

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.Н. Черных

«18» июня 2025г.



## 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-2025

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 №7 от 15.05.2025 г.)

Заведующий кафедрой:



Р.В. Подколзин

Рабочая программа рекомендована к использованию в учебном процессе на заседании методической комиссии экономического факультета (протокол №10 от 17.06.2025 г.)

Председатель методической комиссии:



Л.В. Брянцева

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
  - 4.3. Перечень тем и учебно-методического обеспечения для самостоятельной работы обучающихся
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
    - 7.2.1. Программное обеспечение общего назначения
    - 7.2.2. Специализированное 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

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.06 Обучение пользователей информационных систем

Б1.В.12 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                                                                                                                                      |
|             |                                                                                                                                                                                                                                           | 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  |      |
| Основы информационной безопасности                                                |                   |     |      |
| Информационная безопасность в системе национальной безопасности России            | 3,3               | 3,0 | 10,1 |
| Угрозы информационной безопасности                                                | 3,3               | 3,0 | 10,1 |
| Компьютерные преступления и правовые основы защиты информации                     |                   |     |      |
| Компьютерные преступления и их особенности                                        | 3,3               | 3,0 | 10,2 |
| Законодательные аспекты информационной безопасности в РФ                          | 3,3               | 3,0 | 10,2 |
| Системное обеспечение защиты информации                                           |                   |     |      |
| 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  |      |
| Основы информационной безопасности                                                |                   |     |      |
| Информационная безопасность в системе национальной безопасности России            | 1,0               | 1,0 | 14,4 |
| Угрозы информационной безопасности                                                | 1,0               | 1,0 | 14,4 |
| Компьютерные преступления и правовые основы защиты информации                     |                   |     |      |
| Компьютерные преступления и их особенности                                        | 1,0               | 1,0 | 14,5 |
| Законодательные аспекты информационной безопасности в РФ                          | 1,0               | 1,0 | 14,5 |
| Системное обеспечение защиты информации                                           |                   |     |      |
| Криптографические методы защиты информации                                        | 1,0               | 1,0 | 14,5 |
| Системное обеспечение защиты информации, обрабатываемой в информационных системах | 1,0               | 1,0 | 14,5 |

#### 4.3. Перечень тем и учебно-методического обеспечения для самостоятельной работы обучающихся

| Разделы, подразделы дисциплины                                         | Учебно-методическое обеспечение                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Объем часов СР |         |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|---------|
|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | очная          | заочная |
| Основы информационной безопасности                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                |         |
| Информационная безопасность в системе национальной безопасности России | Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2022 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=393765">https://znanium.com/catalog/document?id=393765</a><br>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><br>Гришина Н. В. Информационная безопасность предприятия [электронный ресурс]: Учебное пособие / Н. В. Гришина - Москва: Издательство "ФОРУМ", 2022 - 239 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=399940">https://znanium.com/catalog/document?id=399940</a><br>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> > | 10,1           | 14,4    |
| Угрозы информационной безопасности                                     | Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2022 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=393765">https://znanium.com/catalog/document?id=393765</a><br>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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 10,1           | 14,4    |
| Компьютерные преступления и правовые основы защиты информации          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                |         |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |      |      |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|
| Компьютерные преступления и их особенности               | <p>Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2024 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.ru/catalog/document?id=442107">https://znanium.ru/catalog/document?id=442107</a></p> <p>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></p> <p>Гришина Н. В. Информационная безопасность предприятия [электронный ресурс]: Учебное пособие / Н. В. Гришина - Москва: Издательство "ФОРУМ", 2022 - 239 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=399940">https://znanium.com/catalog/document?id=399940</a></p> <p>Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова.- Воронеж: ВГАУ, 2015. - 93 с. &lt;URL:<a href="http://catalog.vsau.ru/elib/books/b107312.pdf">http://catalog.vsau.ru/elib/books/b107312.pdf</a>&gt;</p> | 10,2 | 14,5 |
| Законодательные аспекты информационной безопасности в РФ | <p>Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2022 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=393765">https://znanium.com/catalog/document?id=393765</a></p> <p>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></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 10,2 | 14,5 |
| <b>Системное обеспечение защиты информации</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |      |      |
| Криптографические методы защиты информации               | <p>Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2022 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=393765">https://znanium.com/catalog/document?id=393765</a></p> <p>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></p> <p>Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова.- Воронеж: ВГАУ, 2015. - 93 с. &lt;URL:<a href="http://catalog.vsau.ru/elib/books/b107312.pdf">http://catalog.vsau.ru/elib/books/b107312.pdf</a>&gt;</p>                                                                                                                                                                                                                                                                                                    | 10,2 | 14,5 |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |             |             |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|
| <p>Системное обеспечение защиты информации, обрабатываемой в информационных системах</p> | <p>Баранова Е. К. Информационная безопасность и защита информации [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш - Москва: Издательский Центр РИОР, 2024 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.ru/catalog/document?id=442107">https://znanium.ru/catalog/document?id=442107</a></p> <p>Гришина Н. В. Информационная безопасность предприятия [электронный ресурс]: Учебное пособие / Н. В. Гришина - Москва: Издательство "ФОРУМ", 2022 - 239 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=399940">https://znanium.com/catalog/document?id=399940</a></p> <p>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></p> <p>Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова.- Воронеж: ВГАУ, 2015. - 93 с. &lt;URL:<a href="http://catalog.vsau.ru/elib/books/b107312.pdf">http://catalog.vsau.ru/elib/books/b107312.pdf</a>&gt;</p> | <p>10,2</p> | <p>14,5</p> |
| <p>Итого</p>                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>61,0</p> | <p>87,0</p> |

