

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

Утверждена
на заседании ученого совета университета

06 апреля 2026 г. протокол № 8
Приказ № 39 от 08 апреля 2026 г.

Ректор Я.А. Чиговская-Назарова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной профессиональной образовательной программы	Бакалавриат
Направление подготовки	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль)	Физическая культура и Основы безопасности и защиты Родины
Форма обучения	Очная
Семестр(ы)	9

Глазов 2026

1. Цель и задачи изучения дисциплины

1.1. Цель и задачи изучения дисциплины

обеспечить подготовку будущей профессиональной деятельности бакалавра педагогического образования по профилю «Основы безопасности и защиты Родины».

Задачи изучения дисциплины:

1. Сформировать у студентов понимание природы и сущности информации, важности и необходимости информационной защиты.
2. Сформировать умение создавать и поддерживать безопасные условия жизнедеятельности; различать факторы, влекущие возникновение опасных ситуаций; предотвращать возникновение опасных ситуаций, в том числе на основе приемов по оказанию первой медицинской помощи и базовых медицинских знаний.
3. Сформировать навыки комплексного поиска, анализа и систематизации информации по изучаемым проблемам с использованием различных источников, научной и учебной литературы, информационных баз данных, формирует собственные мнения и суждения, аргументирует свою позицию.

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

Код компетенции	ОПК-1
Формулировка компетенции	Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики
Индикатор достижения компетенции	ИОПК 1.1 Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно-правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального образования, законодательства о правах ребенка, трудового законодательства ИОПК 1.2 Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности

Код компетенции	ПК-1
Формулировка компетенции	Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач
Индикатор достижения компетенции	ИПК 1.1 Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета) ИПК 1.2 Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО ИПК 1.3 Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные

1.3. Воспитательная работа

Направление воспитательной работы	Типы задач	Формы работы
гражданское	педагогический	проекты
духовно-нравственное	сопровождения	мастер-классы

1.4. Место дисциплины в структуре образовательной программы

Дисциплина "Информационная безопасность" относится к обязательной части учебного плана.

Для освоения дисциплины необходимы знания дисциплин «Философия безопасности», «Безопасность жизнедеятельности».

Дисциплина «Информационная безопасность» необходима для лучшего усвоения дисциплин «Теория и методика обучения БЖД», «Психология безопасности». Полученные знания должны использоваться студентами во время прохождения педагогических и методических практик.

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 9			
Контактная работа с преподавателем:			
Аудиторные занятия (всего)		54	
Занятия лекционного типа		18	
Лабораторные работы		-	
Занятия семинарского типа		-	
Практические занятия		34	
КСР		2	
Самостоятельная работа обучающихся		54	
Вид промежуточной аттестации: Экзамен		36	

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	пр	лаб	КСР
Семестр 9							

Тема 1. Свойства информации как объекта защиты	12	6	2	4			6
Тема 2. Содержание и анализ исторически сложившихся направлений информационной защиты	14	8	2	4		2	6
Тема 3. Информационные и компьютерные преступления	12	6	2	4			6
Тема 4. Информационные войны и информационное оружие	12	6	2	4			6
Тема 5. Психологическая война. Виды и средства психологического воздействия	12	6	2	4			6
Тема 6. Влияние СМИ на человека	14	6	2	4			8
Тема 7. Интернет и безопасность детей	10	6	2	4			4
Тема 8. Влияние компьютерных игр на поведение человека	12	6	2	4			6
Тема 9. Слухи как неформальный обмен информацией	10	4	2	2			6
Всего – по семестру	108	54	18	34		2	54
Вид промежуточной аттестации – экзамен	36						
Итого по дисциплине	144	54	18	34		2	54

3.2. Занятия лекционного типа

СЕМЕСТР 9

Лекция 1.

Тема: Свойства информации как объекта защиты

Краткая аннотация к лекции.

Три основных вида информационной защиты. Понятие об опасной информации. Виды опасной информации. Способы защиты человека от излишней, назойливой, недобросовестной информации. Вредная информация в формах обмана и злоупотребления доверием. Дезинформация и ее виды. Опасная информация в формах угроз, клеветы, оскорбления.

Защита человека и гражданина от неинформированности. Конституционные права граждан на информированность. Дополнительные права на получения информации для носителей определенных профессий. Информация, доступная по закону, и ее виды. Виды потребностей человека в информации. Информационный голод. Информация и эмоции.

