

Министерство сельского хозяйства Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
"Воронежский государственный аграрный университет имени императора Петра I"

УТВЕРЖДАЮ  
Декан экономического факультета  
А.В. Агибалов  
«25» 2021г.



РАБОЧАЯ ПРОГРАММА ПО ДИСЦИПЛИНЕ  
**Б1.О.23 Информационная безопасность**

Направление: 09.03.03 Прикладная информатика

Профиль: Информационные системы и технологии в менеджменте АПК

Квалификация выпускника: бакалавр

Факультет Экономический

Кафедра Информационного обеспечения и моделирования агроэкономических систем

Разработчик рабочей программы:

Должность:

Ученая степень:

Ученое звание:

Горюхина Елена Юрьевна

доцент

кандидат экономических наук

доцент



Воронеж-2021

Рабочая программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) (утвержден приказом Министерства образования и науки РФ от 19 сентября 2017 № 922).

Рабочая программа утверждена на заседании кафедры Информационного обеспечения и моделирования агроэкономических систем (протокол № 10 от 01.06.2021 г.)

Заведующий кафедрой:



А.В. Улезько

Рабочая программа рекомендована к использованию в учебном процессе на заседании методической комиссии экономического факультета (протокол № 11 от 25.06.2021 г.)

Председатель методической комиссии:



Е.Б. Фалькович

Рецензент: руководитель группы по внедрению информационных технологий ООО «ИНКОНСАЛТ», к.э.н. М. О. Лепендин

## Содержание рабочей программы

1. Общая характеристика дисциплины
  - 1.1. Цель дисциплины
  - 1.2. Задачи дисциплины
  - 1.3. Предмет дисциплины
  - 1.4. Место в образовательной программе
  - 1.5. Связь с другими дисциплинами
  - 1.6. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья
2. Планируемые результаты изучения дисциплины
3. Объем дисциплины и виды учебной работы
  - 3.1. Очная форма обучения
  - 3.2. Заочная форма обучения
4. Содержание дисциплины
  - 4.1. Содержание дисциплины в разрезе разделов и подразделов
  - 4.2. Распределение контактной и самостоятельной работы по подразделам
5. Фонд оценочных средств
  - 5.1. Этапы формирования компетенций
  - 5.2. Шкалы и критерии оценивания достижения компетенций
    - 5.2.1. Шкалы академических оценок освоения дисциплины
    - 5.2.2. Критерии оценки достижения компетенций в ходе освоения дисциплины
  - 5.3. Материалы для оценки достижения компетенций
    - 5.3.1. Вопросы к экзамену
    - 5.3.2. Задания к экзамену
    - 5.3.3. Вопросы к зачету с оценкой
    - 5.3.4. Вопросы к зачету
    - 5.3.5. Темы курсового проекта (работы) и вопросы к защите
      - 5.3.4.1. Темы курсового проекта (работы)
      - 5.3.4.2. Вопросы к защите курсового проекта (работы)
    - 5.3.6. Вопросы тестов
    - 5.3.7. Вопросы для устного опроса
    - 5.3.8. Задания для проверки формирования умений и навыков
  - 5.4. Система оценивания достижения компетенций
    - 5.4.1. Оценка достижения компетенций в ходе промежуточной аттестации
    - 5.4.2. Оценка достижения компетенций в ходе текущего контроля
6. Учебно-методическое и информационное обеспечение дисциплины
  - 6.1. Рекомендуемая литература
  - 6.2. Ресурсы сети Интернет
    - 6.2.1. Электронные библиотечные системы
    - 6.2.2. Профессиональные базы данных и информационные системы
    - 6.2.3. Сайты и информационные порталы
7. Материально-техническое и программное обеспечение дисциплины
  - 7.1. Помещения для ведения образовательного процесса и оборудование
  - 7.2. Программное обеспечение
8. Междисциплинарные связи

## **1. Общая характеристика дисциплины**

### **1.1. Цель дисциплины:**

формирование знаний, умений и навыков проведения анализа информационных угроз для предприятий и организаций, обучение приемам защиты информационных ресурсов в профессиональной деятельности

### **1.2. Задачи дисциплины:**

формирование знаний основ в области информационной безопасности;

формирование знаний, умений и навыков обоснования мероприятий по обеспечению информационной безопасности;

формирование знаний, умений и навыков использования методов информационной безопасности в профессиональной деятельности;

формирование знаний, умений и навыков использования нормативно-правовых актов по вопросам информационной безопасности;

формирование знаний, умений и навыков использования инструментов, средств и методов обеспечения информационной безопасности;

формирование знаний, умений и навыков описания системы обеспечения информационной безопасности и управления информационной безопасностью.

### **1.3. Предмет дисциплины:**

методы и инструменты обеспечения информационной безопасности

### **1.4. Место в образовательной программе:**

обязательная часть

### **1.5. Взаимосвязь с другими дисциплинами:**

Б1.О.05 Право и основы противодействия коррупции

Б1.В.07 Обучение пользователей информационных систем

Б1.В.13 Управление IT-проектами

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

Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья определяются в индивидуальном порядке исходя из специфики заболевания и требований, указанных в Основной образовательной программе

## 2. Планируемые результаты изучения дисциплины

| Компетенция |   | Индикатор достижения компетенции |   |
|-------------|---|----------------------------------|---|
| Код         | Содержание  | Код                              | Содержание  |
| 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 | З1                               | основы личной информационной безопасности   |
|             |   | З6                               | основные информационной безопасности  |
|             |   | У1                               | применять методы обеспечения личной информационной безопасности   |
|             |   | У7                               | использовать инструменты и методы обеспечения информационной безопасности   |
|             |   | Н1                               | обеспечения личной информационной безопасности  |
|             |   | Н7                               | подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности |
|             |   | Н8                               | описания системы обеспечения информационной безопасности  |
| ОПК-4       | Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью   | З5                               | нормативное обеспечение информационной безопасности   |
|             |   | У6                               | использовать нормативно-правовые акты по вопросам информационной безопасности   |
|             |   | Н5                               | обоснования мероприятий по обеспечению информационной безопасности  |
| ПК-10       | Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью   | З5                               | принципы обеспечения информационной безопасности организации  |
|             |   | У5                               | управлять информационной безопасностью  |
|             |   | Н6                               | использования средств обеспечения информационной безопасности   |

### 3. Объем дисциплины и виды учебной работы

#### 3.1. Очная форма обучения

| Показатели  | Семестр | Всего   |
|---|---------|---------|
|   | 4       |         |
| Общая трудоёмкость, з.е./ч  | 3 / 108 | 3 / 108 |
| Общая контактная работа, ч  | 38,15   | 38,15   |
| Общая самостоятельная работа, ч   | 69,85   | 69,85   |
| Контактная работа при проведении учебных занятий, в т.ч. (ч)                      | 38,00   | 38,00   |
| лекции  | 20      | 20,00   |
| практические-всего  | 18      | 18,00   |
| Самостоятельная работа при проведении учебных занятий, ч                          | 61,00   | 61,00   |
| Контактная работа при проведении промежуточной аттестации обучающихся, в т.ч. (ч) | 0,15    | 0,15    |
| зачет   | 0,15    | 0,15    |
| Самостоятельная работа при промежуточной аттестации, в т.ч. (ч)                   | 8,85    | 8,85    |
| подготовка к зачету   | 8,85    | 8,85    |
| Форма промежуточной аттестации  | зачет   | зачет   |

### 3. Объем дисциплины и виды учебной работы

#### 3.2. Заочная форма обучения

| Показатели  | Курс    | Всего   |
|---|---------|---------|
|   | 3       |         |
| Общая трудоёмкость, з.е./ч  | 3 / 108 | 3 / 108 |
| Общая контактная работа, ч  | 12,15   | 12,15   |
| Общая самостоятельная работа, ч   | 95,85   | 95,85   |
| Контактная работа при проведении учебных занятий, в т.ч. (ч)                      | 12,00   | 12,00   |
| лекции  | 6       | 6,00    |
| практические-всего  | 6       | 6,00    |
| Самостоятельная работа при проведении учебных занятий, ч                          | 87,00   | 87,00   |
| Контактная работа при проведении промежуточной аттестации обучающихся, в т.ч. (ч) | 0,15    | 0,15    |
| зачет   | 0,15    | 0,15    |
| Самостоятельная работа при промежуточной аттестации, в т.ч. (ч)                   | 8,85    | 8,85    |
| подготовка к зачету   | 8,85    | 8,85    |
| Форма промежуточной аттестации  | зачет   | зачет   |

## 4. Содержание дисциплины

### 4.1. Содержание дисциплины в разрезе разделов и подразделов

#### Раздел 1.

##### Основы информационной безопасности

###### Подраздел 1.1.

##### Информационная безопасность в системе национальной безопасности России

Основные понятия и определения в области информационной безопасности

Основные составляющие информационной безопасности.

