

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Колесникова Екатерина Дмитриевна  
Должность: Ректор СГИ  
Дата подписания: 13.10.2025 16:03:15  
Уникальный программный ключ:  
5791137b901a0c9e3d118a20e9301d50e14011ca74401



**ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СРЕДНЕ-РУССКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ»**

**УТВЕРЖДАЮ**

Заведующий кафедрой электроэнергетики и  
электротехники

\_\_\_\_\_/Бурцева Т.А./

«10» октября 2025 г.

**Кафедра экономики и управления**

**Рабочая программа учебной дисциплины**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Направление подготовки  
09.03.03 Прикладная информатика

Направленность (профиль) подготовки:

Прикладная информатика в экономике

Квалификация (степень) выпускника:

Бакалавр

Форма обучения:

Очная

Составитель программы:

Караченков П.А.,

старший преподаватель кафедры  
электроэнергетики и электротехники

## СОДЕРЖАНИЕ

1. Аннотация к дисциплине
2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся
- 3.1. Объем дисциплины по видам учебных занятий (в часах)
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
- 4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)
- 4.2. Содержание дисциплины, структурированное по разделам (темам)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
6. Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность»
- 6.1. Описание показателей и критериев оценивания компетенций, описание шкал
- 6.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы
- 6.3. Типовые контрольные задания или иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и(или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы
- 6.4. Типовые задания для проведения промежуточной аттестации обучающихся
- 6.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины
8. Методические указания для обучающихся по освоению дисциплины
9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы.
- 10.1. Лицензионное программное обеспечение
- 10.2. Электронно-библиотечная система
- 10.3. Современные профессиональные баз данных
- 10.4. Информационные справочные системы
11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья
12. Лист регистрации изменений

## **1. Аннотация к дисциплине**

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденный приказом Министерства образования науки России от 19.09.2017 № 922.

Рабочая программа содержит обязательные для изучения темы по дисциплине «Информационная безопасность».

### **Место дисциплины в структуре образовательной программы**

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата).

Дисциплина изучается на 3 курсе в 5 семестре для очной формы обучения, экзамен

### **Цель изучения дисциплины:**

ознакомление с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

Исходя из поставленной цели, для её достижения в рамках дисциплины можно выделить следующие задачи:

- овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;
- ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;
- изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;
- приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными

### **Компетенции обучающегося, формируемые в результате освоения дисциплины:**

УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности

ПК-2 Способен осуществлять проектирование программного обеспечения ИС и разрабатывать техническую документацию на его компоненты

ПК-3 Способен вводить в эксплуатацию и осуществлять сопровождение ИС на всех этапах ее жизненного цикла, включая ее презентацию и начальное обучение пользователей

## 2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование компетенций, предусмотренных ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика и на основе профессионального стандарта:

– 16.019. Профессиональный стандарт "Специалист по информационным системам", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 13 июля 2023 г. N 586н (зарегистрирован Министерством юстиции Российской Федерации 16 августа 2023 г., регистрационный N 74817).

Код компетенции	Результаты освоения ООП (содержание компетенций)	Индикаторы достижения компетенций	Формы образовательной деятельности, способствующие формированию и развитию компетенции
УК-10	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1. Знает понятие и признаки экстремизма, терроризма, коррупции, направления противодействия терроризму, экстремизму и коррупции, сущность профессиональной деформации. УК-10.2. Выявляет и дает оценку экстремизма, терроризма и коррупционного поведения и содействует их пресечению. УК-10.3. Владеет нетерпимым отношением к экстремизму, терроризму коррупционному поведению, уважительным отношением к праву и закону	Контактная работа: Лекции Практические занятия Самостоятельная работа
ПК-2	Способен осуществлять проектирование программного обеспечения ИС и разрабатывать техническую документацию на его компоненты	ПК-2.1. Способен использовать современные языки и системы программирования, технологии проектирования программного обеспечения. ПК-2.2. Способен сформулировать требования к разрабатываемому программному обеспечению, выполнить его реализацию и оформить техническую документацию на его компоненты. ПК-2.3. Способен осуществлять проектирование программного обеспечения конкретной ИС и разработку технической документации на ее компоненты.	Контактная работа: Лекции Практические занятия Самостоятельная работа

