

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

Утверждена
на заседании ученого совета университета

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

Ректор Я.А. Чиговская-Назарова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень основной профессиональной образовательной программы	Бакалавриат
Направление подготовки	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль)	Образовательная робототехника и Технология
Форма обучения	Очная
Семестр(ы)	10

Глазов 2026

1. Цель и задачи изучения дисциплины

1.1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - формирование компетенций у обучающихся, связанных со способностью осваивать и использовать теоретические знания, практические умения и навыки в предметной области при решении профессиональных задач в рамках дисциплины «Информационная безопасность и защита информации».

Задачи изучения дисциплины:

- сформировать знания о структуре, составе и дидактических единицах предметной области информационной безопасности и защиты информации;
- сформировать умения осуществлять отбор учебного содержания в рамках информационной безопасности и защиты информации для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО;
- сформировать умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные в рамках дисциплины «Информационная безопасность и защита информации».

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 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

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	Педагогический, сопровождения, методический	Исследовательская деятельность студентов (выступление с докладом)

1.4. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к обязательной части учебного плана.

Для её успешного изучения необходимы знания, умения и навыки, приобретенные в результате освоения дисциплин «Программное обеспечение систем и сетей», «Теоретические основы информатики», «Информационные системы», «Веб-технологии»

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	2	72	
СЕМЕСТР 10			
Контактная работа с преподавателем:			
Аудиторные занятия (всего)		36	
Занятия лекционного типа		16	
Лабораторные работы		-	
Занятия семинарского типа		-	
Практические занятия		18	
КСР		2	
Самостоятельная работа обучающихся		36	

Вид промежуточной аттестации: Зачет		0	
-------------------------------------	--	---	--

3. Содержание дисциплины

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

Тема	Всего	ауд.	Лекции	Практ.	Семинар	КСР	СРС
Основные понятия «информационной безопасности»	12	6	2	4			6
Правовые основы информационной безопасности и защиты персональных данных	9	3	2			1	6
Программные средства защиты информации	9	3	2			1	6
Технические средства защиты и комплексное обеспечение информационной безопасности	16	10	6	4			6
Элементы криптографии	14	8	2	6			6
Вредоносное ПО	12	6	2	4			6
Итого – по дисциплине	72	36	16	18	-	2	36

3.2. Занятия лекционного типа

СЕМЕСТР 10

Лекция 1.

Тема: Основные понятия «информационной безопасности».

Краткая аннотация к лекции.

Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности. Информация, основные свойства и характеристики безопасности ее применения. Эволюция подходов к обеспечению безопасности информации. Проблемы обеспечения безопасности информации. Роль и место безопасности информации. 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: Правовые основы информационной безопасности и защиты персональных данных.

Краткая аннотация к лекции.

Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность. 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: Программные средства защиты информации.

Краткая аннотация к лекции.

Компьютерные вирусы и антивирусная защита.

Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля. 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: Технические средства защиты и комплексное обеспечение информационной безопасности.

Краткая аннотация к лекции.

Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. 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

Лекция 5.

Тема: Технические средства защиты и комплексное обеспечение информационной безопасности.

Краткая аннотация к лекции.

Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. 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. Основные методы антивирусной защиты. Меры профилактики.

Лекция 6.

Тема: Технические средства защиты и комплексное обеспечение информационной безопасности.

Краткая аннотация к лекции.

Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи. Виды проявлений вредоносного ПО. Методы защиты и профилактики. Основные классы антивирусных программ.

Лекция 7.

Тема: Элементы криптографии

Краткая аннотация к лекции.

Криптография, криптология и криптоанализ. Классификация криптоалгоритмов. Простейшие методы шифрования. Требования к алгоритму шифрования. Симметричный криптоалгоритмы DES, ГОСТ. Криптографические системы с открытым ключом. 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.

Лекция 8.

Тема: Вредоносное ПО

Краткая аннотация к лекции.

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

СЕМЕСТР 10

Практическое занятие 1.

Тема: Основные понятия «информационной безопасности»

Перечень заданий:

Изучение защиты документов и паролей доступа к системе. Введение в понятие информационной безопасности. Основные составляющие информационной безопасности. Важность проблемы информационной безопасности.

Практическое занятие 2.

Тема: Основные понятия «информационной безопасности»

Перечень заданий:

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 3.

Тема: Основные понятия «информационной безопасности»

Перечень заданий:

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.

Практическое занятие 4.

Тема: Технические средства защиты и комплексное обеспечение информационной безопасности.