Защита человека как собственника информации. Формирование прав собственности на информацию. Ценность информации. Уровни представления информации и особенности ее защиты. Характеристика вещественных и энергетических носителей информации. Формы представления компьютерной информации. Семантическая и признаковая информация, особенности их защиты.

Лекция 2.

Тема: Содержание и анализ исторически сложившихся направлений информационной защиты

Краткая аннотация к лекции.

Характеристика исторически сложившихся направлений информационной защиты. Нормативно-правовое регулирование защиты информации. Правовой режим защиты государственной тайны. Степени и грифы секретности. Правовой режим защиты конфиденциальной информации. Виды конфиденциальной информации и режимы ее

защиты. Организационно-распорядительная защита. Работа с кадрами и внутриобъектовый режим.

Инженерно-техническая защита от физического вторжения. Требования к элементам инженерной защиты объекта информатизации. Средства и методы контроля за проникновением человека-нарушителя на территорию объекта. Требования к техническим средствам охраны. Силы и средства реагирования на физическое вторжение.

Понятие утечки и перехвата информации с использованием технических каналов.

Управление доступом к информации. Средства и методы распознавания людей: парольные системы, устройства считывания ключевой информации с физических носителей, биометрические методы, их сравнительная характеристика. Требования к удаленной идентификации и аутентификации.

Защита компьютерных систем от вредоносного программного воздействия. Демаскирующие признаки опасного программного воздействия. Основные организационные и программные меры антивирусной защиты.

Электронная цифровая подпись.

Лекция 3.

Тема: Информационные и компьютерные преступления

Краткая аннотация к лекции.

Понятие о преступлении. Виды преступлений. Субъективная сторона преступления. Понятие виновности. Умысел и неосторожность, их градации. Стадии подготовки преступления и ответственность за их совершение.

Понятие об информационных и компьютерных преступлениях. Особенности и причины информационных преступлений. Понятие о неправомерном обороте информации. Составы информационных преступлений, предусмотренные Уголовным кодексом РФ. Преступления в форме незаконного распространения, разглашения и передачи информации. Незаконное воспрепятствование доступу к информации. Клевета и оскорбление. Незаконное хранение и использование конфиденциальной информации. Формы информационной фальсификации. Компьютерные мошенничества.

Особенности компьютерных преступлений. Преступления в сфере компьютерной информации. Место компьютерных систем в преступной деятельности. Компьютер как непосредственное орудие преступления. Компьютер как средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Особенности подготовки компьютерных преступлений.

Лекция 4.

Тема: Информационные войны и информационное оружие

Краткая аннотация к лекции.

Определение информационных войн (ИВ). Информационно-психологические и информационно-технологические войны. Отличие в целях, характере и способах ведения обычных и информационных войн. Противоборствующие стороны в информационной войне. Признаки поражения в информационной войне.

Виды информационно-психологического оружия. Роль средств массовой информации в ведении ИВ. Виды манипуляции массовым сознанием. Рекламные и политические кампании. Роль телевидения и Интернет в воздействии на сознание людей. Виртуальная реальность и возможности фальсификации.

Виды информационно-энергетического воздействия. Использование модулированного электромагнитного и акустического излучения с целью воздействия на подсознание и организм человека. Психотропные средства. Информационно-генетическое оружие. Психотропные препараты.

Информационно-технологическое оружие. Средства радиоподавления каналов связи и средств радиолокации. Средства электромагнитного терроризма.

Использование радиоэлементов с ограниченным сроком службы. Возможности компьютерных инфекций биологического происхождения. Классификация программного информационного оружия.

Лекция 5.

Тема: Психологическая война. Виды и средства психологического воздействия

Краткая аннотация к лекции.

Понятие психологической войны. Средства воздействия: информационные, военные, политические, система санкций. Виды психологического воздействия: информационно-психологическое, психогенное, психоаналитическое, нейролингвистическое, психотронное, психотропное.

Психологическая операция. Идеологическая война. Арсенал информационно-психологической войны. Информационно-психологическое воздействие. Прямые и косвенные методы воздействия на сознание. Роль политических мифов.

Лекция 6.

Тема: Влияние СМИ на человека

Краткая аннотация к лекции.

