

год начала подготовки 2022

Документ подписан квалифицированной электронной подписью

Сертификат: 03561B9E0021AE10B3437E3B0B4C07E21A3

Владелец: "АНО ВО «РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ»"; АН

Действителен с 2022-01-26 по 2022-01-26

**АНО ВО «Российский новый университет»**

**Елецкий филиал Автономной некоммерческой организации высшего образования «Российский новый университет»  
(Елецкий филиал АНО ВО «Российский новый университет»)**

кафедра прикладной экономики

**Рабочая программа учебной дисциплины (модуля)**

Информационная безопасность  
(наименование учебной дисциплины (модуля))

09.03.03 Прикладная информатика  
(код и направление подготовки/специальности)

Прикладная информатика в экономике  
(код и направление подготовки/специальности, в случаях, если программа разработана для разных направлений подготовки/специальностей)

---

Рабочая программа учебной дисциплины (модуля) рассмотрена и утверждена на заседании кафедры «26» января 2022, протокол № 5.

Заведующий кафедрой Прикладной экономики  
(название кафедры)

к.э.н., доцент Преснякова Д.В.

(ученая степень, ученое звание, фамилия и инициалы, подпись заведующего кафедрой)

Елец  
2022 год

## **1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

Учебная дисциплина «Информационная безопасность» изучается обучающимися, осваивающими образовательную программу «Прикладная информатика» по профилю Прикладная информатика в экономике в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденным приказом Министерства образования и науки РФ от 19.09.2017 N 922 (ФГОС ВО 3++).

Целью изучения дисциплины является обучение студентов основным понятиям, положениям и методам курса «Информационная безопасность для подготовки специалистов, владеющих знаниями и умениями в области современных информационных технологий и практических навыков по их применению. В процессе изучения курса студенты знакомятся с основными тенденциями информатизации, овладевают практическими навыками в использовании информационных технологий в различных областях производственной, управленческой и коммерческой деятельности. Важное значение в процессе обучения приобретает овладение навыками самостоятельной ориентации в многообразном рынке средств реализации ИТ.

Изучение учебной дисциплины направлено на подготовку обучающихся к осуществлению деятельности по концептуальному, функциональному и логическому проектированию систем среднего и крупного масштаба и сложности, планированию разработки или восстановления требований к системе, анализу проблемной ситуации заинтересованных лиц, разработке бизнес-требований заинтересованных лиц, постановки целей создания системы, разработки концепции системы и технического задания на систему, организации оценки соответствия требованиям существующих систем и их аналогов, представлению концепции, технического задания на систему и изменений в них заинтересованным лицам, организации согласования требований к системе, разработке шаблонов документов требований, постановке задачи на разработку требований к подсистемам и контроль их качества, сопровождению приемочных испытаний и ввода в эксплуатацию системы, обработке запросов на изменение требований к системе, определенных профессиональным стандартом «Системный аналитик», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 28.10.2014 N 809н (Регистрационный номер №34882).

## **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Учебная дисциплина Информационная безопасность относится к обязательной части учебного плана и изучается на 3, 4 курсе.

2.1. Требования к предварительной подготовке обучающегося:

Изучению данной учебной дисциплины предшествует освоение следующих учебных дисциплин: Информатика и программирование, Информационные системы и технологии, Программная инженерия, Вычислительные системы, сети и телекоммуникации, Операционные системы.

Параллельно с учебной дисциплиной «Информационная безопасность» изучаются дисциплины: Внедрение информационных систем, Реинжиниринг процессов, Системная архитектура, Системы информационной безопасности, Управление информационными системами.

2.2. Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Результаты освоения дисциплины «Информационная безопасность» являются базой для прохождения обучающимися производственной практики: преддипломной. Развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств обеспечивается чтением лекций по всем темам,

проведением семинарских занятий, нацеленных на профессиональную деятельности выпускников и потребности работодателей.

