АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ СОЦИАЛЬНЫЙ ИНСТИТУТ»

Утверждаю
Декан ФИСТ
_____Ж.В. Игнатенко
«19» мая 2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии защиты конфиденциальной информации организации

Направление подготовки: 09.04.02 Информационные системы и технологии

Направленность (профиль) программы: Информационные системы управления предприятием

Квалификация выпускника: Магистр

Форма обучения: очная, заочная

Год начала подготовки – 2023

Разработана
Канд. техн. наук, доцент, доцент
_____ Д.В. Шлаев

Согласована
зав. кафедрой ИС
_____ А.Ю. Орлова

Рекомендована
на заседании кафедры ИС
от «19» мая 2023 г.
протокол № 9
Зав. кафедрой _____ А.Ю. Орлова

Одобрена
на заседании учебно-методической
комиссии ФИСТ
от «19» мая 2023 г.
протокол № 9
Председатель УМК _____ Ж.В. Игнатенко

Ставрополь, 2023 г.

**Содержание**

1. Цели освоения дисциплины....4
2. Место дисциплины в структуре опоп....4
3. Планируемые результаты обучения по дисциплине....4
4. Объем дисциплины и виды учебной работы....4
5. Содержание и структура дисциплины....6
5.1. Содержание дисциплины....6
5.2. Структура дисциплины....6
5.3. Занятия семинарского типа....7
5.4. Курсовой проект (курсовая работа, расчетно-графическая работа, реферат, контрольная работа)....8
5.5. Самостоятельная работа....8
6. Образовательные технологии....9
7. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации10
7.1 оценочные средства, критерии и шкала оценки....10
7.2. Методические материалы, определяющие процедуры оценивания....21
8. Учебно-методическое и информационное обеспечение дисциплины....23
8.1. Основная литература....23
8.2. Дополнительная литература....24
8.3. Программное обеспечение....24
8.4. Профессиональные базы данных....24
8.5. Информационные справочные системы....24
8.6. Интернет-ресурсы....24
8.7. Методические указания по освоению дисциплины....25
9. Материально-техническое обеспечение дисциплины....27
10. Особенности освоения дисциплины лицами с ограниченными возможностями здоровья....27

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины – приобретение студентами теоретических знаний об информационных угрозах и методах защиты конфиденциальной информации, получения навыков действий по обеспечению информационной безопасности конфиденциальной информации в экономических и управленческих системах организаций.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Технологии защиты конфиденциальной информации организации» входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» образовательной программы Б.1.В.4.

| Предшествующие дисциплины (курсы, модули, практики) | Последующие дисциплины (курсы, модули, практики) |
|---|---|
| Методологии и технологии проектирования информационных систем<br>Управление ИТ-проектами<br>Организационное проектирование информационных систем управления предприятий<br>Информационные системы многокритериальной оптимизации решений | Управление информационными системами предприятий<br>Внедрение и сопровождение информационных систем<br>Подготовка ВКР |

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

| **Код и наименование компетенции** | **Код и наименование индикатора (индикаторов) достижения компетенции** | **Результаты обучения** |
|---|---|---|
| **ПК-2** Способен проводить аудит конфигураций ИС и управлять выпуском релизов в проектах малого и среднего уровня сложности в области ИТ | ПК-2.1. Идентифицирует конфигурацию ИС. | **Знает:** цели, задачи и функции администрирования в информационных системах |
| | ПК-2.3. Проводит аудит конфигураций ИС в проектах малого и среднего уровня сложности в области ИТ | **Умеет** проводить аудит конфигураций ИС в проектах малого и среднего уровня сложности в области ИТ |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общий объем дисциплины составляет 4 зачетных единиц, 144 академических часов.

Очная форма обучения

| Вид учебной работы | Всего часов | Триместр |
|---|---|---|
| | | 4 |
| | | |
| **Контактная работа (всего)** | **20** | **20** |
| в том числе: | | |
| 1) занятия лекционного типа (ЛК) | 10 | 10 |
| из них | | |

| | | |
|---|---|---|
| -лекций | 10 | 10 |
| 2) занятия семинарского типа (ПЗ) | 10 | 10 |
| -семинары (С) | 4 | 4 |
| -практические занятия (ПР) | 6 | 6 |
| -лабораторные работы (ЛР) | | |
| 3) групповые консультации | | |
| 4) индивидуальная работа | | |
| 5) промежуточная аттестация | | |
| **Самостоятельная работа (всего) (СР)** | **124** | **124** |
| в том числе: | | |
| Курсовой проект (работа) | | |
| Расчетно-графические работы | | |
| Контрольная работа | | |
| Реферат | | |
| Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.) | 124 | 124 |
| Подготовка к аттестации | - | - |
| Общий объем, час | **144** | **144** |
| Форма промежуточной аттестации | Диф. зачёт | Диф. зачёт |

Очная форма обучения

| Вид учебной работы | Всего часов | Триместр |
|---|---|---|
| | | 4 |
| **Контактная работа (всего)** | **8,3** | **8,3** |
| в том числе: | | |
| 1) занятия лекционного типа (ЛК) | 4 | 4 |
| из них | | |
| -лекций | 4 | 4 |
| 2) занятия семинарского типа (ПЗ) | 4 | 4 |
| -семинары (С) | 2 | 2 |
| -практические занятия (ПР) | 2 | 2 |
| -лабораторные работы (ЛР) | | |
| 3) групповые консультации | | |
| 4) индивидуальная работа | | |
| 5) промежуточная аттестация | 0,3 | 0,3 |
| **Самостоятельная работа (всего) (СР)** | **135,7** | **135,7** |
| в том числе: | | |
| Курсовой проект (работа) | | |
| Расчетно-графические работы | | |
| Контрольная работа | | |
| Реферат | | |
| Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и | 132 | 132 |

| | | |
|---|---|---|
| практическим занятиям, коллоквиумам и т.д.) | | |
| Подготовка к аттестации | 3,7 | 3,7 |
| Общий объем, час | **144** | **144** |
| Форма промежуточной аттестации | Диф. зачёт | Диф. зачёт |