Понятие и сущность защиты информации. Предмет и объект защиты информации.

###### Подраздел 1.2.

##### Угрозы информационной безопасности

Информационная война, методы и средства ее ведения.

Понятие и классификация угроз информационной безопасности. Случайные угрозы. Преднамеренные угрозы.

Модель гипотетического нарушителя информационной безопасности

#### Раздел 2.

##### Компьютерные преступления и правовые основы защиты информации

###### Подраздел 2.1.

##### Компьютерные преступления и их особенности

Понятие компьютерных преступлений и их виды

Вредоносное программное обеспечение.

Методы и технологии борьбы с вредоносными программами

###### Подраздел 2.2.

##### Законодательные аспекты информационной безопасности в РФ

Законодательство РФ области информационной безопасности

Нормативно-правовые основы информационной безопасности в РФ.

Ответственность за нарушения в сфере информационной безопасности в РФ.

#### Раздел 3.

##### Системное обеспечение защиты информации

###### Подраздел 3.1.

##### Криптографические методы защиты информации

Основные понятия и определения криптографии. История развития криптографии.

Классификация криптографических методов защиты информации.

Электронная подпись и механизмы её реализации.

###### Подраздел 3.2.

##### Системное обеспечение защиты информации, обрабатываемой в информационных системах

Критерии защищенности компьютерных систем.

Концептуальная модель информационной безопасности.

Основные принципы построения системы защиты информации.

Методы защиты информации. Интеллектуальный интерфейс

**4.2. Распределение контактной и самостоятельной работы по подразделам**  
**Очная форма обучения**

| Разделы, подразделы дисциплины  | Контактная работа |     | СР   |
|---|-------------------|-----|------|
|   | лекции            | ПЗ  |      |
| <b>Основы информационной безопасности</b>   |                   |     |      |
| Информационная безопасность в системе национальной безопасности России            | 3,3               | 3,0 | 10,1 |
| Угрозы информационной безопасности  | 3,3               | 3,0 | 10,1 |
| <b>Компьютерные преступления и правовые основы защиты информации</b>              |                   |     |      |
| Компьютерные преступления и их особенности  | 3,3               | 3,0 | 10,2 |
| Законодательные аспекты информационной безопасности в РФ                          | 3,3               | 3,0 | 10,2 |
| <b>Системное обеспечение защиты информации</b>                                    |                   |     |      |
| Криптографические методы защиты информации  | 3,3               | 3,0 | 10,2 |
| Системное обеспечение защиты информации, обрабатываемой в информационных системах | 3,3               | 3,0 | 10,2 |

**4.2. Распределение контактной и самостоятельной работы по подразделам  
Заочная форма обучения**

| Разделы, подразделы дисциплины  | Контактная работа |     | СР   |
|---|-------------------|-----|------|
|   | лекции            | ПЗ  |      |
| <b>Основы информационной безопасности</b>   |                   |     |      |
| Информационная безопасность в системе национальной безопасности России            | 1,0               | 1,0 | 14,4 |
| Угрозы информационной безопасности  | 1,0               | 1,0 | 14,4 |
| <b>Компьютерные преступления и правовые основы защиты информации</b>              |                   |     |      |
| Компьютерные преступления и их особенности  | 1,0               | 1,0 | 14,5 |
| Законодательные аспекты информационной безопасности в РФ                          | 1,0               | 1,0 | 14,5 |
| <b>Системное обеспечение защиты информации</b>                                    |                   |     |      |
| Криптографические методы защиты информации  | 1,0               | 1,0 | 14,5 |
| Системное обеспечение защиты информации, обрабатываемой в информационных системах | 1,0               | 1,0 | 14,5 |

## 5. Фонд оценочных средств

### 5.1. Этапы формирования компетенций

| Разделы, подразделы дисциплины  | Компетенции и ИД                 |            |            |
|---|----------------------------------|------------|------------|
|   | ОПК-3                            | ОПК-4      | ПК-10      |
| <b>Основы информационной безопасности</b>   |                                  |            |            |
| Информационная безопасность в системе национальной безопасности России            | 31, 36, У1,<br>У7, Н1, Н7,<br>Н8 |            |            |
| Угрозы информационной безопасности  | 31, 36, У1,<br>У7, Н1, Н7,       |            |            |
| <b>Компьютерные преступления и правовые основы защиты информации</b>              |                                  |            |            |
| Компьютерные преступления и их особенности  | 31, 36, У1,<br>У7, Н1, Н7,       |            |            |
| Законодательные аспекты информационной безопасности в РФ                          |                                  | 35, У6, Н5 |            |
| <b>Системное обеспечение защиты информации</b>                                    |                                  |            |            |
| Криптографические методы защиты информации  |                                  |            | 35, У5, Н6 |
| Системное обеспечение защиты информации, обрабатываемой в информационных системах |                                  |            | 35, У5, Н6 |

## 5.2. Шкалы и критерии оценивания достижения компетенций

### 5.2.1. Шкалы академических оценок освоения дисциплины

| Вид оценки                                 | Оценки              |                   |        |         |
|--|---------------------|-------------------|--------|---------|
| Академическая оценка по 4-х балльной шкале | неудовлетворительно | удовлетворительно | хорошо | отлично |

| Вид оценки                                 | Оценки     |         |
|--|------------|---------|
| Академическая оценка по 2-х балльной шкале | не зачетно | зачтено |

### 5.2.2. Критерии достижения компетенций в ходе освоения дисциплины

#### Критерии оценки на зачете

| Оценка, уровень достижения         | Описание критериев  |
|------------------------------------|---|
| Зачтено, высокий                   | Студент выполнил все задания, предусмотренные программой, отчитался об их выполнении, демонстрируя отличное знание освоенного материала и умение самостоятельно решать сложные задачи дисциплины            |
| Зачтено, продвинутый               | Студент выполнил все задания, предусмотренные программой, отчитался об их выполнении, демонстрируя хорошее знание освоенного материала и умение самостоятельно решать стандартные задачи дисциплины         |
| Зачтено, пороговый                 | Студент выполнил все задания, предусмотренные программой, отчитался об их выполнении, демонстрируя знание основ освоенного материала и умение решать стандартные задачи дисциплины с помощью преподавателя  |
| Не зачтено, компетенции не освоены | Студент выполнил не все задания, предусмотренные программой или не отчитался об их выполнении, не подтверждает знание освоенного материала и не умеет решать задачи дисциплины даже с помощью преподавателя |