### 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины обучающийся по программе бакалавриата должен овладеть:

*- Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; (ОПК-3)*

#### Планируемые результаты обучения по дисциплине

Формируемая компетенция	Планируемые результаты обучения	Код показателя результатов обучения
Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности – ОПК -3	<b><u>Знать:</u></b>	
	- основы информационной безопасности и защиты информации.	ОПК-3-31
	- главные требования к организации эффективного функционирования системы ИБ.	ОПК-3-32
	- методы анализа информационных рисков и структур нарушения ИБ.	ОПК-3-33
	- методы оценки уровня безопасности корпоративной информационной системы.	ОПК-3-34
	<b><u>Уметь</u></b>	
	- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.	ОПК-3-У1
	- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.	ОПК-3-У2
	- осуществлять формализацию постановки и решения задач обеспечения ИБ компьютерных систем и сетей.	ОПК-3-У3
	- проводить анализ компьютерных систем и сетей с точки зрения обеспечения их ИБ.	ОПК-3-У4
	<b><u>Владеть</u></b>	
	- широкой общей подготовкой (базовыми знаниями) для решения практических задач в области информационных систем и технологий.	ОПК-3-В1
	- навыками принятия организационно-управленческих решений в нестандартных ситуациях. Быть готовыми нести за них ответственность.	ОПК-3-В2
- одним из иностранных языков на уровне не ниже разговорного.	ОПК-3-В3	
- основами построения и эксплуатации информационных систем.	ОПК-3-В4	

### 4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа).

## Общий объем учебной дисциплины

№	Форма обучения	Семестр/сессия, курс	Общая трудоемкость		в том числе контактная работа с преподавателем							СР	Контроль
			в з.е.	в часах	Всего	Л	ПР	КоР	зачет	Конс	экзамен		
1.	Очная	8 семестр, 4 курс	4	144	52	20	28	1,6		2	0,4	58,4	33,6
		Итого:	4	144	52	20	28	1,6		2	0,4	58,4	33,6
2	Заочная	2 сессия, 3 курс	1	36	4	4						32	
		1 сессия, 4 курс	3	108	12	4	4	1,6		2	0,4	89,4	6,6
		Итого	4	144	16	8	4	1,6		2	0,4	121,4	6,6

Распределение учебного времени по темам и видам учебных занятий  
очная форма обучения

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем							СР	Контроль	Формируемые результаты обучения
			Всего	Л	ПЗ	КоР	зачет	Конс	экзамен			
1	2	3	4	5	6	7	8	9	10	11	12	13
1.	<b>Модуль 1. Введение в безопасность информации современного предприятия</b>											
2.	1. Основные понятия, термины и определения в области защиты информации	12	6	2	4					6		ОПК-3-31 ОПК-3-32
3.	2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.	12	6	2	4					6		ОПК-3-34 ОПК-3-У1 ОПК-3-У2
4.	3. Законодательная и нормативная база правового регулирования вопросов защиты информации.	12	6	2	4					6		ОПК-3-33 ОПК-3-34 ОПК-3-У1
5.	4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	12	6	2	4					6		ОПК-3-33 ОПК-3-У1 ОПК-3-У2
6.	<b>Модуль 2. Технологии обеспечения информационной безопасности предприятия</b>											
7.	5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	16	6	2	4					10		ОПК-3-У2 ОПК-3-У4 ОПК-3-В4
8.	6. Меры и средства защиты информации	16	6	2	4					10		ОПК-3-У3 ОПК-3-В2

9.	7. Применения криптографических методов защиты информации при работе в сетях.	12	4	2	2					8		ОПК-3-У3 ОПК-3-В3
10.	8. Аудит информационной безопасности	14	8	6	2					6		ОПК-3-У3 ОПК-3-В3
11.	<i>Промежуточная аттестация (экзамен)</i>	4	4			1,6		2	0,4			
12.	<b>ИТОГО:</b>	<b>144</b>	<b>54</b>	<b>20</b>	<b>28</b>	<b>1,6</b>		<b>2</b>	<b>0,4</b>	<b>54</b>	<b>33,6</b>	