## 5. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

### 5.1. Содержание дисциплины

| № темы | Наименование темы | Содержание темы |
|---|---|---|
| 1 | Информационная безопасность: понятия и определения | Роль информационной безопасности и ее место в системе национальной безопасности, информационная безопасность, её основные составляющие и аспекты |
| 2 | Угрозы информационной безопасности | Понятие угрозы информационной безопасности, классификация угроз по различным признакам |
| 3 | Вредоносные программы | Понятие вредоносных программ, их классификация, способы распространения вредоносных программ |
| 4 | Методы и средства защиты компьютерной информации | Программно-технические методы обнаружения вирусов, административно-технологические методы защиты, особенности защиты информации в персональных компьютерах |
| 5 | Криптографические методы защиты информации | Наука криптография, криптографические методы защиты информации, криптосистемы, управление ключами, электронная цифровая подпись |
| 6 | Лицензирование и сертификация в области защиты информации | Понятия лицензирования и сертификации в области защиты информации, нормативная правовая база системы сертификации средств защиты информации, порядок проведения лицензирования |
| 7 | Критерии безопасности компьютерных систем | Классы безопасности компьютерных систем, категории требований безопасности компьютерных систем |

### 5.2. Структура дисциплины

Очная форма обучения

| № темы | Наименование темы | Количество часов | | | |
|---|---|---|---|---|---|
| | | Всего | Л | ПР | СР |
| 1 | Информационная безопасность: понятия и определения | 20 | 2 | 2 | 16 |
| 2 | Угрозы информационной безопасности | 22 | 2 | 2 | 18 |
| 3 | Вредоносные программы | 22 | 2 | 2 | 18 |
| 4 | Методы и средства защиты компьютерной информации | 22 | 2 | 2 | 18 |
| 5 | Криптографические | 22 | 2 | 2 | 18 |

| | | | | | |
|---|---|---|---|---|---|
| | методы защиты информации | | | | |
| 6 | Лицензирование и сертификация в области защиты информации | 18 | - | - | 18 |
| 7 | Критерии безопасности компьютерных систем | 18 | - | - | 18 |
| Групповая консультация | | - | | | |
| Промежуточная аттестация | | - | | | |
| Общий объем | | 144 | 10 | 10 | 124 |

Заочная форма обучения

| № темы | Наименование темы | Количество часов | | | |
|---|---|---|---|---|---|
| | | Всего | Л | ПР | СР |
| 1 | Информационная безопасность: понятия и определения | 20 | 1 | 1 | 18 |
| 2 | Угрозы информационной безопасности | 20 | 1 | 1 | 18 |
| 3 | Вредоносные программы | 20 | 1 | 1 | 18 |
| 4 | Методы и средства защиты компьютерной информации | 19 | 1 | - | 18 |
| 5 | Криптографические методы защиты информации | 21 | - | 1 | 20 |
| 6 | Лицензирование и сертификация в области защиты информации | 20 | - | - | 20 |
| 7 | Критерии безопасности компьютерных систем | 20 | - | - | 20 |
| Групповая консультация | | - | | | |
| Промежуточная аттестация | | 4 | | | |
| Общий объем | | 144 | 4 | 4 | 132 |

### 5.3. Занятия семинарского типа

Очная форма обучения

| № п/п | № темы | Вид занятия | Наименование | Количество часов |
|---|---|---|---|---|
| 1 | 1 | С | Структура концепции безопасности предприятия. Основные Положения. Разработка концепции безопасности предприятия | 2 |
| 2 | 2 | С | Разработка программы безопасности | 2 |
| 3 | 3 | ПР | Криптографические методы защиты информации | 2 |
| 4 | 4 | ПР | Исследование различных методов защиты | 2 |

| | | | | |
|---|---|---|---|---|
| | | | текстовой информации и их стойкости на основе подбора ключей | |
| 5 | 5 | ПР | Составление плана мероприятий по защите информации при подготовке к проведению совещания | 2 |

Заочная форма обучения

| № п/п | № темы | Вид занятия | Наименование | Количество часов |
|---|---|---|---|---|
| 1 | 1 | С | Структура концепции безопасности предприятия. Основные Положения. Разработка концепции безопасности предприятия | 1 |
| 2 | 2 | С | Разработка программы безопасности | 1 |
| 3 | 3 | ПР | Криптографические методы защиты информации | 1 |
| 4 | 4 | ПР | Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей | - |
| 5 | 5 | ПР | Составление плана мероприятий по защите информации при подготовке к проведению совещания | 1 |

**5.4. Курсовой проект (курсовая работа, расчетно-графическая работа, реферат, контрольная работа)**

не предусмотрен

**5.5. Самостоятельная работа**

Очная форма обучения

| № темы | Виды самостоятельной работы | Количество часов |
|---|---|---|
| 1 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 16 |
| 2 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 3 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 4 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 5 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 6 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 7 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 1-7 | Подготовка к аттестации | - |

Заочная форма обучения

| № темы | Виды самостоятельной работы | Количество часов |
|---|---|---|
| 1 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 2 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 3 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 4 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 18 |
| 5 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 20 |
| 6 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 20 |
| 7 | Проработка и повторение лекционного материала, Подготовка к практическим занятиям | 20 |
| 1-7 | Подготовка к аттестации | 4 |

## 6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

**Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине**

*Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине:*

- сбор, хранение, систематизация, обработка и представление учебной и научной информации;
- обработка различного рода информации с применением современных информационных технологий;
- самостоятельный поиск дополнительного учебного и научного материала, с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных;
- использование электронной почты для рассылки и асинхронного общения, чата преподавателей и обучающихся, переписки и обсуждения возникших учебных проблем для синхронного взаимодействия
- дистанционные образовательные технологии (при необходимости).