ПК-3	Способен вводить в эксплуатацию и осуществлять сопровождение ИС на всех этапах ее жизненного цикла, включая ее презентацию и начальное обучение пользователей	ПК-3.1. Способен использовать знания методологических и технических основ ввода ИС в эксплуатацию. ПК-3.2. Способен организовать репозиторий хранения данных о создании ИС, вводе ее в эксплуатацию и модификации в процессе жизненного цикла. ПК-3.3. Способен осуществлять инсталляцию программного обеспечения ИС, его тестирование и начальное обучение пользователей.	Контактная работа: Лекции Практические занятия Самостоятельная работа
------	---	---	--

**3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 5 зачетные единицы.

**3.1 Объём дисциплины по видам учебных занятий (в часах)**

Объём дисциплины	Всего часов
	очная форма обучения
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (всего)	54
Аудиторная работа (всего):	54
в том числе:	
лекции	18
семинары, практические занятия	36
лабораторные работы	
Контроль	18
Внеаудиторная работа (всего):	108
в том числе:	
Самостоятельная работа обучающихся (всего)	108
Вид промежуточной аттестации обучающегося (экзамен)	+

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

для очной формы обучения

№ п/п	Разделы и темы учебной дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу и трудоемкость (в часах)						Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации (по семестрам)	
			Всего	Из них аудиторные занятия			Самостоятельная работа	Контрольная работа		Курсовая работа
				Лекции	Лабораторный практикум	Практические занятия /семинары				
1	<b>Тема 1.</b> Концепция информационной безопасности	5	30	3		6	21		Опрос	
2	<b>Тема 2.</b> Угрозы информации.	5	30	3		6	21		Коллоквиум	
3	<b>Тема 3.</b> Виды возможных нарушений информационной системы	5	34	4		8	22		Опрос	
4	<b>Тема 4.</b> Информационная безопасность информационных систем	5	34	4		8	22		Коллоквиум	
5	<b>Тема 5.</b> Методы и средства защиты компьютерной информации	5	34	4		8	22		Опрос	
	Экзамен + Курсовая работа	5	<b>18</b>							
	<b>ИТОГО:</b>		<b>180</b>	<b>18</b>		<b>36</b>	<b>108</b>			

4.2. Содержание дисциплины, структурированное по разделам (темам)

### Тема 1. Концепция информационной безопасности

*Содержание лекционных материалов*

#### 1.1. Актуальность информационной безопасности.

Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

#### 1.2. Лицензирование и сертификация в области защиты информации.

Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования.

**1.3. Основные нормативные руководящие документы.** Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.

### *Содержание практических занятий*

1. Национальные интересы РФ в информационной сфере и их обеспечение.
2. Правила функционирования системы лицензирования.
3. Критерии безопасности компьютерных систем

## **Тема 2. Угрозы информации.**

### *Содержание лекционных материалов*

#### **2.1. Информационная безопасность сетей.**

Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.

#### **2.2. Способы совершения компьютерных преступлений.**

Анализ классификации способов, средств, используемых для совершения преступлений, особенностей расследования и законодательства в этой сфере

#### **2.3. Уязвимость сети Интернет.**

Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

### *Содержание практических занятий*

1. Угрозы информационной безопасности для АСОИ.
2. Причины уязвимости сети Интернет.
3. Удаленные атаки на интрасети.

## **Тема 3. Виды возможных нарушений информационной системы.**

### *Содержание лекционных материалов*

#### **3.1. Компьютерные преступления.**

Классификация компьютерных преступлений. Виды противников или «нарушителей».

#### **3.2. Вредоносные программы.**

Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам.

#### **3.3. Вирусы.**

Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

### *Содержание практических занятий*

1. Классификация компьютерных преступлений
2. Хакерские утилиты и прочие вредоносные программы.
3. Классические компьютерные вирусы.

## **Тема 4. Информационная безопасность информационных систем**

### *Содержание лекционных материалов*

#### **4.1. Теория информационной безопасности информационных систем.**

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

#### **4.2. Криптографические способы защиты информации.**

Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

**4.3. Организация информационной безопасности компании.** Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

### *Содержание практических занятий*

1. Модели безопасности и их применение.
2. Использование защищенных компьютерных систем.

### 3. Выбор средств информационной безопасности.

## Тема 5. Методы и средства защиты компьютерной информации

### Содержание лекционных материалов

#### 5.1. Обеспечения информационной безопасности.

Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре.

#### 5.2. Контроль доступа к информации.

Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта).

#### 5.3. Методы и средства защиты информации.

Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.