## 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, У7, Н1, Н7, Н8 |            |            |
| Угрозы информационной безопасности                                                | 31, 36, У1, У7, Н1, Н7,    |            |            |
| <b>Компьютерные преступления и правовые основы защиты информации</b>              |                            |            |            |
| Компьютерные преступления и их особенности                                        | 31, 36, У1, 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                    | 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 проекта (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<br>критичной информацией;<br>информацией общего доступа;<br>персональными данными. | ОПК-3       | 36 |
| 2  | Убытки, которые могут возникнуть вследствие внесения изменений в информацию, если факт модификации не был обнаружен, называются<br>стоимость скрытого нарушения целостности<br>стоимость утраты<br>стоимость потери конфиденциальности                                                                                                                                                                                   | ОПК-3       | 36 |
| 3  | Категория ценности информации, определяющая гарантию того, что источником информации является именно то лицо, которое заявлено как ее автор, называется<br>аутентичность<br>апеллируемость<br>достоверность                                                                                                                                                                                                              | ОПК-3       | 31 |
| 4  | Идентификация и аутентификация применяются:<br>для обеспечения целостности данных<br>для защиты от компьютерных вирусов<br>для ограничения доступа случайных и незаконных субъектов к информационной системе<br>для повышения физической защиты информационной системы                                                                                                                                                   | 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<br>аутентичность<br>апеллируемость                                                                                                                                                                                            | ОПК-3       | 31 |
| 6  | Для ограничения доступа случайных и незаконных субъектов к информационной системе применяются идентификация и .....:<br>Правильный ответ:                                                                                                                                                                                                                                                                                | ОПК-3       | 31 |
| 7  | Процесс распознавания пользователя автоматизированной системой, для чего предъявляется уникальное имя, называется ..... (в им.пад.)<br>Правильный ответ:                                                                                                                                                                                                                                                                 | ОПК-3       | 31 |
| 8  | Подберите слово к данному определению: «..... - присвоение субъектам личного идентификатора и сравнение его с заданным»<br>Правильный ответ:                                                                                                                                                                                                                                                                             | ОПК-3       | 31 |
| 9  | Процедура проверки подлинности, предназначенная для подтверждения истинности пользователя, предъявившего идентификатор, называется «.....» (в им. пад.)<br>Правильный ответ:                                                                                                                                                                                                                                             | ОПК-3       | 31 |
| 10 | Что из перечисленного является составляющей информационной безопасности?<br>антивирусная защита<br>санкционированный доступ к информации<br>несанкционированный доступ к информации<br>целостность информации                                                                                                                                                                                                            | ОПК-3       | 31 |
| 11 | Конфиденциальность информации гарантирует<br>доступность информации только тому кругу лиц, для кого она предназначена<br>защищенность информации от потери<br>доступность информации только автору                                                                                                                                                                                                                       | ОПК-3       | 31 |
| 12 | Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена – это<br>разглашение;<br>утечка;<br>несанкционированный доступ.                                                                                                                                                                                                                                         | ОПК-3       | 31 |

|    |                                                                                                                                                                                                                                                                                          |       |    |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 13 | Укажите, что не является преднамеренным воздействием на информационную систему<br>подбор пароля<br>перехват информации<br>хищение информации<br>модификация информации<br>стихийные бедствия                                                                                             | ОПК-3 | У7 |
| 14 | Укажите, что не является причиной случайных воздействия на информационную систему<br>подбор пароля<br>отказы и сбои аппаратуры<br>ошибки персонала<br>помехи в линиях связи из-за воздействий внешней среды.                                                                             | ОПК-3 | У7 |
| 15 | Ущерб от полного или частичного разрушения информации называется<br>стоимость скрытого нарушения целостности;<br>стоимость утраты;<br>стоимость потери конфиденциальности.                                                                                                               | ОПК-3 | У1 |
| 16 | Укажите составляющие информационной безопасности<br>доступность информации<br>целостность информации<br>конфиденциальность информации<br>проверка прав доступа к информации<br>выявление нарушителей                                                                                     | ОПК-3 | У1 |
| 17 | Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации называется<br>угрозой информационной безопасности<br>несанкционированным доступом к информации<br>фальсификацией информации | ОПК-3 | 36 |
| 18 | Доступность информации гарантирует<br>получение требуемой информации за определенное время<br>неизменность информации в любое время<br>получение требуемой информации за неопределенное время<br>защищенность информации от возможных угроз                                              | ОПК-3 | 36 |
| 19 | Целостность информации гарантирует<br>существование информации в исходном виде<br>принадлежность информации автору<br>доступ информации определенному кругу пользователей<br>защищенность информации от несанкционированного доступа                                                     | ОПК-3 | 36 |
| 20 | Присвоение субъектам идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем идентификаторов, владельцы которых допущены к информационной системе, называется<br>идентификацией<br>аутентификацией<br>аутентичностью<br>конфиденциальностью                           | ОПК-3 | 36 |
| 21 | Подберите слово к данному определению : ..... - присвоение субъектам личного идентификатора и сравнение его с заданным<br>аутентификация<br>идентификация<br>аутентичность<br>конфиденциальность                                                                                         | ОПК-3 | 36 |
| 22 | Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации называется ..... (в им. падеже) информационной безопасности<br>Правильный ответ:                                            | ОПК-3 | 36 |
| 23 | Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним – это<br>разглашение;<br>утечка;<br>несанкционированный доступ.                                                                                            | ОПК-3 | 36 |