**Интерактивные и активные образовательные технологии**

| № раздела (темы) | Вид занятия (Л, ПР, С, ЛР) | Используемые интерактивные образовательные технологии | Количество часов | |
|---|---|---|---|---|
| | | | ОФО | ЗФО |
| 5 | Л | Лекция-визуализация | 2 | - |
| 1,2 | С | Круглый стол | 4 | 2 |
| 4 | Л | Проблемная лекция | 2 | - |

**Практическая подготовка обучающихся**

| № раздела (темы) | Вид занятия (ЛК, ПР, ЛР) | Виды работ | Количество часов ОФО/ЗФО |
|---|---|---|---|
| 2 | ПР | Угрозы информационной безопасности | 2/1 |
| 3 | ПР | Вредоносные программы | 2/1 |

| | | | |
|---|---|---|---|
| 4 | ПР | Методы и средства защиты компьютерной информации | 2/- |

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Описание показателей оценивания компетенций, формируемых в процессе освоения дисциплины и используемые оценочные средства приведены в таблице 1.

Таблица 1 – Показатели оценивания и оценочные средства для оценивания результатов обучения по дисциплине/ практике

| Код и наименование формируемой компетенции | Код и наименование индикатора достижения формируемой компетенции | Показатели оценивания (результаты обучения) | Процедуры оценивания (оценочные средства) | |
|---|---|---|---|---|
| | | | текущий контроль успеваемости | промежуточная аттестация |
| **ПК-2** Способен проводить аудит конфигураций ИС и управлять выпуском релизов в проектах малого и среднего уровня сложности в области ИТ | ПК-2.1. Идентифицирует конфигурацию ИС. | **Знает:** цели, задачи и функции администрирования в информационных системах | Контрольные вопросы, тестирование | Диф.зачет (Контрольные вопросы, тестирование ) |
| | ПК-2.3. Проводит аудит конфигураций ИС в проектах малого и среднего уровня сложности в области ИТ | **Умеет** проводить аудит конфигураций ИС в проектах малого и среднего уровня сложности в области ИТ | Практические/ситуационные задачи | Диф.зачет (Практические/ситуационные задачи ) |
| ПК-2 | | | | Диф. зачет |

### 7.1 ОЦЕНОЧНЫЕ СРЕДСТВА, КРИТЕРИИ И ШКАЛА ОЦЕНКИ

**Типовые задания для текущего контроля**
**Типовые контрольные вопросы для устного опроса при текущем контроле**

Устные опросы проводятся во время лекций, практических занятий и возможны при проведении промежуточной аттестации в качестве дополнительного испытания при недостаточности результатов тестирования. Основные вопросы для устного опроса доводятся до сведения обучающихся на предыдущем занятии.

Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях.

1. Роль информационной безопасности и ее место в системе национальной безопасности.
2. Понятие информационной безопасности.
3. Основные составляющие информационной безопасности.
4. Аспекты информационной безопасности.

5. Понятие угрозы информационной безопасности.
6. Классификация угроз по источнику или местонахождению.
7. Классификация угроз по вероятности реализации.
8. Классификация угроз по размерам наносимого ущерба.
9. Классификация угроз по формам проявления.
10. Классификация угроз по способам воздействия на объекты информационной безопасности.
11. Классификация угроз по способу доступа к ресурсам.
12. Понятие вредоносных программ.
13. Классификация вредоносных программ.
14. Способы распространения вредоносных программ.
15. Обзор вредоносных программ.
16. Программно-технические методы обнаружения вирусов.
17. Административно-технологические методы защиты.
18. Особенности защиты информации в персональных компьютерах.
19. Криптография как наука.
20. Криптографические методы защиты информации.
21. Криптосистемы.
22. Управление ключами в криптосистемах.
23. Электронная цифровая подпись.
24. Лицензирование в области защиты информации.
25. Порядок проведения лицензирования в области защиты информации.
26. Сертификация в области защиты информации.
27. Нормативная правовая база системы сертификации средств защиты информации.
28. Категории требований безопасности компьютерных систем.

