

УТВЕРЖДАЮ  
Декан факультета

\_\_\_\_\_ Матвеев П.В.

« \_\_\_\_ » \_\_\_\_\_ 20\_\_

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

|  |   |
|--|---|
| Направление/специальность подготовки       | 45.05.01 Перевод и переводоведение                        |
| Специализация/профиль/программа подготовки | Специальный перевод                                       |
| Уровень высшего образования                | Специалитет   |
| Форма обучения                             | Очная   |
| Факультет                                  | Р Международного промышленного менеджмента и коммуникации |
| Выпускающая кафедра                        | Р7 ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ ЛИНГВИСТИКА                 |
| Кафедра-разработчик рабочей программы      | О7 Информационные системы и программная инженерия         |

| КУРС | СЕМЕСТР | ОБЩАЯ ТРУДОЁМКОСТЬ<br>(ЗАЧЕТНЫХ ЕДИНИЦ) | ЧАСЫ (по наличию видов занятий) |                    |        |                           |                         |                        |                 |                 |                               | ВИД ПРОМЕЖУТОЧНОГО<br>КОНТРОЛЯ |
|------|---------|---|---------------------------------|--------------------|--------|---------------------------|-------------------------|------------------------|-----------------|-----------------|-------------------------------|--------------------------------|
|      |         |   | ОБЩАЯ ТРУДОЁМКОСТЬ              | АУДИТОРНЫЕ ЗАНЯТИЯ |        |                           |                         | САМОСТОЯТЕЛЬНАЯ РАБОТА |                 |                 |                               |                                |
|      |         |   |                                 | ВСЕГО              | ЛЕКЦИИ | ЛАБОРАТОРНЫЙ<br>ПРАКТИКУМ | ПРАКТИЧЕСКИЕ<br>ЗАНЯТИЯ | ВСЕГО                  | КУРСОВОЙ ПРОЕКТ | КУРСОВАЯ РАБОТА | ДРУГИЕ ВИДЫ<br>САМОСТ. РАБОТЫ |                                |
| 5    | 9       | 3                                       | 108                             | 34                 | 17     | 0                         | 17                      | 74                     | 0               | 0               | 74                            | диф.<br>зач.                   |

*ЛИСТ СОГЛАСОВАНИЯ*

**РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО  
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)**

**45.05.01 Перевод и переводоведение**

год набора группы: 2025

Программу составил:

Кафедра О7 Информационные системы и программная инженерия  
Шимкун Вячеслав Владиславович, старший преподаватель

\_\_\_\_\_

Программа рассмотрена  
на заседании кафедры-разработчика  
рабочей программы **О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

\_\_\_\_\_

Программа рассмотрена  
на заседании выпускающей кафедры

**Р7 ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ ЛИНГВИСТИКА**

Заведующий кафедрой Невзорова Г.Д., к.ф.н., доц.

\_\_\_\_\_

# **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

## **Разделы рабочей программы**

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

## **Приложения к рабочей программе дисциплины**

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПК-2 — Способен использовать современные высокотехнологичные программные продукты в профессиональной деятельности

ОПК-4 — Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий

ОПК-5 — Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Формированию компетенций служит достижение следующих результатов образования:

### **ПК-2**

*знания:*

технологии реализации защиты информации;

методы организации защищенных каналов передачи информации через компьютерные сети общего пользования;

*умения:*

применять полученные знания в практике построения защищенных систем обработки информации, включая конфиденциальную информацию и обработку персональных данных;

*навыки:*

обнаруживать компьютерные вирусы различными способами и применять методы борьбы с вирусами различной природы.

### **ОПК-4**

*знания:*

методы аутентификации в современных операционных системах и специальные средства защиты информации;

классификация компьютерных систем по уровню защищенности;

классификация угроз;

методы организации защищенных каналов передачи информации через компьютерные сети общего пользования;

*умения:*

применять полученные знания в практике построения защищенных систем обработки информации, включая конфиденциальную информацию и обработку персональных данных;

*навыки:*

работать с информацией ограниченного доступа.

### **ОПК-5**

*знания:*

различия защиты физической, организационной, математической и программной;

модели и методы построения защищенных систем обработки информации;

*умения:*

применять полученные знания в практике построения защищенных систем обработки информации, включая конфиденциальную информацию и обработку персональных данных;

*навыки:*

применять программное обеспечение для разграничения доступа к информации.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *45.05.01 Перевод и переводоведение*.

