

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 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уровень основной профессиональной образовательной программы	Бакалавриат
Направление подготовки	44.03.04 Профессиональное обучение (по отраслям)
Направленность (профиль)	Компьютерная графика и дизайн
Форма обучения	Очная
Семестр(ы)	7

Глазов 2026

1. Цель и задачи изучения дисциплины

1.1. Цель и задачи изучения дисциплины

Целью освоения учебной дисциплины является формирование способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности, осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(-ых) языке(-ах), определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений и осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Задачи изучения дисциплины:

- Изучить современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
- Изучить особенности системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение
- Изучить совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм
- Получить практический опыт использования цифровых ресурсов для решения задач профессиональной деятельности
- Получить практический опыт коммуникации в цифровой среде для достижения профессиональных целей и эффективного взаимодействия
- Получить практический опыт оценивания вероятных рисков и ограничений, определения ожидаемых результатов решения поставленных задач
- Получить практический опыт анализа источников информации с целью выявления их противоречий и поиска достоверных суждений

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

Код компетенции	УК-1
Формулировка компетенции	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
Индикатор достижения компетенции	ИУК 1.1 Демонстрирует знание особенностей системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение ИУК 1.3 Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений

Код компетенции	УК-2
Формулировка компетенции	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
Индикатор	ИУК 2.1 Определяет совокупность взаимосвязанных задач и

достижения компетенции	ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм ИУК 2.2 Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных задач
------------------------	---

Код компетенции	УК-4
Формулировка компетенции	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
Индикатор достижения компетенции	ИУК 4.3 Осуществляет коммуникацию в цифровой среде для достижения профессиональных целей и эффективного взаимодействия

Код компетенции	ОПК-9
Формулировка компетенции	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
Индикатор достижения компетенции	ИОПК 9.1 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ИОПК 9.2 Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности

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 сопровождения методический	включение в социокультурную среду путем формирования у студентов практических умений и навыков в рамках профессиональной деятельности
научно-исследовательская работа обучающихся		исследовательская деятельность студентов (публикация статей, выступление с докладом)

1.4. Место дисциплины в структуре образовательной программы

Дисциплина "Основы информационной безопасности" относится к обязательной части учебного плана.

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	3	108	
СЕМЕСТР 7			
Контактная работа с преподавателем:			
Аудиторные занятия (всего)		54	
Занятия лекционного типа		16	
Лабораторные работы		-	
Занятия семинарского типа		-	
Практические занятия		34	
КСР		4	
Самостоятельная работа обучающихся		54	
Вид промежуточной аттестации: Зачет		0	

3. Содержание дисциплины

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

Семестр 7	Всего	ауд.	Лекции	Практ.	Семинар	КСР	СРС
Тема 1. Роль и место безопасности информации. Стандарты и спецификации в области информационной безопасности. Угрозы безопасности информации. Защита информации в ЭВМ.	10	4	2	2			6
Тема 2. Понятия идентификации, аутентификации, авторизации и контроля доступа. Меры контроля доступа. Способы защиты в процессе идентификации, аутентификации, авторизации и контроля доступа.	12	6	2	4			6
Тема 3. Роль человеческого фактора в информационной безопасности. Меры физической защиты данных.	12	6	2	4			6
Тема 4. Программно-аппаратные средства защиты информации.	14	8	2	4		2	6
Тема 5. Обеспечение высокой доступности сервисов информационной безопасности. Несанкционированный доступ к информации, программные средства защиты информации от несанкционированного доступа.	12	6	2	4			6
Тема 6. Криптография. Цифровые подписи, сертификаты.	12	6	2	4			6
Тема 7. Вредоносное ПО. Антивирусные программы.	12	6	2	4			6
Тема 8. Защита от утечки информации по техническим каналам. Сетевая безопасность.	14	8	2	4		2	6

Тема 9. Организационно-правовое обеспечение информационной безопасности. Аудит и отчетность.	10	4		4			6
Зачёт							
Итого – по дисциплине	108	54	16	34		4	54

3.2. Занятия лекционного типа

СЕМЕСТР 7

Лекция 1.

Тема: Роль и место безопасности информации. Стандарты и спецификации в области информационной безопасности. Угрозы безопасности информации. Защита информации в ЭВМ. Роль человеческого фактора в информационной безопасности. Меры физической защиты данных.

Краткая аннотация к лекции.

Информация, основные свойства и характеристики безопасности ее применения. Проблемы обеспечения безопасности информации. Роль и место безопасности информации. Обзор международных и национальных стандартов и спецификаций в области безопасности информации. Сильные и слабые стороны правовых документов. Оценочные стандарты и технические спецификации. Безопасность информации в распределенных системах. "Оранжевая книга" как оценочный стандарт. Механизмы безопасности. Классы безопасности. Рекомендации X.800. Сетевые сервисы безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности.

Лекция 2.

Тема: Понятия идентификации, аутентификации, авторизации и контроля доступа. Меры контроля доступа. Способы защиты в процессе идентификации, аутентификации, авторизации и контроля доступа.

Краткая аннотация к лекции.

Разбор базовых понятий информационной безопасности и разграничения прав пользователей в информационных системах. Изучение сущности и отличий между процессами распознавания пользователя (идентификация), проверки подлинности его данных (аутентификация) и предоставления прав на выполнение действий (авторизация). Классификация мер и моделей контроля доступа (дискреционный, ролевой, мандатный), а также технических методов управления полномочиями. Анализ уязвимостей на каждом этапе проверки и изучение современных способов защиты, включая многофакторную аутентификацию, шифрование учетных данных и ведение журналов аудита доступа.

Лекция 3.

Тема: Роль человеческого фактора в информационной безопасности. Меры физической защиты данных.

Краткая аннотация к лекции.