**5.3. Материалы для оценки достижения компетенций**

**5.3.1. Вопросы к экзамену**

**Не предусмотрено**

**5.3.2. Задания к экзамену**

**Не предусмотрено**

**5.3.3. Вопросы к зачету с оценкой**

**Не предусмотрено**

### 5.3.4. Вопросы к зачету

| №  | Содержание   | Компетенция | ИД |
|----|--|-------------|----|
| 1  | Основные понятия и определения в области информационной безопасности                 | ОПК-3       | 36 |
| 2  | Основные составляющие информационной безопасности                                    | ОПК-3       | 36 |
| 3  | Задачи информационной безопасности   | ОПК-3       | 36 |
| 4  | Понятие и сущность защиты информации   | ОПК-3       | 36 |
| 5  | Цели защиты информации. Предмет защиты информации                                    | ОПК-3       | 31 |
| 6  | Законодательство РФ в области информационной безопасности                            | ОПК-4       | 35 |
| 7  | Нормативно-правовая база защиты информации: основные законы РФ и указы Президента РФ | ОПК-4       | 35 |
| 8  | Информация как объект права собственности. Объект защиты информации                  | ОПК-4       | 35 |
| 9  | Случайные угрозы информационной безопасности   | ОПК-3       | 36 |
| 10 | Преднамеренные угрозы информационной безопасности                                    | ОПК-3       | 36 |
| 11 | Модель гипотетического нарушителя информационной безопасности                        | ОПК-3       | 36 |
| 12 | Анализ компьютерных преступлений   | ОПК-3       | 36 |
| 13 | Несанкционированный доступ к информации и его цели                                   | ОПК-3       | 31 |
| 14 | Компьютерные вирусы  | ОПК-3       | 31 |
| 15 | Шпионские программные закладки   | ОПК-3       | 31 |
| 16 | Основные принципы построения системы защиты информации                               | ПК-10       | 35 |
| 17 | Методы защиты информации. Интеллектуальный интерфейс                                 | ПК-10       | 35 |
| 18 | Основные понятия и определения криптографии  | ПК-10       | 35 |
| 19 | История развития криптографии  | ПК-10       | 35 |
| 20 | Классификация криптографических методов защиты информации                            | ПК-10       | 35 |
| 21 | Современные симметричные криптографические системы: системы с секретным ключом       | ПК-10       | 35 |
| 22 | Современные симметричные криптографические системы: стандарт шифрования DES          | ПК-10       | 35 |
| 23 | Современные симметричные криптографические системы: стандарт шифрования ГОСТ 28147   | ПК-10       | 35 |
| 24 | Асимметричные криптографические системы: системы с открытым ключом;                  | ПК-10       | 35 |
| 25 | Асимметричные криптографические системы: стандарт шифрования RSA                     | ПК-10       | 35 |
| 26 | Электронная цифровая подпись и механизмы её реализации                               | ПК-10       | 35 |
| 27 | Критерии защищенности компьютерных систем  | ПК-10       | 35 |
| 28 | Концептуальная модель информационной безопасности                                    | ПК-10       | 35 |
| 29 | Основные принципы построения системы защиты информации                               | ПК-10       | 35 |
| 30 | Методы защиты информации   | ПК-10       | 35 |

### 5.3.5. Темы курсового проект (работы) и вопросы к защите Не предусмотрено

### 5.3. Материалы для оценки достижения компетенций

#### 5.3.6. Вопросы тестов

| №  | Содержание  | Компетенция | ИД |
|----|---|-------------|----|
| 1  | Информация, несанкционированное копирование, хищение, разглашение (распространение, опубликование), модификация, уничтожение или использование которой может нанести существенный моральный или материальный ущерб ее собственнику или владельцу, а также третьей стороне, интересы которой данная информация затрагивает, называется | ОПК-3       | 36 |
| 2  | Укажите категории ценности информации с точки зрения информационной безопасности  | ОПК-3       | У1 |
| 3  | Категория ценности информации, определяющая гарантию того, что источником информации является именно то лицо, которое заявлено как ее автор, называется   | ОПК-3       | 31 |
| 4  | Аутентичность связана   | ОПК-3       | 31 |
| 5  | Категория ценности информации, гарантирующая, что при необходимости можно доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой, называется  | ОПК-3       | 31 |
| 6  | Убытки, которые могут возникнуть вследствие внесения изменений в информацию, если факт модификации не был обнаружен, называются   | ОПК-3       | 36 |
| 7  | Потенциальные убытки, которые понесет владелец информации, если к ней получают неавторизованный доступ сторонние лица, называются   | ОПК-3       | 31 |
| 8  | Ущерб от полного или частичного разрушения информации называется  | ОПК-3       | У1 |
| 9  | Укажите, что не является преднамеренным воздействием на информационную систему  | ОПК-3       | У7 |
| 10 | Укажите, что не является причиной случайных воздействий на информационную систему   | ОПК-3       | У7 |
| 11 | Укажите пути несанкционированной передачи информации  | ОПК-3       | У1 |
| 12 | Укажите составляющие информационной безопасности  | ОПК-3       | У1 |
| 13 | Конфиденциальность информации гарантирует   | ОПК-3       | 31 |
| 14 | Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации называется   | ОПК-3       | 36 |
| 15 | Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации называется   | ОПК-3       | 36 |
| 16 | Комплекс средств и методов, направленных на предотвращение угроз информационной безопасности и устранение их последствий, называется  | ОПК-3       | 36 |
| 17 | Укажите, что из перечисленного является задачей информационной безопасности   | ОПК-3       | У7 |
| 18 | Доступность информации гарантирует  | ОПК-3       | 36 |
| 19 | Целостность информации гарантирует  | ОПК-3       | 36 |
| 20 | Процесс распознавания пользователя автоматизированной системой, для чего предъявляется уникальное имя, называется   | ОПК-3       | 31 |
| 21 | Процедура проверки подлинности, предназначенная для подтверждения истинности пользователя, предъявившего идентификатор, называется  | ОПК-3       | 31 |
| 22 | Идентификация и аутентификация применяются  | ОПК-3       | 31 |
| 23 | Присвоение субъектам идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем идентификаторов, владельцы которых допущены к информационной системе, называется  | ОПК-3       | 36 |
| 24 | Результатом реализации угроз информационной безопасности может быть   | ОПК-3       | 36 |
| 25 | Угроза перехвата данных может привести  | ОПК-3       | 36 |
| 26 | Идентификация и аутентификация применяются  | ОПК-3       | 31 |
| 27 | Подберите слово к данному определению: ??? - проверка принадлежности субъекту предъявленного им идентификатора и подтверждение его подлинности  | ОПК-3       | 31 |
| 28 | Подберите слово к данному определению: ??? - присвоение субъектам личного идентификатора и сравнение его с заданным   | ОПК-3       | 36 |
| 29 | Под информационной безопасностью (безопасностью информации) понимается  | ОПК-3       | 36 |
| 30 | Что такое угроза?   | ОПК-3       | 36 |
| 31 | Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена – это  | ОПК-3       | 31 |
| 32 | Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним – это   | ОПК-3       | 36 |

