

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Агабекян Раиса Левоновна

Должность: ректор

Дата подписания: 07.02.2024 08:44:31

Уникальный программный ключ:

4237c7ccb9b9e111bbaf1f4fcda9201d015c4dbaa12317747309b9b0cbe

**Негосударственное аккредитованное некоммерческое частное образовательное  
учреждение высшего образования  
«Академия маркетинга и социально-информационных технологий – ИМСИТ»  
(г. Краснодар)**

**(НАН ЧОУ ВО Академия ИМСИТ)**

УТВЕРЖДАЮ

Проректор по учебной работе, доцент

\_\_\_\_\_ Н.И. Севрюгина

20.11.2023

## Б1.О.26

# Информационная безопасность рабочая программа дисциплины (модуля)

|  |  |  |
|--|--|--|
| Закреплена за кафедрой                                       | <b>Кафедра математики и вычислительной техники</b>     |  |
| Учебный план   | 45.03.04 Интеллектуальные системы в гуманитарной сфере |  |
| Квалификация   | <b>бакалавр</b>  |  |
| Форма обучения   | <b>очная</b>   |  |
| Общая трудоемкость   | <b>3 ЗЕТ</b>   |  |
| Часов по учебному плану                                      | 108  | Виды контроля в семестрах:<br>зачеты с оценкой 4 |
| в том числе:   |  |  |
| аудиторные занятия   | 64   |  |
| самостоятельная работа                                       | 43,8   |  |
| контактная работа во время<br>промежуточной аттестации (ИКР) | 0  |  |

### Распределение часов дисциплины по семестрам

| Семестр<br>(<Курс>.<Семестр<br>на курсе>) | 4 (2.2) |      | Итого |      |
|---|---------|------|-------|------|
|   | УП      | РП   | УП    | РП   |
| Неделя                                    | 16 1/6  |      |       |      |
| Вид занятий                               | УП      | РП   | УП    | РП   |
| Лекции                                    | 16      | 16   | 16    | 16   |
| Лабораторные                              | 16      | 16   | 16    | 16   |
| Практические                              | 32      | 32   | 32    | 32   |
| Контактная работа<br>на аттестации        | 0,2     | 0,2  | 0,2   | 0,2  |
| Итого ауд.                                | 64      | 64   | 64    | 64   |
| Контактная работа                         | 64,2    | 64,2 | 64,2  | 64,2 |
| Сам. работа                               | 43,8    | 43,8 | 43,8  | 43,8 |
| Итого                                     | 108     | 108  | 108   | 108  |

Программу составил(и):

*к.тн, доцент, Капустин С.А.*

Рецензент(ы):

*д.тн, Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.*

Рабочая программа дисциплины

**Информационная безопасность**

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 45.03.04 Интеллектуальные системы в гуманитарной сфере (приказ Минобрнауки России от 24.04.2018 г. № 324)

составлена на основании учебного плана:

45.03.04 Интеллектуальные системы в гуманитарной сфере

утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры

**Кафедра математики и вычислительной техники**

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

|  |   |
|--|---|
| 1.1  | приобретение обучающимися знаний, навыков и умений, связанных с правовыми и программно-техническими методами защиты информации государственных и негосударственных организаций и учреждений |
| Задачи: систематизация теоретических знаний по обеспечению безопасности информации в системах управления, использующих современные информационные технологии;<br>выявление сущности, целей, задач и места методов и средств защиты информационных процессов в компьютерных системах в общей системе обеспечения безопасности информации на объектах информатизации;<br>изучение основных принципов применения методов и средств защиты информации при организации защиты информационных процессов в компьютерных системах;<br>изучение нормативно-руководящих документов, регламентирующих вопросы обеспечения безопасности информации в автоматизированных системах |   |

**2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

|                   |   |      |
|-------------------|---|------|
| Цикл (раздел) ОП: |   | Б1.О |
| <b>2.1</b>        | <b>Требования к предварительной подготовке обучающегося:</b>  |      |
| 2.1.1             | Право   |      |
| 2.1.2             | Вычислительные системы, сети и телекоммуникации   |      |
| 2.1.3             | Информатика   |      |
| 2.1.4             | Основы национальной безопасности  |      |
| <b>2.2</b>        | <b>Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b> |      |
| 2.2.1             | Проектирование информационных систем  |      |
| 2.2.2             | Учебная практика: Ознакомительная практика  |      |
| 2.2.3             | Учебная практика: Технологическая (проектно-технологическая) практика   |      |
| 2.2.4             | Администрирование баз данных  |      |