|    |                                                                                                                                                                                                                                                                                       |       |    |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 24 | Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам – это:<br>разглашение;<br>утечка;<br>несанкционированный доступ.                                                                                           | ОПК-3 | 36 |
| 25 | Укажите 3 вида угроз информационной безопасности:<br>угроза доступности информации<br>угроза целостности информации<br>угроза конфиденциальности информации<br>угроза идентификации информации                                                                                        | ПК-10 | 35 |
| 26 | При попытке внесения умышленных или случайных изменений в информацию, хранящуюся в информационной системе, возникает угроза нарушения её .....<br>Правильный ответ:                                                                                                                   | ПК-10 | 35 |
| 27 | Создание условий, при которых доступ к информации или информационной услуге будет невозможен или ограничен, ведёт к угрозе нарушения .....<br>Правильный ответ:                                                                                                                       | ПК-10 | 35 |
| 28 | Создание условий, при которых доступ к информации или информационной услуге будет невозможен или ограничен, ведёт к угрозе нарушения .....<br>Правильный ответ:                                                                                                                       | ПК-10 | 35 |
| 29 | Состояние защищенности информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации называется ..... безопасностью.<br>Правильный ответ: | ПК-10 | 35 |
| 30 | Комплекс средств и методов, направленных на предотвращение угроз информационной безопасности и устранение их последствий, называется ..... (в им. падеже) информации.<br>Правильный ответ:                                                                                            | ПК-10 | 35 |
| 31 | Мероприятия по формированию осознанного отношения сотрудников к обеспечению информационной безопасности относятся к:<br>предупреждению угроз;<br>выявлению угроз;<br>локализации угроз;<br>ликвидации последствий угроз.                                                              | ОПК-3 | 36 |
| 32 | Действия, направленные на устранение действующей угрозы и конкретных преступных действий относятся к :<br>предупреждению угроз;<br>выявлению угроз;<br>локализации угроз;                                                                                                             | ОПК-3 | 36 |
| 33 | Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним – это:<br>разглашение<br>утечка<br>несанкционированный доступ                                                                                           | ОПК-3 | 36 |
| 34 | Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам – это:<br>разглашение<br>утечка<br>несанкционированный доступ                                                                                              | ОПК-3 | 36 |
| 35 | Действия по восстановлению состояния, предшествовавшего возникновению угрозы, относятся к:<br>предупреждению угроз;<br>выявлению угроз;<br>локализации угроз;<br>ликвидации последствий угроз.                                                                                        | ОПК-3 | 36 |
| 36 | Защита от несанкционированного доступа к конфиденциальной информации обеспечивается выполнением:<br>только организационных мероприятий;<br>только технических мероприятий;                                                                                                            | ОПК-3 | 36 |