|    |  |       |    |
|----|--|-------|----|
| 33 | Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам – это:  | ОПК-3 | 36 |
| 34 | В чем выражаются угрозы информационной безопасности?   | ОПК-3 | 36 |
| 35 | Мероприятия по формированию осознанного отношения сотрудников к обеспечению информационной безопасности относятся к:   | ОПК-3 | 36 |
| 36 | Накопление сведений об угрозах информационной безопасности и их аналитическая обработка относится к:   | ОПК-3 | 36 |
| 37 | Действия, направленные на устранение действующей угрозы и конкретных преступных действий относятся к :   | ОПК-3 | 36 |
| 38 | Действия по восстановлению состояния, предшествовавшего возникновению угрозы, относятся к:   | ОПК-3 | 36 |
| 39 | Основными мероприятиями по защите от разглашения является:   | ОПК-3 | 36 |
| 40 | Защита от утечки конфиденциальной информации сводится к:   | ОПК-3 | 36 |
| 41 | Защита от несанкционированного доступа к конфиденциальной информации обеспечивается выполнением:   | ОПК-3 | 36 |
| 42 | Определение состояния технической безопасности объекта относится к:  | ОПК-3 | 36 |
| 43 | Какой из принципов нецелесообразно использовать при организации защиты информации:   | ОПК-3 | 36 |
| 44 | Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства, называют:  | ОПК-3 | 36 |
| 45 | Любая программа, написанная с целью нанесения ущерба или использования ресурсов атакуемого компьютера, называется:   | ОПК-3 | 36 |
| 46 | Класс программ, способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия, называется:   | ОПК-3 | 36 |
| 47 | Укажите этапы жизненного цикла компьютерного вируса:   | ОПК-3 | 36 |
| 48 | По среде обитания компьютерные вирусы подразделяют на:   | ОПК-3 | 36 |
| 49 | Достаточно трудно обнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода, это:  | ОПК-3 | 36 |
| 50 | Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям:   | ОПК-3 | 36 |
| 51 | ??? – это вирусы, заражающие файлы некоторых систем обработки документов (MS Word, MS Excel), которые имеют встроенные макро-языки   | ОПК-3 | 36 |
| 52 | ??? маскируют свое присутствие путем перехвата обращений ОС к пораженным файлам, секторам и переадресуют ОС к незараженным участкам  | ОПК-3 | 36 |
| 53 | ??? - это компьютерные вирусы, которые распространяются в компьютерных сетях и не изменяют файлы или секторы на диска  | ОПК-3 | 36 |
| 54 | Какой из вирусов при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них?   | ОПК-3 | 36 |
| 55 | Самошифрование и полиморфичность используются для:   | ОПК-3 | 36 |
| 56 | Одним из наиболее эффективных способов борьбы с вирусами является:   | ОПК-3 | 36 |
| 57 | ??? - это программа, скрытно внедренная в защищенную систему и позволяющая злоумышленнику, путем модификации свойств системы защиты, осуществлять несанкционированный доступ к ресурсам системы  | ОПК-3 | 36 |
| 58 | К деструктивным действиям, осуществляемым программными закладками относятся:   | ОПК-3 | 36 |
| 59 | Программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия, называется:   | ОПК-3 | 36 |
| 60 | ??? – это компьютерная программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалить вредоносные программы:  | ОПК-3 | 36 |
| 61 | Укажите методы обнаружения компьютерных вирусов:   | ОПК-3 | 36 |
| 62 | ??? - комплекс программных или аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Позволяет блокировать нежелательный сетевой трафик, обеспечивает невидимость ПК в сети с целью предотвращения кибер атак | ОПК-3 | 36 |
| 63 | Маски (сигнатуры) вирусов используются:  | ОПК-3 | 36 |
| 64 | Укажите основные функции антивирусных программ:  | ОПК-3 | 36 |
| 65 | Основополагающими документами по информационной безопасности в РФ являются   | ОПК-4 | 35 |

|    |  |       |    |
|----|--|-------|----|
| 66 | Укажите документ, гарантирующий тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23, ч. 2); право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29, ч. 4); свободу массовой информации (ст. 29, ч. 5):   | ОПК-4 | У6 |
| 67 | Укажите документ, определяющий важнейшие задачи обеспечения информационной безопасности РФ:  | ОПК-4 | У6 |
| 68 | Укажите сведения, имеющие конфиденциальный характер:   | ОПК-4 | У6 |
| 69 | Сколько категорий государственных информационных ресурсов определяет Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.08.2006 г. № 149-ФЗ?   | ОПК-4 | 35 |
| 70 | Документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности, называется:   | ОПК-4 | 35 |
| 71 | Любая информация, с помощью которой можно однозначно идентифицировать физическое лицо, является  | ОПК-4 | 35 |
| 72 | Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ, относятся к   | ОПК-4 | 35 |
| 73 | Неправомерный доступ к компьютерной информации наказывается штрафом  | ОПК-4 | 35 |
| 74 | Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок   | ОПК-4 | 35 |
| 75 | Создание, использование и распространение вредоносных программ для ЭВМ наказывается:   | ОПК-4 | 35 |
| 76 | Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается:   | ОПК-4 | 35 |
| 77 | Что такое Доктрина информационной безопасности РФ  | ОПК-4 | 35 |
| 78 | В предлагаемом перечне укажите мероприятия защиты информации предприятия, относящиеся к правовым?  | ОПК-4 | У6 |
| 79 | Право разрешать или ограничивать доступ к информации и определять условия такого доступа принадлежит:  | ОПК-4 | 35 |
| 80 | Перечень сведений конфиденциального характера определен:   | ОПК-4 | 35 |
| 81 | Перечень сведений, доступ к которым не может быть ограничен определен:   | ОПК-4 | 35 |
| 82 | Наука о методах преобразования информации с целью ее защиты от несанкционированного доступа называется   | ПК-10 | 35 |
| 83 | Наука (и практика ее применения) о методах и способах расшифровки информации без знания ключей называется  | ПК-10 | 35 |
| 84 | Набор средств и методов сокрытия факта передачи сообщения называется   | ПК-10 | 35 |
| 85 | Процесс преобразования исходного (открытого) сообщения в шифрованное по определенным правилам, содержащимся в шифре называется   | ПК-10 | 35 |
| 86 | Процесс преобразования шифрованного сообщения (шифртекста) в исходное (открытое) сообщение с помощью определенных правил, содержащихся в шифре называется  | ПК-10 | 35 |
| 87 | Способ преобразования информации с целью ее защиты от незаконных пользователей называется  | ПК-10 | 35 |
| 88 | Процесс получения защищенного сообщения (открытого текста) из шифрованного сообщения (шифротекста) без знания примененного шифра называется:   | ПК-10 | 35 |
| 89 | Сменный элемент шифра, применяемый для шифрования конкретных сообщений, называется   | ПК-10 | 35 |
| 90 | Укажите способы преобразования при шифровании  | ПК-10 | 35 |
| 91 | Криптосистемой является  | ПК-10 | 35 |
| 92 | Что из перечисленного не входит в криптосистему:   | ПК-10 | 35 |
| 93 | ГОСТ 28147-89 является стандартом  | ПК-10 | 35 |
| 94 | Алгоритм RSA является стандартом:  | ПК-10 | 35 |
| 95 | При асимметричном шифровании для шифрования и расшифровки используются:  | ПК-10 | 35 |
| 96 | Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа, предназначенный для защиты данного документа от подделки, и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе, представляет собой | ПК-10 | 35 |
| 97 | Цифровая подпись не обеспечивает   | ПК-10 | 35 |

|     |   |       |    |
|-----|---|-------|----|
| 98  | Соотнесите виды цифровой подписи и их характеристики  | ПК-10 | У5 |
| 99  | Алгоритмы шифрования бывают   | ПК-10 | 35 |
| 100 | Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа и предназначенный для защиты данного документа от подделки, а также позволяющий идентифицировать владельца ключа и установить отсутствие искажения информации в электронном документе называется | ПК-10 | 35 |
| 101 | Электронная подпись устанавливает ??? информации  | ПК-10 | 35 |
| 102 | Электронная подпись обеспечивает  | ПК-10 | 35 |
| 103 | Программные модули или аппаратные устройства, регистрирующие каждое нажатие клавиши на клавиатуре компьютера  | ПК-10 | 35 |
| 104 | Для генерации электронной подписи может быть использован алгоритм   | ПК-10 | 35 |
| 105 | Какие из перечисленных алгоритмов относятся к симметричным?   | ПК-10 | 35 |
| 106 | Для контроля целостности передаваемых по сетям данных используется  | ПК-10 | 35 |
| 107 | В предлагаемом перечне выделите задачи, не являющиеся задачами криптографии   | ПК-10 | У5 |
| 108 | Что из перечисленного не является функцией управления криптографическими ключами  | ПК-10 | 35 |
| 109 | Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации называется  | ПК-10 | 35 |
| 110 | Электронная подпись позволяет   | ПК-10 | 35 |
| 111 | Размер ключа в ГОСТ 28147-89  | ПК-10 | 35 |
| 112 | Размер ключа в стандарте DES  | ПК-10 | 35 |
| 113 | Символы исходного текста складываются с символами некой случайной последовательности – это  | ПК-10 | 35 |
| 114 | Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это   | ПК-10 | 35 |
| 115 | Какой метод используется при шифровании с помощью аналитических преобразований  | ПК-10 | 35 |
| 116 | Сферы применения DES-алгоритма  | ПК-10 | 35 |
| 117 | Алгоритм ГОСТ 28147-89 использует ключ, являющийся  | ПК-10 | 35 |
| 118 | Основные области применения DES-алгоритма   | ПК-10 | 35 |
| 119 | Криптостойкость – это...  | ПК-10 | 35 |
| 120 | Что не рассматривается в политике безопасности?   | ПК-10 | 35 |
| 121 | Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов, называется:  | ПК-10 | 35 |
| 122 | Стратегию организации в области информационной безопасности, меру внимания и количество ресурсов, которые руководство считает целесообразным выделить для обеспечения информационной безопасности, определяет:  | ПК-10 | 35 |
| 123 | Укажите компоненты концептуальной модели безопасности информации:   | ПК-10 | 35 |
| 124 | На каком из уровней обеспечения информационной безопасности разрабатывается политика безопасности:  | ПК-10 | 35 |

