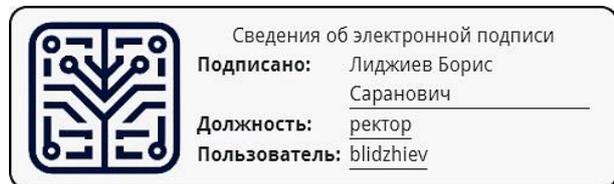


**Автономная некоммерческая организация высшего образования  
«Информационно-технологический университет»  
(АНО ВО ИТУ)**

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ Лиджиев Б.С.



Утверждено протоколом  
заседания кафедры  
математики, информатики и  
естественнонаучных дисциплин  
№ 6 от 21.01.2026 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.О.03 ЗАЩИТА ИНФОРМАЦИИ В ИС**

**Для направления подготовки:**  
09.04.01 Информатика и вычислительная техника  
(уровень магистратуры)

**Направленность (профиль):** Информационные системы

**Типы задач профессиональной деятельности:**  
производственно-технологический  
научно-исследовательский

**Форма обучения:**  
очная

г. Элиста, 2026

Разработчик: Этеев Алексей Петрович, старший преподаватель

Рабочая программа разработана в соответствии с требованиями ФГОС ВО Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом Минобрнауки России от 19 сентября 2017 года № 918, с изменениями и дополнениями от 26 ноября 2020 г., 08 февраля 2021 г.

**СОГЛАСОВАНО:**

Заведующий кафедрой математики, информатики  
и естественнонаучных дисциплин АНО ВО ИТУ  
канд. пед. наук Горяев В.М.

Протокол заседания кафедры № 6 от 21.01.2026 г.



## Содержание

1. Цели и задачи дисциплины	4
2. Место дисциплины в структуре программы	4
3. Планируемые результаты обучения по дисциплине	4
4. Объем дисциплины и виды учебной работы	6
5. Содержание дисциплины	6
5.1 Структура дисциплины	6
5.2. Содержание разделов и тем	6
6. Методические указания по освоению дисциплины	9
6.1 Учебно-методическое обеспечение дисциплины	9
6.2 Методические материалы обучающимся по дисциплине, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности	10
6.3 Особенности реализации дисциплины в отношении лиц из числа инвалидов и лиц с ограниченными возможностями здоровья	10
6.4 Методические рекомендации по самостоятельной работе обучающихся	11
7. Фонд оценочных материалов для проведения текущей и промежуточной аттестации по дисциплине	13
7.1. Система оценивания результатов текущей и промежуточной аттестации и критерии выставления оценок, описание шкал оценивания	13
7.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы	14
8. Учебно-методическое и информационное обеспечение дисциплины	20
8.1. Рекомендуемая литература	20
8.2. Ресурсы информационно-телекоммуникационной сети Интернет	20
9. Материально-техническое обеспечение дисциплины	20
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая программное обеспечение, современные профессиональные базы данных и информационные справочные системы	21

## 1. Цели и задачи дисциплины

**Цель дисциплины** - усвоение общей методологии, современных проблем и широкого круга специальных вопросов информационной безопасности информационных систем (ИС).

### **Задачи дисциплины:**

- раскрыть структуру и содержание круга современных проблем информационной безопасности ИС;
- охарактеризовать основные направления, средства и методы решения проблем обеспечения безопасности ИС;
- сформировать представления о научных основах решения проблем безопасности ИС;
- обеспечить формирование профессиональных навыков в области решения проблем безопасности ИС;
- выработка научного подхода к практике применения теоретических знаний в области защиты информации;
- повышение мотивации к процессу изучения научной дисциплины и научной деятельности.

## 2. Место дисциплины в структуре программы

Дисциплины «Защита информации в ИС» относится к обязательной части Блока 1.