Роль человеческого фактора в информационной безопасности. Меры физической защиты данных. Понятия идентификации, аутентификации, авторизации и контроля доступа. Меры контроля доступа. Способы защиты в процессе идентификации, аутентификации, авторизации и контроля доступа. Факторы аутентификации. Общие методы идентификации и аутентификации. Аппаратные токены. Списки контроля доступа. Модели контроля доступа. Роль человека в информационной безопасности. Типы атак социальной инженерии.

Лекция 4.

Тема: Программно-аппаратные средства защиты информации.

Краткая аннотация к лекции.

Программно-математические средства защиты информации. Контроль доступа к информации, ее подлинности и целостности. Обнаружение вторжения и контроль активности. Доступность. Отказоустойчивость и зона риска. Основы мер обеспечения высокой доступности. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Управление. Возможности типичных систем Туннелирование. Понятие несанкционированного доступа. Способы получения НСД. Методы профилактики НСД. Назначение, классификация средств защиты от НСД. Файерволл. Системы обнаружения вторжений. Обеспечение высокой доступности сервисов информационной безопасности. Несанкционированный доступ к информации, программные средства защиты информации от несанкционированного доступа. Криптография. Цифровые подписи, сертификаты. Криптография, криптология и криптоанализ. Классификация криптоалгоритмов. Простейшие методы шифрования. Требования к алгоритму шифрования. Симметричный криптоалгоритмы DES, ГОСТ. Криптографические системы с открытым ключом.

Лекция 5.

Тема: Обеспечение высокой доступности сервисов информационной безопасности. Несанкционированный доступ к информации, программные средства защиты информации от несанкционированного доступа.

Краткая аннотация к лекции.

Анализ методов поддержания непрерывности бизнес-процессов и высокой доступности критически важных сервисов безопасности. Изучение природы, каналов и последствий несанкционированного доступа (НСД) к конфиденциальным данным со стороны внешних нарушителей и внутренних угроз (инсайдеров). Классификация, принципы работы и архитектура программных средств защиты информации от НСД. Обзор функциональных возможностей современных защитных систем: разграничение прав, контроль целостности программной среды, блокировка несанкционированных действий и аудит событий безопасности.

Лекция 6.

Тема: Криптография. Цифровые подписи, сертификаты.

Краткая аннотация к лекции.

Изучение математических основ и практического применения криптографических методов для обеспечения конфиденциальности, целостности и аутентичности данных. Разбор принципов работы симметричного и асимметричного шифрования, а также механизмов криптографического хэширования. Анализ структуры, алгоритмов формирования и проверки электронной цифровой подписи (ЭЦП) как инструмента подтверждения авторства и неизменности информации. Назначение, архитектура и стандарты цифровых сертификатов открытых ключей, принципы функционирования инфраструктуры открытых ключей (PKI) и роль удостоверяющих центров в обеспечении доверенного сетевого взаимодействия.

Лекция 7.

Тема: Вредоносное ПО. Антивирусные программы. Защита от утечки информации по техническим каналам. Сетевая безопасность.

Краткая аннотация к лекции.

Структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты. Классификация и структура современного вредоносного ПО. Способы распространения и среда обитания вредоносного ПО. Виды проявлений вредоносного ПО. Основные классы антивирусных программ. Основные методы антивирусной защиты. Антивирусная защита. Антивирусная защита домашнего компьютера. Антивирусная защита компьютерной сети. Антивирусная защита мобильных пользователей. Технические средства защиты информации. Методы защиты технических

каналов. Защита сетей. Использование брандмауэров. Защита сетевого трафика. Инструменты сетевой безопасности. Методы защиты и профилактики. Защита от утечки информации, НСД. Автоматизация технического контроля защиты потоков информации. Технологии хранения, резервного копирования и разграничения доступа к информации. Правовые методы защиты информации в РФ. Компьютерная преступность. Компьютерное пиратство.

Лекция 8.

Тема: Защита от утечки информации по техническим каналам. Сетевая безопасность.

Краткая аннотация к лекции.

Классификация и физическая природа возникновения технических каналов утечки информации, включая акустические и каналы побочных электромагнитных излучений и наводок (ПЭМИН). Методы и инженерно-технические средства пассивной и активной защиты речевой и цифровой информации от перехвата. Анализ базовых угроз сетевой безопасности и архитектуры построения защищенных распределенных сетей. Принципы работы программно-аппаратных средств сетевой защиты: межсетевых экранов (Firewalls), систем обнаружения и предотвращения вторжений (IDS/IPS), а также технологий организации защищенных виртуальных каналов (VPN).

3.3. Занятия семинарского типа

Учебным планом не предусмотрены

3.4. Практические занятия

СЕМЕСТР 7

Практическое занятие 1.

Тема: Роль и место безопасности информации. Стандарты и спецификации в области информационной безопасности. Угрозы безопасности информации. Защита информации в ЭВМ.

Перечень заданий:

- Изучение защиты документов и паролей доступа к системе. Введение в понятие информационной безопасности.
- Стандарты и спецификации в области информационной безопасности. Основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем, рекомендации X.800, администрирование средств безопасности
- Изучение защиты документов и паролей доступа к системе.
- Понятия идентификации, аутентификации, авторизации и контроля доступа. Меры контроля доступа. Способы защиты в процессе идентификации, аутентификации, авторизации и контроля доступа. Законодательный уровень информационной безопасности
- Обзор законодательного уровня информационной безопасности и почему он важен, обзор российского законодательства в области информационной безопасности, закон "Об информации, информатизации и защите информации", другие законы и нормативные акты, обзор зарубежного законодательства в области информационной безопасности. Роль человеческого фактора в информационной безопасности.

Практическое занятие 2-3.

Тема: Понятия идентификации, аутентификации, авторизации и контроля доступа. Меры контроля доступа. Способы защиты в процессе идентификации, аутентификации, авторизации и контроля доступа.

