

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Кудрявцев Максим Владимирович

Должность: Проректор по образованию

Дата подписания: 27.05.2026

Уникальный программный ключ:

790a1a8df2525774421adc1fc96453f0e902bfb0

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ  
**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО  
ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»**  
(Университет Вернадского)

## Кафедра Цифровых систем и инженерных технологий

Принято Ученым советом  
Университета Вернадского  
«26» марта 2026 г. протокол № 8



## Рабочая программа дисциплины

### Информационная безопасность и защита информации

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль) программы: Прикладная информатика в энергетических системах

Квалификация бакалавр

Форма обучения: **очная, очно-заочная**

Балашиха 2026 г.

Рабочая программа разработана в соответствии с ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика.  
Рабочая программа дисциплины разработана *доцентом* кафедры цифровых систем и инженерных технологий, кандидатом экономических наук, Сидоровым А.В.

# 1 Планируемые результаты обучения по дисциплине, соотнесенные с установленными в ОПОП ВО индикаторами достижения компетенций

## 1.1 Перечень компетенций, формируемых учебной дисциплиной

Код и наименование компетенции	Индикаторы достижения компетенций Планируемые результаты обучения
<p><b>профессиональная компетенция</b> ПК-1 Способен выполнять и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы</p>	
<p>ИД2 ПК1 Использует современные системы управления базами данных, администрирования информационных систем. Использует системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников. Осуществляет управление содержанием проекта: документирование требований, анализ продукта, моделируемые совещания. Обеспечивает безопасную эксплуатацию и администрирование информационных систем</p>	<p><b>Знать (З):</b> процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами.</p> <p><b>Уметь (У):</b> определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации.</p> <p><b>Владеть (В):</b> интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного ПО, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.</p>

## 2. Цели и задачи освоения учебной дисциплины, место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к обязательной части ОПОП ВО.

**Целью** изучения дисциплины является ознакомление обучающихся с особенностями обеспечения информационной безопасности в среде операционной системы Linux.

**Задачами** изучения являются:

- овладение теоретическими, практическими и методическими вопросами информационной безопасности и защиты информации;
- ознакомление с программными средствами операционной системы Linux;
- расширение мировоззренческого кругозора.

## 3. Объем учебной дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий, текущий и промежуточный контроль по дисциплине) и на самостоятельную работу обучающихся

### 3.1 Очно-заочная форма обучения

Вид учебной работы	8 семестр
Общая трудоемкость дисциплины, зачетных единиц	144
<b>часов</b>	
<b>Аудиторная (контактная) работа, часов</b>	<b>24,3</b>
в т.ч. занятия лекционного типа	8
занятия семинарского типа	16
промежуточная аттестация	0,3
<b>Самостоятельная работа обучающихся, часов</b>	<b>110,7</b>
<b>Контроль</b>	<b>9</b>
Вид промежуточной аттестации	экзамен

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

### 4.1 Перечень разделов дисциплины с указанием трудоемкости аудиторной (контактной) и самостоятельной работы, видов контролей и перечня компетенций

Очно-заочная форма обучения

Наименование разделов и тем	Трудоемкость, часов			Наименование оценочного средства	Код компетенции
	всего	в том числе			
		аудиторной (контактной) работы	самостоятельной работы		
<b>РАЗДЕЛ 1. СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.</b>	<b>53</b>	<b>8</b>	<b>45</b>	Практические задания, тесты	ПК-1
Тема 1.1. Понятие «информационная безопасность»	6	1	5		
Тема 1.2. Общая схема информационной безопасности	6	1	5		