## 3. Планируемые результаты обучения по дисциплине

В результате изучения дисциплины обучающийся должен освоить следующие компетенции:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач;

ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем

**Результаты освоения дисциплины, установленные индикаторы достижения компетенций**

Наименование компетенции	Индикаторы достижения компетенции	Показатели (планируемые) результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает: принципы сбора, отбора и обобщения информации; основы теории систем и системного анализа	<b>Знать:</b> <ul style="list-style-type: none"><li>• основные технологии обеспечения безопасности ИС и соответствующие методы и средства;</li></ul>
	УК-1.2. Умеет: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	<b>Уметь:</b> <ul style="list-style-type: none"><li>• ставить и решать типовые задачи в области разработки и применения защищенных ИС;</li></ul>
	УК-1.3. Владеет: информационными источниками;	<b>Владеть:</b> <ul style="list-style-type: none"><li>• методами обработки результатов;</li></ul>

Наименование компетенции	Индикаторы достижения компетенции	Показатели (планируемые) результаты обучения
	навыками научного поиска, подготовки научных текстов	
ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1. Знает: современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы, применяемые для решения профессиональных задач	<p><b><u>Знать:</u></b></p> <ul style="list-style-type: none"> <li>• научные основы обеспечения безопасности ИС;</li> <li>• сущность и содержание типовых задач в области разработки и применения защищенных ИС;</li> </ul>
	ОПК-2.2. Умеет: обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред и программно-технических платформ; разрабатывать оригинальные алгоритмы и программные средства для решения профессиональных задач	<p><b><u>Уметь:</u></b></p> <ul style="list-style-type: none"> <li>• подбирать и использовать адекватные формы, методы и средства разработки и практического применения защищенных ИС;</li> </ul>
	ОПК-2.3. Владеет: навыками разработки оригинальных алгоритмов и программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий для решения профессиональных задач	<p><b><u>Владеть:</u></b></p> <ul style="list-style-type: none"> <li>• техническими средствами обеспечения безопасности ИС.</li> </ul>
ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.1. Знает: современное программное и аппаратное обеспечение информационных и автоматизированных систем	<p><b><u>Знать:</u></b></p> <ul style="list-style-type: none"> <li>• основные направления и перспективы развития технологий защиты информации в ИС;</li> </ul>
	ОПК-5.2. Умеет: модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач	<p><b><u>Уметь:</u></b></p> <ul style="list-style-type: none"> <li>• оценивать эффективность применения ИС;</li> </ul>
	ОПК-5.3. Владеет: навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	<p><b><u>Владеть:</u></b></p> <ul style="list-style-type: none"> <li>• программными средствами обеспечения безопасности ИС.</li> </ul>

#### 4. Объем дисциплины и виды учебной работы

Учебным планом предусматриваются следующие виды работы по дисциплине:

Вид учебной работы	Всего число часов и (или) зачетных единиц
	Очная
<b>Аудиторные занятия</b>	40
<i>в том числе:</i>	
Лекции	8
Практические занятия	32
Лабораторные работы	
<b>Самостоятельная работа</b>	140
<i>в том числе:</i>	
часы на выполнение КР / КП	36
<b>Промежуточная аттестация:</b>	
Вид	Экзамен – 1 сем. Защита КР
Трудоемкость (час.)	36
<b>Общая трудоемкость з.е. / час.</b>	<b>6 з.е. / 216 час.</b>

#### 5. Содержание дисциплины

##### 5.1 Структура дисциплины

Номер темы дисциплины	Количество часов			
	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)
Раздел 1	1	4	-	23
Раздел 2	1	4	-	23
Раздел 3	1	4	-	23
Раздел 4	1	4	-	23
Раздел 5	2	8	-	24
Раздел 6	2	8	-	24
Итого за семестр (часов)	8	32		140
Форма контроля	Экзамен		<b>36</b>	
<b>Всего по дисциплине</b>	<b>216 час. / 6 з.е.</b>			

##### 5.2. Содержание разделов и тем

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в информационную безопасность ИС	<b>Информация как объект защиты</b> Свойства, виды и формы представления информации. Информация и информационные ресурсы. Информация как объект