Перечень заданий:

- Разбор работы процессов на примерах. Описать по шагам процессы идентификации, аутентификации и авторизации на примере входа в личный кабинет банка или электронную почту.
- Настройка ролевой модели доступа: Создать простую таблицу прав для корпоративного сайта (определить, какие разделы и действия доступны Гостю, Редактору и Администратору).
- Анализ надежности паролей. Проверить несколько тестовых паролей через специализированные сервисы на устойчивость к подбору (брутфорсу) и составить правила создания надежного пароля.

Практическое занятие 4-5.

Тема: Роль человеческого фактора в информационной безопасности. Меры физической защиты данных.

Перечень заданий:

- Изучение методов социальной инженерии. Разобрать примеры популярных психологических уловок мошенников (фишинг, вишинг, претекстинг) и составить памятку по их распознаванию.
- Анализ писем на признаки мошенничества. Изучить несколько подозрительных электронных писем и выявить в них опасные признаки (поддельные адреса, фишинговые ссылки, требования срочности).
- Проектирование системы физической защиты офиса. Составить схему размещения оборудования безопасности (камер видеонаблюдения, СКУД, замков, датчиков движения) для защиты серверной комнаты от проникновения.

Практическое занятие 6-7.

Тема: Программно-аппаратные средства защиты информации.

Перечень заданий:

- Сервисы безопасности, анализ защищенности, обеспечение отказоустойчивости, обеспечение безопасного восстановления
- Администрирование групп и пользователей операционной системы. Настройка прав пользователей и групп в операционной системе. Ограниченный доступа к ресурсам ЭВМ различных группам пользователей. Защита документов путем настройки прав доступа к ресурсам. Защита файловой системы. Методы обеспечения защиты данных в файловой системе. Использование ПО для создания зашифрованных томов файловой системы. Восстановление и удаление данных. Подготовительные этапы управления рисками, основные этапы управления рисками, создания карты информационной системы организации.
- Обеспечение высокой доступности сервисов информационной безопасности. Несанкционированный доступ к информации, программные средства защиты информации от несанкционированного доступа.

Практическое занятие 8-9.

Тема: Обеспечение высокой доступности сервисов информационной безопасности. Несанкционированный доступ к информации, программные средства защиты информации от несанкционированного доступа.

Перечень заданий:

- Изучение методов резервного копирования. Настроить автоматическое создание резервных копий важных файлов операционной системы по расписанию и проверить их восстановление.
- Анализ логов на признаки взлома. Изучить журнал событий (логи) операционной системы, найти записи о неудачных попытках входа и определить признаки несанкционированного доступа.

- Тестирование контроля целостности файлов. Запустить функцию проверки неизменности системных файлов, внести тестовое изменение в защищенный документ и проверить, как программа фиксирует нарушение целостности.

Практическое занятие 10-11.

Тема: Криптография. Цифровые подписи, сертификаты.

Перечень заданий:

- Шифрование текста методом маршрутов. Шифрование текста методом таблиц Вижинера. Работа с ЭЦП. Понятие ЭЦП. Шифрование с открытым ключом.
- Организация многосторонней зашифрованной связи с использованием открытого ключа. Изучение стеганографического скрывания информации. Изучение криптографического закрытия информации.
- Функциональные компоненты и архитектура. Контроль целостности. Цифровые сертификаты. Изучение генераторов псевдослучайных последовательностей. Шифрование текста с использованием бесконечной гаммы.

Практическое занятие 12-13.

Тема: Вредоносное ПО. Антивирусные программы.

Перечень заданий:

- Методы профилактики вирусного заражения. Правила обеспечения безопасности ЭВМ и электронных носителей от вредоносного ПО. Способы борьбы в условиях заражения ЭВМ и электронных носителей. Методы настройки антивирусного ПО.
- Защита от утечки информации по техническим каналам. Сетевая безопасность.
- Обеспечение сетевой безопасности. Программные и программно-аппаратные комплексы сетевой защиты. Брандмауэры. Настройка входящих и исходящих правил брандмауэра. Ограничение передачи пакетов от различных ресурсов.
- Меры обеспечения сетевой безопасности. Настройка виртуальной частной сети. Использование Proxy-серверов. Сетевые протоколы с использованием шифрования. Правила работы в сети Интернет.

Практическое занятие 14-15.

Тема: Защита от утечки информации по техническим каналам. Сетевая безопасность.

Перечень заданий:

- Настройка межсетевого экрана (Брандмауэра). Создать правила фильтрации сетевого трафика (блокировка определенных портов, запрет доступа к выбранным сайтам и IP-адресам).
- Создание защищенного VPN-канала. Настроить виртуальную частную сеть для безопасной передачи данных между двумя компьютерами через незащищенную сеть.

Практическое занятие 16-17.

Тема: Организационно-правовое обеспечение информационной безопасности. Аудит и отчетность.

Перечень заданий:

- Понятие отчетности в информационной безопасности. Роль отчетности. Преимущества внедрения отчетности.
- Ведение журналов. Мониторинг. Аудит с выполнением оценки.
- Типы соответствий нормативным положениям. Структуры для соответствия. Международная организация по стандартизации. Типы мер контроля организационно-правового обеспечения.

3.5. Лабораторные работы

Учебным планом не предусмотрены

3.6. Контроль самостоятельной работы

СЕМЕСТР 7

Контроль самостоятельной работы 1.

Тема: Программно-аппаратные средства защиты информации.

Перечень заданий:

- Выбрать два современных антивирусных комплекса, сравнить их методы обнаружения угроз и занести данные в таблицу.
- Подготовить краткую аналитическую записку о методах контроля целостности операционной системы с помощью встроенных и сторонних программных утилит.

Контроль самостоятельной работы 2.