#### 5.4. Антивирусное ПО.

Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы

### Содержание практических занятий

1. Контроль доступа к аппаратуре.
2. Предоставление привилегий на доступ.
3. Организационные мероприятия по защите информации
4. Антивирусные программы

### 5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Одним из основных видов деятельности студента является самостоятельная работа, которая включает в себя изучение лекционного материала, учебников и учебных пособий, первоисточников, решение задач, выступления на групповых занятиях, выполнение заданий преподавателя.

Методика самостоятельной работы по учебной дисциплине «Информационная безопасность» предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов, в том числе связанных с ограничением возможностей здоровья. Время и место самостоятельной работы выбираются студентами по своему усмотрению с учетом рекомендаций преподавателя.

Самостоятельную работу над дисциплиной следует начинать с изучения программы, которая содержит основные требования к знаниям, умениям и навыкам обучающихся. Обязательно следует вспомнить рекомендации преподавателя, данные в ходе установочных занятий. Затем – приступать к изучению отдельных разделов и тем в порядке, предусмотренном программой.

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Тема 1. Концепция информационной безопасности	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме 1, работа с интернет источниками	Опрос
Тема 2. Угрозы информации.	Угрозы информационной безопасности для АСОИ	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме 2, работа с интернет источниками	Коллоквиум
Тема 3.	Хакерские утилиты и	Работа в	Литература к	Опрос

Виды возможных нарушений информационной системы	прочие вредоносные программы.	библиотеке, включая ЭБС. Дидактическое тестирование	теме 3, работа с интернет источниками	
<b>Тема 4.</b> Информационная безопасность информационных систем	Методы криптографии.	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме 4, работа с интернет источниками	Коллоквиум
<b>Тема 5.</b> Методы и средства защиты компьютерной информации	Источники компьютерных вирусов	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме 5, работа с интернет источниками	Опрос

**6. Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность».**

Промежуточная аттестация по дисциплине проводится в форме экзамена.

**6.1. Описание показателей и критериев оценивания компетенций, описание шкал оценивания**

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Шкала и критерии оценки, балл	Критерии оценивания компетенции
1.	Вопросы опросам	Практическое занятие	Опрос - это средство контроля, организованное как специальная беседа преподавателя со студентом на темы, связанные с изучаемой дисциплиной, и рассчитанное на выявление объема знаний студента по определенному разделу, теме, проблеме и т.п. Проблематика, выносимая на опрос определена в заданиях для самостоятельной работы студента, а также может определяться преподавателем, ведущим практические занятия. Во время проведения опроса студент должен уметь решать стандартные задачи по темам курса.	УК-10 ПК-2 ПК-3
2.	Темы рефератов	Практическое занятие	«5» – реферат выполнен в соответствии с заявленной темой, текст легко читаем и ясен для понимания, грамотное использование терминологии, свободное изложение рассматриваемых проблем; «4» – некорректное оформление реферате, грамотное использование терминологии, в основном свободное изложение рассматриваемых проблем;	УК-10 ПК-2 ПК-3

			«3» – ошибки при использовании терминологии, нечеткое изложение и логика текста.	
3.	Типовые тестовые вопросы	Практическое занятие	<p>Контроль в виде тестов может использоваться после изучения каждой темы курса. Итоговое тестирование можно проводить в форме:</p> <ul style="list-style-type: none"> <li>- компьютерного тестирования, т.е. компьютер произвольно выбирает вопросы из базы данных по степени сложности;</li> <li>- письменных решений предложенных преподавателей задач и примеров.</li> </ul> <p>Оценка результатов тестирования может проводиться двумя способами:</p> <p>1) по 5-балльной системе, когда ответы студентов оцениваются следующим образом:</p> <ul style="list-style-type: none"> <li>- «отлично» – более 80% ответов правильные;</li> <li>- «хорошо» – более 65% ответов правильные;</li> <li>- «удовлетворительно» – более 50% ответов правильные.</li> </ul> <p>Студенты, которые правильно решили менее чем на 70% вопросов, должны в последующем пересдать тест. При этом необходимо проконтролировать, чтобы вариант теста был другой;</p> <p>2) по системе зачет-незачет, когда для зачета по данной дисциплине достаточно правильно решить более чем 70% примеров и задач.</p> <p>Чтобы выявить умение студентов решать задачи, следует проводить текущий контроль (выборочный для нескольких студентов или полный для всей группы). Обучающимся на решение одной задачи дается 15 – 20 минут по пройденным темам. Это способствует, во-первых, более полному усвоению обучающимися пройденного материала, во-вторых, позволяет выявить и исправить ошибки при их подробном рассмотрении на семинарских занятиях.</p>	УК-10 ПК-2 ПК-3