Содержание дисциплины является логическим продолжением дисциплин: **ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ**.

Содержание дисциплины является основой для освоения дисциплин: **ПОДГОТОВКА К ПРОЦЕДУРЕ ЗАЩИТЫ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-5 — Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
- ПК-93 — Способен генерировать новые идеи для решения задач цифровой экономики, абстрагироваться от стандартных моделей, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов
- ПК-94 — Способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

#### 3.1. Содержание (дидактика) дисциплины

| КУРС                       | СЕМЕСТР | Наименование разделов и дидактических единиц  | ВСЕГО | Аудиторные занятия в контактной форме |        |                      | Самостоятельная работа студентов | Формируемая компетенция, % |       |       |
|----------------------------|---------|---|-------|---------------------------------------|--------|----------------------|----------------------------------|----------------------------|-------|-------|
|                            |         |   |       | ВСЕГО                                 | Лекции | Практические занятия |                                  | ПК-2                       | ОПК-4 | ОПК-5 |
| 5                          | 9       | <b>Раздел 1. Понятие о защите информации, виды защищаемой информации.</b> Информационная безопасность в системе национальной безопасности Российской Федерации.   | 11    | 1                                     | 1      | 0                    | 10                               | 10                         | 10    | 10    |
| 5                          | 9       | <b>Раздел 2. Структуры и основные задачи службы безопасности предприятия.</b> 2.1. Этапы процесса организации системы защиты информации предприятия. 2.2. Защита информации в линиях связи. 2.3. Структура современных телефонных кабельных сетей.  | 12    | 2                                     | 2      | 0                    | 10                               | 10                         | 10    | 10    |
| 5                          | 9       | <b>Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.</b> Способы контактного и бесконтактного съема информации.  | 14    | 4                                     | 2      | 2                    | 10                               | 15                         | 10    | 10    |
| 5                          | 9       | <b>Раздел 4. Защита информации в современных информационных системах.</b> 4.1. Возможности атаки на ОС, их классификация. 4.2. Парольная защита ПК. Взлом паролей Windows NT и UNIX. Защита от взлома. 4.3. Идентификация и аутентификация пользователей ОС. Windows, UNIX, Linux. 4.4. Формальные модели защищаемых систем и их применение в современных ОС. | 16    | 6                                     | 2      | 4                    | 10                               | 15                         | 10    | 10    |
| 5                          | 9       | <b>Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.</b> 5.1. Защита программ. 5.2. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. 5.3. Технология хранения ключевой информации.  | 10    | 2                                     | 2      | 0                    | 8                                | 10                         | 10    | 16    |
| 5                          | 9       | <b>Раздел 6. Основные угрозы безопасности сетей.</b> 6.1. Модели угроз. 6.2. Модели противодействия угрозам безопасности. 6.3. Основные требования к формированию и использованию имен пользователей и паролей в сети. 6.4. Методы аутентификации пользователей в сети.   | 12    | 6                                     | 2      | 4                    | 6                                | 10                         | 10    | 10    |
| 5                          | 9       | <b>Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.</b> 7.1. Разновидности вирусных программ. 7.2. Сканеры вирусов. 7.3. Сетевая защита, брандмауэры, демилитаризованные зоны и частные виртуальные сети. 7.4. Системы обнаружения сетевого вторжения.   | 12    | 6                                     | 2      | 4                    | 6                                | 10                         | 10    | 14    |
| 5                          | 9       | <b>Раздел 8. Безопасность Интернета.</b> 8.1. Разрушительные программы: вирусы, черви, троянские кони, мобильные программы. 8.2. Безопасность электронной почты.  | 10    | 4                                     | 1      | 3                    | 6                                | 10                         | 16    | 10    |
| 5                          | 9       | <b>Раздел 9. Криптографические методы защиты информации.</b> 9.1. Неформальные понятия о шифрах. 9.2. Шифрования и дешифрование. 9.3. Математические основы криптографии. 9.4. Алгоритмы шифрования.  | 11    | 3                                     | 3      | 0                    | 8                                | 10                         | 14    | 10    |
| <b>Всего за 9 семестр</b>  |         |   | 108   | 34                                    | 17     | 17                   | 74                               | 100                        | 100   | 100   |
| <b>Всего по дисциплине</b> |         |   | 108   | 34                                    | 17     | 17                   | 74                               | 100                        | 100   | 100   |

