, то сдает экзамен по модулю по вопросам.
2. Сбор, обработка и оценивание результатов промежуточной аттестации проводится преподавателем, ведущим дисциплину.
3. Предъявление результатов оценивания осуществляется: по окончании ответа студента и фиксируется в зачетной книжке и экзаменационной ведомости.
4. При наличии письменных ответов обучающихся, полученных в ходе экзаменационной сессии, материалы хранятся в течение месяца после завершения сессии на кафедрах.
5. Порядок выполнения и защиты курсовой работы регламентирован «Положением о курсовой работе ФГБОУ ВО «Глазовский государственный педагогический институт имени В.Г. Короленко».
6. Считать, что положительные результаты промежуточного контроля свидетельствуют об успешном процессе формирования указанных компетенций и индикаторов достижения компетенций (этапов формирования компетенций).

5 Содержание оценочных средств для проверки сформированности компетенций и индикаторов достижения компетенций (поститоговый контроль) и критерии их оценивания

Задания для проверки компетенции и индикатора достижения компетенции: УК-3:
УК-3.1, УК-3.2, УК-3.3

Код компетенции	УК-3
Формулировка компетенции	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Индикатор достижения компетенции	УК-3.1. Знает: правила командной работы; необходимые условия для эффективной командной работы. УК-3.2. Умеет: планировать командную работу, распределять поручения и делегировать полномочия членам команды; организовывать обсуждение разных идей и мнений; предвидит результаты (последствия) как личных, так и коллективных действий; организовать и руководить работой команды,

	<p>вырабатывая командную стратегию для достижения поставленной цели.</p> <p>УК-3.3. Владеет навыками осуществления деятельности по организации и руководству работой команды для достижения поставленной цели.</p>
--	--

Время выполнения задания не более 30 минут

1. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
 - а) Владельцы данных
 - б) Пользователи
 - в) Администраторы
 - г) Руководство
2. Основные объекты информационной безопасности:
 - д) Компьютерные сети, базы данных
 - е) Технические средства ПК
 - ж) Физическое состояние пользователей
 - з) Психологическое состояние пользователей
3. Основными рисками информационной безопасности являются:
 - д) Искажение, уменьшение объема, перекодировка информации
 - е) Выведение из строя оборудования сети
 - ж) Потеря, искажение, утечка информации
 - з) Техническое вмешательство
4. Угроза информационной системе (компьютерной сети) – это:
 - д) Вероятное событие
 - е) Детерминированное (всегда определенное) событие
 - ж) Событие, происходящее периодически
 - з) Событие, происходящее один раз в год
5. Утечкой информации в системе называется ситуация, характеризующаяся:
 - д) Потерей данных в системе
 - е) Изменением формы информации
 - ж) Изменением содержания информации
 - з) Изменением вида информации
6. Установите соответствие между понятием защиты информации и его описанием:

Название	Описание
1 Эффективность защиты информации	а) Степень соответствия результатов защиты информации поставленной цели
2 Защита информации от утечки	б) деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к ней и от получения защищаемой информации злоумышленниками.
3 Санкционированный доступ к информации	в) это доступ к информации, не нарушающий установленных правил разграничения доступа.

- Правила разграничения доступа служат для регламентации права доступа к компонентам системы
- 4 Несанкционированный доступ к информации г) характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа..
7. Соотнесите понятие с определением:
- | Понятие | Определение |
|---|--|
| 1 Несанкционированный доступ к информации | а) характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа.. |
| 2 Идентификация субъекта | б) это процедура распознавания субъекта по его идентификатору; выполняется при попытке субъекта войти в систему (сеть) |
| 3 Аутентификация субъекта | в) это проверка подлинности субъекта с данным идентификатором. Процедура устанавливает, является ли субъект именно тем, кем он себя объявил. |
| 4 Авторизация субъекта | г) это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети) |

Ключ к тесту:

Номер вопроса	1	2	3	4	5	6	7
Номер правильного ответа	г	а	в	а	а	1 – а, 2 – б, 3 – в, 4 – г.	1 – а, 2 – б, 3 – в, 4 – г.

Практическое задание (выполняется на ПК).

Укажите антивирусное ПО и опишите его назначение.

Ключ к практическому заданию.

Необходимо указать конкретное название антивирусного ПО, описать его назначение (по типу, по назначению, по доступности и т.п.).

Задания для проверки компетенции и индикатора достижения компетенции:

ПК-1: ПК – 1.1, ПК – 1.2, ПК – 1.3.

Код компетенции	ПК-1
Формулировка компетенции	Способен реализовывать образовательный процесс с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде

Индикатор достижения компетенции	<p>ПК – 1.1. Знает: особенности и возможности применения электронного обучения и дистанционных образовательных технологий в процессе реализации образовательных программ.</p> <p>ПК – 1.2. Умеет: осуществлять планирование образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде.</p> <p>ПК – 1.3. Владеет: практическими навыками реализации образовательного процесса с использованием электронного обучения и дистанционных образовательных технологий в цифровой образовательной среде.</p>
----------------------------------	---

Время выполнения задания не более 30 минут

Практическое задание 1.

Опишите каким, образом вы соблюдаете нормы инфобезопасности в личном информационном пространстве.

Практическое задание 2

Опишите способы заражения технических устройств при работе в цифровой образовательной среде.

Ключ к практическому заданию 1.

Задание выполняется на компьютере. Необходимо обратить внимание на важные аспекты: создание безопасного пароля, настройки телефона, планшета для защиты от несанкционированного доступа, защита персональных данных, личный контент в облаке и система его защиты и т.п.

Ключ к практическому заданию 2.