Тема 1.3. Содержание информационной безопасности	6	1	5		
Тема 1.4. Составляющие информационной безопасности	6	1	5		
Тема 1.5. Задачи информационной безопасности общества	6	1	5		
Тема 1.6. Уровни формирования информационной безопасности	11	1	10		
Тема 1.7. Нормативно-правовые основы информационной безопасности в РФ	6	1	5		
Тема 1.8. Стандарты информационной безопасности	6	1	5		
<b>РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ</b>	<b>28,7</b>	<b>8</b>	<b>20,7</b>	Практически задания, тесты	ПК-1
Тема 2.1. Виды угроз информационной безопасности.	4	1	3		
Тема 2.2. Модель нарушителя информационной безопасности.	4	1	3		
Тема 2.3. Принципы построения системы защиты информации.	4	1	3		
Тема 2.4. Методы защиты информации.	6,7	1	5,7		
Тема 2.5. Повышение надежности информационной системы.	5	2	3		
Тема 2.6. Методы и средства защиты информации от шпионажа и несанкционированного доступа.	5	2	3		
<b>РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ</b>	<b>53,3</b>	<b>8,3</b>	<b>45</b>	Практически задания, тесты	ПК-1
Тема 3.1. Компьютерные вирусы и информационная безопасность.	11	1	10		
Тема 3.2. Классификация компьютерных вирусов.	6	1	5		
Тема 3.3. Антивирусные программы.	6	1	5		
Тема 3.4. Особенности безопасности компьютерных сетей.	6	1	5		
Тема 3.5. Классификация удаленных угроз в компьютерных сетях.	6	1	5		
Тема 3.6. Причины успешной реализации удаленных угроз в компьютерных сетях.	6	1	5		
Тема 3.7. Механизмы безопасности компьютерных сетей.	6	1	5		

Тема 3.8. Криптография и шифрование.	6	1	5		
Промежуточная аттестация	9	0,3			
<b>ИТОГО по дисциплине</b>	<b>144</b>	<b>24,3</b>	<b>110,7</b>		

#### *4.2 Содержание дисциплины по темам*

### **РАЗДЕЛ 1. СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

**Цели:** приобретение теоретических знаний об основах информационной безопасности.

**Задачи:**

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

**Перечень учебных элементов раздела:**

**Тема 1.1. Понятие «информационная безопасность».**

информационная безопасность. Задачи по информационной безопасности. Информационная безопасность и "компьютерная безопасность".

**Тема 1.2. Общая схема информационной безопасности**

Проблемы обеспечения информационной безопасности. Схема обеспечения информационной безопасности.

**Тема 1.3. Содержание информационной безопасности.**

Действия для обеспечения информационной безопасности. Обнаружение угроз. Общие признаки защиты охраняемой информации. Основные цели защиты информации.

**Тема 1.4. Составляющие информационной безопасности.**

Три задачи решаемые в рамках обеспечения информационной безопасности. Доступность, целостность и конфиденциальность информации.

**Тема 1.5. Задачи информационной безопасности общества.**

Доктрина информационной безопасности. Четыре основные составляющие национальных интересов РФ в информационной сфере. методы обеспечения информационной безопасности РФ.

**Тема 1.6. Уровни формирования информационной безопасности.**

Три уровня формирования режима информационной безопасности. Шаги при определении политики информационной безопасности. Процедурный и программно-технический уровень программы безопасности.

**Тема 1.7. Нормативно-правовые основы информационной безопасности в РФ.**

Законодательные меры в сфере информационной безопасности. Основные задачи системы защиты информации.

**Тема 1.8. Стандарты информационной безопасности.**

Стандарт ISO/IEC 15408. Классы требований доверия безопасности. Рекомендации X.800. Руководящие документы – стандарты информационной безопасности.

### **РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ**

**Цели:** приобретение знаний об угрозах информационной безопасности и способах противодействия.

**Задачи:**

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

**Тема 2.1. Виды угроз информационной безопасности.**

Угроза информационной безопасности. Классификация угроз информационной безопасности. Непреднамеренные и преднамеренные угрозы. Несанкционированный доступ

(НСД). Каналы НСД. Система разграничения доступа.

**Тема 2.2. Модель нарушителя информационной безопасности.**

Нарушитель. Модель нарушителя. Классификация нарушителей.

**Тема 2.3. Принципы построения системы защиты информации.**

Принципы защиты информации. Прикладной уровень защиты информации. Защита информации.

**Тема 2.4. Методы защиты информации.**

Дублирование информации.

**Тема 2.5. Повышение надежности информационной системы.**

Понятие надежности. Направления повышения надежности программных средств. Три подхода к созданию отказоустойчивых систем. Избыточность. Помехоустойчивость.

**Тема 2.6. Методы и средства защиты информации от шпионажа и несанкционированного доступа.**

Задачи защиты объектов информационных ресурсов от угроз шпионажа. Система защиты от исследования и копирования информации. Два подхода к организации разграничения доступа к информационной системе. Методы криптографического преобразования информации.

### **РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ.**

**Цели:** приобретение знаний и навыков в области обеспечения безопасности компьютерных систем и сетей.

**Задачи:**

- изучение теоретического материала;
- анализ результатов по исследуемой тематике.