#### 3.2. Аудиторный практикум

| № п/п | Номер и наименование раздела дисциплины   | Тема практического занятия  | Объем, ауд. часов |
|-------|---|---|-------------------|
| 1     | Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.  | Практическая работа №1 – «Разработка защищенных приложений. Программное управление учетной записью. Политика безопасности.»                           | 2                 |
| 2     | Раздел 4. Защита информации в современных информационных системах.                    | Практическая работа №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей.»                                      | 4                 |
| 3     | Раздел 6. Основные угрозы безопасности сетей.   | Практическая работа №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows.» | 4                 |
| 4     | Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи. | Практическая работа №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел.»                                     | 4                 |
| 5     | Раздел 8. Безопасность Интернета.   | Практическая работа №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-  | 3                 |

|                           |             |           |
|---------------------------|-------------|-----------|
|                           | адресации.» |           |
| <b>Всего за 9 семестр</b> |             | <b>17</b> |

### 3.3. Самостоятельная работа студента (СРС)

| № п/п                     | Номер и наименование раздела дисциплины   | Содержание учебного задания   | Объем, часов |
|---------------------------|---|---|--------------|
| 1                         | Раздел 1. Понятие о защите информации, виды защищаемой информации.                    | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 10           |
| 2                         | Раздел 2. Структуры и основные задачи службы безопасности предприятия.                | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 10           |
| 3                         | Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.  | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 6            |
| 4                         |   | Подготовка к практической работе №1 – «Разработка защищенных приложений. Программное управление учетной записью. Политика безопасности», оформление отчета.   | 4            |
| 5                         | Раздел 4. Защита информации в современных информационных системах.                    | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 6            |
| 6                         |   | Подготовка к практической работе №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей», оформление отчета.  | 4            |
| 7                         | Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.          | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 4            |
| 8                         |   | Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», оформление отчета.                                 | 4            |
| 9                         | Раздел 6. Основные угрозы безопасности сетей.   | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 4            |
| 10                        |   | Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», посылка отчета по электронной почте преподавателю. | 2            |
| 11                        | Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи. | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 4            |
| 12                        |   | Подготовка к практической работе №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел», оформление отчета.   | 2            |
| 13                        | Раздел 8. Безопасность Интернета.   | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 4            |
| 14                        |   | Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.   | 2            |
| 15                        | Раздел 9. Криптографические методы защиты информации.                                 | Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | 8            |
| <b>Всего за 9 семестр</b> |   |   | <b>74</b>    |

#### 4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| СЕМЕСТР | НЕДЕЛИ СЕМЕСТРА |   |   |   |               |    |               |   |               |    |               |    |    |    |               |    |                            |
|---------|-----------------|---|---|---|---------------|----|---------------|---|---------------|----|---------------|----|----|----|---------------|----|----------------------------|
|         | 1               | 2 | 3 | 4 | 5             | 6  | 7             | 8 | 9             | 10 | 11            | 12 | 13 | 14 | 15            | 16 | 17                         |
| 9       |                 |   |   |   | Отч. по<br>ПЗ | ДР | Отч. по<br>ПЗ |   | Отч. по<br>ПЗ | ДР | Отч. по<br>ПЗ |    |    |    | Отч. по<br>ПЗ | ДР | Вопр.Диф.Зач,<br>диф. зач. |

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр.Диф.Зач – вопросы к дифференцированному зачету;
- диф. зач. – дифференцированный зачет.

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к дифференцированному зачету.

**Промежуточная аттестация** проводится в формах:

- дифференцированный зачет.



## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература по дисциплине:

1. А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
2. А. Голдсмит. . Беспроводные коммуникации. М.: Техносфера, 2011, 5 экз.
3. А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации. М.: КноРус, 2017, 60 экз.
4. В. И. Ярочкин. . Информационная безопасность. М.: Академический Проект, 2006, 48 экз.
5. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2007, эл. рес.
6. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2011, 27 экз.
7. В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.
8. С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. . Операционные системы, сети и интернет-технологии. М.: Академия, 2014, 15 экз.

### 5.2. Дополнительная литература по дисциплине:

1. А. В. Бабаш, Г. П. Шанкин. Криптография. М.: СОЛОН-Пресс, 2007, 3 экз.
2. С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security. М.: БИНОМ, 2007, 3 экз.

### 5.3. Периодические издания:

1. Моделирование и анализ информационных систем.

