

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

«21» апреля 2025 г. протокол № 9  
Приказ № 45 от 21 апреля 2025 г.

Ректор Я.А. Чиговская-Назарова

**АДАПТИРОВАННАЯ РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
(для лиц с нарушениями функций опорно-двигательного аппарата)**

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Уровень основной профессиональной образовательной программы	Бакалавриат
Направление подготовки	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Информатика и вычислительная техника
Форма обучения	Очная
Семестр(ы)	4

Глазов 2025

# 1. Цель и задачи изучения дисциплины

## 1.1. Цель и задачи изучения дисциплины

Целью освоения учебной дисциплины является формирование способности обеспечивать информационную безопасность на уровне баз данных, применять современные информационные технологии, преимущественно отечественные, а так же и технической документации с учетом всех мер информационной безопасности.

Задачи изучения дисциплины:

- изучить основные инструменты обеспечения безопасности данных и их возможности
- изучить основные угрозы безопасности данных, в том числе на уровне баз данных
- работы с инструментальными средствами, поддерживающими основные стандарты, нормы и правила разработки технической документации программных продуктов и программных комплексов;
- изучить основные методики подготовки технической документации программных продуктов;
- получить практический опыт выявления угрозы безопасности данных, в том числе на уровне баз данных
- получить практический опыт выбора основных средств поддержки информационной безопасности, в том числе на уровне баз данных

Программа адаптирована для лиц с нарушениями опорно-двигательного аппарата (ОДА) с учетом их психофизического развития, индивидуальных возможностей и необходимых специальных условий обучения.

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

Код компетенции	ПК-4
Формулировка компетенции	Способен обеспечивать информационную безопасность на уровне баз данных
Индикатор достижения компетенции	ИПК 4.1 Знает: инструменты обеспечения безопасности данных и их возможности ИПК 4.2 Умеет: выявлять угрозы безопасности данных, в том числе на уровне баз данных ИПК 4.3 Владеет: способностями выбора основных средств поддержки информационной безопасности, в том числе на уровне баз данных

## 1.3. Воспитательная работа

Направление воспитательной работы	Типы задач	Формы работы
формирование у обучающихся осознания социальной значимости своей будущей профессии, мотивации к осуществлению профессиональной	производственно-технологический	включение в социокультурную среду путем формирования у студентов практических умений и навыков в рамках профессиональной деятельности

деятельности		
научно-исследовательская работа обучающихся	производственно-технологический	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. Методология курса данной дисциплины опирается на системную согласованность с сопутствующими дисциплинами, а именно «Администрирование операционных систем», «Теория вычислительных процессов и структур».

#### 1.5. Особенности реализации дисциплины

Дисциплина реализуется на русском языке.

Для лиц с нарушениями функций ОДА используется электронное обучение, дистанционные технологии. Для поддержки курса используется сайт: <http://moodle.ggpi.org>.

### 2. Объем дисциплины

Вид учебной работы по семестрам	Всего, зачетных единиц	Академ. часы	Из них в форме практической подготовки
Общая трудоемкость дисциплины	2	72	
<b>СЕМЕСТР 4</b>			
Контактная работа с преподавателем:			
Аудиторные занятия (всего)		36	
Занятия лекционного типа		10	
Лабораторные работы		-	
Занятия семинарского типа		-	
Практические занятия		20	
КСР		6	
Самостоятельная работа обучающихся		36	
Вид промежуточной аттестации: Зачет		0	

### 3. Содержание дисциплины

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

	Всего	ауд.	Лекции	Практ.	Семинар	КСР	СРС
Роль и место безопасности информации. Стандарты и спецификации в области информационной безопасности. Угрозы безопасности информации. Защита информации в ЭВМ.	11	7	2	4			4
Способы хранения конфиденциальной информации. Административные методы	9	3	2			1	6