Перечень заданий:

Стандарты и спецификации в области информационной безопасности. Основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем, рекомендации X.800, администрирование средств безопасности

Практическое занятие 5.

Тема: Элементы криптографии.

Перечень заданий:

Криптография – как один из способов защиты информации. Изучение стеганографического скрытия информации. Изучение криптографического закрытия информации. Шифрование текста гаммированием. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.

Практическое занятие 6.

Тема: Элементы криптографии.

Перечень заданий:

Криптография – как один из способов защиты информации. Изучение генераторов псевдослучайных последовательностей. Шифрование текста с использованием бесконечной гаммы.

Практическое занятие 7.

Тема: Элементы криптографии.

Перечень заданий:

Криптография – как один из способов защиты информации. Шифрование текста методом маршрутов. Шифрование текста методом таблиц Вижинера.

Практическое занятие 8.

Тема: Вредоносное ПО.

Перечень заданий:

Изучение и анализ антивирусных программ и программных пакетов. Методы профилактики вирусного заражения. 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 9.

Тема: Вредоносное ПО.

Перечень заданий:

Системы видеонаблюдения на основе Web – камер. 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.

3.5. Лабораторные работы

Учебным планом не предусмотрены

3.6. Контроль самостоятельной работы

СЕМЕСТР 10

Контроль самостоятельной работы 1.

Тема: Технические средства защиты и комплексное обеспечение информационной безопасности. Элементы криптографии.

Перечень заданий:

Организация и ведение электронной коммерции. Подготовка реферата

3.7. Самостоятельная работа студентов

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

4. Фонд оценочных средств

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

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

5.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544290> (дата обращения: 13.06.2026).
2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544029> (дата обращения: 13.06.2026).
3. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 252 с. — (Высшее образование). — ISBN 978-5-534-18945-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/557730> (дата обращения: 11.05.2026).

5.2. Дополнительная литература

1. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2022. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490026> (дата обращения: 13.06.2026).
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). —

- ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536225> (дата обращения: 13.06.2026).
3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2023. — 416 с. — ISBN 978-5-97060-982-8. — Текст : электронный // ЭБС «Лань» [сайт]. — URL: <https://e.lanbook.com/book/123456> (дата обращения: 11.05.2026).
 4. Криптографические методы защиты информации : учебное пособие для вузов / под ред. В. Н. Носова. — Москва : Издательство Юрайт, 2023. — 240 с. — (Высшее образование). — ISBN 978-5-534-14567-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/521100> (дата обращения: 11.05.2026).
 5. Защита персональных данных в информационных системах : учебно-методическое пособие / С. В. Назаров. — Москва : Горячая линия – Телеком, 2022. — 180 с. — ISBN 978-5-9912-1089-4. — Текст : электронный // ЭБС IPRBooks [сайт]. — URL: <https://www.iprbookshop.ru/12345.html> (дата обращения: 11.05.2026).

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) 222, 237.

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

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	18	-	2	1. Контроль посещаемости лекций 2. Практические работы Контрольные мероприятия: 3. Тестирование по разделам курса (3 разделов) 4. Итоговая контрольная работа Компенсационные мероприятия: 1. Сообщение или интерактивная презентация 2. Индивидуальная контрольная работа по пропущенным разделам	16 48 5 5 2 2	+ 1 балл за дополнения; + 3 балла за подготовку дополнительного дидактического материала	- 2 балла за отсутствии на занятии - 3 балла за невыполнение в установленные сроки	Зачет с оценкой Допуск к зачету с оценкой – 50% «автомат» при зачете с оценкой – 90%
				Итого	74 (без компенсации)			

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

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

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

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

1.3. Результаты оценивания текущего контроля учитываются в рейтинге.

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

Код компетенции	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

Типовой тест 1: Итоговый тест

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

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) технико-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) заплата 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-1, ИУК-1.1, ИУК-1.3, УК-2, УК-4, ИУК-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 (10 сем.).
- 4.2. Содержание оценочного средства. Проверяемые компетенции и индикаторы достижения компетенций: УК-1, ИУК 1.1, ИУК 1.3, УК-2, ИУК 2.1, ИУК 2.2, УК-4, ИУК 4.3, ОПК-9, ИОПК 9.1, ИОПК 9.2