Тема: Защита от утечки информации по техническим каналам. Сетевая безопасность.

Перечень заданий:

- Составить перечень офисной техники (мониторы, системные блоки, кабели), способной создавать побочные электромагнитные излучения, и описать способы их экранирования.
- Создать аналитическую таблицу с техническими характеристиками и стойкостью популярных протоколов сетевой защиты (TLS/SSL, IPsec, WPA3).

3.7. Самостоятельная работа студентов

Рекомендуемые формы самостоятельной работы студентов: закрепление материала по конспекту лекции, подготовка к практическим занятиям, подготовка презентаций к докладам, подготовка к различным формам промежуточной и итоговой аттестации.

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. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142285.html> (дата обращения: 15.03.2026). — Режим доступа: для авторизир. пользователей
2. 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: 04.03.2026) . - Словарь: с. 149-154. - ISBN 978-5-7186-0414-6. - Текст : электронный
3. Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань : РГПУ, 2021. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/220418> (дата обращения: 15.03.2026). — Режим доступа: для авториз. пользователей.

4. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/133957.html> (дата обращения: 15.03.2026). — Режим доступа: для авторизир. пользователей

5.2. Дополнительная литература

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/124242.html> (дата обращения: 15.03.2026). — Режим доступа: для авторизир. пользователей
2. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590420> (дата обращения: 27.03.2026).
3. Мирошников, А. И. Основы информационной безопасности и защита информации : учебное пособие / А. И. Мирошников, А. С. Сысоев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128718.html> (дата обращения: 15.03.2026). — Режим доступа: для авторизир. пользователей
4. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/72345.html> (дата обращения: 15.03.2026). — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/72345>
5. 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: 27.03.2026).

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://moodle.ggpi.org> – сайт дистанционного образования ГГПИ;
2. <http://www.Intuit.ru> - образовательный портал Интуит;
3. <https://upweek.ru/> - UPGRADE информационный ресурс об IT;
4. <https://www.lektorium.tv/> - образовательный проект. Лекториум;
5. <https://itc.ua> – ITC.UA информационный IT ресурс.

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 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 1, аудитории(я) 232.

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

Основы информационной безопасности, 7 сем

Объем аудиторной работы				Виды текущей аттестационной аудиторной и внеаудиторной работы	Максимальное количество баллов (норматив)	Поощрение, количество баллов	Штрафы	Итоговая форма отчета
лк	пр	сем	КСР					
16	34	-	4	1. Контроль посещаемости лекций 2. Контроль посещаемости практических занятий 3. Работа на практических занятиях Контрольные мероприятия: 1. Контрольные работы (№ 1, № 2) 2. Домашняя контрольная работа 3. Тестирование по разделам курса (3 раздела) 4. Итоговая контрольная работа Компенсационные мероприятия: 1. Реферат по одной из предложенных тем (см. РПД) 2. Сообщение или интерактивная презентация 3. Деловая активность 4. Индивидуальная контрольная работа по пропущенным разделам (см. РПД)	16 34 78 10 5 30 10	 20 15 8 15	- 2 балла за отсутствии на занятии - 5 баллов за несвоевременную сдачу отчетных работ (домашних, индивидуальных)	91 балл - допуск к зачету (50%) 128 баллов - зачёт «автомат» (70 %)
				Итого	183 (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

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

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

1.2. Оценивание всех видов контроля(текущего, промежуточного, послитоогового) 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	УК-1
Формулировка компетенции	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
Индикатор достижения компетенции	ИУК 1.1 Демонстрирует знание особенностей системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение ИУК 1.3 Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений

Код компетенции	УК-2
Формулировка компетенции	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
Индикатор достижения компетенции	ИУК 2.1 Определяет совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм ИУК 2.2 Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных задач

Код компетенции	УК-4
Формулировка компетенции	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
Индикатор достижения компетенции	ИУК 4.3 Осуществляет коммуникацию в цифровой среде для достижения профессиональных целей и эффективного взаимодействия

Код компетенции	ОПК-9
Формулировка компетенции	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
Индикатор достижения компетенции	ИОПК 9.1 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ИОПК 9.2 Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности

3. Содержание оценочных средств текущего контроля и критерии их оценивания

3.1. Текущий контроль осуществляется преподавателем дисциплины при проведении занятий в следующих формах: *вставить самостоятельно*

3.2. Формы текущего контроля и критерии их оценивания.

Форма контроля 1 - Типовые тестовые задания

Проверяемые компетенции и индикаторы достижения компетенций: ОПК-9, ИОПК 9.1, ИОПК 9.2, УК-4, ИУК 4.3, УК-2, ИУК 2.1, ИУК 2.2, УК-1, ИУК 1.1, ИУК 1.3

Время выполнения заданий: 30 минут

Критерии оценивания:

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

1. Что такое защита информации?

- а) защита от несанкционированного доступа к информации;
 - б) выпуск бронированных коробочек для дискет;
 - в) комплекс мероприятий, направленных на обеспечение информационной безопасности.
2. К какой группе мер по защите информации относится шифрование информации?

- а) организационным;
- б) техническим;
- в) аппаратным;
- г) программным.

3. Укажите принципы создания комплексной системы защиты информации:

- а) неизменности;
- б) прозрачности;
- в) модульности;
- г) рациональности;
- д) доступности.

4. Внешние техногенные угрозы информационной безопасности обусловлены:

- а) средствами связи и помехами от них;
- б) близко расположенными опасными производствами;
- в) некачественными программными средствами;
- г) взаимодействием технических средств.

5. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?