**3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ  
и планируемые результаты обучения****4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

| Код занятия | Наименование разделов и тем /вид занятия/  | Семестр / Курс | Часов | Компетенции   | Литература и эл. ресурсы  | Практ. подг. |
|-------------|--|----------------|-------|---|---|--------------|
|             | <b>Раздел 1. Информационная безопасность в системе национальной безопасности России</b>  |                |       |   |   |              |
| 1.1         | Доктрина информационной безопасности Российской Федерации<br>Основы информационной безопасности /Лек/  | 4              | 4     | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |              |
| 1.2         | Государственная политика в области обеспечения безопасности автоматизированных систем управления<br>Государственная политика Российской Федерации в области международной информационной безопасности<br>Защита персональных данных<br>Защита Государственной тайны /Пр/ | 4              | 10    | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |              |
| 1.3         | Допуск к Государственной тайне /Лаб/   | 4              | 4     | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |              |

|     |  |   |     |   |   |  |
|-----|--|---|-----|---|---|--|
| 1.4 | /Ср/   | 4 | 10  | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
|     | <b>Раздел 2. Информационная война, методы и средства ее ведения</b>  |   |     |   |   |  |
| 2.1 | Методы и средства ведения информационной войны /Лек/   | 4 | 2   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 2.2 | Сетецентрические войны<br>Фейки /Пр/   | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 2.3 | /Ср/   | 4 | 2   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
|     | <b>Раздел 3. Критерии защищенности компьютерных систем</b>   |   |     |   |   |  |
| 3.1 | Стандарты информационной безопасности /Лек/  | 4 | 2   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 3.2 | Угрозы безопасности информации<br>Основные типы политики безопасности доступа к данным.<br>Дискреционные и мандатные политики /Пр/ | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 3.3 | Защита от НСД /Лаб/  | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 3.4 | /Ср/   | 4 | 7,4 | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
|     | <b>Раздел 4. Защита информации, обрабатываемой в информационных системах</b>   |   |     |   |   |  |

|     |  |   |     |   |   |  |
|-----|--|---|-----|---|---|--|
| 4.1 | Защита информации в ГИС<br>Защита информации в КИИ /Лек/                   | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 4.2 | Работа со средствами защиты информации /Пр/                                | 4 | 10  | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 4.3 | Программно-аппаратная защита информации /Лаб/                              | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 4.4 | /Ср/   | 4 | 14  | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
|     | <b>Раздел 5. Защита АС и СВТ от внешнего электромагнитного воздействия</b> |   |     |   |   |  |
| 5.1 | Защита АС и СВТ от внешнего электромагнитного воздействия /Лек/            | 4 | 2   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 5.2 | Требования руководящих документов по защите от ПЭМИН /Пр/                  | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 5.3 | Методы защиты информации от утечки через ПЭМИН /Лаб/                       | 4 | 4   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 5.4 | /Ср/   | 4 | 8,4 | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14<br>Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 |  |
| 5.5 | DLP-системы. Заключение. /Лек/   | 4 | 2   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14                               |  |

|   |            |   |     |   |  |
|---|------------|---|-----|---|--|
| 5.6                                       | /Ср/       | 4 | 2   | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 | Л1.1 Л1.2 Л1.3 Л1.4 Л1.5<br>Л1.6 Л1.7 Л1.8 Л1.9 Л1.10<br>Л1.11 Л1.12 Л1.13 Л2.1 Л2.2<br>Л2.3 Л2.4 Л2.5 Л2.6 Л2.7<br>Л2.8 Л2.9 Л2.10 Л2.11 Л2.12<br>Л2.13 Л2.14 |
| <b>Раздел 6. Промежуточная аттестация</b> |            |   |     |   |  |
| 6.1                                       | Зачет /КА/ | 4 | 0,2 | ОПК-5.1<br>ОПК-5.2<br>ОПК-5.3<br>ПК-5.1 ПК-5.2 ПК-5.3<br>ПК-6.1 ПК-6.2 ПК-6.3 |  |

## 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

### 5.1. Контрольные вопросы и задания

Примерный перечень вопросов к зачету:

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Понятие политики безопасности информационных систем. Назначение политики безопасности.
6. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
7. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
8. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
9. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
10. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
11. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
12. Идентификация пользователей.
13. Аутентификация пользователей.
14. Авторизация.
15. Средства идентификации и аутентификации пользователей.
16. Защита от НСД.
17. Требования к СВТ.
18. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
19. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
20. Защита персональных данных.
21. Защита информации в ГИС.
22. Концепция информационной безопасности.
23. Распределенные информационные системы. Удаленные атаки на информационную систему.
24. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
25. Физические средства обеспечения информационной безопасности.
26. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
27. DLP-системы.

Задания:

Выполнить классификацию объекта информатизации.