Примерные вопросы и задания к зачету

1. Роль информации в современном мире. Понятие о защищаемой информации. Понятие информационной безопасности. Основные составляющие.
2. Теория информационной безопасности. Основные направления. Распространение объектно-ориентированного подхода на информационную безопасность.
3. Обеспечение ИБ и направления защиты. Основные определения и критерии классификации угроз.
4. Требования к системе и политике ИБ. Закон "Об информации, информатизации и защите информации".
5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
6. Доктрина информационной безопасности РФ. Роль информационной безопасности в обеспечении национальной безопасности государства.
7. Защита государственной тайны в РФ. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
8. Защита коммерческой тайны в РФ.
9. Защита персональных данных в РФ. Виды безопасности личности, общества и государства.
10. Защита служебной и профессиональной тайны в РФ. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях.
11. Процедуры сертификации и аттестации в РФ.
12. Понятие о защищаемой информации. Свойства информации.
13. Угрозы информации. Классификация угроз. Наиболее распространенные угрозы.
14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.
15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз. Примеры
16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.
17. Источники угроз. Классификация источников угроз.
18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.
19. Понятие электронной подписи.
20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия. Управление рисками.

21. Организация внутри объектового режима предприятия. Организация охраны. Примеры
22. Криптографические меры обеспечения информационной безопасности. Классификация криптографических алгоритмов. Примеры
23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.
24. Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения.
25. Особенности защиты беспроводных и мобильных подключений. Примеры
26. Симметричное и ассиметричное шифрование. Примеры
27. Принципы симметричного шифрования. Моделирование и аудит, шифрование, контроль целостности.
28. Односторонние функции и их применение.
29. Простейшие методы ассиметричного шифрования.
30. Метод RSA. Понятие национальной безопасности. Примеры
31. Электронная подпись и ее применение. Примеры
32. Понятие мобильные агенты, вирусов, "червей" статической и динамической целостностью.
33. Механизмы безопасности, классы безопасности, информационная безопасность распределенных систем.
34. Программирование для бизнеса. Важность проблемы. Компьютерные технологии в бизнесе. Примеры
35. Авторское право на ПО. Совокупность правомочий автора Передача авторских прав по договорам. Виды договоров. Договора о передаче исключительных прав на ПО. Примеры

4.3. Критерии оценивания

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

Уровни освоения индикаторов в достижения компетенций	Содержательно е описание уровня	Основные признаки выделения уровня	Академическая оценка	% освоения (рейтинговая оценка)
Повышенный (высокий)	Творческая деятельность	Включает нижестоящий уровень. Умение самостоятельно принимать решение, решать проблему/задачу теоретического или прикладного характера на основе изученных методов, приемов, технологий.	Отлично	90-100
Базовый	Продуктивная деятельность	Включает нижестоящий уровень. Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими	Хорошо	70-89

		теоретические положения или обосновывать практику применения		
Удовлетворительный	Репродуктивная деятельность	Изложение в пределах задач курса теоретического и практического материала	Удовлетворительно	50-69
Недостаточный	Отсутствие признаков удовлетворительного уровня		Неудовлетворительно	менее 50

Шкала оценивания для зачета:

4.4. Методические указания по проведению процедуры промежуточной аттестации

1. Сроки проведения процедуры оценивания: по расписанию экзаменов (зачета - на последнем занятии по предмету). Если обучающийся по результатам рейтинговой системы не набирает нужное количество баллов или желает повысить оценку, то сдает экзамен/зачет согласно требованиям.
2. Сбор, обработка и оценивание результатов промежуточной аттестации проводится преподавателем, ведущим дисциплину.
3. Предъявление результатов оценивания осуществляется: по окончании ответа студента и фиксируется в зачетной книжке и экзаменационной ведомости.
4. При наличии письменных ответов обучающихся, полученных в ходе экзаменационной сессии, материалы хранятся в течение месяца после завершения сессии на кафедрах.
5. Порядок выполнения и защиты курсовой работы регламентирован «Положением о курсовой работе ФГБОУ ВО «Глазовский государственный инженерно-педагогический университет 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: УК-1, ИУК 1.1, ИУК 1.3, УК-2, ИУК 2.1, ИУК 2.2, УК-4, ИУК 4.3, ОПК-9, ИОПК 9.1, ИОПК 9.2

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.

Время выполнения заданий: 30 минут

Практическое задание. 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 практическому заданию.

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.
- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в АС.

Задания для проверки компетенции и индикаторов достижения компетенции: УК-1: УК-2, УК-4., ОПК-9.

Время выполнения заданий: 30 минут

Практическое задание. 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,

Ключ к практическому заданию.

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

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 и индикаторов достижения компетенции

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	Удовлетвор	50-69

ый	теоретического и практического контролируемого материала.	ительно	
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.