|     |   |       |    |
|-----|---|-------|----|
| 125 | Что не является содержанием административного уровня обеспечения информационной безопасности:   | ПК-10 | 35 |
| 126 | Какой из уровней обеспечения информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации: | ПК-10 | 35 |
| 127 | Какой из перечисленных уровней не относится к уровням обеспечения информационной безопасности:  | ПК-10 | 35 |
| 128 | Какие из указанных мероприятий защиты информации относятся к организационным?   | ПК-10 | 35 |
| 129 | Организационные мероприятия защиты информации реализуются на каких уровнях:   | ПК-10 | 35 |
| 130 | Какие из указанных мероприятий защиты информации относятся к инженерно-техническим?   | ПК-10 | 35 |
| 131 | Возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются:                                 | ПК-10 | 35 |
| 132 | Система защиты информации – это:  | ПК-10 | 35 |
| 133 | К недостаткам аппаратных средств инженерно-технической защиты относится:  | ПК-10 | 35 |
| 134 | К достоинствам программных средств инженерно-технической защиты относится:  | ПК-10 | 35 |
| 135 | Началу работ по созданию или совершенствованию системы защиты информации (СЗИ) предшествует:  | ПК-10 | 35 |
| 136 | Мероприятия по созданию системы защиты информации начинаются с:   | ПК-10 | 35 |
| 137 | Информационная модель предприятия формируется после окончания   | ПК-10 | 35 |
| 138 | Разработка системы защиты информации начинается с   | ПК-10 | 35 |
| 139 | Контроль эффективности защиты необходимо начинать с   | ПК-10 | 35 |

### 5.3. Материалы для оценки достижения компетенций

#### 5.3.7. Вопросы для устного опроса

| №  | Содержание  | Компетенция | ИД |
|----|---|-------------|----|
| 1  | Дайте определение понятию информационная безопасность.  | ОПК-3       | 36 |
| 2  | Перечислите основные составляющие информационной безопасности.  | ОПК-3       | 36 |
| 3  | Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?   | ОПК-3       | 31 |
| 4  | Каковы интересы РФ в информационной сфере?  | ОПК-3       | 36 |
| 5  | Определите источники угроз информационной безопасности РФ и постройте их классификацию.                 | ОПК-3       | 36 |
| 6  | Перечислите основные методы обеспечения информационной безопасности РФ.                                 | ОПК-3       | 36 |
| 7  | Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня?                    | ОПК-3       | 36 |
| 8  | Каково, на ваш взгляд, положение дел в области мировой информационной безопасности сегодня?             | ОПК-3       | 36 |
| 9  | Проанализируйте различные определения понятия «защита информации» и «информационная безопасность»       | ОПК-3       | 36 |
| 10 | Дайте определение понятию защита информации.  | ОПК-3       | 36 |
| 11 | Что понимается под термином безопасность информации?  | ОПК-3       | 36 |
| 12 | Что включает в себя защита информации?  | ОПК-3       | 36 |
| 13 | Какие цели преследует защита информации?  | ОПК-3       | 36 |
| 14 | Какое место занимает защита информации в информационной безопасности?                                   | ОПК-3       | 36 |
| 15 | Определите предмет защиты информации.   | ОПК-3       | 36 |
| 16 | Сформулируйте основные свойства информации.   | ОПК-3       | 31 |
| 17 | Дайте определение конфиденциальной информации.  | ОПК-3       | 31 |
| 18 | Перечислите уровни секретности государственной тайны.   | ОПК-3       | 36 |
| 19 | Раскройте сущность основных подходов к измерению количества информации.                                 | ОПК-3       | 36 |
| 20 | Раскройте сущность информации как объекта права собственности.  | ОПК-3       | 36 |
| 21 | Раскройте сущность объекта защиты.  | ОПК-3       | 36 |
| 22 | Определите понятие угрозы информационной безопасности (ИБ).   | ОПК-3       | 36 |
| 23 | Охарактеризуйте случайные угрозы ИБ.  | ОПК-3       | 36 |
| 24 | Охарактеризуйте преднамеренные угрозы ИБ.   | ОПК-3       | 36 |
| 25 | Определите понятия нарушителя ИБ и злоумышленника.  | ОПК-3       | 36 |
| 26 | Какие предположения выдвигаются при разработке модели гипотетического нарушителя ИБ объекта.            | ОПК-3       | 36 |
| 27 | На основании чего строится модель гипотетического нарушителя ИБ?  | ОПК-3       | 36 |
| 28 | Какие категории персонала объекта могут быть внутренними нарушителями ИБ объекта?                       | ОПК-3       | 36 |
| 29 | Какие лица могут быть нарушителями ИБ объекта из числа посторонних лиц?                                 | ОПК-3       | 36 |
| 30 | Назовите основные мотивы нарушений ИБ.  | ОПК-3       | 36 |
| 31 | Дайте определение компьютерного преступления и охарактеризуйте их виды                                  | ОПК-3       | 36 |
| 32 | Определите понятия вредоносного программного обеспечения и компьютерного вируса                         | ОПК-3       | 36 |
| 33 | Перечислите основные классы компьютерных вирусов  | ОПК-3       | 36 |
| 34 | В чем заключаются различия между понятиями компьютерного вируса и шпионской программной закладки?       | ОПК-3       | 36 |
| 35 | Назовите основные методы внедрения программных закладок   | ОПК-3       | 36 |
| 36 | Дайте характеристику основных моделей воздействия программных закладок на компьютер и компьютерную сеть | ОПК-3       | 36 |
| 37 | В чем различия троянских программ и программных закладок?   | ОПК-3       | 36 |
| 38 | Дайте характеристику действий основных разновидностей троянских программ                                | ОПК-3       | 36 |
| 39 | Назовите и охарактеризуйте методы обнаружения вирусов   | ОПК-3       | 36 |
| 40 | Перечислите виды и назначения антивирусных программ   | ОПК-3       | 36 |
| 41 | Какими действиями можно предотвратить вирусную атаку?   | ОПК-3       | 36 |
| 42 | Назовите основополагающие документы по ИБ в РФ.   | ОПК-4       | 35 |
| 43 | Что является предметом правового регулирования в области ИБ?  | ОПК-4       | 35 |
| 44 | Назовите задачи обеспечения ИБ, сформулированные в Концепции национальной безопасности РФ               | ОПК-4       | 35 |
| 45 | Какой закон является базовым в области защиты информации, и какие отношения он регламентирует?          | ОПК-4       | 35 |
| 46 | Назовите категории государственных информационных ресурсов  | ОПК-4       | 35 |
| 47 | Какая информация может быть отнесена к категории конфиденциальной?                                      | ОПК-4       | 35 |
| 48 | Определите данные, которые могут быть отнесены к персональным данным                                    | ОПК-4       | 35 |
| 49 | Назовите статьи УК РФ, предусматривающие ответственность за совершение компьютерных преступлений        | ОПК-4       | 35 |