Понятие, виды и основные признаки средств массовой информации. Функции СМИ. СМИ как средство формирования мировоззрения народных масс. Условия формирования мировоззрения: информация, метафора, личный опыт. Методы влияния СМИ: внушение, дезинформация, информационный резонанс. Положительное влияние СМИ: влияние прессы, радио, телевидения, интернета, рекламы. Отрицательное влияние СМИ.

Лекция 7.

Тема: Интернет и безопасность детей

Краткая аннотация к лекции.

Правила безопасности в интернете. Опасности сети интернет: интернет-зависимость; онлайн-буллинг; сайты, разжигающие национальную рознь, экстремизм, национализм, фашизм; сайты порнографической направленности; депрессивные молодежные течения; наркотики; секты и под. Признаки интернет-зависимости у детей. Способы защиты детей.

Лекция 8.

Тема: Влияние компьютерных игр на поведение человека

Краткая аннотация к лекции.

Положительные эффекты: улучшение когнитивных функций, снижение стресса и тревожности, улучшение социальных навыков, использование в качестве образовательного инструмента. Отрицательные эффекты: зависимость, проблемы с физическим здоровьем (ожирение, синдром запястного канала, напряжение глаз), длительное сидение перед компьютером может увеличить риск развития сердечно-сосудистых заболеваний, некоторые игры содержат жестокое и графическое содержание, что может привести к десенсибилизации к насилию и агрессии.

Лекция 9.

Тема: Слухи как неформальный обмен информацией

Краткая аннотация к лекции.

Слухи как социально-психологический феномен. Определение слуха. Классификация слухов. Причины возникновения и механизмы распространения слухов. Управление слухами. Особенности распространения слухов в чрезвычайных ситуациях. Распространение слухов через интернет.

3.3. Занятия семинарского типа

Учебным планом не предусмотрены

3.4. Практические занятия

СЕМЕСТР 9

Практическое занятие 1.

Тема: Свойства информации как объекта защиты

Перечень заданий: подготовка аргументированных ответов на вопросы: «Что важнее – защищать человека от не информированности или от избытка информации?», «Какие виды информации вам кажутся опасными?»

Практическое занятие 2.

Тема: Содержание и анализ исторически сложившихся направлений информационной защиты

Перечень заданий: заполнение таблицы, письменные ответы на вопросы: «В чем, на ваш взгляд, заключается эффективность инженерно-технической защиты от физического вторжения?», «Какова система защиты информации от утечки по техническим каналам?»

Практическое занятие 3.

Тема: Информационные и компьютерные преступления

Перечень заданий: заполнение таблицы «Информационные и компьютерные преступления» (сопоставление особенностей и причин информационных и компьютерных преступлений по плану: объекты, субъекты преступлений, цели, формы, причины, особенности подготовки преступления).

Практическое занятие 4.

Тема: Информационные и компьютерные преступления

Перечень заданий: изучение ст. 272–274 УК РФ, в которых предусмотрена ответственность за совершение компьютерных и информационных преступлений; конспектирование

Практическое занятие 5.

Тема: Информационные войны и информационное оружие

Перечень заданий: заполнение таблицы «Обычные и информационные войны», сопоставление информационно-психологических и информационно-технологических войн по плану: объекты, субъекты, цели, формы, причины, особенности подготовки информационно-психологических и информационно-технологических войн.

Практическое занятие 6.

Тема: Информационные войны и информационное оружие

Перечень заданий: изучение научной литературы, работа с текстом, сопоставление влияния психотронного, психотропного оружия на организм человека, средств электромагнитного терроризма.

Практическое занятие 7.

Тема: Психологическая война. Виды и средства психологического воздействия

Перечень заданий: подготовка доклада на тему: «Психологическая война в истории человечества», письменные ответы на вопрос: «Какие виды и средства психологического воздействия вам кажутся наиболее эффективными?»

Практическое занятие 8.

Тема: Влияние СМИ на человека

Перечень заданий: доклад на тему: «Особенности рекламы для детей в разных странах», изучение ст. 6 ФЗ «О рекламе», конспектирование, анализ-экспертиза детской рекламы на телевидении с точки зрения соответствия ФЗ «О рекламе».

Практическое занятие 9.

Тема: Влияние СМИ на человека

Перечень заданий: ответы на вопрос: «Как влияют средства массовой информации на формирование потребностей людей, на их самооценку?», поиск в телевизионных рекламных роликах уловок, приемов, воздействующие на покупателя.