|    |                                                                                                                                                                                                                                              |       |    |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 37 | Определение состояния технической безопасности объекта относится к:<br>организационным мероприятиям;<br>техническим мероприятиям;<br>организационно-техническим мероприятиям.                                                                | ОПК-3 | 36 |
| 38 | Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства, называют:<br>компьютерным преступлением<br>несанкционированным действием<br>компьютерным мошенничеством                    | ОПК-3 | 36 |
| 39 | Любая программа, написанная с целью нанесения ущерба или использования ресурсов атакуемого компьютера, называется ..... программой<br>Правильный ответ:                                                                                      | ОПК-3 | 36 |
| 40 | Класс программ, способных к саморазмножению и модификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия, называется компьютерные .....<br>Правильный ответ:                                        | ОПК-3 | 36 |
| 41 | Укажите этапы жизненного цикла компьютерного вируса:<br>внедрение (инфицирование)<br>инкубационный период<br>заражение<br>саморазмножение (репродуцирование)<br>выполнение специальных функций<br>проявление<br>выявление                    | ОПК-3 | 36 |
| 42 | По среде обитания компьютерные вирусы подразделяют на:<br>файловые вирусы<br>загрузочные вирусы<br>файлово-загрузочные вирусы<br>сетевые вирусы<br>полиморфные вирусы<br>стелс-вирусы                                                        | ОПК-3 | 36 |
| 43 | Достаточно трудно обнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода, это:<br>полиморф-вирусы<br>стелс-вирусы<br>макро-вирусы<br>конструкторы вирусов                                         | ОПК-3 | 36 |
| 44 | Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (например, логина и пароля от электронной почты, номера телефона или данных банковской карты) называется ..... (в им. падеже). | ОПК-3 | 36 |
| 45 | ??? – это вирусы, заражающие файлы некоторых систем обработки документов (MS Word, MS Excel), которые имеют встроенные макро-языки<br>масго-вирусы<br>стелс-вирусы<br>полиморф-вирусы                                                        | ОПК-3 | 36 |
| 46 | ??? маскируют свое присутствие путем перехвата обращений ОС к пораженным файлам, секторам и переадресуют ОС к незараженным участкам<br>масго-вирусы<br>стелс-вирусы<br>полиморф-вирусы                                                       | ОПК-3 | 36 |
| 47 | Достаточно трудно обнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода, относятся к ..... вирусам.<br>Правильный ответ:                                                                         | ПК-10 | 35 |
| 48 | Программа, скрытно внедренная в защищенную систему и позволяющая злоумышленнику, путем модификации свойств системы защиты, осуществлять несанкционированный доступ к ресурсам системы, называется программой .....<br>Правильный ответ:      | ПК-10 | 35 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 49 | <p>Укажите 4 метода обнаружения компьютерных вирусов:</p> <p>сканирование</p> <p>обнаружение изменений</p> <p>эвристический анализ</p> <p>использование резидентных сторожей</p> <p>аналитическое преобразование</p>                                                                                                                                                                                                                       | ПК-10 | 35 |
| 50 | <p>Комплекс программных или аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами, позволяющий блокировать нежелательный сетевой трафик и обеспечивающий невидимость ПК в сети с целью предотвращения кибер атак, называется ..... экраном.</p> <p>Правильный ответ:</p>                                                                                     | ПК-10 | 35 |
| 51 | <p>Какие действия необходимо выполнить в случае обнаружения зараженных вредоносными программами файлов:</p> <p>завершить работу персонального компьютера (информационной системы) и немедленно сообщить специалисту по информационной безопасности</p> <p>проигнорировать сообщение антивирусной программы</p> <p>принять самостоятельные меры по предотвращению распространения заражения</p> <p>перезагрузить персональный компьютер</p> | ПК-10 | У5 |
| 52 | <p>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?</p> <p>нерезидентный вирус</p> <p>файловый вирус</p> <p>резидентный вирус</p>                                                                                                                                                              | ОПК-3 | 36 |
| 53 | <p>Самошифрование и полиморфичность используются для:</p> <p>саморазмножения вируса</p> <p>максимального усложнения процедуры обнаружения вируса</p> <p>расшифровки тел вируса</p> <p>для скрытия действий антивирусной программы</p>                                                                                                                                                                                                      | ОПК-3 | 36 |
| 54 | <p>Одним из наиболее эффективных способов борьбы с вирусами является:</p> <p>использование антивирусного программного обеспечения</p> <p>профилактика компьютерных вирусов</p> <p>ограничение доступа пользователей к ЭВМ</p> <p>шифрование данных</p>                                                                                                                                                                                     | ОПК-3 | 36 |
| 55 | <p>??? - это программа, скрытно внедренная в защищенную систему и позволяющая злоумышленнику, путем модификации свойств системы защиты, осуществлять несанкционированный доступ к ресурсам системы</p> <p>программная закладка</p> <p>тройная программа</p>                                                                                                                                                                                | ОПК-3 | 36 |
| 56 | <p>К деструктивным действиям, осуществляемым программными закладками относятся:</p> <p>копирование конфиденциальной информации</p> <p>изменение алгоритмов функционирования системных, прикладных и служебных программ</p> <p>навязывание определенных режимов работы</p> <p>уменьшают объем свободной памяти на диске в результате своего распространения</p> <p>снижают эффективность функционирования компьютерной системы</p>          | ОПК-3 | 36 |
| 57 | <p>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:</p> <p>тройной программой</p> <p>программной закладкой</p> <p>компьютерным вирусом</p>                                                                                                                                       | ОПК-3 | 36 |
| 58 | <p>??? – это компьютерная программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы:</p> <p>антивирусная программа</p> <p>программа обнаружения вторжений</p> <p>программная закладка</p>                                                                                                                                                                          | ОПК-3 | 36 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |    |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 59 | ??? - 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<br>сетевой экран (firewall)<br>маршрутизатор                                                                                              | ОПК-3 | 36 |
| 60 | Маски (сигнатуры) вирусов используются:<br>для поиска известных вирусов<br>для создания известных вирусов<br>для уничтожения известных вирусов<br>для размножения вирусов                                                                                                                                                                                                                                                              | ОПК-3 | 36 |
| 61 | 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):<br>Конституция РФ<br>Стратегия национальной безопасности РФ<br>Доктрина информационной безопасности РФ<br>Уголовный Кодекс РФ | ОПК-4 | У6 |
| 62 | Укажите документ, определяющий важнейшие задачи обеспечения информационной безопасности РФ:<br>Конституция РФ<br>Стратегия национальной безопасности РФ<br>Доктрина информационной безопасности РФ<br>Уголовный Кодекс РФ<br>Закон об информации, информационных технологиях и защите информации □                                                                                                                                     | ОПК-4 | У6 |
| 63 | Укажите сведения, имеющие конфиденциальный характер:<br>персональные данные<br>тайна следствия и судопроизводства<br>служебная тайна<br>профессиональная тайна<br>коммерческая тайна<br>сведения о сущности изобретения<br>план приема студентов в вуз<br>уставные документы бюджетной организации                                                                                                                                     | ОПК-4 | У6 |
| 64 | В предлагаемом перечне укажите мероприятия защиты информации предприятия, относящиеся к правовым?<br>организация режима и охраны;<br>разработка ведомственной нормативной документации;                                                                                                                                                                                                                                                | ОПК-4 | Н5 |
| 65 | Основополагающими документами по информационной безопасности в РФ являются:<br>Конституция РФ<br>Стратегия национальной безопасности РФ<br>Доктрина информационной безопасности РФ<br>Уголовный Кодекс РФ<br>Закон об информации, информационных технологиях и защите информации                                                                                                                                                       | ОПК-4 | Н5 |
| 66 | Сколько категорий государственных информационных ресурсов определяет ФЗ «Об информации, информационных технологиях и о защите информации» от 27.08.2006 г. № 149-ФЗ? (запишите цифрой)<br>Правильный ответ:                                                                                                                                                                                                                            | ОПК-4 | Н5 |
| 67 | Документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности, называется ..... информация.<br>Правильный ответ: конфиденциальная                                                                                                                                                        | ОПК-4 | 35 |
| 68 | Любая информация, с помощью которой можно однозначно идентифицировать физическое лицо, является ..... данными.<br>Правильный ответ:                                                                                                                                                                                                                                                                                                    | ОПК-4 | 35 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |    |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 69 | Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ, относятся к:<br>государственной тайне<br>документированной информации ограниченного доступа<br>служебной тайне                                                                                                         | ОПК-4 | 35 |
| 70 | Неправомерный доступ к компьютерной информации наказывается штрафом:<br>от пяти до двадцати минимальных размеров оплаты труда<br>от двухсот до пятисот минимальных размеров оплаты труда<br>от ста пятидесяти до двухсот минимальных размеров оплаты труда<br>до трехсот минимальных размеров оплаты труда                                                                                                                                                  | ОПК-4 | 35 |
| 71 | Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:<br>до года<br>до двух лет<br>до пяти лет<br>до трех месяцев                                                                                                                                                                                                                                                                                           | ОПК-4 | 35 |
| 72 | Создание, использование и распространение вредоносных программ для ЭВМ наказывается:<br>лишением свободы до года<br>штрафом до двадцати минимальных размеров оплаты труда<br>лишением свободы на срок до 3 лет со штрафом в размере от 200 до 500 минимальных размеров оплаты труда<br>исправительными работами до пяти лет                                                                                                                                 | ОПК-4 | 35 |
| 73 | Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается:<br>лишением права занимать определенные должности или заниматься определенной деятельностью до 5 лет<br>обязательными работами от 180 до 240 часов<br>ограничением свободы до 2 лет                                                                                                                                                                                                | ОПК-4 | 35 |
| 74 | Что такое Доктрина информационной безопасности РФ?<br>совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации;<br>совокупность нормативных актов, обязательных для выполнения всеми хозяйствующими субъектами;<br>совокупность документов, регламентирующих организационно-технические мероприятия по обеспечению информационной безопасности Российской Федерации. | ОПК-4 | 35 |
| 75 | Перечень сведений конфиденциального характера определен:<br>Указом Президента РФ от 6 марта 1997 г. № 188;<br>Федеральным законом от 27 июля 2006 г. N 149-ФЗ;<br>Указом Президента РФ от 30 ноября 1995 г. N 1203.                                                                                                                                                                                                                                         | ОПК-4 | 35 |
| 76 | Перечень сведений, доступ к которым не может быть ограничен, определен:<br>Федеральным законом от 27 июля 2006 г. N 149-ФЗ;<br>Указом Президента РФ от 6 марта 1997 г. № 188;<br>Указом Президента РФ от 30 ноября 1995 г. N 1203.                                                                                                                                                                                                                          | ОПК-4 | 35 |
| 77 | Наука о методах преобразования информации с целью ее защиты от несанкционированного доступа называется<br>Криптологией<br>Криптографией<br>Стеганографией<br>Стенографией<br>Криптоанализом                                                                                                                                                                                                                                                                 | ПК-10 | 35 |
| 78 | Наука (и практика ее применения) о методах и способах расшифрования информации без знания ключей называется<br>Стенографией<br>Стеганографией<br>Криптоанализом<br>Криптологией<br>Криптографией                                                                                                                                                                                                                                                            | ПК-10 | 35 |