|    |  |       |    |
|----|--|-------|----|
| 50 | Сформулируйте основные принципы построения системы защиты информации.  | ПК-10 | 35 |
| 51 | Какие уровни задействованы в обеспечении информационной безопасности?  | ПК-10 | 35 |
| 52 | Что представляет собой политика безопасности организации?  | ПК-10 | 35 |
| 53 | Что входит в анализ рисков?  | ПК-10 | 35 |
| 54 | Что представляет собой программа безопасности организации?   | ПК-10 | 35 |
| 55 | Перечислите основные модели защиты информации и их особенности.  | ПК-10 | 35 |
| 56 | В чем заключается сущность методов защиты от случайных угроз?  | ПК-10 | 35 |
| 57 | Дайте определение понятиям идентификации и аутентификации.   | ПК-10 | 35 |
| 58 | Перечислите основные виды аутентификации.  | ПК-10 | 35 |
| 59 | В чем заключается повышение надежности и отказоустойчивости информационных систем?   | ПК-10 | 35 |
| 60 | Какую роль играет подготовленность персонала в построении системы защиты информации?   | ПК-10 | 35 |
| 61 | Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?                             | ПК-10 | 35 |
| 62 | Раскройте особенность построения защиты от несанкционированного доступа  | ПК-10 | 35 |
| 63 | Какие методы защиты информации относятся к криптографическим?  | ПК-10 | 35 |
| 64 | Дайте определение криптологии.   | ПК-10 | 35 |
| 65 | Какие три основных периода криптологии вы знаете?  | ПК-10 | 35 |
| 66 | Объясните понятие «криптологический алгоритм».   | ПК-10 | 35 |
| 67 | Что такое криптография?  | ПК-10 | 35 |
| 68 | Какова суть преобразований перестановки и замены?  | ПК-10 | 35 |
| 69 | Что собой представляют шифрование и дешифрование?  | ПК-10 | 35 |
| 70 | Дайте определение аналитическому преобразованию, гаммированию и комбинированному шифрованию.   | ПК-10 | 35 |
| 71 | Что такое системы с открытыми ключами?   | ПК-10 | 35 |
| 72 | Приведите структурную схему процесса шифрования с открытым ключом.   | ПК-10 | 35 |
| 73 | Дайте определение стойкости криптосистемы.   | ПК-10 | 35 |
| 74 | Приведите основные программно-аппаратные реализации шифров.  | ПК-10 | 35 |
| 75 | В чем заключается суть DES-алгоритма? Каковы его особенности?  | ПК-10 | 35 |
| 76 | В каких режимах может работать DES-алгоритм?   | ПК-10 | 35 |
| 77 | Дайте описание отечественного алгоритма криптографического преобразования данных (ГОСТ 28147 - 89) и его отличительных особенностей.       | ПК-10 | 35 |
| 78 | Какими характеристиками оценивается стойкость криптографических систем?  | ПК-10 | 35 |
| 79 | В чем заключается суть электронной цифровой подписи?   | ПК-10 | 35 |
| 80 | Как проверяется целостность сообщения?   | ПК-10 | 35 |
| 81 | Дайте определение межсетевому экрану.  | ПК-10 | 35 |
| 82 | Назовите типы межсетевых экранов.  | ПК-10 | 35 |
| 83 | Объясните различия между межсетевыми экранами разных типов.  | ПК-10 | 35 |
| 84 | Что представляет собой политика безопасности организации?  | ПК-10 | 35 |
| 85 | Что не рассматривается в политике безопасности?  | ПК-10 | 35 |
| 86 | Назовите компоненты концептуальной модели безопасности информации?   | ПК-10 | 35 |
| 87 | На каком из уровней обеспечения информационной безопасности разрабатывается политика безопасности?   | ПК-10 | 35 |
| 88 | Что является содержанием административного уровня обеспечения информационной безопасности?   | ПК-10 | 35 |
| 89 | Какой уровень обеспечения информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации? | ПК-10 | 35 |
| 90 | Назовите мероприятия защиты информации, являющиеся организационными?   | ПК-10 | 35 |
| 91 | На каких уровнях защиты информации реализуются организационные мероприятия?  | ПК-10 | 35 |
| 92 | Какие мероприятия защиты информации относятся к классу инженерно-техническим ?   | ПК-10 | 35 |
| 93 | Что понимается под системой защиты информации?   | ПК-10 | 35 |
| 94 | Что можно считать недостатками аппаратных средств инженерно-технической защиты информации?   | ПК-10 | 35 |
| 95 | Что можно считать достоинствами программных средств инженерно-технической защиты информации?   | ПК-10 | 35 |
| 96 | Что предшествует началу работ по созданию или совершенствованию системы защиты информации (СЗИ)?   | ПК-10 | 35 |
| 97 | С чего следует начинать мероприятия по созданию системы защиты информации?   | ПК-10 | 35 |
| 98 | На каком этапе осуществляется формирование информационной модели предприятия?  | ПК-10 | 35 |

### 5.3.8. Задания для проверки формирования навыков

| №  | Содержание   | Компетенция | ИД |
|----|--|-------------|----|
| 1  | Определите время перебора всех паролей, состоящих из 6 цифр  | ОПК-3       | У7 |
| 2  | Определите минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет  | ОПК-3       | У1 |
| 3  | Определите время перебора всех паролей с параметрами   | ОПК-3       | У7 |
| 4  | Определите минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду   | ОПК-3       | У1 |
| 5  | Определите количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.<br>Скорость перебора s паролей в секунду.   | ОПК-3       | У7 |
| 6  | Выполните архивацию файла с паролем. Внесите искажения, попытайтесь разархивировать. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.                | ОПК-3       | У7 |
| 7  | Выполните архивацию файла с паролем, состоящим из 3-х цифр. Выполните попытку подбора пароля с использованием программного обеспечения. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения, время подбора | ОПК-3       | У1 |
| 8  | Восстановите файл (.doc, .docx, .xls, .xlsx) , зараженный макровирусом (не используя антивирусную программу). Затем включите защиту от запуска макросов.   | ОПК-3       | Н1 |
| 9  | Проверьте потенциальные места записей «троянских программ» в системном реестре ОС  | ОПК-3       | Н1 |
| 10 | Определите что такое идентификатор, пароль пользователя и учетная запись пользователя  | ОПК-4       | У6 |
| 11 | Укажите в подготовленном перечне сведения, доступ к которым не может быть ограничен  | ОПК-4       | Н5 |
| 12 | Охарактеризуйте структуру правовых актов, ориентированных на правовую защиту информации  | ОПК-4       | У6 |
| 13 | Укажите как подразделяется информация ограниченного доступа в соответствии с ФЗ-149?   | ОПК-4       | У6 |
| 14 | Выделите информацию конфиденциального характера  | ОПК-4       | Н5 |
| 15 | Выделите информацию ограниченного доступа  | ОПК-4       | Н5 |
| 16 | Выделите основные организационные мероприятия по защите информации   | ОПК-4       | Н5 |
| 17 | Перечислите 6 видов информации конфиденциального характера   | ОПК-4       | У6 |
| 18 | Создайте в Outlook Express систему правил по обработке входящих сообщений электронной почты  | ПК-10       | Н6 |
| 19 | Для отправления сообщения в Outlook Express , подписанного цифровой подписью и зашифрованного, получите цифровой идентификатор   | ПК-10       | Н6 |
| 20 | Настройте параметры локальной политики безопасности ОС   | ПК-10       | Н6 |
| 21 | Создайте учетную запись и локальную группу, измените принадлежность пользователя к локальной группе и заблокируйте учетную запись пользователя   | ПК-10       | Н6 |
| 22 | Загрузите редактор Шаблона безопасности, отредактируйте (модифицируйте настройку безопасности) шаблон безопасности и сохраните его с новым именем  | ПК-10       | Н6 |
| 23 | Создайте VPN-подключение и выполните его настройку   | ПК-10       | Н6 |
| 24 | Используя метод шифрования - "перестановка", зашифровать свои данные: фамилию, имя, отчество   | ПК-10       | У5 |
| 25 | Используя метод шифрования - "замена", зашифровать свои данные: фамилию, имя, отчество   | ПК-10       | У5 |
| 26 | Определите примерный перечень сведений, составляющих коммерческую (служебную) тайну предприятия  | ПК-10       | У5 |
| 27 | Укажите последовательность действий в системе КриптоАРМ при выполнении подписания документа  | ОПК-3       | Н1 |
| 28 | Укажите последовательность действий в системе КриптоАРМ для выполнения открытия документа  | ОПК-3       | Н1 |
| 29 | Подготовить реферат по теме ИБ с учетом требований ИБ  | ОПК-3       | Н7 |
| 30 | Подготовить доклад по теме ИБ с учетом требований ИБ   | ОПК-3       | Н7 |
| 31 | Подготовить научную публикацию по теме ИБ с учетом требований ИБ   | ОПК-3       | Н8 |
| 32 | Разработать Политику безопасности объекта  | ОПК-3       | Н8 |
| 33 | Разработать Концептуальную модель информационной безопасности объекта  | ОПК-3       | Н8 |