Практическое занятие 10.

Тема: Интернет и безопасность детей

Перечень заданий: изучение научной литературы, подготовка ответа на вопрос: «В чем, на ваш взгляд, заключается главная опасность сети Интернет?»

Практическое занятие 11.

Тема: Интернет и безопасность детей

Перечень заданий: составление таблицы «Эффективные способы защиты ребенка от интернет-зависимости», тестирование.

Практическое занятие 12.

Тема: Влияние компьютерных игр на поведение человека

Перечень заданий: составление экспертизы компьютерной игры по плану, организация дискуссии.

Практическое занятие 13.

Тема: Слухи как неформальный обмен информацией

Перечень заданий: подготовка доклада на тему «Слухи как социально-психологический феномен», составление фейковой новости.

Практическое занятие 14.

Тема: Доктрина информационной безопасности Российской Федерации

Перечень заданий: подготовка доклада на тему: «Сущность и содержание Доктрины информационной безопасности Российской Федерации»

Практическое занятие 15.

Тема: Угрозы, каналы несанкционированного получения информации, их классификация

Перечень заданий: подготовка доклада на тему: «Наиболее распространенные угрозы доступности. Некоторые примеры угроз доступности».

Практическое занятие 16.

Тема: Методы и оценки уязвимости информации.

Перечень заданий: заполнение таблицы «Аналитическая модель оценки защищённости информации. Статистическая модель оценки защищённости информации».

Практическое занятие 17.

Тема: Методы проектирования систем защиты информации

Перечень заданий: подготовка доклада на тему: «Классификация и анализ, постановок задач проектирования систем защиты информации. Последовательность и общее содержание проектирования систем защиты информации».

3.5. Лабораторные работы

Учебным планом не предусмотрены

3.6. Контроль самостоятельной работы

СЕМЕСТР 9

Контроль самостоятельной работы 1.

Тема: Содержание и анализ исторически сложившихся направлений информационной защиты

Перечень заданий: выполнение упражнений, просмотр видео и его обсуждение; заполнение таблицы.

3.7. Самостоятельная работа студентов

Рекомендуемые формы самостоятельной работы студентов: перечислить не менее 3 форм работы, используемые для реализации дисциплины. Формы работы можно взять из указаний «Методические рекомендации по организации образовательного процесса при освоении дисциплины».

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. Гафнер, В. В. Информационная безопасность : учебное пособие. Ч. 1 / В. В. Гафнер ; Уральский гос. пед. ун-т. - Екатеринбург : [б. и.], 2009. - 155 с. - Библиогр.: с. 140-146. - URL: <https://icdlib.nspu.ru/views/icdlib/5329/read.php> (дата обращения: 20.03.2026) . - Словарь: с. 149-154. - ISBN 978-5-7186-0414-6. - Текст : электронный
2. Гафнер, В. В. Информационная безопасность : учебное пособие. Ч. 2 / В. В. Гафнер ; Уральский гос. пед. ун-т. - Екатеринбург : [б. и.], 2009. - 196 с. - Библиогр.: с. 160-166. - URL: <https://icdlib.nspu.ru/views/icdlib/5330/read.php> (дата обращения: 20.03.2026) . - Словарь: с. 190. - ISBN 978-5-7186-0414-6. - Текст : электронный
3. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Москва : Московский городской педагогический университет, 2011. — 260 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/26486.html> (дата обращения: 20.03.2026). — Режим доступа: для авторизир. Пользователей
4. Чернова, Е. В. Информационная безопасность человека : учебник для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/587699> (дата обращения: 20.03.2026).

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: 20.03.2026). — Режим доступа: для авторизир. пользователей
2. Безопасность жизнедеятельности для педагогических и гуманитарных направлений : учебник и практикум для вузов / под общей редакцией В. П. Соломина. — Москва : Издательство Юрайт, 2026. — 351 с. — (Высшее образование). — ISBN 978-5-534-18519-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/600369> (дата обращения: 20.03.2026)
3. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/583236> (дата обращения: 20.03.2026)
4. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. — Москва : Евразийский открытый институт, 2010. — 328 с. — ISBN 978-5-374-00381-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/10746.html> (дата обращения: 20.03.2026). — Режим доступа: для авторизир. пользователей

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. <https://whatisgood.ru/> - сайт «Научи хорошему – за возрождение нравственности, разоблачение СМИ»
2. <https://geektimes.ru/hub/infosecurity/> - информационная безопасность в интернет, защита данных.
3. <http://cyberrus.com/> - вопросы кибербезопасности.