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		<p>права собственности. Информация как коммерческая тайна. Информация как рыночный продукт. Автоматизированные системы (АС) как объекты защиты информации. ИС как объекты обработки и защиты информации</p> <p>Классическая архитектура «клиент-сервер». Архитектура «клиент-сервер», основанная на Web-технологии. Технологии распределенной обработки информации. Доступ к базам данных. Управление информацией о ресурсах и пользователях ИС. Условия и режимы эксплуатации ИС.</p> <p>Основные понятия и анализ угроз информационной безопасности</p> <p>Основные понятия защиты информации и информационной безопасности (ИБ). Обзор и классификация угроз информации, обрабатываемой в ИС. Обзор способов реализации угроз безопасности информации. Несанкционированный доступ (НСД) к информации в ИС.</p>
2	Обеспечение безопасности информации в ИС.	<p><b>Анализ существующих подходов к обеспечению безопасности информации</b></p> <p>Законодательный, административный и процедурный уровни информационной безопасности. Основные понятия политики безопасности. Структура политики безопасности организации. Программно-технический уровень информационной безопасности. Сервисы безопасности.</p> <p>Особенности защиты информации в ИС</p> <p>Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС. Защита информации на уровне подсистемы управления ИС. Защита информации в каналах связи. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Особенности защиты информации в базах данных.</p> <p><b>Общие теоретические подходы к защите информации</b></p> <p>Математические модели управления доступом к информации. Политика безопасности и модели доступа. Способы анализа моделей доступа. Модели нарушителей ИБ. Основы построения защиты информации. Модель элементарной защиты. Модель многозвенной защиты. Многоуровневая защита.</p> <p><b>Международные и отечественные стандарты в сфере защиты информации</b></p> <p>Роль стандартов ИБ. Международные стандарты ИБ. Стандарты для беспроводных сетей. Стандарты ИБ в Интернет. Отечественные стандарты в сфере защиты информации.</p> <p><b>Сертификация и аттестация в области защиты информации</b></p> <p>Назначение и общая характеристика. Проведение сертификационных испытаний. Аттестация объектов информатизации. Сертификация на региональном и международном уровнях.</p> <p><b>Основы правового обеспечения защиты информации</b></p> <p>Международный опыт правового обеспечения ИБ. Государственная система правового обеспечения ИБ. Содержание основных законов РФ в области ИБ. Понятие и виды юридической</p>

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		ответственности за нарушение правовых норм по защите информации.
3	Методы и средства технической защиты информации в ИС	<p><b>Виды и методы технической защиты информации</b> Пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры.</p> <p><b>Технические каналы утечки информации</b> Общая характеристика технических каналов утечки информации и их классификация. Каналы утечки речевой информации. Технические средства и методы получения информации по этим каналам. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок. Технические средства и методы получения информации с использованием этих каналов.</p> <p><b>Методы и средства защиты информации от утечки по техническим каналам</b> Основные методы, используемые при создании систем защиты информации. Заземление технических средств передачи информации. Использование сетевых фильтров. Экранирование помещений. Методы защиты от утечек по акустическим каналам. Защита средств связи и телекоммуникаций.</p>
4	Технологии защиты данных в ИС.	<p><b>Современные методы защиты информации в ИС</b> Ограничение и разграничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Идентификация и установление подлинности объекта (субъекта). Криптографическое преобразование информации. Методы защиты информации от компьютерных вирусов.</p> <p><b>Криптографические средства защиты информации</b> Основные принципы и классификация методов криптографического преобразования информации. Обзор методов шифрования. Выбор метода преобразования информации. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Электронная цифровая подпись (ЭЦП) и функции хэширования. Процедуры выработки ЭЦП. Защита электронного документооборота с использованием ЭЦП.</p> <p><b>Технологии аутентификации</b> Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие одноразовые и многоразовые пароли и PIN-коды. Аутентификация, основанная на симметричных и асимметричных алгоритмах. Биометрическая аутентификация пользователей.</p> <p><b>Технологии межсетевых экранов</b> Противодействие несанкционированному межсетевому доступу. Функции меж сетевого экранирования. Особенности меж сетевого экранирования на различных уровнях модели OSI. Установка и конфигурирование межсетевых экранов. Критерии оценки межсетевых экранов. Обзор современных межсетевых экранов.</p>