## заочная форма обучения

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем							СР	Контроль	Формируемые результаты обучения
			Всего	Л	ПЗ	Кор	зачет	Конс	экзамен			
1	2	3	4	5	6	7	8	9	10	11	12	13
13.	<b>Модуль 1. Введение в безопасность информации современного предприятия</b>											
14.	1. Основные понятия, термины и определения в области защиты информации	13	1	1						12		ОПК-3-31 ОПК-3-32
15.	2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.	13	1	1						12		ОПК-3-34 ОПК-3-У1 ОПК-3-У2
16.	3. Законодательная и нормативная база правового регулирования вопросов защиты информации.	14	2	1	1					12		ОПК-3-33 ОПК-3-34 ОПК-3-У1
17.	4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.	13	1	1						12		ОПК-3-33 ОПК-3-У1 ОПК-3-У2
18.	<b>Модуль 2. Технологии обеспечения информационной безопасности предприятия</b>											
19.	5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	14	2	1	1					12		ОПК-3-У2 ОПК-3-У4 ОПК-3-В4
20.	6. Меры и средства защиты информации	13	1	1						12		ОПК-3-У3 ОПК-3-В2
21.	7. Применения криптографических методов защиты информации при работе в сетях.	18	2	1	1					16		ОПК-3-У3 ОПК-3-В3
22.	8. Аудит информационной безопасности	21,4	2	1	1					19,4		ОПК-3-У3 ОПК-3-В3

23.	<i>Промежуточная аттестация (Экзамен)</i>	18	4			1,6		2	0,4	14		
24.	<b>ИТОГО:</b>	<b>144</b>	<b>16</b>	<b>8</b>	<b>4</b>	<b>1,6</b>		<b>2</b>	<b>0,4</b>	<b>121,4</b>	<b>6,6</b>	

## **5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ)**

### **Модуль 1. Введение в безопасность информации современного предприятия.**

#### **Тема 1. Основные понятия, термины и определения в области защиты информации.**

Информация, информационные отношения, субъекты информационных отношений, их интересы и пути нанесения им ущерба. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации.

Литература:

а) основная: 1-2.

б) дополнительная: 3-6.

#### **Тема 2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.**

Формирование модели угроз: угрозы, реализуемые через технические каналы утечки информации, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах или вспомогательных технических средствах и системах; угрозы, реализуемые за счет несанкционированного доступа к персональным данным. Модель угроз и модель нарушителя информационной безопасности. Риски информационной безопасности.

Литература:

а) основная: 1-2.

б) дополнительная: 3-6.

#### **Тема 3. Законодательная и нормативная база правового регулирования вопросов защиты информации.**

Доктрина информационной безопасности Российской Федерации. Федеральные законы Российской Федерации. Постановления правительства Российской Федерации. Указы Президента Российской Федерации. Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации. Порядок проведения инвентаризации персональных данных.

Литература:

а) основная: 1-2.

б) дополнительная: 3-6.

#### **Тема 4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.**

Подготовка к аттестации на соответствие положениям ФЗ №152 Национальные (ГОСТ), международные и отраслевые стандарты в области защиты информации, информационных технологий и непрерывности бизнеса. Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства РФ. Ответственность за правонарушения в области защиты информации.

Литература:

а) основная: 1-2.

б) дополнительная: 3-б.

## **Модуль 2. Технологии обеспечения информационной безопасности предприятия.**

### **Тема 5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии.**

Комплексная система обеспечения информационной безопасности организации. Организационная структура системы обеспечения информационной безопасности организации. Типовая структура, задачи и функции подразделения (службы) информационной безопасности организации. Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности.

#### Литература:

а) основная: 1-2.

б) дополнительная: 3-б.

### **Тема 6. Методы и средства защиты информации и персональных данных.**

Разработка и построение системы защиты персональных данных. Система управления непрерывностью бизнеса организации в соответствии с требованиями стандарта BS25999. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам. Средства защиты информации от ее утечки по техническим каналам. Защита сети электропитания и заземления.