|    |                                                                                                                                                                                                                                                           |       |    |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 79 | Набор средств и методов сокрытия факта передачи сообщения называется<br>Стенографией<br>Криптоанализом<br>Стеганографией<br>Криптологией<br>Криптографией                                                                                                 | ПК-10 | 35 |
| 80 | Процесс преобразования исходного (открытого) сообщения в шифрованное по определенным правилам, содержащимся в шифре называется<br>кодированием<br>шифрованием<br>дешифрованием<br>вскрытием шифра                                                         | ПК-10 | 35 |
| 81 | Процесс преобразования шифрованного сообщения (шифртекста) в исходное (открытое) сообщение с помощью определенных правил, содержащихся в шифре называется<br>кодированием<br>шифрованием<br>дешифрованием<br>вскрытием шифра                              | ПК-10 | 35 |
| 82 | Способ преобразования информации с целью ее защиты от незаконных пользователей называется<br>шифрованием<br>шифром<br>дешифрованием                                                                                                                       | ПК-10 | 35 |
| 83 | Процесс получения защищенного сообщения (открытого текста) из шифрованного сообщения (шифротекста) без знания примененного шифра называется:<br>шифрованием<br>дешифрованием<br>вскрытием шифра                                                           | ПК-10 | 35 |
| 84 | Сменный элемент шифра, применяемый для шифрования конкретных сообщений, называется<br>шифром<br>ключом<br>шифротекстом                                                                                                                                    | ПК-10 | 35 |
| 85 | Укажите способы преобразования при шифровании:<br>подстановка<br>кодирование<br>перестановка<br>аналитическое преобразование<br>сжатие/расширение<br>гаммирование                                                                                         | ПК-10 | 35 |
| 86 | Криптосистемой является<br>средство аппаратной защиты данных<br>система несанкционированного доступа к тексту<br>семейство обратимых преобразований открытого текста в шифрованный<br>семейство необратимых преобразований открытого текста в шифрованный | ПК-10 | 35 |
| 87 | Что из перечисленного не входит в криптосистему:<br>полиморфик-генератор<br>алгоритм шифрования<br>набор ключей, используемых для шифрования<br>система управления ключами                                                                                | ПК-10 | 35 |
| 88 | ГОСТ 28147-89 является стандартом ..... шифрования<br>Правильный ответ:                                                                                                                                                                                   | ПК-10 | 35 |
| 89 | Алгоритм RSA является стандартом:<br>симметричного шифрования<br>асимметричного шифрования<br>гаммирования<br>стеганографии                                                                                                                               | ПК-10 | 35 |

|     |                                                                                                                                                                                                                                                                                                                                                                    |       |    |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 90  | При асимметричном шифровании для шифрования и дешифрования используются:<br>два взаимосвязанных ключа<br>один открытый ключ<br>один закрытый ключ<br>два открытых ключа                                                                                                                                                                                            | ПК-10 | 35 |
| 91  | 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 электронную ..... | ПК-10 | 35 |
| 92  | Электронная подпись не обеспечивает:<br>контроль целостности документа<br>конфиденциальность документа<br>восстановление поврежденного документа<br>доказательное подтверждение авторства документа                                                                                                                                                                | ПК-10 | 35 |
| 93  | Укажите виды электронной подписи:<br>простая подпись<br>квалифицированная электронная подпись<br>усиленная неквалифицированная подпись<br>неквалифицированная электронная подпись<br>усиленная квалифицированная подпись                                                                                                                                           | ПК-10 | У5 |
| 94  | Алгоритмы шифрования бывают<br>многоядерные<br>с использованием хэш-функций<br>периодические<br>рекурсивные<br>симметричные                                                                                                                                                                                                                                        | ПК-10 | 35 |
| 95  | Алгоритмы шифрования бывают:<br>периодические<br>асимметричные<br>рекурсивные<br>симметричные                                                                                                                                                                                                                                                                      | ПК-10 | 35 |
| 96  | Электронная подпись устанавливает ??? информации<br>непротиворечивость<br>однозначность<br>противоречивость<br>целостность                                                                                                                                                                                                                                         | ПК-10 | 35 |
| 97  | Электронная подпись обеспечивает:<br>удостоверение источника документа<br>быструю пересылку документа<br>удаленный доступ к документу                                                                                                                                                                                                                              | ПК-10 | 35 |
| 98  | Электронная подпись обеспечивает<br>невозможность отказа от авторства<br>удаленный доступ к документу<br>быструю пересылку документа<br>невозможность установления автора                                                                                                                                                                                          | ПК-10 | 35 |
| 99  | Укажите программные модули или аппаратные устройства, регистрирующие каждое нажатие клавиши на клавиатуре компьютера<br>скриншоты<br>кейлоггеры<br>браузеры<br>брандмауэры                                                                                                                                                                                         | ПК-10 | 35 |
| 100 | Для генерации электронной подписи может быть использован алгоритм<br>DES<br>RSA<br>AES                                                                                                                                                                                                                                                                             | ПК-10 | 35 |
| 101 | Какие из перечисленных алгоритмов относятся к симметричным?<br>DES<br>RSA<br>ГОСТ 28147-89                                                                                                                                                                                                                                                                         | ПК-10 | 35 |