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 «Руконт». 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 университета (eios.ggpi.org).

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

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

Учебный корпус ____, аудитории(я) ____.

В образовательном процессе используется свободно распространяемое программное обеспечение, в том числе отечественного производства: экосистема Яндекс, Mail.ru и др.

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

9. Рейтинг-план оценки успеваемости студентов

Дисциплина/ семестры	Объем аудиторной работы			Виды текущей аттестационной аудиторной и внеаудиторной работы	Максимальное (норматив) количество баллов	Поощрение	Штрафы	Итоговая форма отчета (мин. балл)
	лк	пр	КСР					
Информационная безопасность / 9 семестр	18	34	2	1. Контроль посещаемости лекций 2. Контроль посещаемости практических занятий 3. Работа на практических занятиях 4. КСР <u>Контрольные мероприятия</u> 1. контрольная работа 2. тестирование <u>Компенсационные мероприятия</u> 1. Письменный реферат по темам практических занятий	18 34 30 5 5x5=25 5x5=25 5	+ 1 балл за дополнения; + 3 балла за подготовку дополнительного дидактического материала	- 1 балл за не-посещение акад. часа - 3 балла за невыполнение в установленные сроки	экзамен Допуск до экзамена – 50 % (68,5 б.) «автомат» при экзамене – 90 % (123 б.)
ИТОГО	18	34	2		137 (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 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

1.1. Настоящий Фонд оценочных средств(ФОС) по дисциплине «Информационная безопасность» является неотъемлемым приложением к рабочей программе дисциплины «Информационная безопасность» (РПД). На данный ФОС распространяются все реквизиты утверждения, представленные в РПД по данной дисциплине.

1.2. Оценивание всех видов контроля(текущего, промежуточного, послитогового) осуществляется по 5-ти 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	ОПК-1
Формулировка компетенции	Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики
Индикатор достижения компетенции	ИОПК 1.1 Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно-правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального образования, законодательства о правах ребенка, трудового законодательства ИОПК 1.2 Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности

Код компетенции	ПК-1
Формулировка компетенции	Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач
Индикатор достижения компетенции	ИПК 1.1 Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета) ИПК 1.2 Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО

	ИПК 1.3 Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные
--	--

3. Содержание оценочных средств текущего контроля и критерии их оценивания

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

3.2. Формы текущего контроля и критерии их оценивания.

Форма контроля 1 - Типовые тестовые задания

Типовой тест.

Тема: Содержание и анализ исторически сложившихся направлений информационной защиты.

Проверяемые компетенции и индикаторы достижения компетенций: ОПК-1: ИОПК 1.1., ИОПК 1.2.

Время выполнения заданий: 15 минут

Критерии оценивания:

100% - 90% правильных ответов – 5 баллов;

89% - 75% правильных ответов – 4 балла;

74% - 60% правильных ответов – 3 балла;

59% - 40% правильных ответов – 2 балла;

меньше 40% правильных ответов – 1 балл.

1. Процедура распознавания и оценка негативных воздействий среды обитания предполагает...

- а) идентификацию опасностей
- б) ликвидацию опасностей
- в) защиту от опасностей
- г) определение риска

2. Чем опасны канцерогенные вещества?

- а) появлением инфекционных заболеваний
- б) возникновением мутаций
- в) образованием злокачественных опухолей
- г) появлением аллергических заболеваний

3. При помощи каких устройств осуществляется организованная естественная вентиляция?

- а) установки кондиционирования воздуха
- б) окна, фрамуги, дефлекторы
- в) увлажнители и ионизаторы
- г) электрические вентиляторы

4. Что в первую очередь вы сделаете при оказании первой помощи при обнаружении открытого перелома с сильным кровотечением?