Экономические аспекты обеспечения безопасности. Риск-ориентированный подход в информационной безопасности.

#### Литература:

а) основная: 1-2.

б) дополнительная: 3-б.

### **Тема 7. Применения криптографических методов защиты информации при работе в сетях.**

Обеспечение безопасности информации при подключении вычислительных средств к международным информационным системам.

Криптографические методы и средства защиты информации. Специфика инфраструктуры открытых ключей. Обеспечение безопасности типовых технологических процессов организации с использованием средств криптографической защиты, электронная подпись.

#### Литература:

а) основная: 1-2.

б) дополнительная: 3-б.

### **Тема 8. Аудит информационной безопасности.**

Самооценка и аудит как показатели эффективности процессов обеспечения информационной безопасности.

Роли, цели и задачи аудита в процессе обеспечения информационной безопасности.

#### Литература:

а) основная: 1-2.

б) дополнительная: 3-б.

**Планы семинарских, практических, лабораторных занятий**  
очная форма обучения

**Тема. Практическое занятие: Законодательная и нормативная база правового регулирования вопросов защиты информации.**

Продолжительность занятия - 4 часа

Основные вопросы:

1. Доктрина информационной безопасности Российской Федерации.
2. Федеральные законы Российской Федерации. Классификация рисков ИБ.

**Тема. Практическое занятие: Политика безопасности и формирование организационной структуры системы защиты информации на предприятии.**

Продолжительность занятия - 4 часа

Основные вопросы:

1. Понятие политики безопасности предприятия.
2. Формирование организационной структуры СЗИ в организации.

**Тема. Практическое занятие: Применения криптографических методов защиты информации при работе в сетях.**

Продолжительность занятия - 4 часа

Основные вопросы:

1. Использование открытых и закрытых ключей.
2. Шифр Цезаря.
3. Шифр Виженера.

**Тема. Практическое занятие: Аудит информационной безопасности.**

Продолжительность занятия - 4 часа

Основные вопросы:

1. Роли, цели и задачи аудита в процессе обеспечения информационной безопасности.
2. Этапы аудита ИБ.

**Планы семинарских, практических, лабораторных занятий**  
заочная форма обучения

**Тема. Практическое занятие: Законодательная и нормативная база правового регулирования вопросов защиты информации.**

Продолжительность занятия - 1 час

Основные вопросы:

1. Доктрина информационной безопасности Российской Федерации.
2. Федеральные законы Российской Федерации. Классификация рисков ИБ.

**Тема. Практическое занятие: Политика безопасности и формирование организационной структуры системы защиты информации на предприятии.**

Продолжительность занятия - 1 час

Основные вопросы:

1. Понятие политики безопасности предприятия.
2. Формирование организационной структуры СЗИ в организации.

**Тема. Практическое занятие: Применения криптографических методов защиты информации при работе в сетях.**

Продолжительность занятия - 1 час



Основные вопросы:

1. Использование открытых и закрытых ключей.
2. Шифр Цезаря.
3. Шифр Виженера.

**Тема. Практическое занятие: Аудит информационной безопасности.**

Продолжительность занятия - 1 час

Основные вопросы:

1. Роли, цели и задачи аудита в процессе обеспечения информационной безопасности.
2. Этапы аудита ИБ.

## **6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

### 6.1. Задания для повторения и углубления приобретаемых знаний.

№	Код результата обучения	Задания
1.	ОПК-3-31	Охарактеризуйте основные методы защиты информации
2.	ОПК-3-31	Проведите сравнительный анализ программного обеспечения на рынке информационной безопасности
3.	ОПК-3-32	Назовите основные стандарты безопасности
4.	ОПК-3-32	Назовите типовые программно-аппаратные средства и системы защиты информации в системах связи от несанкционированного доступа
5.	ОПК-3-33	Опишите современные подходы к построению систем защиты информации
6.	ОПК-3-33	Назовите критерии оценки защищенности ИС
7.	ОПК-3-34	Что такое политика и процедуры обеспечения ИБ
8.	ОПК-3-34	Сформулируйте требования к защите персональных данных