1. Дано: В организации с частной формой собственности в качестве средств идентификации внедрена система, работающая на основе распознавания человека по отпечатку пальца или сетчатке глаза. Информация для распознавания хранится на сервере, работающем на платформе с сертифицированной ФСТЭК ОС Astra Linux Special Edition. Все системное и прикладное программное обеспечение выполнено в защищенном исполнении и проверено на отсутствие недеklarированных возможностей.

В базе данных сотрудников обрабатывается менее 10000 субъектов ПДн. Выполнить классификацию ИСПДн сотрудников организации, хранящейся на сервере и используемой для проверки их личности.

2. Дано: В частной поликлинике обработка персональных данных пациентов. Обработывается менее 20000 записей о субъектах ПДн. Выполнить классификацию ИСПДн пациентов поликлиники при условии, что актуальны НДВ в прикладном программном обеспечении. В системном программном обеспечении угрозы не актуальны.
3. Дано: В районной управе ведется автоматизированная обработка информации о планируемой и проведенной работе по благоустройству территории. Определить класс защищенности информационной системы при условии, что невозможность работы с ней приведет к увеличению времени получения и обработки информации, снизит эффективность работы соответствующего подразделения.
4. Дано: В государственной организации на одном из компьютеров ведется обработка секретных сведений. За компьютером, кроме администратора, работают пользователи user1 и user2. При этом они обрабатывают одну и ту же информацию, имеют одинаковый доступ к файлам друг друга. Определить класс автоматизированной системы.
5. Дано: В библиотеке ведется учет посетителей на сервере с сертифицированной ФСТЭК ОС Astra Linux Special Edition. Для регистрации в библиотеке указываются паспортные данные – ФИО, адрес, номер телефона, учитывается выбор изданий. Обработывается менее 30000 записей о субъектах ПДн. Выполнить классификацию ИСПДн при условии, что НДВ в системном и прикладном программном обеспечении не актуальны.
6. Дано: В государственной организации проводятся исследования в области повышения эффективности изготовления и прочности строительных материалов. Материалы исследований засекречены. На компьютере, где хранится секретная информация с итогами исследования, работают два пользователя. Они проводят опыты с разными строительными материалами и не имеют доступ к файлам друг друга. Определите класс автоматизированной системы.
7. Дано: В земельном фонде автоматизированная система ведет учет участков, находящихся в государственной и муниципальной собственности в масштабах одного региона. Обработка персональных данных в информационной системе не ведется. Нарушение достоверности обрабатываемой информации может повлечь умеренные негативные последствия для экономики региона.
8. Дано: В частной торговой организации ведется учет покупателей с целью предоставления им бонусных скидок при последующей покупке товаров. В информационной системе ведется учет фамилии, имени, отчества, номера телефона и номера водительского удостоверения клиента. В базе данных клиентов организации на момент классификации указано менее 3 тысяч человек. Потенциальный рост базы клиентов – не более 50 тысяч. Обработка ведется на АРМ, где установлено лицензионное программное обеспечение. Выполнить классификацию при условии, что:
- 1) НДВ в прикладном и системном ПО не актуальны.

## 5.2. Темы письменных работ

1. Основные принципы информационной безопасности.
2. Понятие и классификация угроз информационной безопасности.
3. Методы и средства защиты информационной безопасности.
4. Аутентификация и управление доступом в информационной безопасности.
5. Защита персональных данных в информационной безопасности.
6. Защита информационных систем от вредоносных программ.
7. Криптография и ее применение в информационной безопасности.
8. Защита беспроводных сетей и мобильных устройств.
9. Анализ уязвимостей и планирование реагирования на инциденты в информационной безопасности.
10. Управление рисками в информационной безопасности.
11. Социальная инженерия и защита от нее в информационной безопасности.
12. Защита от фишинга и спама в информационной безопасности.
13. Защита от DDoS-атак в информационной безопасности.
14. Защита от межсетевых атак в информационной безопасности.
15. Защита от внутренних угроз в информационной безопасности.
16. Защита от утечек информации в информационной безопасности.
17. Защита от направленных атак в информационной безопасности.
18. Международное сотрудничество в области информационной безопасности.
19. Правовые аспекты информационной безопасности.
20. Этические и профессиональные аспекты информационной безопасности.
21. Защита от внутренних угроз в компьютерных сетях.
22. Защита от вредоносных воздействий на промышленные системы.
23. Защита от киберпреступлений в информационной сфере.

24. Защита от спама и вирусов в электронной почте.
25. Защита от хищения информации в облачных системах.
26. Защита данных в системах электронного голосования.
27. Защита от угроз в сети Интернет в информационной безопасности.
28. Защита цифровых прав и свобод в информационной безопасности.
29. Защита информационных ресурсов и систем управления в информационной безопасности.
30. Роль государства в обеспечении информационной безопасности.