- а) стихийные;

- б) техногенные;
 - в) антропогенные.
6. Основные цели организационных мер защиты информации:
- а) обеспечение правильности функционирования механизмов защиты;
 - б) предоставление бесперебойного доступа к необходимой информации авторизованным сотрудникам;
 - в) регламентация автоматизированной обработки информации;
 - г) шифрование информации.
7. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода:
- а) макровирус;
 - б) троянский конь;
 - в) червь;
 - г) файловый вирус.
8. Самым слабым элементом в помещении с точки зрения звукоизоляции являются:
- а) двери, стены, система заземления;
 - б) двери, пол, потолок;
 - в) двери, окна;
 - г) окна, система заземления, пол.
9. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?
- а) организационное;
 - б) организационно-техническое;
 - в) техническо-организационное;
 - г) техническое.
10. Какие пункты относятся к активным методам защиты речевой информации?
- а) создание маскирующих акустических и вибрационных помех;
 - б) выявление факта несанкционированного подключения к линии;
 - в) создание прицельных электромагнитных помех акустическим закладным устройствам;
 - г) выявление излучений акустических закладных устройств;
 - д) уничтожение средств несанкционированного подключения к телефонной линии.
11. В число основных принципов построения системы безопасности, с точки зрения её архитектуры, входят:
- а) следование признанным стандартам;
 - б) применение нестандартных решений, не известных злоумышленникам;
 - в) разнообразие защитных средств.
12. Оценка рисков позволяет ответить на следующие вопросы:
- а) Как спроектировать надежную защиту?
 - б) Какую политику безопасности предпочесть?
 - в) Какие защитные средства экономически целесообразно использовать?
13. Окно опасности появляется, когда:
- а) становится известно о средствах использования уязвимости;
 - б) появляется возможность использовать уязвимость;
 - в) устанавливается новое программное обеспечение.
14. Окно опасности перестает существовать, когда:
- а) администратор безопасности узнает об угрозе;
 - б) производитель программного обеспечения выпускает заплату;
 - в) заплатка устанавливается в защищаемой информационной системе.
15. В число направлений физической защиты входят:
- а) мобильная защита систем;
 - б) системная защита средств мобильной связи;

- в) защита мобильных систем;
- г) противопожарные меры;
- д) межсетевое экранирование;
- е) контроль защищенности;
- ж) физическая защита пользователей;
- з) защита поддерживающей инфраструктуры;
- и) защита от перехвата данных.

16. Политика безопасности:

- а) строится на основе общих представлений об информационной системе организации;
- б) строится на основе изучения политик родственных организаций;
- в) строится на основе анализа рисков;
- г) фиксирует правила разграничения доступа;
- д) отражает подход организации к защите своих информационных активов;
- е) описывает способы защиты руководства организации.

17. Оценка рисков позволяет ответить на следующие вопросы:

- а) Как спроектировать надежную защиту?
- б) Какую политику безопасности предпочесть?
- в) Какие защитные средства экономически целесообразно использовать?
- г) Чем рискует организация, используя информационную систему?
- д) Чем рискуют пользователи информационной системы?
- е) Чем рискуют системные администраторы?
- ж) Существующие риски приемлемы?
- з) Кто виноват в том, что риски неприемлемы?
- и) Что делать, чтобы риски стали приемлемыми?

18. Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией о методах использования уязвимостей?

- а) да, поскольку знание таких методов помогает ликвидировать уязвимости;
- б) нет, поскольку это плодит новых злоумышленников;
- в) не имеет значения, поскольку если информация об использовании уязвимостей понадобится, ее легко найти.

19. Риск является функцией:

- а) вероятности реализации угрозы;
- б) стоимости защитных средств;
- в) числа уязвимостей в системе.

20. В число принципов физической защиты входят:

- а) беспощадный отпор;
- б) непрерывность защиты в пространстве и времени;
- в) минимизация защитных средств.

21. В число основных принципов архитектурной безопасности входят:

- а) применение наиболее передовых технических решений;
- б) применение простых, апробированных решений;
- в) сочетание простых и сложных защитных средств.

22. Меры информационной безопасности направлены на защиту от:

- а) нанесения неприемлемого ущерба;
- б) нанесения любого ущерба;
- в) подглядывания в замочную скважину.

23. Из принципа разнообразия защитных средств следует, что:

- а) в разных точках подключения корпоративной сети к Internet необходимо устанавливать разные межсетевые экраны;
- б) каждую точку подключения корпоративной сети к Internet необходимо защищать несколькими видами средств безопасности;
- в) защитные средства нужно менять как можно чаще.

24. При анализе стоимости защитных мер следует учитывать:

- а) расходы на закупку оборудования;
- б) расходы на закупку программ;
- в) расходы на обучение персонала.

25. Обеспечение информационной безопасности зависит от:

- а) руководства организаций;
- б) системных и сетевых администраторов;
- в) пользователей.

Форма контроля 2 – Типовая контрольная работа

Проверяемые компетенции и индикаторы достижения компетенций: ОПК-9, ИОПК 9.1, ИОПК 9.2, УК-4, ИУК 4.3, УК-2, ИУК 2.1, ИУК 2.2, УК-1, ИУК 1.1, ИУК 1.3

Время выполнения заданий: 45 минут

Критерии оценивания: Результаты выполнения обучающимся заданий оцениваются по пятибалльной шкале.