### 5.3.9. Вопросы для контрольной (расчетно-графической) работы

Не предусмотрено

## 5.4. Система оценивания достижения компетенций

### 5.4.1. Оценка достижения компетенций в ходе промежуточной аттестации

| Индикаторы дотижения компетенций  |   | Номера           |
|---|---|------------------|
| Код   | Содержание  | вопросы к зачету |
| 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 |   |                  |
| З1  | основы личной информационной безопасности   | 5, 13-15         |
| З6  | основные информационной безопасности  | 1-4, 9-12        |
| У1  | применять методы обеспечения личной информационной безопасности   |                  |
| У7  | использовать инструменты и методы обеспечения информационной безопасности   |                  |
| Н1  | обеспечения личной информационной безопасности  |                  |
| Н7  | подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности |                  |
| Н8  | описания системы обеспечения информационной безопасности  |                  |
| ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью   |   |                  |
| З5  | нормативное обеспечение информационной безопасности   | 6-8              |
| У6  | использовать нормативно-правовые акты по вопросам информационной безопасности   |                  |
| Н5  | обоснования мероприятий по обеспечению информационной безопасности  |                  |
| ПК-10 Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью   |   |                  |
| З5  | принципы обеспечения информационной безопасности организации  | 16-30            |
| У5  | управлять информационной безопасностью  |                  |
| Н6  | использования средств обеспечения информационной безопасности   |                  |

**5.4. Система оценивания достижения компетенций**  
**5.4.2. Оценка достижения компетенций в ходе текущего контроля**

| Индикаторы достижения компетенций   |   | Номера вопросов и задач                  |                        |                             |
|---|---|--|------------------------|-----------------------------|
| Код   | Содержание  | вопросы тестов                           | вопросы устного опроса | задачи для проверки навыков |
| 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 |   |  |                        |                             |
| 31  | основы личной информационной безопасности   | 3-5, 7, 13, 20-22, 26, 27, 31            | 3, 16, 17              |                             |
| 36  | основные информационной безопасности  | 1, 6, 14-16, 18, 19, 23-25, 28-30, 32-64 | 1, 2, 4-15, 18-41      |                             |
| У1  | применять методы обеспечения личной информационной безопасности   | 2, 8, 11, 12                             |                        | 2, 4, 7                     |
| У7  | использовать инструменты и методы обеспечения информационной безопасности   | 9, 10, 17                                |                        | 1, 3, 5, 6                  |
| Н1  | обеспечения личной информационной безопасности  |  |                        | 8, 9, 27, 28                |
| Н7  | подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности |  |                        | 29, 30                      |
| Н8  | описания системы обеспечения информационной безопасности  |  |                        | 31-33                       |
| ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью   |   |  |                        |                             |
| 35  | нормативное обеспечение информационной безопасности   | 65, 69-77, 79-81                         | 42-49                  |                             |
| У6  | использовать нормативно-правовые акты по вопросам информационной безопасности   | 66-68, 78                                |                        | 10, 12, 13, 17              |
| Н6  | обоснования мероприятий по обеспечению информационной безопасности  |  |                        | 11,14-16                    |
| ПК-10 Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью   |   |  |                        |                             |
| 35  | принципы обеспечения информационной безопасности организации  | 82-97, 99-106, 108-139                   | 50-98                  |                             |
| У5  | управлять информационной безопасностью  | 98, 107                                  |                        | 24-26                       |
| Н6  | использования средств обеспечения информационной безопасности   |  |                        | 18-23                       |

## 6. Учебно-методическое обеспечение дисциплины

### 6.1. Рекомендуемая литература

| № | Библиографическое описание   | Вид издания   |
|---|--|---------------|
| 1 | Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2019 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="http://znanium.com/catalog/document?id=336219">http://znanium.com/catalog/document?id=336219</a>  | Учебное       |
| 2 | Горюхина Е. Ю. Информационная безопасность: учебное пособие: для студентов, обучающихся по специальности 38.05.01 "Экономическая безопасность" / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева; Воронежский государственный аграрный университет - Воронеж: Воронежский государственный аграрный университет, 2015 - 221 с. [ЦИТ 13054] [ПТ] URL: <a href="http://catalog.vsau.ru/elib/books/b107623.pdf">http://catalog.vsau.ru/elib/books/b107623.pdf</a> | Учебное       |
| 3 | Гришина Н. В. Информационная безопасность предприятия [электронный ресурс]: Учебное пособие / Н. В. Гришина - Москва: Издательство "ФОРУМ", 2017 - 239 с. [ЭИ] [ЭБС Знаниум] URL: <a href="http://znanium.com/catalog/document?id=188855">http://znanium.com/catalog/document?id=188855</a>  | Учебное       |
| 4 | Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова.- Воронеж: ВГАУ, 2015. - 93 с. <URL: <a href="http://catalog.vsau.ru/elib/books/b107312.pdf">http://catalog.vsau.ru/elib/books/b107312.pdf</a> >  | Методическое  |
| 5 | Улезько А.В. Порядок оценивания результатов достижения компетенций: методические материалы для основной образовательной программы по направлению: 09.03.03 Прикладная информатика, профиль: Информационные системы и технологии в менеджменте АПК / А.В. Улезько, С.А. Кулев, А.А. Толстых. – Воронеж: ВГАУ, 2019. – 24 с.   | Методическое  |
| 6 | Улезько А. В. Порядок формирования компетенций: методические материалы для основной образовательной программы бакалавриата по направлению: 09.03.03 Прикладная информатика, профиль: Информационные системы и технологии в менеджменте АПК / А.В. Улезько, С.А. Кулев, А.А. Толстых. – Воронеж: ВГАУ, 2019. – 39 с   | Методическое  |
| 7 | Бизнес - информатика: рецензируемый междисциплинарный научный журнал / Учредитель : Национальный исследовательский университет "Высшая школа экономики" - Москва: Национальный исследовательский университет "Высшая школа экономики", 2020 [ЭИ] URL: <a href="https://www.elibrary.ru/contents.asp?titleid=27958">https://www.elibrary.ru/contents.asp?titleid=27958</a>  | Периодическое |
| 8 | Информация и безопасность: [научный журнал] / Учредитель : Воронежский государственный технический университет - Воронеж: Воронежский государственный технический университет, 2020 [ЭИ] URL: <a href="https://www.elibrary.ru/contents.asp?titleid=8748">https://www.elibrary.ru/contents.asp?titleid=8748</a>  | Периодическое |