### 5.3. Фонд оценочных средств

Контрольные вопросы для проведения текущего контроля

#### 1. Угроза информационной безопасности Российской Федерации

совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере

совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в сфере общества и государства

#### 2. Информационная безопасность Российской Федерации

состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

взаимовязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

#### 3. Обеспечение информационной безопасности

осуществление взаимовязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

#### 4. Силы обеспечения информационной безопасности

государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

взаимовязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

#### 5. Средства обеспечения информационной безопасности

правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

взаимовязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

#### 6. Система обеспечения информационной безопасности

совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

взаимовязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

#### 7. Информационная инфраструктура Российской Федерации

совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

совокупность объектов информатизации, глобальных информационных систем, государственных информационных систем,



критических информационных инфраструктур, расположенных на территории Российской Федерации.

8. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?

законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;  
конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;  
соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;  
создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;  
продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

9. Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности?

обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;  
оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;  
планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;  
укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;  
повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности;

10. Свойства информации:

конфиденциальность  
целостность  
доступность  
непротиворечивость  
доказуемость  
все перечисленное

12. Информация, составляющая государственную тайну не может иметь гриф...

для служебного пользования  
секретно  
совершенно секретно  
особой важности

13. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации  
соблюдение норм международного права в сфере информационной безопасности  
выявление нарушителей и привлечение их к ответственности  
соблюдение конфиденциальности информации ограниченного доступа  
разработку методов и усовершенствование средств информационной безопасности

14. Система защиты государственных секретов

основывается на Уголовном Кодексе РФ  
регулируется секретными нормативными документами  
определена Законом РФ "О государственной тайне"  
все перечисленное

15. Действие Закона "О государственной тайне" распространяется

на всех граждан и должностных лиц РФ  
только на должностных лиц  
на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне  
на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

16. К государственной тайне относится...

сведения в военной области  
сведения о внешнеполитической и внешнеэкономической деятельности государства  
сведения в области экономики, науки и техники  
сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности  
все перечисленное

17. Документы, содержащие государственную тайну снабжаются грифом  
"секретно"  
"совершенно секретно"  
"особой важности"  
все перечисленное

18. Гриф "ДСП" используется  
для секретных документов  
для документов, содержащих коммерческую тайну  
как промежуточный для несекретных документов  
в учебных целях

19. Порядок засекречивания состоит в установлении следующих принципов:  
целесообразности и объективности  
необходимости и обязательности  
законности, обоснованности и своевременности  
всех перечисленных

20. Предельный срок пересмотра ранее установленных грифов секретности составляет  
5 лет  
1 год  
10 лет  
15 лет  
30 лет

21. Срок засекречивания сведений, составляющих государственную тайну  
составляет 10 лет  
ограничен 30 годами

22. Информация, составляющая государственную тайну не может иметь гриф...  
«для служебного пользования»  
«секретно»  
«совершенно секретно»  
«особой важности»

23. К государственной тайне относятся сведения о:  
о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации  
о размерах золотого запаса и государственных валютных резервах Российской Федерации  
о состоянии здоровья высших должностных лиц Российской Федерации

24. К государственной тайне относятся сведения о:  
о финансовой политике в отношении иностранных государств  
о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях  
о фактах нарушения законности органами государственной власти и их должностными лицами

25. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать ... лет.  
30  
25  
15  
10  
50

26. Перечни сведений, подлежащих засекречиванию, подлежат пересмотру не реже, чем раз в ... лет  
5  
7  
10  
15  
30

27. Информация это –  
сведения, поступающие от СМИ  
только документированные сведения о лицах, предметах, фактах, событиях  
сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления  
только сведения, содержащиеся в электронных базах данных

28. Степени секретности информации  
особой важности  
совершенно секретно  
секретно  
для служебного пользования  
не секретно