**6.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и(или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

№	Форма контроля/ коды оцениваемых компетенций	Процедура оценивания	Шкала и критерии оценки, балл
1.	Экзамен УК-10 ПК-2 ПК-3	<p>Правильность ответов на все вопросы (верное, четкое и достаточно глубокое изложение идей, понятий, фактов и т.д.); Сочетание полноты и лаконичности ответа; Наличие практических навыков по дисциплине (решение задач или заданий); Ориентирование в учебной, научной и специальной литературе; Логика и аргументированность изложения; Грамотное комментирование, приведение примеров, аналогий; Культура ответа.</p>	<p>Отлично - Студент должен:</p> <ul style="list-style-type: none"> <li>- продемонстрировать глубокое и прочное усвоение знаний программного материала;</li> <li>- исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал;</li> <li>- правильно формулировать определения;</li> <li>- продемонстрировать умения самостоятельной работы с литературой;</li> <li>- уметь сделать выводы по излагаемому материалу.</li> </ul> <p>Хорошо - Студент должен:</p> <ul style="list-style-type: none"> <li>- продемонстрировать достаточно полное знание программного материала;</li> <li>- продемонстрировать знание основных теоретических понятий;</li> <li>- достаточно последовательно, грамотно и логически стройно излагать материал;</li> <li>- продемонстрировать умение ориентироваться в литературе;</li> <li>- уметь сделать достаточно обоснованные выводы по излагаемому материалу.</li> </ul> <p>Удовлетворительно - Студент должен:</p> <ul style="list-style-type: none"> <li>- продемонстрировать общее знание изучаемого материала;</li> <li>- показать общее владение понятийным аппаратом дисциплины;</li> <li>- уметь строить ответ в соответствии со структурой излагаемого вопроса;</li> <li>- знать основную рекомендуемую программой учебную литературу.</li> </ul> <p>Неудовлетворительно - Студент демонстрирует:</p> <ul style="list-style-type: none"> <li>- незнание значительной части программного материала;</li> <li>- не владение понятийным аппаратом дисциплины;</li> <li>- существенные ошибки при изложении учебного материала;</li> <li>- неумение строить ответ в соответствии со структурой излагаемого вопроса;</li> <li>- неумение делать выводы по излагаемому материалу.</li> </ul>

**6.3. Типовые контрольные задания или иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и(или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

**Тема 1. Концепция информационной безопасности**

Перечень вопросов для обсуждения на практических занятиях:

1. Национальные интересы РФ в информационной сфере и их обеспечение.
2. Правила функционирования системы лицензирования.
3. Критерии безопасности компьютерных систем

**Тема 2. Угрозы информации.**

Перечень вопросов для обсуждения на практических занятиях:

1. Угрозы информационной безопасности для АСОИ.
2. Причины уязвимости сети Интернет.
3. Удаленные атаки на интрасети.

**Тема 3. Виды возможных нарушений информационной системы.**

Перечень вопросов для обсуждения на практических занятиях:

1. Классификация компьютерных преступлений
2. Хакерские утилиты и прочие вредоносные программы.
3. Классические компьютерные вирусы.

**Тема 4. Информационная безопасность информационных систем**

Перечень вопросов для обсуждения на практических занятиях:

1. Модели безопасности и их применение.
2. Использование защищенных компьютерных систем.
3. Выбор средств информационной безопасности.

**Тема 5. Методы и средства защиты компьютерной информации**

Перечень вопросов для обсуждения на практических занятиях:

1. Контроль доступа к аппаратуре.
2. Предоставление привилегий на доступ.
3. Организационные мероприятия по защите информации
4. Антивирусные программы

**6.4. Типовые задания для проведения промежуточной аттестации обучающихся.**

Промежуточная аттестация по дисциплине "Информационная безопасность" проводится в форме экзамена

**Задания 1 типа (теоретический вопрос на знание базовых понятий предметной области дисциплины):**

**Типовые вопросы**

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.

11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.
16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
18. Способы наблюдения с использованием технических средств

**Задания 2 типа (задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем)**

1. Задание.