- «Отлично» – оценка соответствует повышенному уровню и выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
- «Хорошо» – оценка соответствует повышенному уровню и выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос или выполнении заданий, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
- «Удовлетворительно» – оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
- «Неудовлетворительно» – оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Примерные варианты вопроса 1

1. Регистрация авторских прав на компьютерные программы
2. Закон РФ "О правовой охране программ для ЭВМ и баз данных"
3. Закон РФ "О правовой охране программ ...". Основные понятия
4. Закон РФ "О правовой охране программ ...". Отношения, регулируемые Законом
5. Закон РФ "О правовой охране программ ...". Объект правовой охраны
6. Закон РФ "О правовой охране программ ...". Условия признания авторского права
7. Закон РФ "О правовой охране программ ...". Авторское право на базу данных
8. Закон РФ "О правовой охране программ ...". Срок действия авторского права
9. Закон РФ "О правовой охране программ ...". Авторство
10. Закон РФ "О правовой охране программ ...". Личные права
11. Закон РФ "О правовой охране программ ...". Исключительное право

12. Закон РФ "О правовой охране программ ...". Передача исключительного права
13. Закон РФ "О правовой охране программ ...". Принадлежность исключительного права на программу
14. Закон РФ "О правовой охране программ ...". Право на регистрацию
15. Закон РФ "О правовой охране программ ...". Использование программы
16. Закон РФ "О правовой охране программ ...". Свободное воспроизведение и адаптация программы
17. Закон РФ "О правовой охране программ ...". Контрафактные экземпляры программы
18. Закон РФ "О правовой охране программ ...". Защита прав на программу
19. Свободно программное обеспечение
20. Жизненный цикл экземпляра программы и «общая стоимость владения им.
21. Свободная и несвободная модели коммерческого ПО
22. Несвободное программное обеспечение
23. Несвободное программное обеспечение. Монополизация услуг
24. Возможности экономии за счет свободы ПО
25. Государство как правообладатель свободного ПО

Примерные варианты вопроса 2

1. Выделить нормативно-правовые акты, регулирующие циркулирование информации в организации (из списка организаций).
 2. Выявить категории персональных данных и порядок обращения с ними в ситуации обращения за услугой в организацию (из списка ситуаций).
 3. Выделить нормативно-правовые акты, закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций).
 4. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в социальной сети, передача логина пароля специалисту обслуживающей организации).
 5. Оценить действия сотрудника предприятия, приведшие к инциденту, СВЯЗАННОМУ С УГРОЗОЙ информационной безопасности (в предлагаемой ситуации).
 6. Установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла.
 7. Проектирование модели угроз путем сопоставления угроз и методов их парирования (в предлагаемой ситуации).
- 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).

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: зачета (9 сем.).
- 4.2. Содержание оценочного средства. Проверяемые компетенции и индикаторы достижения компетенций: ОПК-9, ИОПК 9.1, ИОПК 9.2, УК-4, ИУК 4.3, УК-2, ИУК 2.1, ИУК 2.2, УК-1, ИУК 1.1, ИУК 1.3

Примерные вопросы и задания к зачету

1. Защита информации.
2. Группа мер по защите информации.
3. Принципы создания комплексной системы защиты информации.
4. Внешние техногенные угрозы информационной безопасности.
5. Группа угроз информационной безопасности - ошибки программного обеспечения. Приведите примеры
6. Основные цели организационных мер защиты информации.
7. Мероприятия по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений. Приведите примеры
8. Активные методы защиты речевой информации.
9. Основные принципы построения системы безопасности, с точки зрения её архитектуры.
10. Оценка рисков. Приведите примеры
11. Проектирование защиты
12. Направления физической защиты. Приведите примеры.
13. Политика безопасности.
14. Оценка рисков.
15. Ресурсы по информационной безопасности.
16. Принципы физической защиты.
17. Основные принципы архитектурной безопасности.
18. Меры информационной безопасности.
19. Принцип разнообразия защитных средств.
20. Анализ стоимости защитных мер.
21. Обеспечение информационной безопасности.

Задания:

1. Выделить нормативно-правовые акты, регулирующие циркулирование информации в организации (из списка организаций).
2. Выявить категории персональных данных и порядок обращения с ними в ситуации обращения за услугой в организацию (из списка ситуаций).
3. Выделить нормативно-правовые акты, закрепляющие недопустимость сокрытия или ограничения доступа к информации (из списка организаций).
4. Выявить угрозы информационной безопасности в предлагаемой ситуации (общение в

- социальной сети, передача логина пароля специалисту обслуживающей организации).
5. Оценить действия сотрудника предприятия, приведшие к инциденту, СВЯЗАННОМУ С УГРОЗОЙ информационной безопасности (в предлагаемой ситуации).
 6. Установка, настройка антивируса, проверка его работоспособности путем создания тестового вирусного файла.
 7. Проектирование модели угроз путем сопоставления угроз и методов их парирования (в предлагаемой ситуации).

4.3. Критерии оценивания

Зачет выставляется по результатам рейтинга. Если обучающийся набрал недостаточное количество баллов, то он сдает зачет.

Шкала оценивания для зачета:

Уровни освоения компетенции	Основные признаки выделения уровня	Академическая оценка	% освоения (рейтинговая оценка)
Сформирована	Студент показал достаточно прочные знания основных положений учебной дисциплины, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты.	Зачтено	50-100
Не сформирована	При ответе выявились существенные пробелы в знаниях основных положений учебной дисциплины, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.	Не зачтено	менее 50

4.4. Методические указания по проведению процедуры промежуточной аттестации

1. Сроки проведения процедуры оценивания: на последнем занятии по предмету. Если обучающийся по результатам рейтинговой системы не набирает нужное количество баллов, то сдает 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 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 индикаторов достижения компетенции: ОПК-9, ИОПК 9.1, ИОПК 9.2, УК-4, ИУК 4.3, УК-2, ИУК 2.1, ИУК 2.2, УК-1, ИУК 1.1, ИУК 1.3

Код компетенции	ОПК-9
Формулировка компетенции	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
Индикатор достижения компетенции	ИОПК 9.1 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ИОПК 9.2 Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности

Практическое задание 1. (ИОПК 9.1). На примере компании, где вы проходили практику(или предложенной преподавателем, или компания, по которой планируете выполнять дипломный проект, или компания, описание и данные по которой вы использовали в рамках другого курса) опишите этапы разработки нормативной и административно-организационной документации для обеспечения информационной безопасности. Приведите краткое описание компании по плану:

- название, организационно-правовая форма, учредители, краткая история компании (год основания, основные этапы развития), сфера деятельности, миссия
- количество сотрудников, организационная структура (представить в виде рисунка)
- способы ведения бизнеса, основные конкуренты и конкурентная стратегия
- основные поставщики и потребители (клиенты), цели компании на ближайший год,

Практическое задание 2. (ИОПК 9.2). Определите направления политики информационной безопасности (ИБ) компании (общая политика ИБ без указания конкретных деталей, примерных сроков, ответственных лиц). Остановитесь подробно на следующих аспектах:

- цели политики ИБ;
- основные принципы;
- на кого будет распространяться эта политика;
- выделение групп пользователей;
- выделение основных видов информационных ресурсов;
- определение уровней доступа (атрибутов безопасности) к информации определение политики в отношении паролей (повторяемость, количество паролей, хранимое системой, максимальный срок действия пароля, минимальная длина пароля, соответствие требованиям сложности, параметры блокировки учетных записей)
- определение политики в отношении доступа к ресурсам сети Internet (использование доступа к сети Internet в личных целях, ведение «белого» или «черного» списка сайтов, временной интервал доступа сети Internet, объем скачиваемой и загружаемой информации, возможности использования ресурсов сети Internet различными группами

- пользователей, использование почтовых и иных сервисов, контроль за использованием ресурсов сети Internet)
- что разрешено, а что запрещено различным группам пользователей, рекомендации для пользователей.

Ключ к практическому заданию 1.

Этапы стадии создания системы защиты информации:

Этап 1. Формирование требований к системе защиты информации (предпроектный этап).

Этап 2. Разработка системы защиты информации (этап проектирования).

Этап 3. Внедрение системы защиты информации (этап установки, настройки, испытаний).

Этап 4. Подтверждение соответствия системы защиты информации (этап оценки)

Формирование требований к системе защиты информации

Этап 1 осуществляется владельцем информации (заказчиком).

Перечень работ на этапе 1:

1. Принятие решения о необходимости защиты обрабатываемой информации.
2. Классификация объекта по требованиям защиты информации (установление уровня защищенности обрабатываемой информации).
3. Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации.
4. Определение требований к системе защиты информации.

Основные документы, формируемые по результатам исполнения работ на этапе формирования требований к системе защиты информации:

Действие	Документ
1. Принятие решения о необходимости защиты информации	Локальный нормативный правовой акт, определяющий необходимость создания системы защиты информации
2. Классификация по требованиям защиты информации (по уровню защищенности информации)	Акт классификации по требованиям безопасности информации
3. Определение актуальных угроз безопасности информации	Частная модель угроз безопасности информации
4. Определение требований к системе защиты информации	ТЗ на создание системы защиты информации с указанием требований к мерам и средствам защиты информации

Этап 2 - разработка системы защиты информации – организуется владельцем информации (заказчиком).

Перечень работ на этапе 2:

1. Проектирование системы защиты информации.
2. Разработка эксплуатационной документации на систему защиты информации.

Действие	Документ
1. Проектирование системы защиты информации	Технический проект (рабочая документация) на создание системы защиты информации
2. Разработка эксплуатационной документации на систему защиты информации	Описание структуры системы защиты информации. Технический паспорт с указанием наименования, состава и мест установки аппаратных и программных средств.

	Перечень параметров настройки средств защиты информации. Правила эксплуатации средств защиты информации.
--	---

Этап 3 - Внедрение системы защиты информации – организуется обладателем информации (заказчиком) с привлечением оператора. Перечень работ на этапе 3:

1. Установка и настройка средств защиты информации.
2. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта.
3. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению;
4. Испытания и опытная эксплуатации системы защиты информации.

Действие	Документ
1. Установка и настройка средств защиты информации	Акт установки средств защиты информации
2. Внедрение организационных мер, разработка организационно-распорядительных документов	Документы по регламентации правил по эксплуатации и вывода из эксплуатации системы защиты информации
3. Выявление и анализ уязвимостей	Протокол контроля уязвимостей программного обеспечения и технических средств
4. Испытания и опытная эксплуатации системы защиты информации	Протоколы контроля оценки эффективности средств и оценки защищенности информации

Этап 4 - подтверждение соответствия системы защиты информации – организуется обладателем информации (заказчиком) или оператором.

Перечень работ на этапе 4 определяется в Программе и методиках аттестационных испытаний, разрабатываемой до их начала. Документ формируется исполнителем работ и согласовывается с заявителем.

Основные документы, формируемые по результатам исполнения работ на этапе подтверждения соответствия системы защиты информации:

Действие	Документ
1. Аттестационные испытания системы защиты информации	Протоколы и заключение по результатам аттестационных испытаний
2. Оформление результатов аттестационных испытаний	Рекомендации по обеспечению защищенности информации на аттестуемом объекте и Аттестат соответствия

Ключ к практическому заданию 2.

Общие принципы безопасного функционирования

1. Своевременность обнаружения проблем. Организация должна своевременно обнаруживать проблемы, потенциально способные повлиять на его бизнес-цели.
2. Прогнозируемость развития проблем. Организация должна выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.
3. Оценка влияния проблем на бизнес-цели. Организация должна адекватно оценивать степень влияния выявленных проблем.

4. Адекватность защитных мер. Организация должна выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.
5. Эффективность защитных мер. Организация должна эффективно реализовывать принятые защитные меры.
6. Использование опыта при принятии и реализации решений. Организация должна накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.
7. Непрерывность принципов безопасного функционирования. Организация должна обеспечивать непрерывность реализации принципов безопасного функционирования.
8. Контролируемость защитных мер. Организация должна применять только те защитные меры, правильность работы которых может быть проверена, при этом организация должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели организации.