- а) наложу импровизированную шину на перелом
- б) остановлю кровотечение
- в) наложу повязку на рану
- г) вызову скорую помощь

5. Какие угрозы информационной безопасности не влекут за собой изменение структуры данных (копирование)?
- а) естественные угрозы
 - б) пассивные угрозы
 - в) активные угрозы
 - г) искусственные угрозы.
6. Какие угрозы информационной безопасности меняют структуру и содержание компьютерной системы (внедрение специальных программ)?
- а) естественные угрозы
 - б) пассивные угрозы
 - в) активные угрозы
 - г) искусственные угрозы.
7. Как определяется степень доступности информации, при которой антропогенный источник угроз имеет полный доступ к техническим и программным средствам обработки защищаемой информации?
- а) низкая степень доступности;
 - б) высокая степень доступности;
 - в) первая средняя степень доступности;
 - г) вторая средняя степень доступности.

Форма контроля 2 –Типовая контрольная работа

Типовая контрольная работа.

Тема: Слухи как неформальный обмен информацией

Проверяемые компетенции и индикаторы достижения компетенций: ПК-1: ИПК 1.1, ИПК 1.2; ИПК 1.3.

Время выполнения заданий: 45 минут

Критерии оценивания:

100% - 90% правильных ответов – 5 баллов;

89% - 75% правильных ответов – 4 балла;

74% - 60% правильных ответов – 3 балла;

59% - 40% правильных ответов – 2 балла;

меньше 40% правильных ответов – 1 балл.

1 задание. Ответьте на вопрос: «Каким образом следование рекламным призывам может привести к ухудшению здоровья человека?»

2 задание. Приведите примеры, иллюстрирующие понятия «информационное оружие», «информационная атака».

3 задание. Подготовьте аргументированный ответ на вопрос: «В чем заключается опасность распространения слухов в чрезвычайных ситуациях?»

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 (9 сем.).
- 4.2. Содержание оценочного средства. Проверяемые компетенции и индикаторы достижения компетенций: ОПК-1, ИОПК 1.1, ИОПК 1.2, ПК-1, ИПК 1.1, ИПК 1.2, ИПК 1.3

Примерные вопросы и задания к экзамену

Примерные вопросы и задания к экзамену:

Теория

1. Формы психологической защиты человека от информационной перегрузки.
2. Социально вредная информация в СМИ.
3. Вредная и опасная информация в Интернет.
4. Формы и методы недобросовестной рекламной деятельности.
5. Формы обмана и мошенничества в Интернет.
6. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак.
7. Способы подделки компьютерной информации (денег, документов, доказательств) и программный инструментарий.
8. Компьютерное «пиратство» и его формы. Перспективы противодействия незаконному копированию компьютерной информации.
9. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.
10. Формы и методы диверсионно-террористической деятельности с использованием современных информационных технологий.
11. Виды и формы применения информационно-технологического оружия.
12. Доктрина информационной безопасности России и реальности ее осуществления.
13. Анализ способов информационного воздействия и форм информационной защиты, отраженных в сказках, сказаниях, былинах и мифах.
14. Государственная система защиты граждан и общества от опасной информации (законодательство и практика).
15. Вопросы информационной безопасности в теории военного искусства.
16. Вопросы информационной безопасности в политике и дипломатии.
17. Формы и методы выживания биологических особей и возможности их применения при защите информации.
18. Стратегия пассивной информационной защиты.

19. Стратегия уничтожения источника угроз в сфере информационной защиты.
20. Стратегия обмана и ее использование в сфере информационной защиты.
21. Модель комплексной информационной защиты и ее элементы.

Практика

1. Продемонстрируйте формы психологической защиты человека от информационной перегрузки.
2. Приведите примеры социально вредной информации в СМИ. Дайте комментарий.
3. Приведите примеры вредной и опасной информации в Интернет. Дайте комментарий.
4. Приведите примеры недобросовестной рекламной деятельности. Какие формы и методы она имеет?
5. Приведите примеры форм обмана и мошенничества в Интернет.
6. Приведите известные вам способы подделки компьютерной информации (денег, документов, доказательств).
7. Приведите примеры компьютерного «пиратства». В каких формах оно используется?
8. Приведите примеры незаконного использования информации.
9. Приведите примеры форм и методов диверсионно-террористической деятельности с использованием современных информационных технологий.
10. Проиллюстрируйте виды и формы применения информационно-технологического оружия.
11. Приведите примеры способов информационного воздействия и форм информационной защиты, отраженных в сказках, сказаниях, былинах и мифах.
12. Проиллюстрируйте проявление информационной безопасности в теории военного искусства.
13. Проиллюстрируйте проявление информационной безопасности в политике и дипломатии.
14. Приведите примеры форм и методов выживания биологических особей и возможностей их применения при защите информации.
15. Проиллюстрируйте применение стратегии уничтожения источника угроз в сфере информационной защиты.
16. Проиллюстрируйте применение стратегии обмана и ее использования в сфере информационной защиты.
17. Приведите примеры угроз скрытого информационного воздействия на пользователей Интернет.
18. Докажите на примерах, что информация может являться объектом преступных посягательств.
19. Сконструируйте модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.
20. Сконструируйте модель компьютерного вирмейкера.
21. Проиллюстрируйте направления информационной защиты и пути их интеграции.