### 6.2. Задания, направленные на формирование профессиональных умений

№	Код результата обучения	Задания
9.	ОПК-3-У1	Разработайте требования к защищенной информационной системе
10.	ОПК-3-У1	Классифицируйте современные технологии информационной безопасности
11.	ОПК-3-У2	Сделайте сравнительный анализ методов формальной постановки и решения задачи обеспечения ИБ компьютерных систем и сетей
12.	ОПК-3-У2	Представьте структуру технико-экономического обоснования
13.	ОПК-3-У3	Проанализируйте базовые понятия ГОСТ Р 15408
14.	ОПК-3-У3	Проанализировать информационную инфраструктуру объекта и его безопасности
15.	ОПК-3-У4	Проанализируйте меры противодействия угрозам ИБ с использованием различных программно-аппаратных средств защиты
16.	ОПК-3-У4	Разработайте модель телекоммуникационных систем и информационной безопасности, используя известные подходы, методы, средства и теоретические основы

## 6.3. Задания, направленные на формирование профессиональных навыков, владений.

№	Код результата обучения	Задания
17.	ОПК-3-В1	Проанализируйте основные угрозы информационному обеспечению государственной политики Российской Федерации
18.	ОПК-3-В1	Разработайте требования и общую стратегию построения системы ИБ
19.	ОПК-3-В2	Выберите профили защиты в зависимости от модели угроз
20.	ОПК-3-В2	Проведите обзор современной научно-технической информации проблемам и задачам информационной безопасности
21.	ОПК-3-В3	Графически проиллюстрировать соотношения программных, аппаратных и административных средств в комплексном обеспечении
22.	ОПК-3-В3	Проанализируйте процесс организационного обеспечения информационной безопасности автоматизированных систем обработки данных
23.	ОПК-3-В4	Оцените роли, цели и задачи аудита в процессе обеспечения информационной безопасности
24.	ОПК-3-В4	Проведите сравнительный анализ закона РФ «О коммерческой тайне» и Закона РФ «О персональных данных»

### 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

## 7.1. Средства оценивания текущего контроля:

- письменные краткие опросы в ходе аудиторных занятий на знание категорий учебной дисциплины;
- задания и упражнения, рекомендованные для самостоятельной работы;
- практическая работа;
- задания, упражнения и выполнение теста в ходе практических занятий.

## 7.2. ФОС для текущего контроля

№	Показатели результата обучения	ФОС текущего контроля
1	ОПК-3-31	Письменный опрос на занятиях на знание категорий учебной дисциплины; Задания для повторения и приобретения знаний 1-2.
2	ОПК-3-32	Задания для и приобретения, закрепления и углубления знаний 3-4
3	ОПК-2-33	Задания для и приобретения, закрепления и углубления знаний 5-6
4	ОПК-3-34	Задания для и приобретения, закрепления и углубления знаний 7-8
5	ОПК-3-У1	Задания, направленные на формирование профессиональных умений 9-10
6	ОПК-3-У2	Задания, направленные на формирование профессиональных умений 11-12
7	ОПК-3-У3	Задания, направленные на формирование профессиональных умений 13-14
8	ОПК-3-У4	Задания, направленные на формирование профессиональных умений 15-16
13	ОПК-3-В1	Задания, направленные на формирование профессиональных навыков, владений 17-18

14	ОПК-3-В2	Задания, направленные на формирование профессиональных навыков, владений 19-20
15	ОПК-3-В3	Задания, направленные на формирование профессиональных навыков, владений 21-22
16	ОПК-3-В4	Задания, направленные на формирование профессиональных навыков, владений 23-24