**Критерии и шкала оценивания устного опроса**

| | |
|---|---|
| отлично | 1) студент полно излагает материал, дает правильное определение основных понятий;<br>2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные;<br>3) излагает материал последовательно и правильно с точки зрения норм литературного языка. |
| хорошо | студент дает ответ, удовлетворяющий тем же требованиям, что и для отметки, но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого. |
| удовлетворительно | студент обнаруживает знание и понимание основных положений данной темы, но:<br>1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил;<br>2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;<br>3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого. |
| неудовлетворительно | студент обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке, которые являются серьезным препятствием к успешному овладению последующим материалом. |

**Типовые тестовые задания**

1. Что такое шифрование?
   а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого+
   б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
   в) удобная среда для вычисления конечного пользователя
2. Что такое кодирование?
   а) преобразование обычного, понятного текста в код+
   б) преобразование
   в) написание программы
3. Для восстановления защитного текста требуется:
   а) ключ
   б) матрица
   в) вектор
4. Сколько лет назад появилось шифрование?
   а) четыре тысячи лет назад+
   б) две тысячи лет назад
   в) пять тысяч лет назад
5. Первое известное применение шифра:
   а) египетский текст+
   б) русский
   в) нет правильного ответа
6. Секретная информация, которая хранится вWindows:
   а) пароли для доступа к сетевым ресурсам+
   б) пароли для доступа в Интернет+
   в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере+
7. Что такое алфавит?
   а) конечное множество используемых для кодирования информации знаков+
   б) буквы текста
   в) нет правильного ответа
8. Что такое текст?
   а) упорядоченный набор из элементов алфавита+
   б) конечное множество используемых для кодирования информации знаков
   в) все правильные
9. Выберите примеры алфавитов:
   а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8+
   б) восьмеричный и шестнадцатеричный алфавиты+
   в) AEE
10. Что такое шифрование?
    а) преобразовательный процесс исходного текста в зашифрованный+
    б) упорядоченный набор из элементов алфавита
    в) нет правильного ответа
11. Что такое дешифрование?
    а) на основе ключа шифрованный текст преобразуется в исходный+
    б) пароли для доступа к сетевым ресурсам
    в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Что представляет собой криптографическая система?
    а) семейство T преобразований открытого текста, члены его семейства индексируются символом k+
    б) программу
    в) систему
13. Что такое пространство ключей k?
    а) набор возможных значений ключа+
    б) длина ключа
    в) нет правильного ответа
14. На какие виды подразделяют криптосистемы?
    а) симметричные+
    б) ассиметричные+
    в) с открытым ключом+
15. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
    а) 1+
    б) 2
    в) 3
16. Количество используемых ключей в системах с открытым ключом:
    а) 2+
    б) 3
    в) 1
17. Ключи, используемые в системах с открытым ключом:
    а) открытый+
    б) закрытый+
    в) нет правильного ответа
18. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:
    а) математически+
    б) логически
    в) алгоритмически
19. Что принято называть электронной подписью?
    а) присоединяемое к тексту его криптографическое преобразование+
    б) текст
    в) зашифрованный текст
20. Что такое криптостойкость?
    а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа+
    б) свойство гаммы
    в) все ответы верны
21. Выберите то, что относится к показателям криптостойкости:
    а) количество всех возможных ключей+
    б) среднее время, необходимое для криптоанализа+
    в) количество символов в ключе
22. Требования, предъявляемые к современным криптографическим системам защиты информации:
    а) знание алгоритма шифрования не должно влиять на надежность защиты+
    б) структурные элементы алгоритма шифрования должны быть неизменными+
    в) не должно быть простых и легко устанавливаемых зависимостью между ключами +последовательно используемыми в процессе шифрования+
23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
    а) длина шифрованного текста должна быть равной лине исходного текста+

б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа+
в) нет правильного ответа

24. Основными современными методами шифрования являются:
а) алгоритм гаммирования+
б) алгоритмы сложных математических преобразований+
в) алгоритм перестановки+

25. Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?
а) алгоритмом гаммирования+
б) алгоритмом перестановки
в) алгоритмом аналитических преобразований

26. Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?
а) алгоритм перестановки+
б) алгоритм подстановки
в) алгоритм гаммирования

27. Самая простая разновидность подстановки:
а) простая замена+
б) перестановка
в) простая перестановка

28. Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
а) 3+
б) 4
в) 5

29. Таблицы Вижинера, применяемые для повышения стойкости шифрования:
а) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке+
б) в качестве ключа используется случайность последовательных чисел+
в) нет правильного ответа

**Критерии и шкала оценки результатов тестирования**

Количество правильных ответов:
Менее 52% - «неудовлетворительно»
53-70% – «удовлетворительно»
71-85% – «хорошо»
86-100% – «отлично»

**Типовые практические задания**
**Тема: Криптографические методы защиты информации**

*Цель работы: изучение различных методов защиты информации*

**Методы перестановки.**

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода.

1. Самая простая перестановка - написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы:

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ,

получится такой шифртекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, его следует дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется ничего сложного, но при расшифровке возникнут серьезные неудобства.

2. Во время Гражданской войны в США использовался был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки ничего не значащими буквами).

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| П | У | С | Т | Ь | Б | У | Д | Е | Т | Т | А | К | К | А |
| К | М | Ы | Х | О | Т | Е | Л | И | К | Л | М | Н | О | П |

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки:

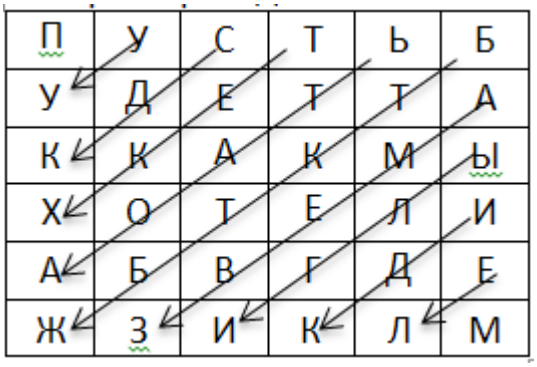
ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

3. Вариант этого шифра: исходную фразу писать в столбцы, а затем на пятерки разбивать строки:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| П | С | Ь | У | Е | Т | К | А | М | Х | Т | Л | А | В | Д |
| У | Т | Б | Д | Т | А | К | К | Ы | О | Е | И | Б | Г | Е |