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		<p><b>Технологии защищенных виртуальных сетей</b> Способы создания защищенных виртуальных каналов. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне. Построение защищенных виртуальных сетей на сеансовом уровне. Организация безопасного удаленного доступа. Обзор средств построения защищенных виртуальных сетей. Построение защищенных виртуальных сетей на базе маршрутизаторов, межсетевых экранов, специализированного программного обеспечения, специализированных аппаратных средств.</p>
5	Технологии обнаружения вторжений в ИС.	<p><b>Анализ защищенности и обнаружения атак</b> Концепции адаптивного управления безопасностью. Технологии анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционных систем (ОС). Технологии обнаружения атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Методы реагирования.</p> <p><b>Защита от вирусов в ИС</b> Компьютерные вирусы и проблемы антивирусной защиты. Основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты ИС.</p> <p><b>Методы управления средствами сетевой безопасности ИС</b> Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности. Стандарты, используемые при проведении аудита. Анализ рисков и управление рисками. Программные средства, используемые для анализа и управления рисками.</p>
6	Построение и организация функционирования комплексных систем защиты информации в ИС	<p><b>Построение комплексных систем защиты информации</b> Концепция создания защищенных ИС. Этапы создания комплексной системы защиты информации (КСЗИ). Моделирование КСЗИ. Выбор показателей эффективности и критериев оптимальности КСЗИ. Математическая постановка задачи разработки КСЗИ. Подходы к оценке эффективности КСЗИ. Создание организационной структуры КСЗИ.</p> <p><b>Организация функционирования комплексных систем защиты информации</b> Пути и проблемы практической реализации концепции комплексной защиты информации. Применение КСЗИ. Техническая эксплуатация КСЗИ.</p>

## 6. Методические указания по освоению дисциплины

### 6.1 Учебно-методическое обеспечение дисциплины

Изучение дисциплины проводится в форме лекций, практических занятий, организации самостоятельной работы обучающихся, консультаций. Главное назначение лекции - обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у обучающихся

ориентиры для самостоятельной работы над курсом.

Основной целью практических занятий является обсуждение наиболее сложных теоретических вопросов курса, их методологическая и методическая проработка. Они проводятся в форме опроса, диспута, тестирования, обсуждения докладов и пр.

Самостоятельная работа с научной и учебной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с информационными базами, образовательным ресурсом электронной информационно-образовательной среды и сети Интернет.

### **6.2 Методические материалы обучающимся по дисциплине, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Методические материалы для обучающихся доступны в Личной студии обучающегося, в разделе ресурсы.

### **6.3 Особенности реализации дисциплины в отношении лиц из числа инвалидов и лиц с ограниченными возможностями здоровья**

Обучающиеся с ограниченными возможностями здоровья, в отличие от остальных обучающихся, имеют свои специфические особенности восприятия и переработки учебного материала.

Подбор и разработка учебных материалов должны производиться с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Выбор средств и методов обучения осуществляется самим преподавателем. При этом в образовательном процессе рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений обучающихся с ограниченными возможностями здоровья с преподавателями и другими обучающимися, создания комфортного психологического климата в студенческой группе.

Разработка учебных материалов и организация учебного процесса проводится с учетом нормативных документов и локальных актов образовательной организации.

В соответствии с нормативными документами инвалиды и лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь; инвалиды и лица с ограниченными возможностями здоровья по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;

- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочесть и оформить задание, общаться с экзаменатором);

- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении аттестации:

а) для слепых:

- задания и иные материалы для сдачи экзамена оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

- письменные задания выполняются обучающимися с использованием клавиатуры с азбукой Брайля, либо надиктовываются ассистенту;

б) для слабовидящих:

- задания и иные материалы для сдачи экзамена оформляются увеличенным шрифтом и/или использованием специализированным программным обеспечением Jaws;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- имеется в наличии информационная система "Исток" для слабослышащих коллективного пользования;

- по их желанию испытания проводятся в электронной или письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата:

- тестовые и тренинговые задания по текущей и промежуточной аттестации выполняются обучающимися на компьютере через сайт «Личная студия» с использованием электронного обучения, дистанционных технологий;

- для обучения лиц с нарушениями опорно-двигательного аппарата используется электронный образовательный ресурс, электронная информационно-образовательная среда;

- по их желанию испытания проводятся в устной форме.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

#### **6.4 Методические рекомендации по самостоятельной работе обучающихся**

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление

и расширение теоретических знаний с целью их применения на уровне межпредметных связей;

- систематизация и закрепление полученных теоретических знаний и практических навыков;

- формирование умений по поиску и использованию нормативной, правовой, справочной

и специальной литературы, а также других источников информации;

- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;

- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;
- развитие научно-исследовательских навыков;
- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа является неотъемлемой частью образовательного процесса.