## 7.3 ФОС для промежуточной аттестации

## 7.3.1.Задания для оценки знаний

№	Показатели результата обучения	ФОС для оценки знаний
1	ОПК-3-31	<p>Вопросы к экзамену 1-15</p> <ol style="list-style-type: none"> <li>1. Информация как объект правового регулирования.</li> <li>2. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.</li> <li>3. Законодательство РФ в области информационной безопасности.</li> <li>4. Информационная безопасность объекта при осуществлении международного сотрудничества.</li> <li>5. Виды угроз информационной безопасности.</li> <li>6. Угрозы конституционным правам и свободам гражданина в области информационной деятельности.</li> <li>7. Угрозы информационному обеспечению государственной политики Российской Федерации.</li> <li>8. Угрозы безопасности информационных и телекоммуникационных средств и систем.</li> <li>9. Внешние и внутренние источники угроз информационной безопасности.</li> <li>10. Основные виды угроз безопасности субъектов информационных отношений.</li> <li>11. Основные непреднамеренные и преднамеренные искусственные угрозы.</li> <li>12. Основные преднамеренные искусственные угрозы.</li> <li>13. Закон РФ от 21.09.93 "О государственной тайне".</li> <li>14. Закон РФ от 09.07.2004г. «О коммерческой тайне».</li> <li>15. Закон РФ от 08.07.2006г. «О персональных данных».</li> </ol>
2	ОПК-3-32	<p>Вопросы к экзамену 16-30</p> <ol style="list-style-type: none"> <li>16. «Концепция защиты СВТ и АС от НСД», предназначение, основные понятия и направления.</li> <li>17. Основные принципы защиты от НСД, изложенные в нормативных документах концепции защиты СВТ и АС.</li> <li>18. Свойства защищенных автоматизированных систем обработки информации.</li> <li>19. Специфика возникновения угроз и рисков в открытых сетях.</li> <li>20. Что понимается под уязвимостью защищенных компьютерных систем?</li> <li>21. Основные направления обеспечения информационной</li> </ol>

		<p>безопасности в компьютерных системах.</p> <p>22.Основные понятия безопасности компьютерных систем.</p> <p>23.Что понимается под лицензированием деятельности в области защиты информации?</p> <p>24.Перечислить основные мероприятия, позволяющие решить задачу построения системы защиты рабочей станции.</p> <p>25.Для чего используются системы многоуровневой защиты?</p> <p>26.Какие вы знаете аспекты защиты информации в системе с разграничением полномочий?</p> <p>27.Перечислите и дайте характеристику основным методам построения систем защиты с многоуровневым доступом.</p> <p>28.Какое место занимает механизм подотчетности в политике безопасности и, на какие категории делятся средства подотчетности?</p> <p>29.Какие проблемы возникают при использовании защиты информации путем ограничения доступа?</p> <p>30.Какие принципы положены в концепцию построения защищенных систем?</p>
3	ОПК-3-33	<p>Вопросы к экзамену 31-45</p> <p>31.Перечислить и дать характеристику основным компонентам защищенной компьютерной системы.</p> <p>32.Каким способом происходит интеграция средств защиты и распространенных приложений в защищенной компьютерной системе?</p> <p>33.Что понимается под несанкционированным доступом к информации.</p> <p>34.Перечислить и дать характеристику обобщенным методам защиты от НСД.</p> <p>35.Что понимается под стойкостью системы идентификации?</p> <p>36.Что является интегральной характеристикой защищенной системы?</p> <p>37.Понятие политики безопасности и её основные базовые представления.</p> <p>38.В каких случаях используют модели безопасности производители защищенных компьютерных систем?</p> <p>39.Из каких частей состоит ГОСТ Р 15408?</p> <p>40.На каких базовых представлениях основаны модели безопасности?</p> <p>41.Какие элементы должна включать в себя политика безопасности организации?</p> <p>42. В чем различие субъекта компьютерной системы от человека-пользователя?</p> <p>43.Какими качествами должен обладать монитор обращений?</p> <p>44.Как определяется доверенная система в ГОСТ Р 15408, и по каким критериям оценивается степень доверия?</p> <p>45.Показатели защищенности СВТ от НСД.</p>
4	ОПК-3-34	<p>Вопросы к экзамену 46-60</p> <p>46.Для каких целей разрабатывался ГОСТ Р 15408?</p> <p>47.Базовые понятия ГОСТ Р 15408.</p>