защиты информации. Аудит действий пользователя в ИС.							
Программно-математические средства защиты информации.	6	2	1			1	4
Обеспечение высокой доступности сервисов информационной безопасности. Несанкционированный доступ к информации, программные средства защиты информации от несанкционированного доступа.	8	4	1	2		1	4
Криптография.	13	9	2	6		1	4
Вредоносное ПО. Антивирусные программы.	9,5	3,5	0,5	4		1	6
Защита от утечки информации по техническим каналам.	8	4	1	2		1	4
Организационно- правовое обеспечение информационной безопасности.	7,5	3,5	0,5	2			4
<b>Итого – по дисциплине</b>	<b>72</b>	<b>36</b>	<b>10</b>	<b>20</b>	<b>-</b>	<b>6</b>	<b>36</b>

### 3.2. Занятия лекционного типа

Для лиц с нарушениями функций ОДА лекция сопровождается текстом с увеличенным шрифтом или усиливающей звуковой аппаратурой.

Занятия, при возможности, проводятся в мультимедийной аудитории, где имеется возможность подкрепления основных положений лекционного материала необходимым иллюстративным материалом (письменная презентация ключевых вопросов, являющихся темой обсуждения во время беседы; использование необходимых электронных видеоматериалов для иллюстрирования вопросов и контекста обсуждаемой проблемы, и т.п.). Есть возможность предоставлять необходимый учебный материал электронно для последующей самостоятельной работы с ним.

При объяснении материала мысли излагаются четко и лаконично (в простые предложения), информация подается в виде небольших логически и по смыслу законченных фрагментов.

#### СЕМЕСТР 4

##### Лекция 1.

Тема: Роль и место безопасности информации

Краткая аннотация к лекции.

Информация, основные свойства и характеристики безопасности ее применения. Эволюция подходов к обеспечению безопасности информации. Проблемы обеспечения безопасности информации. Роль и место безопасности информации. Обзор международных и национальных стандартов и спецификаций в области безопасности информации. От "Оранжевой книги" до ISO 15408. 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. Понятие угрозы безопасности. Классификация угроз безопасности информации по различным параметрам. Основные модели и принципы защиты

информации. Комплексный подход к построению системы безопасности и защите информации.

## Лекция 2.

Тема: Способы хранения конфиденциальной информации

Краткая аннотация к лекции.

Положение о конфиденциальной информации в электронном виде.

Классификация информации по уровню конфиденциальности. Метки документов.

Хранение информации. Способы хранения конфиденциальной

информации. Интеллектуальная собственность. Неструктурированная информация.

Локальные копии. Разграничение доступа к информации. Идентификация субъектов и

контроль за их действиями. Политика безопасности и программа безопасности.

Синхронизация программы безопасности с жизненным циклом систем. Достижение

информационной безопасности экономически оправданными мерами. Протоколирование в

компьютерной системе. Аудит. Цели аудита. Основные политики аудита. Объекты аудита.

Средства, методы и способы аудита. Обзор видов аудита в различных ОС и программных

продуктах.

## Лекция 3.

Тема: Программно-математические 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.

## Лекция 4.

Тема: Криптография

Краткая аннотация к лекции.

Криптография, криптология и криптоанализ. Классификация

криптоалгоритмов. Простейшие методы шифрования. Требования к алгоритму

шифрования. Симметричные криптоалгоритмы DES, ГОСТ. Криптографические системы

с открытым ключом.

## Лекция 5.

Тема: Проблема вирусного заражения программ. Защита от утечки информации по

техническим каналам. Организационно- правовое обеспечение информационной

безопасности

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. Методы защиты и профилактики. Основные классы

антивирусных программ. Основные методы антивирусной защиты. Меры профилактики.

Антивирусная защита. Антивирусная защита домашнего компьютера. Антивирусная

защита компьютерной сети. Антивирусная защита мобильных пользователей. Технические

средства защиты информации. 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.

### **3.3. Занятия семинарского типа**

Учебным планом не предусмотрены

### **3.4. Практические занятия**

Для лиц с нарушениями функций ОДА материал в электронном виде можно найти по адресу: <http://moodle.ggpi.org>.