#### 5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

### 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

#### 6.1. Рекомендуемая литература

##### 6.1.1. Основная литература

|       | Авторы, составители                                     | Заглавие  | Издательство, год  |
|-------|---|---|--|
| Л1.1  | Шаньгин В. Ф.   | Информационная безопасность компьютерных систем и сетей                                 | Москва: Форум, 2021, URL: <a href="https://ibooks.ru/reading.php?short=1&amp;productid=361273">https://ibooks.ru/reading.php?short=1&amp;productid=361273</a>            |
| Л1.2  | Медведев В. А.  | Информационная безопасность. Введение в специальность + eПриложение: Тесты: Учебник     | Москва: КноРус, 2021, URL: <a href="https://book.ru/book/936335">https://book.ru/book/936335</a>   |
| Л1.3  | Бабаш А. В.,<br>Баранова Е. К.,<br>Мельников Ю. Н.      | Информационная безопасность. Лабораторный практикум + eПриложение: Учебное пособие      | Москва: КноРус, 2021, URL: <a href="https://book.ru/book/936566">https://book.ru/book/936566</a>   |
| Л1.4  | Мельников В. П., под ред.,<br>Куприянов А. И.           | Информационная безопасность: Учебник  | Москва: КноРус, 2021, URL: <a href="https://book.ru/book/939292">https://book.ru/book/939292</a>   |
| Л1.5  | Мельников В. П., под ред.,<br>Куприянов А. И.           | Информационная безопасность: Учебник  | Москва: КноРус, 2020, URL: <a href="https://book.ru/book/932059">https://book.ru/book/932059</a>   |
| Л1.6  | Мельников В. П.,<br>Куприянов А. И.,<br>Васильева Т. Ю. | Информационная безопасность: Учебник  | Москва: КноРус, 2020, URL: <a href="https://book.ru/book/932908">https://book.ru/book/932908</a>   |
| Л1.7  | Мельников В. П.,<br>Куприянов А. И.,<br>Васильева Т. Ю. | Информационная безопасность: Учебник  | Москва: КноРус, 2022, URL: <a href="https://book.ru/book/941809">https://book.ru/book/941809</a>   |
| Л1.8  | Озерский С.В.,<br>Попов И.В.                            | Информационная безопасность: Учебное пособие  | Самара: Самарский юридический институт ФСИН России, 2019, URL: <a href="http://znanium.com/catalog/document?id=358668">http://znanium.com/catalog/document?id=358668</a> |
| Л1.9  | Клименко И.С.   | Информационная безопасность и защита информации: модели и методы управления: Монография | Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: <a href="http://znanium.com/catalog/document?id=360289">http://znanium.com/catalog/document?id=360289</a>    |
| Л1.10 | Шаньгин В.Ф.  | Информационная безопасность компьютерных систем и сетей: Учебное пособие                | Москва: Издательский Дом "ФОРУМ", 2021, URL: <a href="http://znanium.com/catalog/document?id=364622">http://znanium.com/catalog/document?id=364622</a>                   |
| Л1.11 | Баранова Е.К., Бабаш А.В.                               | Информационная безопасность и защита информации: Учебное пособие                        | Москва: Издательский Центр РИО, 2021, URL: <a href="http://znanium.com/catalog/document?id=364911">http://znanium.com/catalog/document?id=364911</a>                     |
| Л1.12 | Сычев Ю.Н.  | Защита информации и информационная безопасность: Учебное пособие                        | Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: <a href="http://znanium.com/catalog/document?id=366835">http://znanium.com/catalog/document?id=366835</a>    |