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

4. Исходный текст можно записать в квадратную таблицу и списать из нее, например по диагоналям:




ПУУСДК ТЕКХЬТ АОАБТК ТБЖАМЕ ВЗЫЛГИ ИДКЕЛМ

5. Часто используются перестановки с ключом

Выберем в качестве ключа слово «*информация*». Пронумеруем ключ (первая, из имеющихся в ключе, в алфавите буква А, следовательно ей присваивается номер 1; следующая по алфавиту буква И, следовательно первая буква И будет иметь номер 2, а вторая – 3; далее идет буква М, ей присваиваем номер 4 и т.д.):

| и | н | ф | о | р | м | а | ц | и | я |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 5 | 8 | 6 | 7 | 4 | 1 | 9 | 3 | 10 |

Запишем в таблицу нашу фразу под ключом. Оставшиеся ячейки до конца строки заполняют «пустышками».

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| и | н | ф | о | р | м | а | ц | и | я |
| 2 | 5 | 8 | 6 | 7 | 4 | 1 | 9 | 3 | 10 |
| П | У | С | Т | Ь | | Б | У | Д | Е |
| Т | | Т | А | К | | К | А | К | |
| М | Ы | | Х | О | Т | Е | Л | И | Ф |

Переписываем столбцы, учитывая их номер:
БКЕПТМДКИ ТУ ЫТАХЬКОСТ УАЛЕ Ф
Для дешифрования зашифрованный текст записывается в таблицу по столбцам, учитывая их номер.

6. Гамильтоновы пути.
Выбираем ключ и нумеруем его как в предыдущем методе. Символы шифруемой фразы нумеруем по порядку в пределах ключа. Затем переставляем символы исходного текста, учитывая номер ключа.
Ключ: л е г е н д а
6 4 2 5 7 3 1

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| П | У | С | Т | Ь | | Б | У | Д | Е | Т | | Т | А | К | | К | А | К |

| 6 | 7 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| М | Ы | | Х | О | Т | Е | Л | И |

Получаем текст: ☐ТУЬБСПТТД☐АЕУМА☐КЫККЛТХЕИО☐

**Критерии и шкала оценивания практического задания**

| | |
|---|---|
| отлично | студент правильно ответил на вопрос, уверенно, логично, последовательно и аргументировано излагал свой ответ, используя понятия дисциплины. |
| хорошо | студент самостоятельно и в основном правильно ответил на вопрос, уверенно, логично, последовательно и аргументировано излагал свой ответ, используя понятия дисциплины. |
| удовлетворительно | студент в основном ответил на вопрос, допустил несущественные ошибки, слабо аргументировал свое мнение, используя в основном понятия дисциплины. |
| неудовлетворительно | студент не ответил на вопросы. |

**Типовые задания для промежуточной аттестации**
**Перечень типовых контрольных вопросов для устного опроса на промежуточной аттестации**
**(диф. зачет)**

1. Роль информационной безопасности и ее место в системе национальной безопасности.
2. Понятие информационной безопасности.
3. Основные составляющие информационной безопасности.
4. Аспекты информационной безопасности.
5. Понятие угрозы информационной безопасности.
6. Классификация угроз по источнику или местонахождению.

7. Классификация угроз по вероятности реализации.
8. Классификация угроз по размерам наносимого ущерба.
9. Классификация угроз по формам проявления.
10. Классификация угроз по способам воздействия на объекты информационной безопасности.
11. Классификация угроз по способу доступа к ресурсам.
12. Понятие вредоносных программ.
13. Классификация вредоносных программ.
14. Способы распространения вредоносных программ.
15. Обзор вредоносных программ.
16. Программно-технические методы обнаружения вирусов.
17. Административно-технологические методы защиты.
18. Особенности защиты информации в персональных компьютерах.
19. Криптография как наука.
20. Криптографические методы защиты информации.
21. Криптосистемы.
22. Управление ключами в криптосистемах.
23. Электронная цифровая подпись.
24. Лицензирование в области защиты информации.
25. Порядок проведения лицензирования в области защиты информации.
26. Сертификация в области защиты информации.
27. Нормативная правовая база системы сертификации средств защиты информации.

**Тестовые задания для промежуточной аттестации**

1. Суть метода перестановки:
   а) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов+
   б) замена алфавита
   в) все правильные
2. Цель криптоанализа:
   а) Определение стойкости алгоритма+
   б) Увеличение количества функций замещения в криптографическом алгоритме
   в) Уменьшение количества функций подстановок в криптографическом алгоритме
   г) Определение использованных перестановок
3. По какой причине произойдет рост частоты применения брутфорс-атак?
   а) Возросло используемое в алгоритмах количество перестановок и замещений
   б) Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
   в) Мощность и скорость работы процессоров возросла+
   г) Длина ключа со временем уменьшилась
4. Не будет являться свойством или характеристикой односторонней функции хэширования:
   а) Она преобразует сообщение произвольной длины в значение фиксированной длины
   б) Имея значение дайджеста сообщения, невозможно получить само сообщение
   в) Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
   г) Она преобразует сообщение фиксированной длины в значение переменной длины+
5. Выберите то, что указывает на изменение сообщения:
   а) Изменился открытый ключ
   б) Изменился закрытый ключ
   в) Изменился дайджест сообщения+
   г) Сообщение было правильно зашифровано

6. Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:
   а) Data Encryption Algorithm
   б) Digital Signature Standard
   в) Secure Hash Algorithm+
   г) Data Signature Algorithm
7. Выберите то, что лучшеописывает отличия между HMAC и CBC-MAC?
   а) HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
   б) HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
   в) HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC+
   г) HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком
8. Определите преимущество RSA над DSA?
   а) Он может обеспечить функциональность цифровой подписи и шифрования+
   б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
   в) Это блочный шифр и он лучше поточного
   г) Он использует одноразовые шифровальные блокноты
9. С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?
   а) Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
   б) Эти системы могут использоваться некоторыми странами против их местного населения
   в) Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования+
   г) Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему
10. Выберите то, что используют для создания цифровой подписи:
   а) Закрытый ключ получателя
   б) Открытый ключ отправителя
   в) Закрытый ключ отправителя+
   г) Открытый ключ получателя
11. Выберите то, что лучше всего описывает цифровую подпись:
   а) Это метод переноса собственноручной подписи на электронный документ
   б) Это метод шифрования конфиденциальной информации
   в) Это метод, обеспечивающий электронную подпись и шифрование
   г) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения+
12.Эффективная длина ключа в DES:
   а) 56+
   б) 64
   в) 32
   г) 16
13. Причина, по которой удостоверяющий центр отзывает сертификат:
   а) Если открытый ключ пользователя скомпрометирован
   б) Если пользователь переходит на использование модели PEM, которая использует сеть доверия

в) Если закрытый ключ пользователя скомпрометирован+
г) Если пользователь переходит работать в другой офис

14. Выберите то, что лучше всего описывает удостоверяющий центр?
а) Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
б) Организация, которая проверяет процессы шифрования
в) Организация, которая проверяет ключи шифрования
г) Организация, которая выпускает сертификаты+

15. Расшифруйте аббревиатуру DEA:
а) Data Encoding Algorithm
б) Data Encoding Application
в) Data Encryption Algorithm+
г) Digital Encryption Algorithm

16. Разработчик первого алгоритма с открытыми ключами:
а) Ади Шамир
б) Росс Андерсон
в) Брюс Шнайер
г) Мартин Хеллман+

17. Процесс, выполняемый после создания сеансового ключа DES:
а) Подписание ключа
б) Передача ключа на хранение третьей стороне (key escrow)
в) Кластеризация ключа
г) Обмен ключом+

18. Количество циклов перестановки и замещения, выполняемый DES:
а) 16+
б) 32
в) 64
г) 56

19. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:
а) Оно обеспечивает проверку целостности и правильности данных
б) Оно требует внимательного отношения к процессу управления ключами+
в) Оно не требует большого количества системных ресурсов
г) Оно требует передачи ключа на хранение третьей стороне (escrowed)

20. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:
а) Коллизия
б) Хэширование
в) MAC
г) Кластеризация ключей+

21. Определение фактора трудозатрат для алгоритма:
а) Время зашифрования и расшифрования открытого текста
б) Время, которое займет взлом шифрования+
в)Время, которое занимает выполнение 16 циклов преобразований
г) Время, которое занимает выполнение функций подстановки

22. Основная цельиспользования одностороннего хэширования пароля пользователя:
а) Это снижает требуемый объем дискового пространства для хранения пароля пользователя
б) Это предотвращает ознакомление кого-либо с открытым текстом пароля+
в) Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
г) Это предотвращает атаки повтора (replay attack)

23. Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя:
    а) ECC
    б) RSA+
    в)DES
    г) Диффи-Хеллман
24. Что является описанием разницы алгоритмов DES и RSA:
    а) DES – это симметричный алгоритм, а RSA – асимметричный +
    б) DES – это асимметричный алгоритм, а RSA – симметричный
    в) Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
    г) DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений
25. Алгоритм, использующий симметричный ключ и алгоритм хэширования:
    а) HMAC+
    б) 3DES
    в) ISAKMP-OAKLEY
    г) RSA
26. Количество способов гаммирования:
    а) 2+
    б) 5
    в) 3
27. Показатель стойкости шифрования методом гаммирования:
    а) свойство гаммы+
    б) длина ключа
    в) нет правильного ответа
28. То, что применяют в качестве гаммы:
    а) любая последовательность случайных символов+
    б) число
    в) все ответы верны
29. Метод, который применяют при шифровании с помощью аналитических преобразований:
    а) алгебры матриц+
    б) матрица
    в) факториал
30. То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований:
    а) матрица А+
    б) вектор
    в) обратная матрица

**Критерии и шкала оценки результатов тестирования**

Количество правильных ответов:
Менее 52% - «неудовлетворительно»
53-70% – «удовлетворительно»
71-85% – «хорошо»
86-100% – «отлично»

**Перечень типовых ситуационных задач для промежуточной аттестации**

1. Зашифруйте полученную у преподавателя фразу всеми методами перестановки.
2. Зашифруйте фразу методом гаммирования.
3. Зашифруйте фразу шифром Цезаря.

4. Расшифруйте полученную у преподавателя информацию.
5. Расшифруйте фразу методом гаммирования.
6. Расшифруйте фразу шифром Цезаря.