|     |                                                                                                                                                                                                                                                             |       |    |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 102 | Для контроля целостности передаваемых по сетям данных используется<br>аутентификация данных<br>аудит событий<br>электронная подпись<br>межсетевое экранирование                                                                                             | ПК-10 | 35 |
| 103 | В предлагаемом перечне выделите задачи, НЕ являющиеся задачами криптографии<br>межсетевое экранирование<br>шифровка информации в целях ее защиты от несанкционированного доступа<br>обеспечение целостности данных<br>аутентификация данных и их источников | ПК-10 | У5 |
| 104 | Что из перечисленного не является функцией управления криптографическими ключами<br>генерация<br>изучение<br>хранение<br>распределение                                                                                                                      | ПК-10 | 35 |
| 105 | Электронная подпись позволяет:<br>удостовериться в истинности отправителя и целостности сообщения<br>восстанавливать поврежденные сообщения<br>пересылать сообщения по секретному каналу<br>обеспечить конфиденциальность документа                         | ПК-10 | 35 |
| 106 | Размер ключа в ГОСТ 28147-89 равен:<br>64 бита<br>56 бит<br>128 бит<br>256 бит                                                                                                                                                                              | ПК-10 | 35 |
| 107 | Размер ключа в стандарте DES равен:<br>256 бит<br>128 бит<br>64 бита<br>56 бит                                                                                                                                                                              | ПК-10 | 35 |
| 108 | Символы исходного текста складываются с символами некой случайной последовательности – это<br>алгоритм перестановки<br>алгоритм аналитических преобразований<br>алгоритм гаммирования                                                                       | ПК-10 | 35 |
| 109 | Символы оригинального текста меняются местами по определенному принципу, являющемуся<br>секретным ключом – это<br>алгоритм подстановки<br>алгоритм перестановки<br>алгоритм гаммирования                                                                    | ПК-10 | 35 |
| 110 | Сферы применения DES-алгоритма<br>шифрование сведений, являющихся государственной тайной<br>заккрытие коммерческой информации<br>реализация электронной подписи                                                                                             | ПК-10 | 35 |
| 111 | Алгоритм ГОСТ 28147-89 использует ключ, являющийся<br>последовательностью чисел<br>массивом, состоящим из 32-мерных векторов<br>алфавитом                                                                                                                   | ПК-10 | 35 |
| 112 | Укажите основные области применения DES-алгоритма:<br>реализация электронной подписи<br>хранение данных на компьютере<br>электронная система платежей<br>аутентификация сообщений                                                                           | ПК-10 | 35 |
| 113 | Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов предприятия или организации, называется..... (в им. падеже)<br>безопасности.<br>Правильный ответ:                                 | ПК-10 | 35 |

|     |                                                                                                                                                                                                                                                                                             |       |    |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 114 | Стратегию организации в области информационной безопасности, меру внимания и количество ресурсов, которые руководство считает целесообразным выделить для обеспечения информационной безопасности, определяет:<br>концепция безопасности<br>стратегия безопасности<br>политика безопасности | ПК-10 | 35 |
| 115 | Организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз, называется ..... (в им. падеже) защиты информации.                                                                                         | ПК-10 | 35 |
| 116 | Каким способом в MS Word можно установить защиту документов от макровирусов?<br>Файл – Параметры – Центр управления безопасностью;<br>Файл – Параметры – Специальные возможности;<br>Файл – Учетная запись – Параметры обновления;<br>Рецензирование – Защитить;                            | ПК-10 | Н6 |
| 117 | Укажите верный вариант пароля с точки зрения современных требований:<br>1R#gO*v\$85<br>IvaNova2005<br>89089521318<br>электрификация                                                                                                                                                         | ПК-10 | Н6 |
| 118 | Каким способом в MS Word можно установить защиту на документ?<br>Файл – Сведения – Защитить документ<br>Файл - Сохранить<br>Файл – Общий доступ<br>Файл – Сохранить как                                                                                                                     | ПК-10 | Н6 |
| 119 | Каким способом в MS Excel можно установить защиту на ячейку от редактирования?<br>Формат ячеек – Защита затем Рецензирование - Защитить лист<br>Рецензирование - Защитить лист<br>Формат ячеек – Защита<br>Рецензирование – Защитить книгу                                                  | ПК-10 | Н6 |
| 120 | Вам позвонил человек, представился сотрудником службы безопасности и попросил предоставить Ваш пароль учетной записи или корпоративной почты для проведения работ по повышению защиты информации. Ваши действия:<br>откажу<br>предоставлю<br>поинтересуюсь для каких целей и предоставлю    | ПК-10 | У5 |
|     |                                                                                                                                                                                                                                                                                             |       |    |