**Тема 3.1. Компьютерные вирусы и информационная безопасность.**

Понятие о компьютерных вирусах. Программный вирус – определение. Внешние признаки проявления деятельности вируса. Пути проникновения вирусов на компьютер.

**Тема 3.2. Классификация компьютерных вирусов.**

Классификация компьютерных вирусов. Утилиты скрытого администрирования.

**Тема 3.3. Антивирусные программы.**

Понятие антивирусной программы. Виды антивирусных программ. Наиболее популярные сегодня антивирусные решения.

**Тема 3.4. Особенности безопасности компьютерных сетей.**

Удаленная угроза. Использование технологии клиент/сервер с точки зрения информационной безопасности.

**Тема 3.5. Классификация удаленных угроз в компьютерных сетях.**

Классификация удаленных угроз. Удаленные атаки.

**Тема 3.6. Причины успешной реализации удаленных угроз в компьютерных сетях.**

Отсутствие выделенного канала связи между объектами вычислительной сети. Недостаточная идентификация объектов и субъектов сети. Взаимодействие объектов без установления виртуального канала. Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений. Отсутствие в распределенных вычислительных сетях полной информации об ее объектах. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений. Отсутствие контроля за маршрутом сообщения в сети. Контроль за виртуальным соединением.

**Тема 3.7. Механизмы безопасности компьютерных сетей.**

Идентификация и аутентификация. Три категории аутентификации.

**Тема 3.8. Криптография и шифрование.**

Понятие криптосистемы. Два класса систем шифрования. Типы классических криптографических методов шифрования. Понятие электронно-цифровой подписи. Дискретное управление доступом. Мандатное управление доступом.

### 5. Оценочные материалы по дисциплине

Оценочные материалы по дисциплине представлены в виде фонда оценочных средств.

### 6. Материально-техническое и учебно-методическое обеспечение дисциплины

#### 6.1 Перечень учебно-методического обеспечения по дисциплине

№ п/п	Автор, название, место издания, издательство, год издания, количество страниц, режим доступа
1	Методические указания по изучению дисциплины и задания для лабораторно-практических занятий. Сидоров А.В., РГУНХ, 2023 год

#### 6.2 Перечень учебных изданий, необходимых для освоения дисциплины

Электронные учебные издания в электронно-библиотечных системах (ЭБС):

№ п/п	Автор, название, место издания, год издания, количество страниц	Ссылка на учебное издание в ЭБС
<b>Основная:</b>		
1	Капустин, Д.А. Информационно-вычислительные сети [Электронный ресурс]: учеб. пособие / Д.А.Капустин, В.Е. Дементьев /Ульяновск: Ульяновский ГТУ, 2011. - 141 с.	Электронно-библиотечная система «AgriLib»: сайт – Балашиха, 2011. URL: <a href="http://ebs.rgunh.ru/?q=node/3525">http://ebs.rgunh.ru/?q=node/3525</a> .
2	Платунова, С.М. Администрирование вычислительных сетей на базе MS Winsows Server® 2008 [Электронный ресурс]: учеб. пособие / С.М. Платунова /СПб.: СПбГУ ИТМО, 2012. - 41 с.	Электронно-библиотечная система «AgriLib»: сайт – Балашиха, 2012. URL: <a href="http://ebs.rgunh.ru/?q=node/3169">http://ebs.rgunh.ru/?q=node/3169</a> .
<b>Дополнительная</b>		
1	Пользовательская документация	<a href="http://help.ubuntu.ru">http://help.ubuntu.ru</a>
2	Документация по ОС Linux	<a href="https://linuxcookbook.ru">https://linuxcookbook.ru</a>

#### 6.3 Перечень электронных образовательных ресурсов \*

№ п/п	Электронный образовательный ресурс	Доступ в ЭОР (сеть Интернет, локальная сеть, авторизованный/свободный доступ)
1	Учебник по администрированию Linux	<a href="https://coderlessons.com/tutorials/devops/izuchite-linux-admin/uchebnik-po-administirovaniu-linux">https://coderlessons.com/tutorials/devops/izuchite-linux-admin/uchebnik-po-administirovaniu-linux</a>

#### 6.4 Современные профессиональные базы данных, информационные справочные системы и лицензионное программное обеспечение

Современные профессиональные базы данных, информационные справочные системы, цифровые электронные библиотеки и другие электронные образователь-

## ные ресурсы

### Современные профессиональные базы данных, информационные справочные системы, цифровые электронные библиотеки и другие электронные образовательные ресурсы