**Критерии и шкала оценки дифференцированного зачета по дисциплине**

| Оценка | **Характеристики ответа обучающегося** |
|---|---|
| Отлично | - студент глубоко и всесторонне усвоил программный материал;<br>- уверенно, логично, последовательно и грамотно его излагает;<br>- опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью;<br>- умело обосновывает и аргументирует выдвигаемые им идеи;<br>- делает выводы и обобщения;<br>- свободно владеет системой понятий по дисциплине;<br>-правильно решил ситуационную задачу. |
| Хорошо | - студент твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;<br>- не допускает существенных неточностей;<br>- увязывает усвоенные знания с практической деятельностью;<br>- аргументирует научные положения;<br>- делает выводы и обобщения;<br>- владеет системой понятий по дисциплине;<br>-правильно решил ситуационную задачу. |
| Удовлетворительно | - студент усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;<br>- допускает несущественные ошибки и неточности;<br>- испытывает затруднения в практическом применении знаний;<br>- слабо аргументирует научные положения;<br>- затрудняется в формулировании выводов и обобщений;<br>- частично владеет системой понятий по дисциплине;<br>- с затруднениями решил ситуационную задачу. |
| Неудовлетворительно | - студент не усвоил значительной части программного материала;<br>- допускает существенные ошибки и неточности при рассмотрении проблем;<br>- испытывает трудности в практическом применении знаний;<br>- не может аргументировать научные положения;<br>- не формулирует выводов и обобщений;<br>- не решил ситуационную задачу |

## 7.2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося.

Краткая характеристика процедуры реализации текущего и промежуточного контроля для оценки компетенций обучающихся представлена в таблице.

| Процедура оценивания | Организация деятельности обучающегося |
|---|---|
| Семинарское занятие | Участие в семинарских занятиях предполагает отработку и закрепление студентами навыков работы с информацией, взаимодействия с коллегами и профессиональных навыков (участия в публичных выступлениях, ведения дискуссий и т.п.). При подготовке к занятию можно выделить 2 этапа: организационный; закрепление и углубление теоретических знаний.<br>На первом этапе студент планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор рекомендованной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе.<br>Второй этап включает непосредственную подготовку студента к занятию. |
| Устный опрос | Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.<br>Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях.<br>Показатели для оценки устного ответа: 1) знание материала; 2) последовательность изложения; 3) владение речью и профессиональной терминологией; 4) применение конкретных примеров; 5) знание ранее изученного материала; 6) уровень теоретического анализа; 7) степень самостоятельности; 8) степень активности в процессе; 9) выполнение регламента.<br>Уровень знаний обучающегося определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».<br>Критерии и шкала оценки приведены в п. 3. Фонда оценочных средств. |
| Тестирование | Это средство контроля полноты усвоения понятий, представлений, существенных положений отдельных тем (разделов) дисциплины.<br>Процедура проведения данного оценочного мероприятия включает в себя: осуществляется по вариантам; количество вопросов в каждом варианте –10-15; отведенное время– 90 мин. Решение заданий в тестовой форме проводится в течение изучения дисциплины.<br>Для подготовки к данному оценочному мероприятию студенты должны изучить разделы (темы, вопросы), по которым будут задания в тестовой форме, и теоретические источники для подготовки.<br>При проведении тестирования, студенту запрещается пользоваться дополнительной литературой. |

## Методические материалы, определяющие процедуры оценивания в рамках промежуточной аттестации

**Дифференцированный зачет** – это форма промежуточной аттестации, задачей которой является комплексная оценка уровней достижения планируемых результатов обучения по дисциплине.

Дифференцированный зачет по дисциплине проводится за счет часов, отведённых на изучение дисциплины.

Дифференцированный зачет по дисциплине проводится включает в себя: собеседование

преподавателя со студентами по контрольным вопросам (не более 5) и 1 ситуационную задачу.

| | |
|---|---|
| Контрольные вопросы | Контрольный вопрос — это средство контроля усвоения учебного материала дисциплины.<br>Процедура проведения данного оценочного мероприятия включает в себя: беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме дисциплины. |
| Ситуационная задача | Оценочное средство, включающее совокупность условий, направленных на решение практически значимой ситуации с целью формирования компетенций, соответствующих основным типам профессиональной деятельности.<br>Процедура проведения данного оценочного мероприятия включает в себя: оценку правильности решения задач, кратко изложить ее содержание. В случае вариативности решения задачи следует обосновать все возможные варианты решения. |
| Тестовое задание | Оценочное средство, варьирующееся по элементам содержания и по трудности единица контрольного материала, сформулированная в утвердительной форме предложения с неизвестным. Подстановка правильного ответа вместо неизвестного компонента превращает задание в истинное высказывание, подстановка неправильного ответа приводит к образованию ложного высказывания, что свидетельствует о незнании студентом данного учебного материала. |

Перечень контрольных вопросов и ситуационные задачи к дифференцированный зачету, а также критерии и шкала оценки приведены в п. 3. Фонда оценочных средств.

Контрольные вопросы и ситуационные задачи к дифференцированному зачету доводятся до сведения студентов заранее.

При подготовке к ответу пользование учебниками, учебно-методическими пособиями, средствами связи и электронными ресурсами на любых носителях запрещено.

На ответ студента по каждому контрольному вопросу и ситуационной задачи отводится, как правило, 3-5 минут.

После окончания ответа преподаватель объявляет обучающемуся оценку по результатам дифференцированного зачета, а также вносит эту оценку в зачетно-экзаменационную ведомость, зачетную книжку.

Уровень знаний, умений и навыков обучающегося определяется оценками «отлично», «хорошо», «удовлетворительно», «не удовлетворительно».

В критерии итоговой оценки уровня подготовки обучающегося по дисциплине входят:

уровень усвоения студентом материала, предусмотренного рабочей программой;

уровень практических умений, продемонстрированных студентом при выполнении практических заданий;

уровень освоения компетенций, позволяющих выполнять практические задания;

логика мышления, обоснованность, четкость, полнота ответов.

