**Государственное профессиональное образовательное учреждение
Тулской области «Донской политехнический колледж»**

Задания для выполнения самостоятельной работы

по МДК 02.02 Криптографические средства защиты информации

Преподаватель *Филатова Е.А.*

1) Самостоятельная работа по теме «Перспективные направления криптоанализа, квантовый криптоанализ», 2 часа

Изучите теоретический материал по данной теме и в письменной форме, в тетради, дайте ответы на следующие вопросы:

- 1) Перечислите перспективные направления криптоанализа.
- 2) Дайте определение атаки по времени.
- 3) Перечислите атаки на основе побочных каналов.
- 4) Какие бывают атаки по мощности?
- 5) Как использует криптоанализ аппаратные ошибки?
- 6) Как можно использовать квантовый криптоанализ?
- 7) Какие возможности дает квантовый криптоанализ при дешифрации?

Рекомендуемая литература

Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинин, В.Н. Пржегорлинский. — М.: Издательский центр «Академия», 2019, С. 156-159.

2) Самостоятельная работа по теме «Кодирование информации», 2 часа

Изучите теоретический материал по данной теме и в письменной форме, в тетради, дайте ответ на вопрос: Какие задачи решает кодирование при передаче информации по каналам связи?

Рекомендуемая литература

Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинин, В.Н. Пржегорлинский. — М.: Издательский центр «Академия», 2019, С. 80-81.

3) Самостоятельная работа по теме «Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4», 2 часа

Изучите теоретический материал по данной теме и в письменной форме, в тетради, дайте ответы на следующие вопросы:

- 1) Перечислите основные требования к блочному алгоритму шифрования.
- 2) Какой стандарт принят в России в качестве стандарта на блочные алгоритмы шифрования?
- 3) Какие режимы шифрования данных предусматривает ГОСТ 28147—89?
- 4) Назовите, в чем состоит отличие режима гаммирования с обратной связью от режима гаммирования.
- 5) Дайте характеристику криптографическому алгоритму «Магма».
- 6) Какие вы знаете зарубежные криптографические алгоритмы?
- 7) Опишите общую структуру криптографического алгоритма DES.
- 8) Какие проблемы возникают при распределении ключей симметричного шифрования?
- 9) Дайте определение понятия «сеансовый ключ».

Рекомендуемая литература

Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинин, В.Н. Пржегорлинский. — М.: Издательский центр «Академия», 2019, С. 113-133.

4) Самостоятельная работа по теме «Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ», 2 часа

Изучите теоретический материал по данной теме и в письменной форме, в тетради, дайте ответы на следующие вопросы:

1. Понятие цифрового водяного знака. Его преимущества перед печатным водяным знаком.
2. Виды цифровых водяных знаков.
3. Методы защиты с помощью цифровых водяных знаков.
4. Программы для создания цифровых водяных знаков.

Задание 1. Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

Задание 2. Подготовьте сравнительную таблицу программ, используемых для создания цифровых водяных знаков: PhotoWatermark Professional, Image Tuner, EasyWatermark, CryptoFoto. Сравнительный анализ проведите по следующими критериям:

- поддерживаемые типы мультимедийных файлов
- устойчивость водяных знаков к попыткам искажения, повреждения или компрессии
- качество встраивания и извлечения водяных знаков
- юзабилити и интерфейс
- поддержка автоматизации и скриптов
- стоимость и лицензирование
- безопасность и степень защиты контента

Рекомендуемая литература

- Иванов В. П., Смирнова Е. А. (2020). Методы встраивания цифровых водяных знаков. Москва: Наука и технологии.
- Литвинов А. В. (2019). Защита информации и цифровые водяные знаки. Санкт-Петербург: БХВ-Петербург.
- Официальные сайты разработчиков программных решений для встраивания водяных знаков.

5) Самостоятельная работа по теме «Нормативные правовые акты и документы, определяющие технические требования в криптографической сфере», 2 часа

1. Изучите основные нормативные правовые акты, регулирующие использование и развитие криптографических средств в Российской Федерации.

2. Проанализируйте содержание и основные положения следующих документов: - Федеральный закон «Об информации, информатике и защите информации» №149-ФЗ от 27.07.2006 - Постановление Правительства РФ №781 от 08.09.2016 «Об утверждении требований к государственным криптографическим средствам защиты информации» - ГОСТы и технические условия, касающиеся криптографических алгоритмов (например, ГОСТ Р 34.12-2015 «Криптографические протоколы и средства защиты информации») - Документы ФСТЭК России, регламентирующие использование криптографических технологий и сертификацию средств защиты информации.

3. Ответьте письменно в тетради на следующие вопросы:

а) Какие основные нормативные документы регулируют использование криптографических средств в России?

б) Какие технические требования предъявляются к криптографическим алгоритмам и средствам защиты информации?

в) Как осуществляется сертификация криптографического оборудования и программных средств в РФ?

г) Какие обязанности возлагаются на организации и граждан в сфере использования криптографии?