Задание выполняется на компьютере. Обязательно наличие одного, двух, трех способов из ниже перечисленных.

1) Просмотр сайтов. Данный случай – один из лидеров среди способов заразить ваш компьютер. Чаще всего вирусы проникают на наши ПК через сайты, целевой аудиторией которых являются люди старше 18 лет. Данный вид сайтов весьма ненадёжен – через них вирусы распространяются наиболее часто. Вторыми в этом рейтинге идут игровые сайты, а также те, на которых можно скачать взломанные программы. Нередко мошенники умышленно создают Интернет-странички такого рода, чтобы распространить некий вирус, при помощи которого затем получают доступ к заражённым компьютерам пользователей. Чтобы уберечься от подобных махинаций, настройте свой антивирус так, чтобы все соединения извне, а также установка программ, не могли произойти без вашего непосредственного участия.

2) Электронные письма с вложениями (файлами). Это очень простой способ разослать вирус по электронной почте, прикрепив заражённый файл к письму. Большинство людей открывает неопознанные входящие письма из простого любопытства, получая впоследствии проблемы. Способ защититься от подобного прост: нужно удалять письма, пришедшие от неопознанных пользователей, не открывая их. Не смотря на кажущуюся радикальность, это самая разумная мера в данном случае.

3) **Заражённое программное обеспечение.** Схема заражения компьютера вирусами в этом случае элементарна – пользователь просто загружает на свой компьютер заражённую программу и устанавливает её. Мало кто хочет платить за лицензии программ – все хотят халявы. Тем более, что сегодня в Интернете можно скачать всё что угодно.

4) **USB-флешки.** В этом случае наиболее подвергнуты заражению те пользователи, чей антивирус не поддерживает проверку флеш накопителей на лету. Флешки сегодня распространены повсеместно, и именно поэтому заражение компьютеров посредством переноса вирусов через USB-накопители так распространено.

5) **Сеть.** Если ваш компьютер является частью какой-нибудь сети, даже домашней – велик риск заразить все компьютеры этой сети с одного.

6) **Фишинг.** Речь идёт о фальшивых сайтах, переходя на которые, пользователь часто получает автоматически устанавливаемые вирусы и шпионские программы. В результате фишинга нередко теряются не только данные, но и личные сбережения. Поэтому прежде чем переходить по фишинговым ссылкам, сообщаящим вам о якобы каких-то проблемах с вашим банковским счетом, лучше просто позвонить в банк, и не переходить ни по каким ссылкам.

7) **Лже антивирусные программы.** Это очень распространённый путь инфицирования персональных компьютеров. Никогда не скачивайте антивирус из непроверенного источника – всегда делайте это только с официального сайта антивирусной программы. Иначе вы подвергните свой компьютер повышенному риску инфицирования. Покупка лицензии – оптимальный способ защиты в этом случае.

8) **Хакеры.** В наши дни с этими людьми проблем стало меньше, но они по-прежнему умудряются портить жизнь пользователям Интернета.

Критерии оценивания:

Каждый индикатор достижения компетенции оценивается в 10 баллов:

- Тестовое задание оценивается в 10 баллов (ответ на вопрос теста стоит 0 или 2 балла);
- Задания на соответствие оцениваются в 10 баллов (каждое оценивается 0-5 баллов)
 - 5 баллов – полностью правильно найденные соответствия;
 - 4 балла – три правильных соответствия;
 - 3 балла – два правильных соответствия;
 - 2 балла – одно правильно соответствие;
 - 1 балл – отсутствие правильных соответствий;
 - 0 баллов – не приступал к выполнению задания;
- Каждое практическое задание оценивается в 10 баллов:
 - 10 баллов – студент правильно выполнил предложенные задания на основе изученной теории, методов, приемов, технологий;
 - 8 баллов – студент способен применять полученные теоретические знания в практической деятельности, решать типичные задачи на основе воспроизведения стандартных алгоритмов, при выполнении заданий допускает незначительные ошибки;
 - 6 баллов – при выполнении задания допущены грубые ошибки;
 - 0 баллов – студент не выполнил задание.

Оценка зависит от процента выполнения всех заданий.

Шкала оценивания сформированности компетенции(ий) и индикатора(ов) достижения компетенции(ий)

Уровни освоения индикатора (ов) достижений компетенций	Основные признаки выделения уровня	Академическая оценка	% выполнения всех заданий
Повышенный (высокий)	Включает нижестоящий уровень. Умение самостоятельно принимать решение, решать проблему/задачу теоретического или прикладного характера на основе изученных методов, приемов, технологий.	Отлично	90-100
Базовый	Включает нижестоящий уровень. Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	Хорошо	70-89
Удовлетворительный	Изложение в пределах задач курса теоретического и практического контролируемого материала	Удовлетворительно	50-69
Недостаточный	Отсутствие признаков удовлетворительного уровня	Неудовлетворительно	менее 50

Считать, что положительные результаты поститогового контроля свидетельствуют об успешном процессе формирования компетенции(ий) и индикатора(ов) достижения компетенции(ий) (этапа формирования компетенции). Если обучающийся получил оценку «неудовлетворительно», то считать компетенцию не сформированной на данном этапе. При получении оценок «удовлетворительно», «хорошо» или «отлично» считать, что проверяемая компетенция сформирована на достаточном уровне.

Методические указания для проверки остаточных знаний

1. Сроки проведения процедуры оценивания: по графику деканата.
2. Сбор, обработка и оценивание результатов поститогового контроля проводится преподавателем по распоряжению деканата.
3. Предъявление результатов оценивания осуществляется в течение недели после проведения контрольного мероприятия, оформляется в виде отчета и хранится в деканате в течение всего срока обучения обучающегося.