### 5.3. Материалы для оценки достижения компетенций

#### 5.3.7. Вопросы для устного опроса

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

|    |                                                                                                                                                                                                              |       |    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|----|
| 34 | Что понимается под системой защиты информации? Сформулируйте основные принципы построения системы защиты информации. Какую роль играет подготовленность персонала в построении системы защиты информации?    | ПК-10 | 35 |
| 35 | Какие уровни задействованы в обеспечении информационной безопасности?                                                                                                                                        | ПК-10 | 35 |
| 36 | Что представляет собой политика безопасности организации?                                                                                                                                                    | ПК-10 | 35 |
| 37 | Что входит в анализ рисков?                                                                                                                                                                                  | ПК-10 | 35 |
| 38 | Перечислите основные модели защиты информации и их особенности.                                                                                                                                              | ПК-10 | 35 |
| 39 | В чем заключается сущность методов защиты от случайных угроз?                                                                                                                                                | ПК-10 | 35 |
| 40 | Дайте определение понятиям идентификации и аутентификации.                                                                                                                                                   | ПК-10 | 35 |
| 41 | В чем заключается повышение надежности и отказоустойчивости информационных систем?                                                                                                                           | ПК-10 | 35 |
| 42 | Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?                                                                                               | ПК-10 | 35 |
| 43 | Раскройте особенность построения защиты от несанкционированного доступа                                                                                                                                      | ПК-10 | 35 |
| 44 | Какие методы защиты информации относятся к криптографическим?                                                                                                                                                | ПК-10 | 35 |
| 45 | Дайте определение криптологии. Какие три основных периода криптологии вы знаете?                                                                                                                             | ПК-10 | 35 |
| 46 | Объясните понятие «криптологический алгоритм».                                                                                                                                                               | ПК-10 | 35 |
| 47 | Что такое криптография? Что собой представляют шифрование и дешифрование?                                                                                                                                    | ПК-10 | 35 |
| 48 | Какова суть преобразований перестановки и замены?                                                                                                                                                            | ПК-10 | 35 |
| 49 | Дайте определение аналитическому преобразованию, гаммированию и комбинированному                                                                                                                             | ПК-10 | 35 |
| 50 | Что такое системы с открытыми ключами? Приведите структурную схему процесса шифрования с открытым ключом. Дайте определение стойкости криптосистемы.                                                         | ПК-10 | 35 |
| 51 | Приведите основные программно-аппаратные реализации шифров.                                                                                                                                                  | ПК-10 | 35 |
| 52 | В чем заключается суть DES-алгоритма? Каковы его особенности? В каких режимах может работать DES-алгоритм?                                                                                                   | ПК-10 | 35 |
| 53 | Дайте описание отечественного алгоритма криптографического преобразования данных (ГОСТ 28147 - 89) и его отличительных особенностей. Какими характеристиками оценивается стойкость криптографических систем? | ПК-10 | 35 |
| 54 | В чем заключается суть электронной подписи?                                                                                                                                                                  | ПК-10 | 35 |
| 55 | Дайте определение межсетевого экрана. Назовите типы межсетевых экранов. Объясните различия между межсетевыми экранами разных типов.                                                                          | ПК-10 | 35 |
| 56 | Что представляет собой политика безопасности организации? На каком из уровней обеспечения информационной безопасности разрабатывается политика безопасности?                                                 | ПК-10 | 35 |
| 57 | Назовите компоненты концептуальной модели безопасности информации?                                                                                                                                           | ПК-10 | 35 |
| 58 | Что является содержанием административного уровня обеспечения информационной безопасности? На каких уровнях защиты информации реализуются организационные мероприятия?                                       | ПК-10 | 35 |
| 59 | Какой уровень обеспечения информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации?                                                                   | ПК-10 | 35 |
| 60 | Какие мероприятия защиты информации относятся к классу инженерно-техническим ?                                                                                                                               | ПК-10 | 35 |
| 61 | Что можно считать достоинствами и недостатками аппаратных средств инженерно-технической защиты информации?                                                                                                   | ПК-10 | 35 |
| 62 | Что предшествует началу работ по созданию или совершенствованию системы защиты информации (СЗИ)? С чего следует начинать мероприятия по созданию системы защиты информации?                                  | ПК-10 | 35 |

### 5.3.8. Задания для проверки формирования навыков

| №  | Содержание                                                                                                                                                                                                                                       | Компетенция | ИД |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----|
| 1  | Определите минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет                                                                                                                      | ОПК-3       | У1 |
| 2  | 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 |
| 3  | 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 |
| 4  | Определите время перебора всех паролей, состоящих из 6 цифр. Определите время перебора всех паролей с параметрами                                                                                                                                | ОПК-3       | У7 |
| 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  | Укажите последовательность действий в системе КриптоАРМ при выполнении подписания документа . Укажите последовательность действий в системе КриптоАРМ для выполнения открытия документа                                                          | ОПК-3       | Н1 |
| 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 | Охарактеризуйте структуру правовых актов, ориентированных на правовую защиту информации                                                                                                                                                          | ОПК-4       | У6 |
| 12 | Укажите как подразделяется информация ограниченного доступа в соответствии с ФЗ-149?                                                                                                                                                             | ОПК-4       | У6 |
| 13 | Перечислите 6 видов информации конфиденциального характера                                                                                                                                                                                       | ОПК-4       | У6 |
| 14 | Укажите в подготовленном перечне сведения, доступ к которым не может быть ограничен                                                                                                                                                              | ОПК-4       | Н5 |
| 15 | Выделите информацию конфиденциального характера. Выделите информацию ограниченного доступа                                                                                                                                                       | ОПК-4       | Н5 |
| 16 | Выделите основные организационные мероприятия по защите информации                                                                                                                                                                               | ОПК-4       | Н5 |
| 17 | Создайте в Outlook Express систему правил по обработке входящих сообщений электронной почты                                                                                                                                                      | ПК-10       | Н6 |
| 18 | Для отправления сообщения в Outlook Express , подписанного цифровой подписью и зашифрованного, получите цифровой идентификатор                                                                                                                   | ПК-10       | Н6 |
| 19 | Настройте параметры локальной политики безопасности ОС                                                                                                                                                                                           | ПК-10       | Н6 |
| 20 | Создайте учетную запись и локальную группу, измените принадлежность пользователя к локальной группе и заблокируйте учетную запись пользователя                                                                                                   | ПК-10       | Н6 |
| 21 | Загрузите редактор Шаблона безопасности, отредактируйте (модифицируйте настройку безопасности) шаблон безопасности и сохраните его с новым именем                                                                                                | ПК-10       | Н6 |
| 22 | Создайте VPN-подключение и выполните его настройку                                                                                                                                                                                               | ПК-10       | Н6 |
| 23 | Используя метод шифрования - "перестановка", зашифровать свои данные: фамилию, имя, отчество                                                                                                                                                     | ПК-10       | У5 |
| 24 | Используя метод шифрования - "замена", зашифровать свои данные: фамилию, имя, отчество                                                                                                                                                           | ПК-10       | У5 |
| 25 | Определите примерный перечень сведений, составляющих коммерческую (служебную) тайну                                                                                                                                                              | ПК-10       | У5 |
| 26 | Подготовить реферат по теме ИБ с учетом требований ИБ                                                                                                                                                                                            | ОПК-3       | Н7 |
| 27 | Подготовить доклад по теме ИБ с учетом требований ИБ                                                                                                                                                                                             | ОПК-3       | Н7 |
| 28 | Подготовить научную публикацию по теме ИБ с учетом требований ИБ                                                                                                                                                                                 | ОПК-3       | Н8 |
| 29 | Разработать Политику безопасности объекта                                                                                                                                                                                                        | ОПК-3       | Н8 |
| 30 | 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                                                                                                                                        |                  |
|                                                                                                                                                                                                                                                 | подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности |                  |
| Н7                                                                                                                                                                                                                                              |                                                                                                                                                                                       |                  |
| 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                                                                                                                      |                  |
| 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 дотижения 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                                                                                                                                             | 3-12                                 | 1-2                    |                             |
| 36                                                                                                                                                                                                                                              | основы информационной безопасности                                                                                                                                                    | 1-2,17-24, 31-46, 53-60              | 3-27                   |                             |
| У1                                                                                                                                                                                                                                              | применять методы обеспечения личной информационной безопасности                                                                                                                       | 15-16                                |                        | 1-3                         |
| У7                                                                                                                                                                                                                                              | использовать инструменты и методы обеспечения информационной безопасности                                                                                                             | 13-14                                |                        | 4-6                         |
| Н1                                                                                                                                                                                                                                              | обеспечения личной информационной безопасности                                                                                                                                        |                                      |                        | 7-9                         |
| Н7                                                                                                                                                                                                                                              | подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности |                                      |                        | 26-27                       |
| Н8                                                                                                                                                                                                                                              | описания системы обеспечения информационной безопасности                                                                                                                              |                                      |                        | 29-30                       |
| ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью                                                                                                 |                                                                                                                                                                                       |                                      |                        |                             |
| 35                                                                                                                                                                                                                                              | нормативное обеспечение информационной безопасности                                                                                                                                   | 67-76                                | 28-33                  |                             |
| У6                                                                                                                                                                                                                                              | использовать нормативно-правовые акты по вопросам информационной                                                                                                                      | 61-63                                |                        | 10-13                       |
| Н5                                                                                                                                                                                                                                              | обоснования мероприятий по обеспечению информационной безопасности                                                                                                                    | 64-66                                |                        | 14-16                       |
| ПК-10 Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью                                                                                                                                   |                                                                                                                                                                                       |                                      |                        |                             |
| 35                                                                                                                                                                                                                                              | принципы обеспечения информационной безопасности организации                                                                                                                          | 25-30, 47-51, 77-92, 94-102, 104-115 | 34-62                  |                             |
| У5                                                                                                                                                                                                                                              | управлять информационной безопасностью                                                                                                                                                | 103, 120                             |                        | 23-25                       |
| Н6                                                                                                                                                                                                                                              | использования средств обеспечения информационной безопасности                                                                                                                         | 116-119                              |                        | 17-22                       |