### 6.2. Ресурсы сети Интернет

#### 6.2.1. Электронные библиотечные системы

| № | Название                    |
|---|-----------------------------|
| 1 | Лань                        |
| 2 | ZNANIUM.COM                 |
| 3 | ЮРАЙТ                       |
| 4 | IPRbooks                    |
| 5 | E-library                   |
| 6 | Электронная библиотека ВГАУ |

### 6.2.2. Профессиональные базы данных и информационные системы

| № | Название  | Размещение  |
|---|---|---|
| 1 | База данных показателей муниципальных образований | <a href="http://www.gks.ru/free_doc/new_site/bd_munst/munst.htm">http://www.gks.ru/free_doc/new_site/bd_munst/munst.htm</a> |
| 2 | Справочная правовая система Гарант                | <a href="http://www.consultant.ru/">http://www.consultant.ru/</a>   |
| 3 | Справочная правовая система Консультант Плюс      | <a href="http://ivo.garant.ru">http://ivo.garant.ru</a>   |

### 6.2.3. Сайты и информационные порталы

| № | Название  | Размещение  |
|---|---|---|
| 1 | Information Security/Информационная безопасность                  | <a href="http://www.egovernment.ru">http://www.egovernment.ru</a>       |
| 2 | SecurityLab: защита информации и информационная безопасность      | <a href="http://www.securitylab.ru/">http://www.securitylab.ru/</a>     |
| 3 | Threatpost - сайт об информационной безопасности от Kaspersky Lab | <a href="https://threatpos">https://threatpos</a>                       |
| 4 | Anti-Malware - сайт Информационно-аналитического центра           | <a href="https://www.anti-malware.ru/">https://www.anti-malware.ru/</a> |

## 7. Материально-техническое и программное обеспечение дисциплины

### 7.1. Помещения для ведения образовательного процесса и оборудование




| № | Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения  | Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор) |
|---|---|--|
| 1 | Учебная аудитория для проведения занятий лекционного типа: комплект учебной мебели, демонстрационное оборудование, учебно-наглядные пособия в виде презентаций, программное обеспечение: MS Windows /Linux /Ред ОС  | 394087, Воронежская область, г. Воронеж, ул. Мичурина, д.1   |
| 2 | Учебная аудитория для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации: комплект учебной мебели, учебно-наглядные пособия в электронном виде, компьютеры с возможностью подключения к Интернет и доступом в ЭИОС; программное обеспечение: MS Windows /Linux /Ред ОС, MS Office / OpenOffice/ LibreOffice, DrWeb ES, 7-Zip, MediaPlayer Classic, Яндекс браузер / Mozilla Firefox / Internet Explorer, AST Test | 394087, Воронежская область, г. Воронеж, ул. Мичурина, д.1   |
| 3 | Учебная аудитория для проведения лабораторных и практических занятий, индивидуальных и групповых консультаций: комплект учебной мебели, компьютеры с возможностью подключения к "Интернет" и обеспечением доступа в ЭИОС; программное обеспечение: MS Windows /Linux /Ред ОС, MS Office / OpenOffice/LibreOffice, DrWeb ES, 7-Zip, MediaPlayer Classic, Яндекс браузер / Mozilla Firefox / Internet Explorer, AST Test                                      | 394087, Воронежская область, г. Воронеж, ул. Мичурина, д.1   |
| 4 | Помещение для хранения и профилактического обслуживания учебного оборудования: мебель для хранения и обслуживания учебного оборудования, специализированное оборудование для ремонта компьютеров  | 394087, Воронежская область, г. Воронеж, ул. Мичурина, д.1, а.: 117, 118   |
| 5 | Помещение для самостоятельной работы: комплект учебной мебели, компьютеры с возможностью подключения к "Интернет" и обеспечением доступа в ЭИОС; программное обеспечение: MS Windows /Linux /Ред ОС, MS Office / OpenOffice/LibreOffice, DrWeb ES, 7-Zip, MediaPlayer Classic, Яндекс браузер / Mozilla Firefox / Internet Explorer, AST Test   | 394087, Воронежская область, г. Воронеж, ул. Мичурина, д.1, а.: 113, 115, 116, 119, 120, 122, 122а, 126, 219 (с 16.00 до 20.00)  |

## 7. Материально-техническое и программное обеспечение дисциплины

### 7.2. Программное обеспечение

| № | Название   | Размещение               |
|---|--|--------------------------|
| 1 | Операционные системы MS Windows /Linux /Ред ОС               | ПК в локальной сети ВГАУ |
| 2 | Пакеты офисных приложений MS Office / OpenOffice/LibreOffice | ПК в локальной сети ВГАУ |
| 3 | Программы для просмотра файлов Adobe Reader / DjVu Reader    | ПК в локальной сети ВГАУ |
| 4 | Браузеры Яндекс Браузер / Mozilla Firefox / Microsoft Edge   | ПК в локальной сети ВГАУ |
| 5 | Антивирусная программа DrWeb ES                              | ПК в локальной сети ВГАУ |
| 6 | Программа-архиватор 7-Zip                                    | ПК в локальной сети ВГАУ |
| 7 | Мультимедиа проигрыватель MediaPlayer Classic                | ПК в локальной сети ВГАУ |
| 8 | Платформа онлайн-обучения eLearning server                   | ПК в локальной сети ВГАУ |
| 9 | Система компьютерного тестирования AST Test                  | ПК в локальной сети ВГАУ |

## 8. Междисциплинарные связи

| Взаимосвязанные дисциплины |  | Кафедра, на которой преподается дисциплина                           | Подпись заведующего кафедрой  |
|----------------------------|--|--|---|
| Код                        | Название                                     |  |   |
| Б1.О.05                    | Право и основы противодействия коррупции     | Истории, философии и социально-политических дисциплин                |  |
| Б1.В.07                    | Обучение пользователей информационных систем | Информационного обеспечения и моделирования агроэкономических систем |  |
| Б1.В.13                    | Управление IT-проектами                      | Информационного обеспечения и моделирования агроэкономических систем |  |

Лист периодических проверок рабочей программы и информация о внесенных изменениях

| Должностное лицо,<br>проводившее проверку<br>Ф.И.О., должность,<br>подпись | Дата                              | Потребность<br>в корректировке указанием<br>соответствующих разделов рабочей<br>программы                            | Информация о внесенных изменениях   |
|--|-----------------------------------|--|---|
| Зав. кафедрой<br>А.В. Улезько  | Протокол № 11 от<br>09.06.2022 г. | Имеется<br>п. 3, 3.1, 3.2 п. 4.2, п. 7.1, п. 7.2<br>Рабочая программа актуализирована на<br>2022-2023<br>учебный год | Скорректирован объем часов по видам<br>контактной и самостоятельной работы,<br>изменен браузер, уточнено<br>программное обеспечение |
| И.о. зав. кафедрой<br>А.Н. Черных  | Протокол № 12 от<br>20.06.2023 г. | Нет<br>Рабочая программа актуализирована на<br>2023-2024<br>учебный год  | Нет   |
| Зав. кафедрой<br>Р.В. Подколзин  | Протокол № 8 от<br>26.04.2024 г.  | Нет<br>Рабочая программа актуализирована на<br>2024-2025 учебный год   | Нет   |
| Зав. кафедрой<br>Р.В. Подколзин  | Протокол №7 от<br>15.05.2025 г.   | Нет<br>Рабочая программа актуализирована на<br>2025-2026<br>учебный год  | Нет   |
|  |                                   |  |   |
|  |                                   |  |   |
|  |                                   |  |   |
|  |                                   |  |   |
|  |                                   |  |   |
|  |                                   |  |   |
|  |                                   |  |   |
|  |                                   |  |   |