### 5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <http://www.intuit.ru/department/security/secbasics/> — НОУ ИНТУИТ | Основы информационной безопасности | Информация;
2. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
3. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.,;
4. <http://e.lanbook.com/> — ЭБС Лань;;
5. <http://library.voenmeh.ru/jirbis2/> — Р«Р»Р°РІРSP°СЦ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
6. <http://library.voenmeh.ru/jirbis2/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
7. <https://urait.ru/> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
8. <http://library.voenmeh.ru/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

### Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;  
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

### Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. [http://library.voenmeh.ru/jirbis2/index.php?option=com\\_irbis&view=irbis&Itemid=457](http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457) - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

### 5.5. Программное обеспечение:

1. LibreOffice;
2. Linux.

#### 5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

## **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **6.1. Лекционные занятия:**

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

### **6.2. Практические занятия:**

1. Проектор;
2. LibreOffice;
3. Linux.

### **6.3. Прочее:**

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

### **Аннотация рабочей программы**

Дисциплина **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *45.05.01 Перевод и переводоведение*. Дисциплина реализуется на факультете *О Естественнотехнический БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ПК-2 Способен использовать современные высокотехнологичные программные продукты в профессиональной деятельности;

ОПК-4 Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий;

ОПК-5 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Содержание дисциплины охватывает круг вопросов, связанных с основными понятиями и видами защищаемой информации, процессом организации системы защиты предприятия, утечками информации, методами защиты информации и алгоритмами шифрования. Рассматриваются основные способы проникновения вирусов в информационные системы и сети, виды вирусов и защита от них, формальные модели защищаемых систем и их применение. Сетевая защита и безопасность web и электронной почты.

Программой дисциплины предусмотрены следующие **виды контроля**:

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к дифференцированному зачету.

**Промежуточная аттестация** проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены лекционные занятия (**17 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**74 ч.**).

## ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

### Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 34 ч. аудиторных занятий, и 74 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

| Наименование работы   | Рекомендуемая литература  | Трудоемкость, час. |
|---|---|--------------------|
| <b>Раздел 1. Понятие о защите информации, виды защищаемой информации.</b>   |   |                    |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (1)<br>А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .<br>Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)   | 10                 |
| Итого по разделу 1  |   | 10                 |
| <b>Раздел 2. Структуры и основные задачи службы безопасности предприятия.</b>   |   |                    |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (4)<br>В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (1)<br>А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .<br>Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8) | 10                 |
| Итого по разделу 2  |   | 10                 |
| <b>Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.</b>   |   |                    |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (1)<br>А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .  | 6                  |
| Подготовка к практической работе №1 – «Разработка защищенных приложений. Программное управление учетной записью. Политика безопасности», оформление отчета. | Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8-9)<br>В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (2)   | 4                  |
| Итого по разделу 3  |   | 10                 |

| Раздел 4. Защита информации в современных информационных системах.  |  |    |
|---|--|----|
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)<br>В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (9)  | 6  |
| Подготовка к практической работе №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей», оформление отчета.  | А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (3)<br>А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .<br>Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)<br>В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3) | 4  |
| Итого по разделу 4  |  | 10 |
| Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.  |  |    |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (9)<br>В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)  | 4  |
| Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», оформление отчета.                                 | А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (8)<br>В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3)<br>А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .<br>Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8) | 4  |
| Итого по разделу 5  |  | 8  |
| Раздел 6. Основные угрозы безопасности сетей.   |  |    |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (8)   | 4  |
| Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», посылка отчета по электронной почте преподавателю. | А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (8)<br>В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (9)<br>В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3)                  | 2  |

|   |   |   |
|---|---|---|
|   | А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .<br>Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)<br>В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)  |   |
| Итого по разделу 6  |   | 6 |
| <b>Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.</b>  |   |   |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (2-3)<br>В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (9)<br>В. И. Ярочкин. .   | 4 |
| Подготовка к практической работе №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел», оформление отчета. | Информационная безопасность: М.: Академический Проект, 2006 (5)<br>А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (2)<br>А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .<br>Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)<br>В. Л. Бройдо, О. П. Ильина. .<br>Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (2-3) | 2 |
| Итого по разделу 7  |   | 6 |
| <b>Раздел 8. Безопасность Интернета.</b>  |   |   |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .<br>Информационная безопасность: М.: РУСАЙНС, 2017 (20)<br>А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы защиты информации: М.: КноРус, 2018 (5)   | 4 |
| Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.           | С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. .<br>Операционные системы, сети и интернет-технологии: М.: Академия, 2014 (8)  | 2 |
| Итого по разделу 8  |   | 6 |
| <b>Раздел 9. Криптографические методы защиты информации.</b>  |   |   |
| Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе  | С. Бернет, С. Пэйн.<br>Криптография. Официальное руководство RSA Security: М.: БИНОМ, 2007 (1-3)<br>А. В. Бабаш, Г. П. Шанкин.<br>Криптография: М.: СОЛОН-Пресс, 2007 (4-6)<br>А. В. Бабаш, Е. К. Баранова. .<br>Криптографические методы   | 8 |