|   | Авторы, составители  | Заглавие   | Издательство, год   |
|---|--|--|---|
| Л1.13   | Сычев Ю.Н.   | Защита информации и информационная безопасность: Учебное пособие   | Москва: ООО "Научно-издательский центр ИНФРА-М", 2022, URL: <a href="http://znanium.com/catalog/document?id=388766">http://znanium.com/catalog/document?id=388766</a>   |
| <b>6.1.2. Дополнительная литература</b>                                       |  |  |   |
|   | Авторы, составители  | Заглавие   | Издательство, год   |
| Л2.1  | Козьминых С. И.  | Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики: Монография  | Москва: КноРус, 2021, URL: <a href="https://book.ru/book/941548">https://book.ru/book/941548</a>  |
| Л2.2  | Бабаш А. В.,<br>Баранова Е. К.,<br>Мельников Ю. Н.   | Информационная безопасность. Практикум (+CD) (для бакалавров): Учебное пособие   | Москва: КноРус, 2016, URL: <a href="https://book.ru/book/918700">https://book.ru/book/918700</a>  |
| Л2.3  | Бабаш А. В.,<br>Баранова Е. К.,<br>Мельников Ю. Н.   | Информационная безопасность. Лабораторный практикум (для бакалавров)+ Электронные приложения на сайте <a href="http://www.book.ru">www.book.ru</a> : Учебное пособие | Москва: КноРус, 2018, URL: <a href="https://book.ru/book/926191">https://book.ru/book/926191</a>  |
| Л2.4  | Ищейнов В. Я.  | Информационная безопасность и защита информации: словарь терминов и понятий: Словарь   | Москва: Русайнс, 2019, URL: <a href="https://book.ru/book/932909">https://book.ru/book/932909</a>   |
| Л2.5  | Мельников В. П., под ред.,<br>Куприянов А. И.  | Информационная безопасность: Учебник   | Москва: КноРус, 2018, URL: <a href="https://book.ru/book/924214">https://book.ru/book/924214</a>  |
| Л2.6  | Ищейнов В. Я.  | Информационная безопасность и защита информации: словарь терминов и понятий: Словарь   | Москва: Русайнс, 2021, URL: <a href="https://book.ru/book/938255">https://book.ru/book/938255</a>   |
| Л2.7  | Мельников В. П.,<br>Куприянов А. И.,<br>Васильева Т. Ю.  | Информационная безопасность: Учебник   | Москва: КноРус, 2018, URL: <a href="https://book.ru/book/929884">https://book.ru/book/929884</a>  |
| Л2.8  | Ищейнов В. Я.  | Информационная безопасность и защита информации: словарь терминов и понятий: Словарь   | Москва: Русайнс, 2018, URL: <a href="https://book.ru/book/931784">https://book.ru/book/931784</a>   |
| Л2.9  | Мельников В. П.,<br>Куприянов А. И.,<br>Васильева Т. Ю.  | Информационная безопасность: Учебник   | Москва: Русайнс, 2016, URL: <a href="https://book.ru/book/920736">https://book.ru/book/920736</a>   |
| Л2.10   | Башлы П.Н., Бабаш А.В.   | Информационная безопасность и защита информации: Учебник   | Москва: Издательский Центр РИО, 2013, URL: <a href="http://znanium.com/catalog/document?id=213488">http://znanium.com/catalog/document?id=213488</a>  |
| Л2.11   | Ковалев Д.В.,<br>Богданова Е.А.  | Информационная безопасность: Учебное пособие   | Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2016, URL: <a href="http://znanium.com/catalog/document?id=330789">http://znanium.com/catalog/document?id=330789</a>   |
| Л2.12   | Глинская Е.В.,<br>Чичварин Н.В.  | Информационная безопасность конструкций ЭВМ и систем: Учебное пособие  | Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: <a href="https://znanium.com/catalog/document?id=362430">https://znanium.com/catalog/document?id=362430</a>   |
| Л2.13   | Панфилова О.А.,<br>Крюкова Д.Ю.  | Информационная безопасность и защита информации: Учебное пособие   | Вологда: федеральное казенное образовательное учреждение высшего образования «Вологодский институт права и экономики Федеральной службы исполнения наказаний», 2018, URL: <a href="http://znanium.com/catalog/document?id=370184">http://znanium.com/catalog/document?id=370184</a> |
| Л2.14   | Баранова Е.К., Бабаш А.В.,<br>Ларин Д.А.   | Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие   | Москва: Издательский Центр РИО, 2022, URL: <a href="https://znanium.com/catalog/document?id=388319">https://znanium.com/catalog/document?id=388319</a>  |
| <b>6.2. Электронные учебные издания и электронные образовательные ресурсы</b> |  |  |   |
| Э1  | Совет Безопасности Российской Федерации . - Режим доступа: <a href="http://www.scrf.gov.ru/">http://www.scrf.gov.ru/</a>       |  |   |
| Э2  | Федеральная служба по техническому и экспортному контролю . - Режим доступа: <a href="https://fstec.ru/">https://fstec.ru/</a> |  |   |