Самостоятельная работа предполагает инициативу самого обучающегося в процессе сбора и усвоения информации, приобретения новых знаний, умений и навыков и ответственность его за планирование, реализацию и оценку результатов учебной деятельности. Процесс освоения знаний при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа должна:

- быть выполнена индивидуально (или являться частью коллективной работы). В случае, когда СР подготовлена в порядке выполнения группового задания, в работе делается соответствующая оговорка;

- представлять собой законченную разработку (этап разработки), в которой анализируются актуальные проблемы по определенной теме и ее отдельных аспектов;

- отражать необходимую и достаточную компетентность автора;

- иметь учебную, научную и/или практическую направленность;

- быть оформлена структурно и в логической последовательности: титульный лист, оглавление, основная часть, заключение, выводы, список литературы, приложения,

- содержать краткие и четкие формулировки, убедительную аргументацию, доказательность и обоснованность выводов;

- соответствовать этическим нормам (правила цитирования и парафраз; ссылки на использованные библиографические источники; исключение плагиата, дублирования собственного текста и использования чужих работ).

## 7. Фонд оценочных материалов для проведения текущей и промежуточной аттестации по дисциплине

### 7.1. Система оценивания результатов текущей и промежуточной аттестации и критерии выставления оценок, описание шкал оценивания

4-балльная шкала и 2-балльная шкалы	Критерии
«Отлично» или «зачтено»	<p>1. Полные и качественные ответы на вопросы, охватывающие все необходимые аспекты темы. Обучающийся обосновывает свои выводы с использованием соответствующих фактов, данных или источников, демонстрируя глубокую аргументацию.</p> <p>2. Обучающийся успешно переносит свои теоретические знания в практическую реализацию. Выполненные задания соответствуют высокому уровню качества, включая использование правильных форматов, методологий и инструментов.</p> <p>3. Обучающийся анализирует и оценивает различные аспекты темы, демонстрируя способность к критическому мышлению и самостоятельному исследованию.</p>
«Хорошо» или «зачтено»	<p>1. Обучающийся предоставляет достаточно полные ответы на вопросы с учетом основных аспектов темы. Ответы обучающегося имеют ясную структуру и последовательность, делая их понятными и логически связанными.</p> <p>2. Обучающийся способен применить теоретические знания в практических заданиях. Выполнение задания в целом соответствует требованиям, хотя могут быть некоторые недочеты или неточные выводы по полученным результатам.</p> <p>3. Обучающийся представляет хорошее понимание темы вопроса, охватывая основные аспекты и направления ее изучения. Ответы обучающегося содержат достаточно информации, но могут быть некоторые пропуски или недостаточно глубокие суждения.</p>
«Удовлетворительно» или «зачтено»	<p>1. Ответы на вопросы неполные, не охватывают всех аспектов темы и не всегда структурированы или логически связаны. Обучающийся предоставляет верные выводы, но они недостаточно аргументированы или основаны на поверхностном понимании предмета вопроса.</p> <p>2. Обучающийся способен перенести теоретические знания в практические задания, но недостаточно уверен в верности примененных методов и точности в их выполнении. Выполненное задание может содержать некоторые ошибки, недочеты или расхождения.</p> <p>3. Обучающийся охватывает большинство основных аспектов темы вопроса, но демонстрирует неполное или поверхностное их понимание, дает недостаточно развернутые объяснения.</p>
«Неудовлетворительно»	<p>1. Обучающийся отвечает на вопросы неполно, не раскрывая основных аспектов темы. Ответы обучающегося</p>

или «не зачтено»	<p>не структурированы, не связаны с заданным вопросом, отсутствует их логическая обоснованность. Выводы, предоставляемые обучающимся, представляют собой простые утверждения без анализа или четкой аргументации.</p> <p>2. Обучающийся не умеет переносить теоретические знания в практический контекст и не способен применять их для выполнения задания. Выполненное задание содержит много ошибок, а его результаты не соответствуют поставленным требованиям и (или) неправильно интерпретируются.</p> <p>3. Обучающийся ограничивается поверхностным рассмотрением темы и не показывает понимания ее существенных аспектов. Ответ обучающегося частичный или незавершенный, не включает анализ рассматриваемого вопроса, пропущены важные детали или связи.</p>
---------------------	---