		<p>48.Что включает в себя процесс квалификационного анализа в соответствии с ГОСТ Р 15408?</p> <p>49.Структура Профиля защиты ГОСТ Р 15408.</p> <p>50.Основные разделы ГОСТ Р 15408.</p> <p>51.Что понимается под оценочным стандартом и технической спецификацией.</p> <p>52.Основные понятия закона «Об электронной подписи».</p> <p>53.Критерии классификации угроз компьютерным системам.</p> <p>54.Каковы недостатки традиционного подхода к информационной безопасности с объектной точки зрения?</p> <p>55.Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.</p> <p>56.Что понимается под сертификацией средств защиты информации? Перечислить основные схемы сертификации.</p> <p>57.Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.</p> <p>58.Что понимается под категорированием средств защиты информации?</p> <p>59.Для каких целей мы можем использовать понятие лицензирование деятельности в области защиты информации.</p> <p>60.Что понимается под анализом рисков в компьютерной системе?</p>
--	--	--

## Задания для оценки умений.

№	Код результата обучения	Задания
1.	ОПК-3-У1-У.4	В качестве фонда оценочных средств для оценивания умений обучающегося используются задания 9-16, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.2.)

## Задания для оценивания навыков, владений, опыта деятельности

№	Код результата обучения	Задания
1	ОПК-6-В1-В.4	В качестве фонда оценочных средств для оценивания навыков, владений, опыта деятельности обучающегося используются задания 17-24, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.3), а также задания, для практической работы.

## 8. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 8.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450371>

2. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449350>

## **8.2. Дополнительная литература**

1. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 с. — 978-5-4487-0299-0. — Режим доступа: <http://www.iprbookshop.ru/77318.html>
2. Семененко В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)
3. Информационная безопасность: учебно-методич. комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

## **9. ПЕРЕЧЕНЬ КОМПЛЕКТОВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**

При изучении учебной дисциплины (в том числе в интерактивной форме) предполагается применение современных информационных технологий. Комплект программного обеспечения для их использования включает в себя: операционная система Microsoft Windows 7 Pro, офисный пакет программ Microsoft Office Professional Plus 2010, офисный пакет программ Microsoft Office Professional Plus 2007, антивирусная программа Dr. Web Desktop Security Suite, архиватор 7-zip, аудиопроигрыватель AIMP, просмотр изображений FastStone Image Viewer, ПО для чтения файлов формата PDF Adobe Acrobat Reader, ПО для сканирования документов NAPS2, ПО для записи видео и проведения видеотрансляций OBS Studio, ПО для удалённого администрирования Aspia, правовой справочник Гарант Аэро, онлайн-версия КонсультантПлюс: Студент, электронно-библиотечная система IPRBooks, электронно-библиотечная система Юрайт, математические вычисления Mathcad 14 University, версия 1С для обучения программированию: 1С: Предприятие 8.2 Версия для обучения программированию

## **10. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

### **10.1. Интернет- ресурсы**

1. <http://citforum.ru/> Сервер информационных технологий. Содержит большое количество информации по всем областям ИТ-технологий, в том числе новости ИТ-мира
2. <http://www.intuit.ru/> Образовательный проект, главными целями которого являются свободное распространение знаний во Всемирной Сети и предоставление услуг дистанционного обучения.
3. <http://www.microsoft.com/rus/> Официальная страница Microsoft
4. <http://www.infoforum.ru/> Национальный форум информационной безопасности «Инфофорум»
5. <http://www.securitylab.ru> Информационный портал по безопасности SecurityLab.ru
6. <http://www.fstec.ru> Официальный сайт Федеральной службы по техническому и экспортному контролю.
7. ЭБС IPRbooks (АйПиАрбукс) <http://www.iprbookshop.ru>
8. Образовательная платформа ЮРАЙТ <https://urait.ru>