*В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?*

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Задание.

*Сертификации подлежат:*

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

3. Задание.

*В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:*

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.

*Естественные угрозы безопасности информации вызваны:*

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

5. Задание.

*Хакер – это:*

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

6. Задание.

*Активный перехват информации это – перехват, который:*

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Задание.

*Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:*

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

8. Задание.

*По среде обитания классические вирусы разделяются:*

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

9. Задание.

*Шифрование методом подстановки:*

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, затыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

10. Задание.

*Метод защиты информации ограничение доступа заключается:*

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

#### 11. Задание.

*Перехват, который неправомерно использует технологические отходы информационного процесса, называется:*

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

#### 12. Задание.

*Спам, периодически проводящий рассылки не рекламных сообщений:*

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

#### 13. Задание.

*Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от ...*

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

#### 14. Задание.

*Попытка одного субъекта выдать себя за другого - это:*

1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

#### 15. Задание.

*В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:*

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;
5. оператор.

## 16. Задание.

*Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:*

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

**Задания 3 типа (задание на проверку умений и навыков, полученных в результате освоения дисциплины)**

### **Типовые вопросы к экзамену**

1. Необходимость защиты информации.
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация".
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация.
5. Характеристика антивирусного программного обеспечения.
6. Способы ограничения доступа к информации.
7. Предотвращение технических сбоев оборудования.
8. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных.
9. Методы взлома компьютерных систем. Атаки на уровне операционной системы.
10. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
11. Методы взлома компьютерных систем. Защита системы от взлома.
12. Характеристика троянских программ. Возникновение троянских программ.
13. Характеристика троянских программ. Где и как часто встречаются троянские программы.
14. Характеристика троянских программ. Распознавание троянской программы.
15. Программные закладки и их классификация.
16. Модели воздействия программных закладок на компьютеры.
17. Защита системы от программных закладок.
18. Разновидность ПЗ (имитаторы, фильтры и заместители).
19. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.
20. Взлом парольной защиты ОС UNIX.
21. Взлом парольной защиты ОС Windows NT.
22. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
23. Информационная безопасность компьютерной сети. Характеристика и назначение анализаторов протоколов
24. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
25. Значение и современные методы шифрования информации в информатизированном обществе
26. Методологические основы технологии шифрования программными средствами.
27. Применение и проблемы стандартизации криптографических алгоритмов.
28. Средства безопасности ОС Windows 2003. Понятия и термины защиты данных. Характеристики безопасности.
29. Средства безопасности ОС Windows 2003. Применение шифрования с открытым и закрытым ключами.

30. Средства безопасности ОС Windows 2003. Алгоритмы и компоненты Windows 2003 обеспечивающие шифрование данных.
31. Средства безопасности ОС Windows 2003. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.
32. Средства безопасности ОС Windows 2003. Характеристика протоколов обмена сообщениями.
33. Аутентификация протокола Kerberos в доменах ОС Windows 2003.
34. Шифрующая файловая система EPS и ее архитектура.
35. Средства безопасности ОС Windows 2003. Применение EPS в ОС Windows 2003.
36. Средства безопасности ОС Windows 2003. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.
37. Средства безопасности ОС Windows 2003. Архивация и восстановление зашифрованных файлов на другом компьютере.
38. Средства безопасности ОС Windows 2003. Восстановление данных зашифрованных с помощью неизвестного личного ключа.
39. Протокол безопасности IP в ОС Windows 2003. Характеристика средств безопасности протокола IP.
40. Архитектура протокола безопасности IP в ОС Windows 2003.
41. Разработка плана безопасности IP в ОС Windows 2003.
42. Администрирование безопасности в ОС Windows 2003.
43. Использование сертификатов для обеспечения безопасности в ОС Windows 2003. Хранилища сертификатов безопасности.
44. Планирование мероприятий по защите информации.
45. Характеристика программных средств шифрования информации.
46. Применение средства криптографической защиты информации Pretty good Privacy (PGP).