|   |   |
|---|---|
| Э3  | Информационно-правовой портал ГАРАНТ.РУ . - Режим доступа: <a href="https://www.garant.ru/">https://www.garant.ru/</a>  |
| Э4  | Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» . - Режим доступа: <a href="https://docs.cntd.ru/">https://docs.cntd.ru/</a>  |
| Э5  | Национальный Открытый Университет "ИНТУИТ". - Режим доступа: <a href="https://intuit.ru/">https://intuit.ru/</a>  |
| Э6  | Электронные ресурсы Академии ИМСИТ. - Режим доступа: <a href="http://eios.imsit.ru/">http://eios.imsit.ru/</a>  |
| Э7  | Электронная библиотечная система Znanium. - Режим доступа: <a href="http://znanium.com">http://znanium.com</a>  |
| Э8  | Электронная библиотечная система Ibooks. - Режим доступа: <a href="http://www.ibooks.ru/">http://www.ibooks.ru/</a>   |
| Э9  | Электронная библиотечная система BOOK.ru. - Режим доступа: <a href="http://www.book.ru">http://www.book.ru</a>  |
| <b>6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства</b> |   |
| 6.3.1.1   | Windows 10 Pro RUS Операционная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021   |
| 6.3.1.2   | 7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL   |
| 6.3.1.3   | Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер <a href="https://yandex.ru/legal/browser_agreement/">https://yandex.ru/legal/browser_agreement/</a>  |
| 6.3.1.4   | Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL   |
| 6.3.1.5   | LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL   |
| 6.3.1.6   | Notepad++. Текстовый редактор Notepad++. Программное обеспечение по лицензии GNU GPL  |
| 6.3.1.7   | Kaspersky Endpoint Security Антивирусное ПО Kaspersky Endpoint Security для бизнеса Стандартный (350шт). Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)  |
| 6.3.1.8   | Oracle VM VirtualBox VM VirtualBox — программный продукт виртуализации для операционных систем Программное обеспечение по лицензии GNU GPL  |
| 6.3.1.9   | Adobe Reader DC Adobe Acrobat — пакет программ, предназначенный для создания и просмотра электронных публикаций в формате PDF Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017 |
| 6.3.1.1   | MS Office Standart 2010 Офисный пакет Microsoft Office Microsoft Open License 48587685 от 02.06.2011  |
| 6.3.1.1   | MS Visio Pro 2010 Интегрированная среда разработки Microsoft Visio профессиональный 2010 Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021   |
| 6.3.1.1   | Windows 7 Pro Операционная система Microsoft Windows 7 Professional Microsoft Open License 48587685 от 02.06.2011   |
| 6.3.1.1   | Консоль Kaspersky Security Center Консоль администрирования Kaspersky Security Center Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)   |
| 6.3.1.1   | Kaspersky Endpoint Security 11 Kaspersky Endpoint Security 11 для Windows Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)   |
| 6.3.1.1   | Microsoft Windows 10 PRO x64 DSP OEM Операционная система Microsoft Windows 10 PRO Счет №93 от 21.05.2019, Акт передачи прав №31 от 05.06.2019.   |
| 6.3.1.1   | 10-Страйк Сканирование Сети Сканирование Сети - программа-сканер TCP-портов и IP-адресов Лицензионный сертификат от 01.01.2011  |
| 6.3.1.1   | 10-Страйк Инвентаризация Компьютеров Программа для учета ПК в сети предприятия Лицензионный сертификат от 01.01.2011  |
| 6.3.1.1   | 10-Strike File search pro Программа поиска файлов и документов в сети Лицензионный сертификат от 01.01.2011   |
| 6.3.1.1   | Windows Server 2003 R2 Standart Операционная система Microsoft Windows Server 2003 R2 Microsoft Open License № 42060616 от 20.04.2007   |
| 6.3.1.2   | Open SuSe Linux Операционная система Open Source GNU/Linux Программное обеспечение по лицензии GNU GPL  |
| 6.3.1.2   | Windows Server 2008 R2 Standart Операционная система Microsoft Windows Server 2008 Microsoft Open License № 46794243 от 19.04.2010  |
| 6.3.1.2   | Traffic inspector Special Unlimited ОРГАНИЗАЦИЯ ДОСТУПА В ИНТЕРНЕТ. NAT, ПРОКСИ-СЕРВЕР, VPN, AD Лицензионный договор №649 от 23.09.2019   |
| 6.3.1.2   | Эшэлон II “Кредо-диалог” Система защиты Эшэлон II “Кредо-диалог” Акт № 123 от 01.11.2018, Сертификат от 24.08.2018  |
| 6.3.1.2   | Система управления хранилищем документов “Кредо-диалог” Система управления хранилищем документов “Кредо-диалог” Акт № 123 от 01.11.2018, Сертификат от 24.08.2018   |
| 6.3.1.2   | Astra Linux Операционная система семейства Linux. Версия "Орел" Программное обеспечение по лицензии GNU GPL   |
| 6.3.1.2   | vGate Средство микросегментации и защиты жизненного цикла виртуальных машин Договор №КБ/04085/1/11 от 14.02.2022  |
| 6.3.1.2   | Secren Net Studio Единая система управление продуктами для защиты Windows, Linux и платями доверенной загрузки Договор №КБ/04085/1/11 от 14.02.2022   |

|   |  |
|---|--|
| 6.3.1.2<br>8  | Secren Net LSP Средство защиты информации от несанкционированного доступа для операционных систем семейства Linux Договор №КБ/04085/1/11 от 14.02.2022       |
| <b>6.3.2. Перечень профессиональных баз данных и информационных справочных систем</b> |  |
| 6.3.2.1   | Консультант Плюс <a href="http://www.consultant.ru">http://www.consultant.ru</a>   |
| 6.3.2.2   | Global CIO Официальный портал ИТ-директоров <a href="http://www.globalcio.ru">http://www.globalcio.ru</a>  |
| 6.3.2.3   | ARIS BPM Community <a href="https://www.ariscommunity.com">https://www.ariscommunity.com</a>   |
| 6.3.2.4   | ИСО Международная организация по стандартизации <a href="https://www.iso.org/ru/home.html">https://www.iso.org/ru/home.html</a>                              |
| 6.3.2.5   | РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии <a href="https://www.gost.ru/portal/gost/">https://www.gost.ru/portal/gost/</a> |
| 6.3.2.6   | Кодекс – Профессиональные справочные системы <a href="https://kodeks.ru">https://kodeks.ru</a>   |