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 достижения 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 экзаменов (зачета - на последнем занятии по предмету). Если обучающийся по результатам рейтинговой системы не набирает нужное количество баллов или желает повысить оценку, то сдает экзамен/ зачет согласно требованиям.
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 инженерно-педагогический университет».

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 индикаторов достижения компетенции: ОПК-1, ИОПК 1.1, ИОПК 1.2, ПК-1, ИПК 1.1, ИПК 1.2, ИПК 1.3

Задания для проверки компетенции и индикатора достижения компетенции: ОПК-1, ИОПК 1.1, ИОПК 1.2.

ОПК-1 Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций
ИОПК 1.1. Умеет: создавать и поддерживать безопасные условия жизнедеятельности; различать факторы, влекущие возникновение опасных ситуаций; предотвращать возникновение опасных ситуаций, в том числе на основе приемов по оказанию первой медицинской помощи и базовых медицинских знаний.

Время выполнения заданий: 10 минут.

1. Установите соответствие между номерами гнезд аптечки индивидуальной АИ-2 и медицинскими препаратами, расположенными в них

- | | |
|--------------|-------------------------------------|
| 1 Гнездо № 1 | а) противоболевое средство |
| 2 Гнездо № 3 | б) противобактериальное средство №2 |
| 3 Гнездо № 4 | в) противорвотное средство |
| 4 Гнездо № 7 | г) радиозащитное средство №1 |

2. Установите соответствие между средствами индивидуальной защиты органов дыхания и их характеристикой.

- | | |
|--|----------------------------------|
| 1 состоит из фильтрующе-поглощающей коробки и лицевой части | а) респиратор |
| 2 представляет собой фильтрующую полумаску с носовым зажимом и эластичными тесемками | б) ватно-марлевая повязка |
| 3 состоит из корпуса и крепления; корпус сделан из 204 слоев ткани | в) противогаз |
| 4 изготавливается из куска марли размером 100х50 см | г) противопыльная тканевая маска |

Ключ к тесту:

Номер вопроса	1	2
---------------	---	---

Номер правильного ответа	1-а	1-в
	2-б	2-а
	3-г	3-г
	4-в	4-б

Задания для проверки компетенции и индикатора достижения компетенции: ПК-5, ИПК-1.1, ИПК-1.2, ИПК 1.3

ПК-1. Способен осваивать и использовать базовые научно-теоретические знания и практические умения по предмету в профессиональной деятельности	
ИПК-1.1. Применяет навыки комплексного поиска, анализа и систематизации информации по изучаемым проблемам с использованием различных источников, научной и учебной литературы, информационных баз данных, формирует собственные мнения и суждения, аргументирует свою позицию.	Практическое задание Смоделируйте последовательность действий для защиты от копирования информации.

Ключ на практическое задание.

Говоря о защите от копирования, следует помнить, что основная идея, на которой она строится, очень проста. Во внешнем (по отношению к защищаемой программе или документу) мире нужно найти объект, который обладает двумя свойствами: во-первых, он должен иметься у законного пользователя, а во-вторых, его должно быть сложно воспроизвести при распространении нелегальных копий. Этот объект называется «объектом привязки». В качестве объекта привязки может выступать оптический диск, компьютер пользователя, а также локальный или удалённый сервер. После выбора объекта привязки разработчик системы защиты от копирования должен сделать так, чтобы защищаемую программу или документ нельзя было использовать без наличия объекта привязки, и это «нельзя» было бы сложно преодолеть с помощью технологий взлома (т. е. анализа и модификации) программного кода.

Шкала оценивания сформированности компетенций и индикаторов достижения компетенций

Уровни освоения индикаторов 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 компетенций и индикаторов достижения компетенций (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.