Выполнение практических работ проводятся в микрогруппах или парами, в которых присутствует смешанный состав обучающихся: в паре – один обычный обучающийся и один обучающийся с двигательным нарушением; микрогруппа включает одного обучающегося с двигательным нарушением и несколько обычных обучающихся.

В ходе практического занятия используются следующие методы:

- опора на определенные и точные понятия;
- использование для иллюстрации конкретных примеров;
- применение вопросов для мониторинга понимания;
- разделение изучаемого материала на небольшие логические блоки;
- увеличение доли конкретного материала и соблюдение принципа от простого к сложному при объяснении материала.

## **СЕМЕСТР 4**

### **Практическое занятие 1.**

Тема: Изучение защиты документов и паролей доступа к системе

Перечень заданий:

Введение в понятие информационной безопасности. Основные составляющие информационной безопасности. Важность проблемы информационной безопасности. Законодательный уровень информационной безопасности. Одноразовые пароли, сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом в Java-среде. Правила разграничения доступа.

### **Практическое занятие 2.**

Тема: Законодательный уровень информационной безопасности

Перечень заданий:

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.

### **Практическое занятие 3.**

Тема: Стандарты и спецификации в области информационной безопасности

Перечень заданий:

Основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем, рекомендации X.800, администрирование средств безопасности

### **Практическое занятие 4.**

Тема: Криптография – как один из способов защиты информации

Перечень заданий:

Изучение стеганографического скрывания информации. Изучение криптографического зашифрования информации. Шифрование текста гаммированием. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.

Практическое занятие 5.

Тема: Криптография – как один из способов защиты информации

Перечень заданий:

Изучение генераторов псевдослучайных последовательностей. Шифрование текста с использованием бесконечной гаммы.

Практическое занятие 6.

Тема: Криптография – как один из способов защиты информации

Перечень заданий:

Шифрование текста методом маршрутов. Шифрование текста методом таблиц Вижинера.

Практическое занятие 7.

Тема: Изучение и анализ антивирусных программ и программных пакетов. Методы профилактики вирусного заражения

Перечень заданий:

Разработка практических рекомендаций по обеспечению безопасности информационных систем. Основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем, рекомендации X.800, администрирование средств безопасности. Разработка архитектуры модели безопасности информационных систем и сетей. Синхронизация программы безопасности с жизненным циклом систем.

Практическое занятие 8.

Тема: системы видеонаблюдения на основе Web – камер

Перечень заданий:

Разработка архитектуры модели безопасности информационных систем и сетей. Синхронизация программы безопасности с жизненным циклом систем. Подготовительные этапы управления рисками, основные этапы управления рисками, создания карты информационной системы организации.

Практическое занятие 9.

Тема: Изучение работы межсетевых экранов и программ защиты документов от фальсификации.

Перечень заданий:

Экранирование. Понятие конфиденциальности. Архитектурные аспекты. Анализ защищенности. Управление персоналом, физическая защита, планирование восстановительных работ. Туннелирование, управление, многоуровневая архитектура менеджер/агент, контроль производительности.

Практическое занятие 10.

Тема: Сервисы безопасности

Перечень заданий:

Сервисы безопасности, анализ защищенности, обеспечение отказоустойчивости, обеспечение безопасного восстановления

### **3.5. Лабораторные работы**

Учебным планом не предусмотрены

### 3.6. Контроль самостоятельной работы

Для лиц с нарушениями функций ОДА материал в электронном виде можно найти по адресу: <http://moodle.ggpi.org>.

Для лиц с нарушениями функций опорно-двигательного аппарата учебно-методическое обеспечение для контроля самостоятельной работы обучающихся по дисциплине предьявляется (по выбору обучающегося): устно, письменно на бумаге или на компьютере, в форме тестирования, электронных тренажеров и т.п.

Конкретные формы и виды самостоятельной работы обучающихся с нарушениями функций ОДА устанавливаются преподавателем с учетом индивидуальных психофизических особенностей. При необходимости обучающимся предоставляется дополнительное время для консультаций и выполнения заданий.