1. Договор о подключении к Национальной электронной библиотеке и предоставлении доступа к объектам Национальной электронной библиотеки №101/НЭБ/0502-п от 26.02.2020 5 лет с пролонгацией
2. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 27.04.2016 бессрочно
3. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 02.03.2020 бессрочно
4. Информационно-справочная система «Гарант» – URL: <https://www.garant.ru/> Информационно-справочная система Лицензионный договор № 261709/ОП-2 от 25.06.2021
5. «Консультант Плюс». – URL: <http://www.consultant.ru/> свободный доступ
6. Электронно-библиотечная система AgriLib <http://ebs.rgunh.ru/> (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014).

### Доступ к электронной информационно-образовательной среде, информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения Moodle [www.portfolio.rgunh.ru](http://www.portfolio.rgunh.ru) (свободно распространяемое)
2. Право использования программ для ЭВМ Mirapolis HCM в составе функциональных блоков и модулей: Виртуальная комната.
3. Инновационная система тестирования – программное обеспечение на платформе 1С (Договор № К/06/03 от 13.06.2017). Бессрочный.
4. Образовательный интернет – портал Российского государственного аграрного заочного университета (свидетельство о регистрации средства массовой информации Эл № ФС77-51402 от 19.10.2012).

### Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice – свободный пакет офисных приложений (свободно распространяемое)
2. linuxmint.com <https://linuxmint.com/> (свободно распространяемое)
3. Электронно-библиотечная система AgriLib <http://ebs.rgunh.ru/> (свидетельство о государственной регистрации базы данных № 2014620472 от 21.03.2014) собственность университета.
4. Официальная страница ФГБОУ ВО «Российский государственный университет народного хозяйства имени В.И. Вернадского» <https://vk.com/rgunh> (свободно распространяемое)
5. Антивирусное программное обеспечение Dr. WEB Desktop Security Suite (Сублицензионный договор № 13740 на передачу неисключительных прав на программы для ЭВМ от 01.07.2021).

## 6.5 Перечень учебных аудиторий, оборудования и технических средств обучения

Учебная аудитория для проведения лекционных занятий (поточная). Специализированная мебель, экран рулонный настенный, Персональный компьютер в сборке с выходом в интернет	143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 501 Площадь помещения 73,2 кв.м № по технической инвентаризации 501, этаж 5
---	--

<p>Учебная аудитория для занятий лекционного типа, семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы), для проведения групповых консультаций и индивидуальной работы обучавшихся с педагогическими работниками, для проведения текущего контроля и промежуточной аттестации. Специализированная мебель, доска меловая. Персональные компьютеры в сборке с выходом в интернет.</p>	<p>143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 413 № по технической инвентаризации 413, этаж 4</p>
<p>Помещение для самостоятельной работы. Персональные компьютеры в сборке с выходом в интернет.</p>	<p>143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, читальный зал Площадь помещения 497,4 кв. м. № по технической инвентаризации 177, этаж 1</p>
<p>Помещение для самостоятельной работы. Специализированная мебель, персональные компьютеры в сборке с выходом в интернет.</p>	<p>143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 320 Площадь помещения 49,7 кв. м. № по технической инвентаризации 313, этаж 3</p>
<p>Учебная аудитория для учебных занятий обучающихся из числа инвалидов и лиц с ОВЗ. Специализированная мебель. Автоматизированное рабочее место для инвалидов-колясочников с коррекционной техникой и индукционной системой ЭлСис 290; Автоматизированное рабочее место для слабовидящих и незрячих пользователей со стационарным видеоувеличителем ЭлСис 29 ON; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с портативным видеоувеличителем ЭлСис 207 CF; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с читающей машиной ЭлСис 207 CN; Аппаратный комплекс с функцией видеоувеличения и чтения для слабовидящих и незрячих пользователей ЭлСис 207 OS.</p>	<p>143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, каб. 105 Площадь помещения 52,8 кв. м. № по технической инвентаризации 116, этаж 1</p>

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ  
**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО  
ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»**  
(Университет Вернадского)

**Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине**

**Информационная безопасность и защита информации**

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль) программы: Прикладная информатика в энергетических системах

Квалификация бакалавр

Форма обучения: **очная, очно-заочная**

Балашиха 2026г.