## 8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 8.1. Основная литература

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. – 3-е изд. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 266 с. – Режим доступа: http://www.iprbookshop.ru/97562.html. – ЭБС «IPRbooks».

2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. – 3-е изд. – Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 154 с. – Режим доступа: http://www.iprbookshop.ru/89453.html . – ЭБС «IPRbooks».

3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов : Профобразование, 2019. – 702 с. – Режим доступа: http://www.iprbookshop.ru/87995.html . – ЭБС «IPRbooks».

**8.2. Дополнительная литература**

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — Режим доступа: http://www.iprbookshop.ru/89443.html

2. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. – Электрон.текстовые данные. – Саратов: Ай Пи Ар Букс, 2015. – 326 с. – 978-5-906-17271-6. – Режим доступа: http://www.iprbookshop.ru/33857.html

3. Артемов А.В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов. – Электрон.текстовые данные. – Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 256 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/33430.html

4. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html



Периодические издания

1. IT-Expert https://www.it-world.ru/itexpert/
2. Прикладная информатика http://www.appliedinformatics.ru/
3. Программные продукты и системы http://www.swsys.ru/
4. ITNews https://www.it-world.ru/itnews/
5. IT Manager https://www.it-world.ru/itmanager/

**8.3. Программное обеспечение**

Microsoft Windows, Яндекс 360, Microsoft Office Professional Plus 2019, Google Chrome, Яндекс.Браузер.

**8.4. Профессиональные базы данных**

1. База данных IT специалиста: http://info-comp.ru/
2. База данных программного обеспечения Oracle»: https://www.oracle.com/ru/index.html
3. База данных рекламы и PR: https://www.oracle.com/ru/index.html

**8.5. Информационные справочные системы**

1С: Библиотека - https://www.sksi.ru/environment/eor/library/

Справочно-правовая система «КонсультантПлюс» - http://www.consultant.ru/

*Поисковые системы*

Поисковая система Yandex- https://www.yandex.ru/

Поисковая система Rambler – https://www.rambler.ru/

**8.6. Интернет-ресурсы**

1. Единая коллекция цифровых образовательных ресурсов - http://school-collection.edu.ru/
2. Электронная библиотечная система «СКСИ» https://www.sksi.ru/environment/ebs/1363/
3. Электронная библиотека «Все учебники» - http://www.vse-ychebniki.ru/
4. Цифровой образовательный ресурс IPRsmart - http://www.iprbookshop.ru/
5. Образовательная платформа ЮРАЙТ - https://urait.ru/

## 8.7. Методические указания по освоению дисциплины

*Методические указания при работе над конспектом во время проведения лекции*

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Общие и утвердившиеся в практике правила и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их.

В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

В конспект следует заносить всё, что преподаватель пишет на доске, а также рекомендуемые схемы, таблицы, диаграммы и т.д.

*Методические указания по подготовке к практическим работам*

Целью практических работ является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, а, следовательно, формирование у них определенных умений и навыков.

В ходе подготовки к практическим работам необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой, выполнить выданные преподавателем задания. При этом учесть указания преподавателя и требования программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы. Желательно при подготовке к практическим и лабораторным работам по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

*Методические указания по организации самостоятельной работы*

Самостоятельная работа приводит обучающегося к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений.

Самостоятельная работа выполняет ряд функций:

- развивающую;
- информационно-обучающую;
- ориентирующую и стимулирующую;
- воспитывающую;
- исследовательскую.

Виды самостоятельной работы, выполняемые в рамках курса:

1. Проработка и повторение лекционного материала
2. Подготовка к практическим занятиям
3. Подготовка к аттестации

Обучающимся рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые обучающийся получает в аудитории.

Можно отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой.

Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала.

*Методические указания по работе с литературой*

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой следует учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность обучающемуся сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к лабораторным практикумам по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов обучающийся будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в приведенном в ФОС перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью изучающего чтения является глубокое и всестороннее понимание учебной информации.

Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.

2. Прием постановки вопросов к тексту имеет следующий алгоритм:

- медленно прочитать текст, стараясь понять смысл изложенного;
- выделить ключевые слова в тексте;
- постараться понять основные идеи, подтекст и общий замысел автора.

3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

**Методические указания по подготовке к промежуточной аттестации**

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета.

Дифференцированный зачет – это форма промежуточной аттестации, задачей которой является комплексная оценка уровней достижения планируемых результатов обучения по дисциплине.

При подготовке к дифференцированному зачету необходимо повторить конспекты лекций по всем разделам дисциплины. На зачете студент должен подтвердить усвоение учебного материала, предусмотренного рабочей программой дисциплины, а также продемонстрировать приобретенные навыки адаптации полученных теоретических знаний к своей профессиональной деятельности. Дифференцированный зачет проводится в форме устного собеседования по контрольным вопросам, а также обучающемуся необходимо решить ситуационную задачу.

## 9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины требуется следующее материально-техническое обеспечение (специальные помещения):

- для проведения занятий лекционного типа

учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.

- для проведения занятий семинарского типа, практических занятий

учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.

- для проведения , текущего контроля и промежуточной аттестации

учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.

- для групповых и индивидуальных консультаций

учебная аудитория, оснащенная учебной мебелью, оборудованная проектором, ПК, экраном, доской.

- для самостоятельной работы:

помещение, оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института

## 10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (тьютора), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

– присутствие тьютора, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

– специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

– индивидуальное равномерное освещение не менее 300 люкс,

– при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

– присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются тьютору;

– по желанию студента задания могут выполняться в устной форме.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.04.02 Информационные системы и технологии.