## 7.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Назовите основные понятия:

№	Определение	Понятие
1.	Принятие правовых, организационных и технических мер, направленных:	Защита информации
2.	Проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам защиты информации.	Контроль состояния защиты информации
3.	Установление градации важности защищаемой информации (объекта защиты)	Категорирование
4.	Изменение информации или ресурсов автоматизированной информационной системы, осуществляемое с нарушением установленных прав и (или) правил	Несанкционированное воздействие
5.	Деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации	Защита информации от разглашения
6.	Бесконтрольный процесс распространения или передачи конфиденциальных данных третьим лицам, представляющий собой «слив» сведений за пределы компании, группы или круга людей, имеющих разрешение на доступ	Утечка информации
7.	Доступ к информации, нарушающий правила разграничения доступа	несанкционированный доступ

8.	Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации	Замысел защиты информации
9.	Наука об обеспечении секретности и/или подлинности (аутентичности) передаваемых сообщений	Криптография
10.	Вредоносная программа, способная самостоятельно распространяться и заражать компьютеры, системы или сети.	Компьютерный вирус

#### Вопросы открытого типа

№	Вопрос	Ответ
1.	Специальные устройства, службы или программы, обеспечивающие шифрование (кодирование) и расшифрование (раскодирование) информации с целью ее защиты от несанкционированной обработки, доступа и хранения при обмене ею по каналам связи, а также отвечающие за генерацию электронной подписи (ЭП)	Средства криптографической защиты информации
2.	Сколько существует каналов утечки информации?	Четыре
3.	совокупность приемов научного познания, представляющая собой последовательность действий по установлению структурных связей между переменными или элементами исследуемой системы, опирающийся на комплекс общенаучных, экспериментальных, естественнонаучных методов	Системный анализ
4.	Какую информацию можно считать полной?	Достаточную
5.	Как классифицируются угрозы информационной безопасности по степени преднамеренности проявления?	По степени преднамеренности
6.	На чём строится политика безопасности информационной системы?	На основе анализа рисков
7.	К каким средствам защиты информации относятся специальные устройства, службы или программы, обеспечивающие шифрование (кодирование) и расшифрование (раскодирование) информации	Криптографическим
8.	Что является целью системного анализа?	Упорядочение последовательности

		действий
9.	Какие существуют способы шифрования?	Симметричное и несимметричное
10.	Процесс проверки принадлежности субъекту прав доступа к информационным ресурсам системы или веб-сайта в соответствии с предъявленным им идентификатором; подтверждение (установление) подлинности субъекта	Аутентификация

Тестовые задания:

1.	Все большее распространение получает _____ аутентификация пользователя, позволяющая аутентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.
А)	строгая
<b>Б)</b>	<b>биометрическая</b>
В)	авторизованная
Г)	административная

2.	Дактилоскопические системы аутентификации в качестве параметра идентификации используют
А)	голос и «клавиатурный почерк»
Б)	форму кисти руки
В)	форму и размер лица
<b>Г)</b>	<b>отпечатки пальцев</b>

3.	Объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей
А)	стеганография
<b>Б)</b>	<b>криптоанализ</b>
В)	криптография

Г)	криптология
----	-------------

4.	В асимметричных системах шифрования
А)	<b>открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения</b>
Б)	для зашифрования и расшифрования используется один ключ
В)	секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
Г)	секретный и открытый ключи доступны всем желающим

5.	Верны ли утверждения? А) Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей) В) От идентификации и аутентификации зависит последующее решение системы о том, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу Подберите правильный ответ
А)	А – да, В - нет
Б)	<b>А – да, В - да</b>
В)	А – нет, В - нет
Г)	А – нет, В - да

6.	_____ пароль – пароль, который после однократного применения больше не используется
А)	Открытый
Б)	Асимметричный
В)	<b>Динамический</b>
Г)	Многоразовый

7.	Первым шагом процедуры опознавания пользователя с использованием простого пароля является то, что
А)	<b>пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор</b>

Б)	система запрашивает пароль
В)	пользователь вводит пароль
Г)	система сравнивает полученный пароль с паролем пользователя и разрешает/запрещает доступ

8.	Одним из наиболее распространенных протоколов аутентификации на основе динамических паролей является стандартизованный в Интернете протокол
А)	SecurID
Б)	PIN
В)	DES
Г)	<b>S/Key</b>

9.	Правила, на основании которых диспетчер доступа принимает решение о предоставлении субъекту доступа к объекту (либо отказе в нем), называют
А)	<b>политикой</b>
Б)	диспетчером
В)	контроллером
Г)	реестром