## **11. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ.**

Изучение учебной дисциплины « Информационная безопасность» обучающимися инвалидами и лицами с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства образования и науки РФ от 9 ноября 2015 г. № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи» (с изменениями и дополнениями), Методическими рекомендациями по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса, утвержденными Министерством образования и науки РФ 08.04.2014г. № АК-44/05вн, Положением об организации обучения студентов – инвалидов и лиц с ограниченными возможностями здоровья, утвержденным приказом ректора Университета от 6 ноября 2015 года №60/о, Положением о Центре инклюзивного образования и психологической помощи АНО ВО «Российский новый университет», утвержденного приказом ректора от 20 мая 2016 года № 187/о.

Лица с ограниченными возможностями здоровья и инвалиды обеспечиваются электронными образовательными ресурсами, адаптированными к состоянию их здоровья.

Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом индивидуальных психофизиологических особенностей обучающихся и специфики приема-передачи учебной информации на основании просьбы, выраженной в письменной форме.

С обучающимися по индивидуальному плану или индивидуальному графику проводятся индивидуальные занятия и консультации.

## **12. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации

Ауд. 403 (компьютерный класс № 4)

Специализированная мебель:

- столы студенческие;
- стулья студенческие;
- стол для преподавателя;
- стул для преподавателя;
- столы компьютерные;
- кресла компьютерные;
- шкаф для хранения раздаточного материала;
- доска (меловая);
- маркерная доска (переносная).

Технические средства обучения:

- проектор;
- ПК для преподавателя с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза;

год начала подготовки 2022

- ПК для с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза;

- веб-камера;

- экран;

- колонки;

- микрофон.

Специализированное оборудование:

- наглядные пособия (плакаты)

Автор (составитель): ст.преподаватель Суздальская Е.А.

  
(подпись)



## Аннотация рабочей программы учебной дисциплины

### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Код и направление подготовки 09.03.03 Прикладная информатика

#### Прикладная информатика в экономике

Учебная дисциплина «Информационная безопасность» изучается обучающимися, осваивающими образовательную программу «Прикладная информатика» по профилю Прикладная информатика в экономике в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденным приказом Министерства образования и науки РФ от 19.09.2017 N 922 (ФГОС ВО 3++).

Целью изучения дисциплины является обучение студентов основным понятиям, положениям и методам курса «Информационная безопасность для подготовки специалистов, владеющих знаниями и умениями в области современных информационных технологий и практических навыков по их применению. В процессе изучения курса студенты знакомятся с основными тенденциями информатизации, овладевают практическими навыками в использовании информационных технологий в различных областях производственной, управленческой и коммерческой деятельности. Важное значение в процессе обучения приобретает овладение навыками самостоятельной ориентации в многообразном рынке средств реализации ИТ.

Изучение учебной дисциплины направлено на подготовку обучающихся к осуществлению деятельности по концептуальному, функциональному и логическому проектированию систем среднего и крупного масштаба и сложности, планированию разработки или восстановления требований к системе, анализу проблемной ситуации заинтересованных лиц, разработке бизнес-требований заинтересованных лиц, постановки целей создания системы, разработки концепции системы и технического задания на систему, организации оценки соответствия требованиям существующих систем и их аналогов, представлению концепции, технического задания на систему и изменений в них заинтересованным лицам, организации согласования требований к системе, разработке шаблонов документов требований, постановке задачи на разработку требований к подсистемам и контроль их качества, сопровождению приемочных испытаний и ввода в эксплуатацию системы, обработке запросов на изменение требований к системе, определенных профессиональным стандартом «Системный аналитик», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 28.10.2014 N 809н (Регистрационный номер №34882).

Учебная дисциплина Информационная безопасность относится к обязательной части учебного плана и изучается на 3, 4 курсе.

В результате освоения дисциплины обучающийся должен овладеть

**ОПК-3 - способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**