## 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, 2024 - 336 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.ru/catalog/document?id=442107">https://znanium.ru/catalog/document?id=442107</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", 2022 - 239 с. [ЭИ] [ЭБС Знаниум] URL: <a href="https://znanium.com/catalog/document?id=399940">https://znanium.com/catalog/document?id=399940</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.<br><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 | <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 учебных занятий : комплект учебной мебели, демонстрационное оборудование, учебно-наглядные пособия в виде презентаций, программное обеспечение: MS Windows /Linux /Пед ОС                                                                                                                                                                                | Российская Федерация, Воронежская область, городской округ город Воронеж, город Воронеж, улица Мичурина, дом 1                                                                                                                                                 |
| 2 | Учебная аудитория для проведения учебных занятий: комплект учебной мебели, учебно-наглядные пособия в электронном виде, компьютеры с возможностью подключения к Интернет и доступом в ЭИОС; программное обеспечение: MS Windows /Linux /Пед ОС, MS Office / OpenOffice/ LibreOffice, DrWeb ES, 7-Zip, MediaPlayer Classic, Яндекс браузер / Mozilla Firefox / Internet Explorer, AST Test | Российская Федерация, Воронежская область, городской округ город Воронеж, город Воронеж, улица Мичурина, дом 1, а. 113, 115, 116, 119, 120, 122, 122а, 219, 220                                                                                                |
| 3 | Учебная аудитория для проведения учебных занятий: комплект учебной мебели, компьютеры с возможностью подключения к "Интернет" и обеспечением доступа в ЭИОС; программное обеспечение: MS Windows /Linux /Пед ОС, MS Office / OpenOffice/LibreOffice, DrWeb ES, 7-Zip, MediaPlayer Classic, Яндекс браузер / Mozilla Firefox / Internet Explorer, AST Test                                 | Российская Федерация, Воронежская область, городской округ город Воронеж, город Воронеж, улица Мичурина, дом 1, а. а. 113, 115, 116, 119, 120, 122, 122а, 219, 220                                                                                             |
| 4 | Помещение для самостоятельной работы: комплект учебной мебели, компьютеры с возможностью подключения к "Интернет" и обеспечением доступа в ЭИОС; программное обеспечение: MS Windows /Linux /Пед ОС, MS Office / OpenOffice/LibreOffice, DrWeb ES, 7-Zip, MediaPlayer Classic, Яндекс браузер / Mozilla Firefox / Internet Explorer, AST Test                                             | Российская Федерация, Воронежская область, городской округ город Воронеж, город Воронеж, улица Мичурина, дом 1, а.: 113, 115, 116, 119, 120, 122, 122а, 126, 219 (с 16.00 до 20.00)                                                                            |

## **7.2. Программное обеспечение**

### **7.2.1. Программное обеспечение общего назначения**

| № | 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 |

### **7.2.2. Специализированное программное обеспечение**

**Не предусмотрено**

## 8. Междисциплинарные связи

| Взаимосвязанные дисциплины |                                                          | Кафедра, на которой преподается дисциплина                           | Подпись заведующего кафедрой                                                        |
|----------------------------|----------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Код                        | Название                                                 |                                                                      |                                                                                     |
| Б1.О.05                    | Правоведение и правовые основы противодействия коррупции | Истории, философии и социально-политических дисциплин                |  |
| Б1.В.06                    | Обучение пользователей информационных систем             | Информационного обеспечения и моделирования агроэкономических систем |  |
| Б1.В.12                    | Управление IT-проектами                                  | Информационного обеспечения и моделирования агроэкономических систем |  |

## Приложение 1

## Лист периодических проверок рабочей программы и информация о внесенных изменениях

[illegible]