Самостоятельная работа включает следующие виды деятельности: работа с книгой и другими источниками информации, планы-конспекты; реферативные (воспроизводящие), реконструктивно-вариативные, эвристические, творческие самостоятельные работы; проектные работы; дистанционные технологии.

Уделяется внимание индивидуальной работе. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету становятся важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся с нарушениями функций ОДА.

#### СЕМЕСТР 4

##### Контроль самостоятельной работы 1.

Тема: Основное назначение защиты информации. Гармонизация стандартов в области информационной безопасности. Классификация и примеры угроз безопасности информации

Перечень заданий:

Подготовка сообщения по теме. Привести примеры угроз безопасности информации для домашнего пользователя.

##### Контроль самостоятельной работы 2.

Тема: Организация и ведение электронной коммерции

Перечень заданий:

Подготовка реферата

##### Контроль самостоятельной работы 3.

Тема: Защита информации средствами ОС

Перечень заданий:

Обзор способов защиты информации средствами ОС. Обзор методов идентификации пользователя в ОС. Обзор средств и методов разграничения прав пользователей в клиентских ОС. Обзор средств и методов разграничения прав пользователей в серверных ОС. Обзор средств обнаружения несанкционированного доступа в ИС и наличия программно – аппаратных закладок.

### 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**

Формы текущего контроля, промежуточной аттестации и поститоговый контроль для лиц с нарушениями функций ОДА устанавливаются с учетом их психофизиологических особенностей. При необходимости все виды аттестации проходит в несколько этапов.

Текущий контроль результатов обучения осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, а также выполнения индивидуальных работ и домашних заданий, или в режиме тренировочного тестирования в целях получения информации о выполнении обучаемым требуемых действий в процессе учебной деятельности; правильности выполнения требуемых действий; соответствии формы действия данному этапу усвоения учебного материала; формировании действия с должной мерой обобщения, освоения и т.д.

Формы и сроки проведения промежуточного контроля определяются преподавателем с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Для лиц с нарушениями функций опорно-двигательного аппарата формами текущего контроля, промежуточной аттестации и поститогового контроля используются (в зависимости от индивидуальных особенностей и потребностей):

- устный ответ;
- письменный ответ;
- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

При проведении всех форм контроля учитываются психофизическое развитие и ограничения здоровья. Время выполнения заданий для лиц с нарушениями функций ОДА может быть увеличено, но не более чем на 30 минут.

Для лиц с нарушениями опорно-двигательного аппарата материалы ко всем видам аттестации предъявляться (в зависимости от индивидуальных особенностей и потребностей):

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

#### **Рекомендуемые формы контроля и оценки результатов обучения лиц с нарушением функций ОДА:**

- письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
- устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;
- с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические

работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.

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. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146405.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей
2. 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: 31.03.2025). — Режим доступа: для авторизир. пользователей
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87995.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей

### **5.2. Дополнительная литература**

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 210 с. — ISBN 978-5-4497-2408-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/133946.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей
2. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/10677.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей
3. Кришталюк, А. Н. Правовые аспекты системы безопасности : курс лекций / А. Н. Кришталюк. — Орел : Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. — 204 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/33433.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей
4. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/33857.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей

5. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/77320.html> (дата обращения: 31.03.2025). — Режим доступа: для авторизир. пользователей

1. Обучающиеся с нарушениями функций опорно-двигательного аппарата обеспечены печатными и электронными ресурсами в форме, адаптированной к ограниченным возможностям здоровья и восприятия информации:

- в печатной форме
- в форме электронного документа
- в форме аудиофайла

2. Каждому обучающемуся с нарушениями функций ОДА обеспечен доступ к библиотечным ресурсам и сети Интернет и предоставлен не менее чем одним учебным, методическим и (или) электронным изданием в форме, адаптированной к ограничениям здоровья.