|                    |  |   |
|--------------------|--|---|
|                    | защиты информации: М.:<br>КноРус, 2018 (8) |   |
| Итого по разделу 9 |  | 8 |



## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- отчет по практическому заданию;
- вопросы к дифференцированному зачету;
- дифференцированный зачет.

### Критерии оценивания

#### Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

#### Отчет по практическому заданию

К каждой ПР необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При выполнении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждой ПР.

ПР считается выполненным и защищенным успешно при условии:

- наличия программного приложения, реализующего поставленную задачу;
- наличия отчета;
- защиты ПР по комплекту тестовых вопросов для защиты ПР, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие программного приложения указанным требованиям, его работоспособность и эффективность – 7 баллов;
- отчет оформлен полностью в соответствии с ГОСТ 7.32-2017 – 3 балла;
- правильность ответов на вопросы – 7 баллов;
- своевременность выполнения и защиты индивидуального задания – 3 балла.

Основанием для снижения количества баллов являются:

- несоответствие программного приложения указанным требованиям, его неэффективность или некорректная работа;
- оформление отчета не соответствует ГОСТ 7.32-2017 в 3 и более пунктах;
- неверные ответы на вопросы или отсутствие ответов;
- несвоевременность выполнения и защиты индивидуального задания.

В случае, если ПР и отчет к нему выполнены своевременно в соответствии с указанными требованиями, а также получены правильные ответы на вопросы при его защите студент получает максимальное количество баллов – 20.

Для того, чтобы ПР была сдана, требуется набрать 12 баллов.

#### Вопросы к дифференцированному зачету

Перечень теоретических вопросов к дифф. зачету предоставляется преподавателем. Перечень вопросов лежит в УМК дисциплины. При подготовке ответов на теоретические вопросы рекомендуется помимо конспектов лекций использовать источники основной и дополнительной литературы.

#### Дифференцированный зачет

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4. Зачёт проводится в виде собеседования. Два основных вопроса и один дополнительный в случае, если ответы студента на первые два не позволяют однозначно определиться с оценкой. Студенты должны продемонстрировать знание и понимание теоретического материала курса.

При выполнении и защите всех практических работ предусмотрена отметка "зачтено-хорошо" по результатам работы в семестре.

Зачтено-отлично:

- все задачи практики решены полностью,
- в процессе собеседования студент продемонстрировал полное знание вопросов.

Зачтено-хорошо:

- все задачи практики решены полностью,
- в процессе собеседования студент продемонстрировал в целом достаточно полное знание вопросов, но допускал мелкие неточности в формулировках ответов.

Зачтено-удовлетворительно:

- все задачи практики решены полностью
- в процессе собеседования студент продемонстрировал удовлетворительное знание вопросов, но допускал неполные ответы, затруднялся в формулировках ответов.

Не зачтено:

- не все задачи практики решены,
- в процессе собеседования студент продемонстрировал неудовлетворительное знание вопросов.