#### **Тематика курсовых работ**

1. Блок защиты информации каналов управления автоматизированной системы спутниковой связи
2. Внедрение системы обнаружения вторжений в ...
3. Выбор технологии проектирования систем защиты информации
4. Защита информации при использовании электронной почты.
5. Защита от SQL атак
6. ЗКИ. Получение лицензии. Возможности лицензиата
7. Имитация многолучевого канала на основе IEEE 802.11b
8. Информационная безопасность предприятия...
9. Использование стандарта IEEE 802.1x на предприятии для защиты от несанкционированного доступа»
10. Использование системы TOR при ведении двойной бухгалтерии
11. Исследование ошибок к операционных системах
12. Комплексная защита информации на предприятии ...
13. Комплексная защита информации на примере какого-нибудь предприятия...
14. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему
15. Комплексный подход к обеспечению защиты конфиденциальной информации в компании ...
16. Концепция политики безопасности и систем контроля доступа для локальных вычислительных сетей.
17. Модель системы управления информационной безопасностью в условиях неопределенности воздействия
18. Модернизация комплекса антивирусной защиты ...
19. Обеспечение информационной безопасности в ...
20. Организация защиты персональных данных в ...

21. Организация защиты персональных данных в организации
22. Организация порядка установления внутриобъектного спецрежима на объекте информатизации ...
23. Организация противодействия угрозам безопасности персонала организации на примере ...
24. Основные направления, принципы и методы обеспечения информационной безопасности
25. Построение типовой модели угроз безопасности информации кредитной организации...
26. Проблемы информационной безопасности банков.
27. Разработка алгоритма и программного обеспечения маскирования данных, исследование вопросов стойкости к частотному анализу
28. Разработка комплекса режимных мероприятий по сохранности конфиденциальной информации на примере ...
29. Разработка комплексной защиты информации
30. Разработка комплексной системы защиты коммерческой информации.
31. Разработка корпоративной сети авиапредприятия с подключением удаленных филиалов по каналам VPN
32. Разработка мер по технической защите конфиденциальной информации в организации...
33. Разработка политики безопасности ...
34. Разработка политики информационной безопасности.
35. Разработка предложений по созданию системы защиты информации в локальной вычислительной сети ...
36. Разработка проекта по созданию защищенной корпоративной сети с применением технологий VPN
37. Разработка системы защиты информации предприятия на примере ...
38. Разработка системы защиты конфиденциальной информации в процессинговой компании
39. Разработка системы защиты персональных данных в предприятии...
40. Разработка системы информационной безопасности банка
41. Разработка системы управления кадровой безопасностью организации
42. Разработка средств защиты информации на предприятии ...
43. Разработка типового проекта защиты локальной вычислительной сети предприятия
44. Система защиты персональных данных на предприятии
45. Система обеспечения защиты информации в переговорной комнате ...
46. Системы управления обменными пунктами валют. организация защиты баз данных
47. Создание Концепции ИБ
48. Создание службы безопасности на предприятии.
49. Средства и способы защиты информации по ПЭМИН, аттестация объектов, помещений и информ.систем.
50. ЭЦП (проблемы использования и применения в России и т.п.)

**6.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.**

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются на практических занятиях. Исключение составляет устный опрос, который может проводиться в начале или конце лекции в течение 15-20 мин. с целью закрепления

знаний терминологии по дисциплине. При оценке компетенций принимается во внимание формирование профессионального мировоззрения, определенного уровня культуры, этические навыки, а также личные качества обучающегося формирования.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (1 раз в неделю).
2. Многоступенчатость: оценка (как преподавателем, так и обучающимися группы) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.
3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.
4. Соблюдение последовательности проведения оценки.

**Текущая аттестация обучающихся.** Текущая аттестация обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами СГТИ и является обязательной.

Текущая аттестация по дисциплине «Информационная безопасность» проводится в форме опроса и контрольных мероприятий по оцениванию фактических результатов обучения обучающихся осуществляется ведущим преподавателем.

Объектами оценивания выступают:

- учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);
- степень усвоения теоретических знаний (анализ и оценка активности и эффективности участия в практических занятиях, тестирование и т.д.);
- уровень овладения практическими умениями и навыками по всем видам учебной работы (работа на семинарах или практических занятиях, включая интерактив);
- результаты самостоятельной работы (работа на семинарских занятиях, изучение книг из списка основной и дополнительной литературы).

Активность обучающегося на занятиях оценивается на основе выполненных обучающимся работ и заданий, предусмотренных данной рабочей программой дисциплины.

Кроме того, оценивание обучающегося проводится на текущем контроле по дисциплине. Оценивание обучающегося на контрольной неделе проводится преподавателем независимо от наличия или отсутствия обучающегося (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период.

Оценивание обучающегося носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период с выставлением оценок в ведомости.