| <b>7. МТО (оборудование и технические средства обучения)</b> |   |   |  |
|--|---|---|--|
| Ауд  | Наименование  | ПО  | Оснащение  |
| 208  | Лекционная аудитория  | Windows 10 Pro RUS<br>7-Zip<br>Яндекс Браузер<br>Mozilla Firefox<br>LibreOffice<br>Notepad++.<br>Adobe Reader DC<br>Klite Mega Codec Pack   | Стол - 10 шт., стул - 21 шт., рабочее место преподавателя - 1 шт., персональных компьютеров с выходом в интернет - 20 шт., доска учебная - 1 шт., многофункциональное устройство - 1 шт., мультимедийный проектор - 1 шт., проекционный экран - 1 шт.  |
| 123  | Кабинет информационной безопасности                                     | Windows 10 Pro RUS<br>7-Zip<br>Яндекс Браузер<br>Mozilla Firefox<br>LibreOffice<br>LibreCAD<br>Inkscape<br>Notepad++.<br>1С:Предприятие 8. Комплект<br>Kaspersky Endpoint Security<br>MS Access 2016<br>MS Project Pro 2016<br>MS SQL Server 2019<br>MS SQL Server Management Studio 18.8<br>MS Visio Pro 2016<br>MS Visual Studio Community Edition<br>Visual Studio Code<br>Blender<br>Gimp<br>Maxima<br>Oracle VM VirtualBox<br>StarUML V1<br>PostgreSQL<br>IntelliJ IDEA<br>PyCharm Community Edition<br>Eclips<br>Adobe Reader DC<br>Arduino Software (IDE)<br>NetBeans IDE<br>ZEAL<br>ARIS Express<br>Archimate<br>Ramus Educational<br>Micro-Cap Evaluation<br>gvSIG Desktop<br>Python | Стол - 20 шт., стул - 21 шт., рабочее место преподавателя - 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная - 1 шт., многофункциональное устройство - 1 шт., мультимедийный проектор - 1 шт., проекционный экран - 1 шт., соответствующее программное обеспечение |
| Читальный зал  | Информационно-библиотечный центр (помещение для самостоятельной работы) | 7-Zip<br>Яндекс Браузер<br>Mozilla Firefox<br>LibreOffice<br>LibreCAD<br>Inkscape   | Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии - 17 шт., многофункциональное устройство - 2 шт.   |

|  |              |  |  |
|--|--------------|--|--|
|  | обучающихся) | Notepad++.<br>Kaspersky Endpoint Security<br>MS Access 2016<br>MS Project Pro 2016<br>MS Visio Pro 2016<br>Visual Studio Code<br>Blender<br>Gimp<br>Maxima<br>IntelliJ IDEA<br>PyCharm Community Edition<br>Adobe Reader DC<br>MS Office Standart 2007<br>Windows 10 Pro |  |
|--|--------------|--|--|

### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой. В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Информационная безопасность» разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).

Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.

Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.

Методические указания и материалы по видам учебных занятий по дисциплине:

Вид учебных занятий, работ - Организация деятельности обучающегося

Лекция - написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь.

### 9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа студентов в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических и интерактивных занятиях, а также для индивидуального изучения дисциплины «Информационная безопасность» в соответствии с программой и рекомендованной литературой.

Самостоятельная работа выполняется в виде подготовки домашнего задания или сообщения по отдельным вопросам, написание и защита научно-исследовательского проекта.

Контроль качества выполнения самостоятельной (домашней) работы может осуществляться с помощью устного опроса на лекциях или практических занятиях, обсуждения подготовленных научно-исследовательских проектов, проведения тестирования.

Устные формы контроля помогут оценить владение студентами жанрами научной речи (дискуссия, диспут, сообщение, доклад и др.), в которых раскрывается умение студентов передать нужную информацию, грамотно использовать языковые средства, а также ораторские приемы для контакта с аудиторией.

Письменные работы позволяют оценить владение источниками, научным стилем изложения, для которого характерны: логичность, точность терминологии, обобщенность и отвлеченность, насыщенность фактической информацией.