Паспорт фонда оценочных средств

| КУРС                | СЕМЕСТР | Наименование разделов и дидактических единиц  | ВСЕГО | Аудиторные занятия в контактной форме |        |                      | Самостоятельная работа студентов | Формируемая компетенция, % |       |       | НАИМЕНОВАНИЕ<br>ОЦЕНОЧНОГО СРЕДСТВА                                  |
|---------------------|---------|---|-------|---------------------------------------|--------|----------------------|----------------------------------|----------------------------|-------|-------|--|
|                     |         |   |       | ВСЕГО                                 | Лекции | Практические занятия |                                  | ПК-2                       | ОПК-4 | ОПК-5 |  |
| 5                   | 9       | Раздел 1. Понятие о защите информации, виды защищаемой информации.                    | 11    | 1                                     | 1      | 0                    | 10                               | 10                         | 10    | 10    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 2. Структуры и основные задачи службы безопасности предприятия.                | 12    | 2                                     | 2      | 0                    | 10                               | 10                         | 10    | 10    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.  | 14    | 4                                     | 2      | 2                    | 10                               | 15                         | 10    | 10    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 4. Защита информации в современных информационных системах.                    | 16    | 6                                     | 2      | 4                    | 10                               | 15                         | 10    | 10    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.          | 10    | 2                                     | 2      | 0                    | 8                                | 10                         | 10    | 16    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 6. Основные угрозы безопасности сетей.   | 12    | 6                                     | 2      | 4                    | 6                                | 10                         | 10    | 10    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи. | 12    | 6                                     | 2      | 4                    | 6                                | 10                         | 10    | 14    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 8. Безопасность Интернета.   | 10    | 4                                     | 1      | 3                    | 6                                | 10                         | 16    | 10    | Отчет по практическому заданию                                       |
| 5                   | 9       | Раздел 9. Криптографические методы защиты информации.                                 | 11    | 3                                     | 3      | 0                    | 8                                | 10                         | 14    | 10    | Отчет по практическому заданию, Вопросы к дифференцированному зачету |
| Всего за 9 семестр  |         |   | 108   | 34                                    | 17     | 17                   | 74                               | 100                        | 100   | 100   |  |
| Всего по дисциплине |         |   | 108   | 34                                    | 17     | 17                   | 74                               | 100                        | 100   | 100   |  |

## Оценочные материалы по дисциплине ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### ПК-2 - Способен использовать современные высокотехнологичные программные продукты в профессиональной деятельности

№ 1 Прочитайте текст и запишите развернутый обоснованный ответ

В чём заключается суть Демилитаризованной зоны DMZ (*Demilitarized Zone*)?

№ 2 Прочитайте текст и запишите развернутый обоснованный ответ

Что такое сетевой, или межсетевой, экран?

№ 3 Прочитайте текст и установите соответствие

|   |   |   |
|---|---|---|
| 1 | Активная сущность, которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов - | А объект доступа                            |
| 2 | Пассивная сущность, процессы над которой могут в определенных случаях быть источником порождения новых субъектов -  | Б монитор безопасности<br>В субъект доступа |

№ 4 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Угроза информации – это ...

1. опасность нарушения физической целостности информационной системы (уничтожение, разрушение элементов).

2. неблагоприятное намерение в адрес информации, высказанное в устной или письменной форме.

3. опасность изменения содержания (изменение блоков информации, внешнее навязывание ложной информации).

4. возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

№ 5 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Целостность информации – это ...

1. свойство информации, характеризующее ее состояние.

2. свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению.

3. свойство информации не изменяться со временем.

4. свойство информации, характеризующее ее неизменность.
- № 6 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
- Введите номер пункта с несуществующим грифом:

1. С (Секретно)
2. ДСП (Служебная тайна)
3. КФД (Конфиденциальные данные)
4. СС (Совершенно Секретно)

- № 7 Прочитайте текст и установите соответствие

|   |   |                               |
|---|---|-------------------------------|
| 1 | Состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам) -   | А безопасность информации     |
| 2 | Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования - | Б информационная безопасность |
|   |   | В защита информации           |

- № 8 Прочитайте текст и установите последовательность

Расставьте уровни представления информации по порядку от уровня носителей к семантическому уровню:

1. Логический уровень
2. Синтаксический уровень
3. Уровень средств взаимодействия с носителем

- № 9 Прочитайте текст и установите последовательность

Распределите нарушителей по уровню возможностей от самого низкого к высокому:

1. Определяет возможность управления функционированием системы, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.
2. Определяет самый низкий уровень возможностей ведения диалога: запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.
3. Определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав собственных технических средств с новыми функциями по обработке информации.
4. Определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.