## 1. Описание показателей и критериев оценивания планируемых результатов обучения по учебной дисциплине

Компетенций	Уровень освоения*	Планируемые результаты обучения	Наименование оценочного средства
ПК-1 Способен выполнять и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	<b>Пороговый (удовлетворительно)</b>	<p><b>Знает:</b> процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами.</p> <p><b>Умеет:</b> определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации.</p> <p><b>Владеет:</b> интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного ПО, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.</p>	Выполнение практического задания Итоговое тестирование
	<b>Продвинутый (хорошо)</b>	<p><b>Твердо знает:</b> процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической под-</p>	Выполнение практического задания

		<p>держки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами.</p> <p><b>Уверенно умеет:</b> определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации.</p> <p><b>Уверенно владеет:</b> интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного ПО, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.</p>	Итоговое тестирование
	<p><b>Высокий (отлично)</b></p>	<p><b>Сформировавшееся систематическое знание:</b> процесс согласования и утверждения требований к типовой ИС; основы инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика;</p>	<p>Выполнение практического задания Итоговое тестирование</p>

		<p>процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения прямо-сдаточных испытаний (валидации) ИС в соответствии с установленными регламентами.</p> <p><b>Сформировавшееся систематическое умение:</b> определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации.</p> <p><b>Сформировавшееся систематическое владение:</b> интеграционного тестирование ИС; настройки оборудования, необходимого для работы ИС; адаптации бизнес-процессов заказчика к возможностям типовой ИС; выявления требований к типовой ИС; разработки прототипов ИС на базе типовой ИС; кодирования на языках программирования; создания пользовательской документации к модифицированным элементам типовой ИС; установки и настройка системного и прикладного ПО, необходимого для функционирования ИС; проведения аудитов качества в соответствии с планами проведения аудита.</p>	
--	--	---	--

## 2. Описание шкал оценивания

### 2.1 Шкала оценивания на этапе текущего контроля

\* Студенты, показавшие уровень усвоения ниже порогового, не допускаются к промежуточной аттестации по дисциплине.

Форма текущего контроля	Отсутствие усвоения (ниже порогового)*	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Выполнение практического задания	не выполнена или все задания решены неправильно	Решено более 50% задания, но менее 70%	Решено более 70% задания, но есть ошибки	все задания решены без ошибок
Тест	Менее 51%	51-79%	80-90%	91% и более

### 2.2 Шкала оценивания на этапе промежуточной аттестации (зачет и экзамен в виде итогового теста, курсовая работа)

Форма промежуточной аттестации	Отсутствие усвоения (ниже порогового)	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Выполнение итоговых тестов (не менее 15 вопросов на вариант)	Менее 51%	51-79%	80-90%	91% и более

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### КОМПЛЕКТ ТЕСТОВ для промежуточной аттестации (зачет) по дисциплине Информационная безопасность

Задания открытого типа – 2 мин. на ответ, задания закрытого типа – 5 мин. на ответ.

№ п.п	Задание	Варианты ответов	Формируемая компетенция
Задания закрытого типа			
1.	Основная масса угроз информационной безопасности приходится на:	Троянские программы  Шпионские программы  Черви	ПК-1
2.	Какой вид идентификации и аутентификации получил наибольшее распространение:	системы PKI  постоянные пароли  одноразовые пароли	ПК-1
3.	Какие угрозы безопасности информации являются преднамеренными:	ошибки персонала  открытие электронного письма, содержащего вирус  не авторизованный доступ	ПК-1
4.	Системой криптографической защиты информации является:	BFox Pro  CAudit  Крипто Про	ПК-1
5.	Под информационной безопасностью	защищенность информации и поддерживающей инфраструктуры	ПК-1

	понимается:	от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре  программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия  нет верного ответа	
Задания открытого типа (в т.ч. примерные вопросы к зачету/экзамену)			
1.	Информационная безопасность-		ПК-1
2.	Защита информации—это...		ПК-1
3.	Поясните термин «Конфиденциальность»?		ПК-1
4.	Для чего создаются информационные системы?		ПК-1
5.	Что такое Процедура?		ПК-1
6.	Виды информационной безопасности		ПК-1
7.	Основны риски информационной безопасности		ПК-1
8.	ЭЦП – это?		ПК-1
9.	Ошибки эксплуатации и неумышленного изменения режима работы системы		ПК-1
10.	Наиболее распространены средства воздействия на сеть офиса в контексте нарушения информационной безопасности?		ПК-1