**Промежуточная аттестация обучающихся.** Промежуточная аттестация обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами СГТИ и является обязательной.

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в соответствии с учебным планом в виде экзамена.

в период зачетно-экзаменационной сессии в соответствии с графиком проведения экзаменов.

Обучающиеся допускаются к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины.

Оценка знаний обучающегося на экзамене определяется его учебными достижениями в семестровый период и результатами текущего контроля знаний и ответом на экзамене.

Знания умения, навыки обучающегося на экзамене оцениваются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

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

### а) основная учебная литература:

1. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/108227.html>

2. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург: Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст: электронный// Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/103997.html>

3. Суворова, Г. М. Информационная безопасность: учебное пособие/ Г. М. Суворова. — Саратов: Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/86938.html>

4. Шаньгин, В. Ф. Информационная безопасность и защита информации/ В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/87995.html>

### б) дополнительная учебная литература

1. Информационная безопасность: учебное пособие/ Кирколуп сост., Е. М. Скурыдина. — Барнаул: Алтайский государственный педагогический университет, 2017. — 313 с. — ISBN 978-5-88210-898-3. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/102889.html>

2. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие/ А. В. Моргунов. — Новосибирск: Новосибирский государственный технический университет, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/98708.html>

3. Бахаров, Л. Е. Информационная безопасность и защита информации (разделы криптография и стеганография): практикум/ Л. Е. Бахаров. — Москва: Издательский Дом МИСиС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/98171.html>

Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/80290.html>

## 8. Методические указания для обучающихся по освоению дисциплины

Вид деятельности	Методические указания по организации деятельности обучающегося
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом практических занятий, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы.
Самостоятельная работа	Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; формирования умений использовать основную и дополнительную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций;

	<p>развитию практических умений обучающихся.</p> <p>Формы и виды самостоятельной работы обучающихся: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; поиск необходимой информации в сети Интернет; подготовка к различным формам текущей и промежуточной аттестации (к экзамену).</p> <p>Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов; компьютерные классы с возможностью работы в сети Интернет; основную и дополнительную литературу, разработанную с учетом увеличения доли самостоятельной работы обучающихся, и иные методические материалы.</p> <p>Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, которое включает цель задания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.</p> <p>Формы контроля самостоятельной работы: просмотр и проверка выполнения самостоятельной работы преподавателем; рефлексия выполненного задания в группе; обсуждение результатов выполненной работы на занятии – предоставление обратной связи; проведение устного опроса</p>
Опрос	<p>Устный опрос по основной терминологии может проводиться в процессе практического занятия в течение 15-20 мин. Позволяет оценить полноту знаний контролируемого материала</p>
Подготовка к экзамену	<p>При подготовке к экзамену необходимо ориентироваться на рекомендуемую литературу и др.</p> <p>Основное в подготовке к сдаче экзамена по дисциплине «Информационная безопасность» - это повторение всего материала дисциплины, по которому необходимо сдавать промежуточную аттестацию. При подготовке к сдаче экзамена обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнение намеченной работы.</p> <p>Подготовка обучающегося к экзамену включает в себя три этапа: самостоятельная работа в течение семестра; непосредственная подготовка в дни, предшествующие экзамену по темам курса; подготовка к ответу на задания, содержащиеся в вопросах экзамена.</p> <p>Экзамен проводится по вопросам, охватывающим весь пройденный материал дисциплины, включая вопросы, отведенные для самостоятельного изучения.</p> <p>Для успешной сдачи экзамена по дисциплине «Информационная безопасность» обучающиеся должны принимать во внимание, что: все основные вопросы, указанные в рабочей программе, нужно знать, понимать их смысл и уметь его разъяснить; указанные в рабочей</p>

	<p>программе формируемые профессиональные компетенции в результате освоения дисциплины должны быть продемонстрированы обучающимся; семинарские занятия способствуют получению более высокого уровня знаний и, как следствие, более высокой оценке на экзамене; готовиться к промежуточной аттестации необходимо начинать с первого практического занятия.</p>
--	---

## **9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Для осуществления образовательного процесса по дисциплине «Информационная безопасность» необходимо использование следующих помещений:

Материально-техническое обеспечение дисциплины включает в себя:

- Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения (аудитория 5)  
Оснащение:

Ноутбук с выходом в интернет (лицензионное программное обеспечение, образовательный контент, система защиты от вредоносной информации) - 1 шт.