- № 10 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Применение модели безопасности:

1. при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности

2. в процессе анализа безопасности системы, при этом модель используется в качестве эталонной модели
3. при составлении формальной спецификации политики безопасности разрабатываемой системы
4. при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты
5. при защите информации от утечки по техническим каналам

№ 11 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Виды моделей разграничения доступа:

1. Дискреционные
2. Защищённые
3. Тематические
4. Парольные
5. Физико-математические
6. Теоретико-информационные
7. Мандатные
8. Ролевые

№ 12 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Задачи модели безопасности:

1. прохождение сертификации ФСТЭК
2. защита от НСД
3. составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных систем
4. подтверждение свойства защищенности разрабатываемых систем путем формального доказательства соблюдения политики безопасности
5. выбор и обоснование базовых принципов архитектуры защищенных систем, определяющих механизмы реализации средств и методов защиты информации

**ОПК-4 - Способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий**

№ 1 Прочитайте текст и запишите развернутый обоснованный ответ

Государственная тайна это:

№ 2 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Конфиденциальность информации – это ...

1. свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам).
2. свойство информации ограниченного доступа в силу личного характера.

3. свойство информации быть известной только ее владельцу.

4. свойство информации быть известной только субъектам информационной системы.

№ 3 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Защита информации это:

1. это одна из характеристик информационной системы.

2. комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

3. комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности.

4. совокупность информационных технологий и технических средств.

№ 4 Прочитайте текст и запишите развернутый обоснованный ответ

Определение электронной подписи, виды электронной подписи по ФЗ №63-ФЗ «Об электронной подписи»

№ 5 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Виды скрытых каналов утечки информации:

1. скрытые каналы по памяти

2. скрытые статистические каналы

3. скрытые каналы по времени

4. скрытые каналы по вводу-выводу

5. скрытые семантические каналы

№ 6 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Верно ли, что под субъектами информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры?

Верно

Неверно

№ 7 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Верно ли, что информация с ограниченным доступом делится на государственную тайну, служебную тайну и конфиденциальную?

Верно

Неверно

№ 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Основным назначением компьютерной сети является:

1. Совместное удалённое использование ресурсов сети сетевыми пользователями
2. Физическое соединение всех компьютеров сети

Совместное решение распределённой задачи пользователями сети

№ 9 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Маршрутизатор - устройство, соединяющее различные:

1. Компьютерные сети
2. По архитектуре компьютеры
3. Маршруты передачи адресов для e-mail

№ 10 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Информационная угроза – это:

1. потенциальная возможность потери информации.
2. потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере информации.
3. потенциальная возможность неправомерного или случайного воздействия на объект защиты.
4. потенциальная возможность неправомерного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.

№ 11 Прочитайте текст и установите соответствие

1 Информационная безопасность – это

2 Уровень защищенности – это

3 Защита информации – это

одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным уровнем защищенности. процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы. состояние защищенности информации и поддерживающей инфраструктуры.



№ 12 Прочитайте текст и установите соответствие

|   |                              |   |  |
|---|------------------------------|---|--|
| 1 | Формальные средства защиты   | А | выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека. |
| 2 | Неформальные средства защиты | Б | регламентируют деятельность человека.  |
|   |                              | В | выполняют защитные функции без заранее предусмотренной процедуры.                            |

№ 13 Прочитайте текст и установите последовательность

Распределите этапы работы с исходящими конфиденциальными документами в порядке выполнения.

1. Подписание документа
2. Помещение второго экземпляра в дело
3. Разработка проекта документа
4. Регистрация документа
5. Согласование документа
6. Отправка документа

№ 14 Прочитайте текст и установите последовательность

Распределите этапы работы с входящими конфиденциальными документами в порядке выполнения.

1. Принятие решения о дальнейшем использовании
2. Направление на исполнение
3. Регистрация
4. Дальнейшее использование / Передача в архив / Уничтожение
5. Рассмотрение руководством и принятие решения
6. Доклад руководителей о полученных документах
7. Помещение документа в дело
8. Прием входящих документов
9. Исполнение

№ 15 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Отметьте задачи собственноручной подписи на бумажном документе:

1. Будучи частью документа, защитить ее от мошеннического переноса в другой документ (подпись невозможно использовать повторно)

2. Защитить сам документ (подписанный документ невозможно изменить)
3. Доказать, что именно этот человек, и никто другой, сознательно подписал документ (подпись неподдельна)
4. Убедить читателя в том, что человек, подписавший документ, сделал это сознательно (подпись достоверна)

№ 16 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Задачи ЭЦП в ЭДО:

1. Обеспечить убедительность — подтверждение уникальности документа.
2. Подтвердить подлинность — подтверждение авторства документа.
3. Обеспечить целостность — документ не может быть изменен после подписания.
4. Обеспечить неотрицание авторства (неотрекаемость) — автор впоследствии не сможет отказаться от своей подписи.