3. Для обучения лиц с нарушениями функций ОДА комплектация библиотечного фонда осуществляется электронными изданиями основной и дополнительной литературы по дисциплинам.

## **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 «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](https://eios.ggpi.org)).

Методические рекомендации для работы с инвалидами и лицами с ОВЗ размещены в ЭИОС университета ([eios.ggpi.org](https://eios.ggpi.org)).

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

Программное обеспечение: Microsoft Windows 10, Microsoft Office 2010, Яндекс.Браузер.

Учебный корпус 222, аудитории(я) 235.

Полный перечень материально-технической базы и программного обеспечения размещены в ЭИОС института ([eios.ggpi.org](https://eios.ggpi.org)).

Образовательная среда организации, организация рабочих мест обучающихся, технические и программные средства общего и специального назначения соответствуют Методическим рекомендациям по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса (утв. Министерством образования и науки РФ 8 апреля 2014 г. N АК-44/05вн), а именно:

- наличие компьютерной техники, адаптированной для инвалидов со специальным программным обеспечением, альтернативных устройств ввода информации и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата;

- для студентов с нарушениями функций опорно-двигательного аппарата используются альтернативные устройств ввода информации (при необходимости);

- используются специальные возможности операционной системы Windows, такие как экранная клавиатура, с помощью которой можно вводить текст, настройка действий Windows при вводе с помощью клавиатуры или мыши.

Для студентов с нарушениями функций опорно-двигательного аппарата предусмотрено расположение рабочих мест в первых рядах у окна и в среднем ряду.

### 9. Рейтинг-план оценки успеваемости студентов

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					
10	20	-	6	1. Контроль посещаемости лекций 2. Контроль посещаемости практических занятий 3. Практические работы  <b>Контрольные мероприятия:</b> 1. Контрольные работы (№ 1, № 2) 2. Домашняя контрольная работа 3. Тестирование по разделам курса (3 разделов) 4. Итоговая контрольная работа  <b>Компенсационные мероприятия:</b> 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)	10 20 60  30 7 140 20	        20 15 8 15	- 2 балла за отсутствии на занятии  - 5 баллов за несвоевременную сдачу отчетных работ (домашних, индивидуальных)	допуск к зачету- (50%)  «автомат» - (70 %)
				Итого	287 (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 поститогового 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, поститогового) 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	ПК-4
Формулировка компетенции	Способен обеспечивать информационную безопасность на уровне баз данных
Индикатор достижения компетенции	ИПК 4.1 Знает: инструменты обеспечения безопасности данных и их возможности ИПК 4.2 Умеет: выявлять угрозы безопасности данных, в том числе на уровне баз данных ИПК 4.3 Владеет: способностями выбора основных средств поддержки информационной безопасности, в том числе на уровне баз данных

### 3. Содержание оценочных средств текущего контроля и критерии их оценивания

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

3.2. Формы текущего контроля и критерии их оценивания.

#### Форма контроля 1 - Типовые тестовые задания

Типовой тест 1: Итоговый тест

Проверяемые компетенции и индикаторы достижения компетенций: ПК-4, ИПК 4.1, ИПК 4.2, ИПК 4.3

Время выполнения заданий: 25 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 Internetнеобходимоустанавливать разные межсетевые экраны;
- б) каждую точку подключения корпоративной сети к Internetнеобходимозащищать 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: ПК-4, ИПК 4.1, ИПК 4.2, ИПК 4.3

Время выполнения заданий: 45 минут

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

В основе оценивания лежат критерии порогового и повышенного уровня характеристик компетенций или их составляющих частей, формируемых на учебных занятиях по дисциплине «Архитектура компьютера».

**«Отлично» (5)**– 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» (г)** - 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» (в)** - 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» (б)** - 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**

#### **Задание**

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).