Экран – 1 шт.

Проектор – 1 шт.

Меловая доска – 1 шт.

Шкаф закрытый для хранения учебного оборудования – 4 шт.

Стол компьютерный – 12 шт.

Стул ученический – 12 шт.

Стол для преподавателя – 1 шт.

Стул для преподавателя – 1 шт.

Стенды – 6 шт.: структура передачи данных модели OSI, программное обеспечение, сектора информационного рынка, состав системного программного обеспечения, состав основных подсистем экономических ИС, структурная схема ПК.

Программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО:

Microsoft Open License,

Windows 7 Professional,

Microsoft Office Professional, WinRAR,

AST Test,

Антивирус Avira,

Autodesk Education Master Suite 2013,

Графическая платформа LabVIEW для лабораторных практикумов – NI Academic Site License,

Mathcad Education – University Edition,

Пакет программ 1С V8.5,

Система автоматизированного проектирования КОМПАС 3D, свободное распространение

Табличный процессор OpenOffice.org Calc,

Специализированное программное обеспечение для лабораторных работ по дисциплинам «Физика».

- Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения (аудитория 12)

Оснащение:

Стол ученический – 13 шт.

Стул ученический – 13 шт.

Персональный компьютер с периферией и выходом в интернет (лицензионное программное обеспечение, образовательный контент, система защиты от вредоносной информации) - 13 шт.

Телевизор – 1 шт.

Меловая доска – 1 шт.

Наушники с гарнитурой – 13 шт.

Программное обеспечение общего и профессионального назначения, в том числе включающее в

себя следующее ПО:  
Microsoft Open License,  
Windows 7 Professional,  
Microsoft Office Professional, WinRAR,  
AST Test,  
Антивирус Avira,  
Autodesk Education Master Suite 2013,  
Графическая платформа LabVIEW для лабораторных практикумов – NI Academic Site License,  
Mathcad Education – University Edition,  
Пакет программ 1С V8.5,  
Система автоматизированного проектирования КОМПАС 3D, свободное распространение  
Табличный процессор OpenOffice.org Calc,  
Специализированное программное обеспечение для лабораторных работ по дисциплинам  
«Физика».

- Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду (аудитория 4)

Оснащение:

Стол ученический – 4 шт.

Стул ученический – 8 шт.

Ноутбук с выходом в интернет (лицензионное программное обеспечение, образовательный контент, система защиты от вредоносной информации),

Справочно-правовая система "Консультант плюс" – 4 шт.

Доска магнитно-маркерная - 1 шт.

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы**

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде СГТИ из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

### **10.1 Лицензионное программное обеспечение:**

1. Microsoft Open License, Windows 7 Professional.
2. Microsoft Office Professional.

### **10.2. Электронно-библиотечные системы:**

Электронная библиотечная система (ЭБС): <http://www.iprsmart.ru>

Образовательная платформа Юрайт. Для вузов и ссузов: <https://urait.ru>

### **10.3. Современные профессиональные баз данных:**

– Электронная библиотечная система «IPRsmart» [Электронный ресурс]. – Электрон. дан. – Режим доступа: <http://www.iprsmart.ru>

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

Образовательная платформа Юрайт. Для вузов и ссузов: <https://urait.ru>

### **10.4. Информационные справочные системы:**

Компьютерная справочная правовая система «Консультант Плюс»  
<http://www.consultant.ru/>

## **11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья по личному заявлению обучающегося разрабатывается адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья библиотека комплекзует фонд основной учебной литературой, адаптированной к ограничению их здоровья, предоставляет возможность удаленного использования электронных образовательных ресурсов, доступ к которым организован в СГТИ. В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале, оборудованные программами не визуального доступа к информации, экранными увеличителями и техническими средствами усиления остаточного зрения: Microsoft Windows 7, Центр специальных возможностей, Экранная лупа; Microsoft Windows 7, Центр специальных возможностей, Экранный диктор; Microsoft Windows 7, Центр специальных возможностей, Экранная клавиатура.

### Лист регистрации изменений

Рабочая программа учебной дисциплины обсуждена и утверждена на заседании Ученого совета от «10» октября 2025 г. протокол № 3

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.	Утверждена решением Ученого совета на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденного приказом Минобрнауки России от 19.09.2017 № 922.	Протокол заседания Ученого совета от «10» октября 2025 года протокол № 3	10.10.2025
2.			