**ОПК-5 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности**

№ 1 Прочитайте текст и запишите развернутый обоснованный ответ

Что означает MAC-адрес?

№ 2 Прочитайте текст и запишите развернутый обоснованный ответ

Сертификат электронной подписи, назначение и содержание сертификата по ФЗ №63-ФЗ «Об электронной подписи»

№ 3 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Протоколом является:

1. устройство для работы локальной сети
2. стандарт отправки сообщений через электронную почту
3. стандарт передачи данных через компьютерную сеть

№ 4 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Основными видами компьютерных сетей являются сети:

1. клиентские, корпоративные, международные
2. локальные, глобальные, региональные
3. социальные, развлекательные, бизнес-ориентированные

№ 5 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие из перечисленных САВЗ имеют сертификат ФСТЭК и официально продаются на российском рынке?

Avast

Trend Micro

McAfee

Dr.Web

ESET NOD32

Panda

AVG

Norton

Kaspersky

№ 6 Прочитайте текст и установите соответствие

Выберите утверждение, соответствующее виду ЭЦП.

1. Усиленная неквалифицированная электронная подпись.
2. Простая электронная подпись.
3. Усиленная квалифицированная электронная подпись.

А - Она тождественна собственноручной.

Б - Это сочетание логина и пароля.

В - Подлинность подписи и неизменность документа подтверждается квалифицированным сертификатом.

Г - Она надежнее простой ЭП, но, по своей сути, тождественна собственноручной.

Д - Это сочетание логина и пароля или SMS-код подтверждения

№ 7 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что должен иметь каждый компьютер или принтер подключённый к локальной сети:

1. сетевой адаптер
2. маршрутизатор
3. коммутатор

№ 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Сеть, объединяющая несколько компьютеров и позволяет использовать ресурсы компьютеров и подключённых к сети периферийных устройств, называется:

1. замкнутая
2. региональная
3. локальная

№ 9 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Обобщённая геометрическая характеристика компьютерной сети - это:

1. Топология сети
2. Сервер сети

3. Удалённость компьютеров сети

№ 10 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Протокол компьютерной сети - совокупность:

1. Электронный журнал для протоколирования действий пользователей сети
2. Технических характеристик трафика сети
3. Правил, регламентирующих приём-передачу, активацию данных в сети

№ 11 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Для чего нужна машиночитаемая доверенность (МЧД)?

Чтобы подписывать документы своей ЭЦП от лица организации и руководителя выдавших доверенность.

Чтобы подписывать документы своей ЭЦП.

Чтобы подписывать документы ЭЦП руководителя от его лица.

Чтобы подписывать документы ЭЦП руководителя от лица организации выдавшей доверенность.

Чтобы подписывать документы ЭЦП руководителя.

№ 12 Прочитайте текст и установите соответствие

Распределите средства антивирусной защиты (САВЗ) по типам.

1. САВЗ типа «А»
2. САВЗ типа «Б»
3. САВЗ типа «В»
4. САВЗ типа «Г»

А - Предназначены для применения на автономных автоматизированных рабочих местах (АРМ) .

Б - Предназначены для применения на автоматизированных рабочих местах (АРМ) информационных систем.

В - Предназначены для применения на серверах информационных систем.

Г - Предназначены для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем - серверах, автоматизированных рабочих местах (АРМ).

№ 13 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Категории методов защиты от НСД:

1. финансовые
2. военные
3. организационные
4. технологические

5. научные
6. конфиденциальные
7. морально-этические
8. правовые

№ 14 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

По каким признакам классифицируют государственные информационные системы (ГИС)?

1. По признаку отраслевой принадлежности.
2. По масштабу ГИС.
3. По значимости обрабатываемой в ГИС информации.
4. По географическому признаку.

№ 15 Прочитайте текст и установите последовательность

Распределите по порядку этапы жизненного цикла информации от "Оценки" до "Использования":

1. Оценка
2. Выборка
3. Подготовка к хранению
4. Обработка
5. Хранение
6. Использование

№ 16 Прочитайте текст и установите последовательность

Распределите нарушителей по уровню возможностей от первого до четвертого:

1. Определяет возможность управления функционированием системы, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.
2. Определяет самый низкий уровень возможностей ведения диалога: запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.
3. Определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав собственных технических средств с новыми функциями по обработке информации.
4. Определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.