Код компетенции	УК-4
Формулировка компетенции	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
Индикатор достижения компетенции	ИУК 4.3 Осуществляет коммуникацию в цифровой среде для достижения профессиональных целей и эффективного взаимодействия

Практическое задание 1.

Произвести настройку системного ПО согласно основным положениям и концепциям архитектуры компьютера и сети (локальной и глобальной), используя современные языки программирования и технологии эксплуатации программных комплексов.

Дополнительные вопросы

1. Насколько возможно использование интернета в личных целях?
2. Следует ли ограничивать работу в интернете в нерабочее время?
3. Как решаются вопросы конфиденциальности корпоративной информации?
4. Какое место занимают вопросы безопасности в политике ИБ?
5. На кого распространяется эта политика?
6. Какие права оставляет за собой организация?
7. Какие юридические аспекты необходимо учитывать?

Ключ к практическому заданию 1.

Решение задач обеспечения безопасности информации достигается:

1. строгим учетом всех подлежащих защите ресурсов системы (*информации, задач, каналов связи, серверов, АРМ*);
2. регламентацией процессов обработки информации и действий работников структурных подразделений организации, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, на основе организационно-распорядительных документов по вопросам обеспечения безопасности информации;
3. полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
4. назначением и подготовкой работников, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации;

5. наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам АС;
6. четким знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
7. персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;
8. реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;
9. принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности компонентов АС;
10. применением технических (*программно-аппаратных*) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
11. разграничением потоков информации и запрещением передачи информации ограниченного распространения по незащищенным каналам связи;
12. эффективным контролем за соблюдением работниками требований по обеспечению безопасности информации;
13. постоянным мониторингом сетевых ресурсов, выявлением уязвимостей, своевременным обнаружением и нейтрализацией внешних и внутренних угроз безопасности компьютерной сети;
14. юридической защитой интересов организации от противоправных действий в области информационной безопасности.
15. проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в АС.

Код компетенции	УК-2
Формулировка компетенции	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
Индикатор достижения компетенции	ИУК 2.1 Определяет совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм ИУК 2.2 Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных задач

Время выполнения заданий: не более 30 минут

1. Что такое защита информации?
 - а) защита от несанкционированного доступа к информации;
 - б) выпуск бронированных коробочек для дискет;
 - в) комплекс мероприятий по шифрованию данных;
 - г) комплекс мероприятий, направленных на обеспечение информационной безопасности.
2. К какой группе мер по защите информации относится шифрование информации?
 - а) организационным;
 - б) техническим;
 - в) аппаратным;

г) программным.

3. Укажите принципы создания комплексной системы защиты информации:

а) прозрачности;

б) модульности;

в) рациональности;

г) доступности.

4. Внешние техногенные угрозы информационной безопасности обусловлены:

а) средствами связи и помехами от них;

б) близко расположенными опасными производствами;

в) некачественными программными средствами;

г) взаимодействием технических средств.

5. К какой группе угроз информационной безопасности относятся ошибки программного обеспечения?

а) стихийные;

б) техногенные;

в) антропогенные;

г) антропоцентрические.

6. Текст задания на соответствие:

Расположите в правильном порядке указанные процессы

1 Аутентификация

а) Первый этап

2 Авторизация

б) Второй этап

3 Идентификация

в) Третий этап

4 Регистрация

г) Четвертый этап

7. Текст задания на соответствие:

1 Техногенный фактор

а) Компьютерный вирус

2 Стихийный фактор

б) Взлом системы

3 Антропогенный фактор

в) Землетрясение

г) Аппаратный сбой системы

Ключ к тесту:

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

Код компетенции	УК-1
Формулировка компетенции	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
Индикатор достижения компетенции	ИУК 1.1 Демонстрирует знание особенностей системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение ИУК 1.3 Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений

Время выполнения заданий: не более 30 минут

1. Основные цели организационных мер защиты информации:

- а) обеспечение правильности функционирования механизмов защиты;
- б) предоставление бесперебойного доступа к необходимой информации авторизованным сотрудникам;
- в) регламентация автоматизированной обработки информации;
- г) шифрование информации.

2. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода:

- а) макровирус;
- б) троянский конь;
- в) червь;
- г) файловый вирус.

3. Самым слабым элементом в помещении с точки зрения звукоизоляции являются:

- а) двери, стены, система заземления;
- б) двери, пол, потолок;
- в) двери, окна;
- г) окна, система заземления, пол.

4. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?

- а) организационное;
- б) организационно-техническое;
- в) техническо-организационное;
- г) техническое.

5. Какие пункты относятся к активным методам защиты речевой информации?

- а) создание маскирующих акустических и вибрационных помех;
- б) выявление факта несанкционированного подключения к линии;
- в) создание прицельных электромагнитных помех акустическим закладным устройствам;
- г) выявление излучений акустических закладных устройств.

Практическое задание

Подготовить текстовый документ, а также табличный документ таким образом, чтобы ограничить их чтение паролем, а также защиту от редактирования определенных областей документов по другому паролю (в случае с табличным документом ограничить доступ к одному листу и области на другом листе, а в случае с текстовым документом – обеспечить возможность добавления комментариев к документу без возможности менять само содержимое).

Ключ к тесту:

Номер вопроса	1	2	3	4	5
Номер правильного ответа	б	в	в	г	в

Ключ к практическому заданию:

Задание выполняется через функционал ПО для редактирования текстовых и табличных документов. При сохранении документов в дополнительных параметрах есть возможность установки парольной защиты на их чтение. В таком случае при попытке открытия файла,

потребуется ввод пароля. Также во вкладке «Рецензирование» можно настроить возможность защиты части документов по соответствующим функциональным кнопкам «Ограничить редактирование», «Защита листа» и прочее.

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.