## **4. Содержание оценочных средств промежуточной аттестации и критерии их оценивания**

- 4.1. Промежуточная аттестация проводится в виде: зачета.
- 4.2. Содержание оценочного средства. Проверяемые компетенции и индикаторы достижения компетенций: ПК-4, ИПК 4.1, ИПК 4.2, ИПК 4.3

Примерные вопросы и задания к зачету

1. Понятие информационной безопасности. Основные составляющие.
2. Распространение объектно-ориентированного подхода на информационную безопасность.
3. Основные определения и критерии классификации угроз.
4. Законодательный уровень информационной безопасности.
5. Вредоносное программное обеспечение.
6. Закон "Об информации, информатизации и защите информации".
7. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
8. Наиболее распространенные угрозы.
9. Стандарты и спецификации в области информационной безопасности.
10. Административный уровень информационной безопасности.
11. Управление рисками.
12. Процедурный уровень информационной безопасности.
13. Основные программно-технические меры.
14. Идентификация и аутентификация, управление доступом.
15. Моделирование и аудит, шифрование, контроль целостности.
16. Экранирование, анализ защищенности.
17. Туннелирование и управление.

18. Понятие национальной безопасности.
19. Виды безопасности личности, общества и государства.
20. Роль информационной безопасности в обеспечении национальной безопасности государства.
21. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях.
22. Основные правовые и нормативные акты в области информационной безопасности.
23. Понятие класса, компонента.
24. Структурированное программирование, декомпозиции, структурный подход. Основным инструментом борьбы со сложностью в объектно-ориентированном подходе.
25. Понятие мобильных агентов, вирусов, "червей" статической и динамической целостностью.
26. Механизмы безопасности, классы безопасности, информационная безопасность распределенных систем.
27. Программирование для бизнеса
28. Важность проблемы.
29. Компьютерные технологии в бизнесе
30. Бизнес в программировании
31. Программа как товар
32. Оффшорное программирование. Достоинства и недостатки
33. Лицензионные программные продукты. Основные правила использования
34. Получение сертификата у полномочного представителя (CertificationAuthority). Сертификация 2 и 3 класса
35. Авторское право на ПО. Совокупность правомочий автора
36. Передача авторских прав по договорам. Виды договоров. Договора о передаче исключительных прав на ПО

#### 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 (-ий)	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	Не зачтено	менее 50

	предусмотренных рабочей программой учебной дисциплины.		
--	--	--	--

#### 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 или желает повысить оценку, то сдает зачет по вопросам.
2. Сбор, обработка и оценивание результатов промежуточной аттестации проводится преподавателем, ведущим дисциплину.
3. Предъявление результатов оценивания осуществляется: по окончании ответа студента и фиксируется в зачетной книжке и экзаменационной ведомости.
4. При наличии письменных ответов обучающихся, полученных в ходе экзаменационной сессии, материалы хранятся в течение месяца после завершения сессии на кафедрах.
5. Порядок выполнения и защиты курсовой работы регламентирован «Положением о курсовой работе ФГБОУ ВО «Глазовский государственный 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: ПК-4, ИПК 4.1, ИПК 4.2, ИПК 4.3

Код компетенции	ПК-4
Формулировка компетенции	Способен обеспечивать информационную безопасность на уровне баз данных
Индикатор достижения компетенции	ИПК 4.1. Знает: инструменты обеспечения безопасности данных и их возможности. ИПК 4.2. Умеет: выявлять угрозы безопасности данных, в том числе на уровне баз данных. ИПК 4.3. Владеет: способностями выбора основных средств поддержки информационной безопасности, в том числе на уровне баз данных.

Время выполнения заданий: 15 минут

**Задание 1.** (ИПК-4.1). 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,

**Задание 2.** (ИПК 4.2.). 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 к 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.

**Задание 3.** (ИПК 4.3.). 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 согласно плана, предложенного вами в задании 2.

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 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 обладателем 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 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.

Ключ к Заданию 3.

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.

#### 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)**

<b>Уровни освоения индикатора (ов) достижений компетенций</b>	<b>Основные признаки выделения уровня</b>	<b>Академическая оценка</b>	<b>% выполнения всех заданий</b>
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.