10.	Первым этапом жизненного цикла любого компьютерного вируса является
А)	подготовка и внедрение копий вируса
Б)	активация вируса
В)	поиск объектов для заражения
Г)	<b>проникновение на чужой компьютер</b>

Ключ к тестовым заданиям

<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
Б	Г	Б	А	Б
<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>
В	А	Г	А	Г

## **8. Учебно-методическое и информационное обеспечение дисциплины**

### **8.1. Рекомендуемая литература**

#### **Основная литература**

1. Дмитриев, В. Т. Защита информации в инфокоммуникационных системах. Ч.1 : учебное пособие / В. Т. Дмитриев. — Рязань : Рязанский государственный радиотехнический университет, 2023. — 160 с. — ISBN 978-5-7722-0370-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/134852.html>
2. Дмитриев, В. Т. Защита информации в инфокоммуникационных системах. Ч.2 : учебное пособие / В. Т. Дмитриев. — Рязань : Рязанский государственный радиотехнический университет, 2023. — 148 с. — ISBN 978-5-7722-0371-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/137319.html>
3. Левина И.А. Защита автономных автоматизированных систем. [Электронный ресурс] : рабочий учебник / Левина И.А. - 2022. - <http://library.roweb.online>
4. Левина И.А. Основные принципы программной и программно-аппаратной защиты информации. [Электронный ресурс] : рабочий учебник / Левина И.А. - 2022. - <http://library.roweb.online>

#### **Дополнительная литература**

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146404.html>

### **8.2. Ресурсы информационно-телекоммуникационной сети Интернет**

- <http://citforum.ru/> - Сервер Информационных технологий
- <http://www.rushelp.com/> - сайт-каталог компьютерной документации, информация по языкам программирования
- <http://www.gnpbu.ru/> - Научная педагогическая библиотека им. К.Д. Ушинского.
- <https://ro-edu.ru/> - Медиалпортал «Российское образование»

## **9. Материально-техническое обеспечение дисциплины**

Помещения для осуществления образовательного процесса по дисциплине представляет собой аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

Список аудиторий:

1. Аудитория для проведения учебных занятий.
2. Помещение для самостоятельной работы обучающихся.
3. Многофункциональная аудитория для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов).

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая программное обеспечение, современные профессиональные базы данных и информационные справочные системы**

Программное обеспечение АНО ВО ИТУ, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных технологиях:

- тренинговые и тестирующие программы;
- интеллектуальные роботизированные системы оценки качества выполнения работ.

Информационные и роботизированные системы, программные комплексы, программное обеспечение для доступа к компьютерным обучающим, тренинговым и тестирующим программам:

- ПК «КОП»;
- ИР «Каскад».

Программное обеспечение, необходимое для реализации дисциплины:

*Лицензионное программное обеспечение (в том числе, отечественного производства):*

Операционная система Windows Professional 10

ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц

Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО)

Платформа проведения вебинаров (отечественное ПО)

Информационная технология. Онлайн тестирование цифровой платформы Ровеб (отечественное ПО)

Электронный информационный ресурс. Экспертный интеллектуальный информационный робот Аттестация ассессоров (отечественное ПО)

Информационная технология. Аттестационный интеллектуальный информационный робот контроля оригинальности и профессионализма «ИИР КОП» (отечественное ПО)

Электронный информационный ресурс «Личная студия обучающегося» (отечественное ПО)

*Свободно распространяемое программное обеспечение (в том числе отечественного производства):*

Мой Офис Веб-редакторы <https://edit.myoffice.ru> (отечественное ПО)

ПО OpenOffice.Org Calc.

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО OpenOffice.Org.Base

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО OpenOffice.org.Impress

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО OpenOffice.Org Writer

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО Open Office.org Draw

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами;

*Современные профессиональные базы данных:*

Реестр профессиональных стандартов <https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/>

Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» <https://reestr.digital.gov.ru/>

Общество с ограниченной ответственностью «Интерактивные обучающие технологии» <https://htmlacademy.ru/tutorial/php/mysql>

Web-технологии <https://htmlweb.ru/php/mysql.php>

Научная электронная библиотека. <http://elibrary.ru>

Электронно-библиотечная система IPR SMART <http://www.iprbookshop.ru>

*Информационно-справочные системы:*

1. <http://www.consultant.ru/> - справочная правовая система КонсультантПлюс

2. <https://www.garant.ru/> - справочная правовая система Гарант