**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Н.В. Калинина
17 марта 2022 г

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

по междисциплинарному курсу
МДК.02.02. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

МДК.02.02. Криптографическая защита информации. Методические указания по выполнению лабораторных работ.

Составил: Кривоносова Н.В. – Санкт-Петербург, 2022.

Методические указания содержат описания лабораторных работ, предусмотренных рабочей программой **МДК.02.02. Криптографическая защита информации**. Каждая работа рассчитана на 2 академических часа, общий объём составляет 20 часов. Методические указания предназначены для обучающихся очной формы обучения по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рассмотрено и одобрено предметной (цикловой) комиссией информационной безопасности телекоммуникационных систем Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля.

СОДЕРЖАНИЕ

МДК 02.02. Криптографическая защита информации
Лабораторная работа 1
ИЗУЧЕНИЕ ПРОГРАММНЫХ ПРОДУКТОВ ЗАЩИТЫ ИНФОРМАЦИИ. ПРОГРАММА PGP (PRETTY GOOD PRIVACY)

1. **Цель работы**: исследование электромагнитных процессов и характеристик выпрямителей, выполненных по трехфазной схеме с нулевым выводом и трехфазной мостовой схеме, при работе на активную и активно-индуктивную нагрузку в режиме непрерывного тока.

2. **Задачи работы:**
   - Изучение основных принципов криптографии, на которых основаны системы защиты информации.
   - Изучение основных принципов работы программы PGP и ее компонентов.
   - Установка программы PGP и создание ключевых пар для шифрования и подписи сообщений.
   - Шифрование сообщений с помощью программы PGP и расшифровка полученных зашифрованных сообщений.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:
- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- возможные угрозы безопасности информации в ИТКС;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:
- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Выбрать тему и подготовить доклад:
1. Контроль доступа
2. Анти-кейлоггеры

3. Анти-шпионы (anti-spyware)
4. Анти-эксплуататоры (anti-subversion)
5. Анти-модификаторы (anti-tampering)
6. Антивирусы
7. Шифрование
8. Брандмауэры (firewall)
9. Системы обнаружения вторжений
10. Системы предотвращения вторжений
11. Песочница

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

Приложение 1

Краткие сведения из теории

Программная защита информации – система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации. Защитный программный код может выступать как отдельно, в качестве отдельного защитного программного продукта, так и включаться в состав других, многофункциональных программ, с целью защиты обрабатываемых ими данных или самозащиты от вредоносного кода. Так как защитные функции многофункциональных программ зачастую даже не имеют существенных средств самозащиты и по определению проигрывают специализированному защитному программному обеспечению, любая значимая компьютерная система требует развёртывания и полноценной интеграции программных средств защиты информации на всех или хотя бы самых уязвимых элементах системы.

Программные средства защиты информации делятся на типы так:

- Контроль доступа
- Анти-кейлоггеры
- Анти-шпионы (anti-spyware)
- Анти-эксплуататоры (anti-subversion)
- Анти-модификаторы (anti-tampering)
- Антивирусы
- Шифрование
- Брандмауэры (firewall)
- Системы обнаружения вторжений
- Системы предотвращения вторжений
- Песочница

Полноценная программная защита информации на сервере или рабочем компьютере требует использования различных типов защитных программ или специализированных защитных решений, совмещающих в себе несколько типов защиты одновременно.

Например, важно понимать, что господствующий на данный момент антивирусный подход, обычно объединяющий в себе антивирусы, анти-шпионы, анти-эксплуататоры и анти-модификаторы, недостаточен против целевых атак, так как он основан на сравнении программного кода с имеющимися у производителя сигнатурами вредоносного кода. Имеющаяся в некоторых случаях возможность применения поведенческого анализа также не даёт гарантии сохранности данных и сохранения работоспособности системы. Аналогично, контроль доступа сам по себе не способен гарантировать использование программ и данных исключительно имеющими право на это лицами, так как помимо программных уязвимостей такой тип защиты может быть «вскрыт» обычной социальной инженерией без использования высокотехнологичных способов нападения в принципе. Системы обнаружения вторжений могут помочь при последующем расследовании инцидента, но без систем предотвращения вторжений повреждения, полученные при атаке, могут оказаться слишком серьёзными, чтобы расследование в принципе понадобилось. Шифрование данных может помочь против попыток украсть эти данные, но не остановит злоумышленника, желающего эти данные уничтожить.

Подобные недостатки узкоспециализированной защиты можно найти в любой комбинации малого числа схожих типов программных средств защиты информации, поэтому защита всегда должна быть основана на множестве параллельных и зачастую пересекающихся алгоритмах. При использовании нескольких решений это чревато внутренними конфликтами в системе, поэтому наиболее логичным выводом является использование комплексных защитных систем, использующих большинство упомянутых типов защиты информации для защиты данных, защиты программ и самозащиты от вторжений, копирования, модификации и уничтожения.

Лабораторная работа 2
ШИФР ПЛЕЙФЕРА.

1. **Цель работы**: реализовать шифр Плейфера на языке программирования Python.
2. **Задачи работы:**
   - Изучить принципы работы шифра Плейфера.
   - Написать программу для шифрования и дешифрования текста с использованием шифра Плейфера.
   - Протестировать работу программы на нескольких примерах.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.
-

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание и порядок выполнения работы:

- Создать матрицу 5x5, содержащую все буквы английского алфавита, кроме буквы J.
- Написать функцию, которая принимает на вход текст для шифрования и матрицу Плейфера, и возвращает зашифрованный текст.
- Написать функцию, которая принимает на вход зашифрованный текст и матрицу Плейфера, и возвращает исходный текст.
- Протестировать шифр Плейфера на нескольких примерах.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;
   7. ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
   1. Что такое Шифр Плейфера?

2. Какую матрицу использует Шифр Плейфера?
3. Алгоритм шифрования в шифре Плейфера.

Приложение 1

Краткие сведения из теории

Шифр Плейфера - ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 году Чарльзом Уитстоном. Шифр предусматривает шифрование пар символов (биграмм), вместо одиночных символов, как в шифре подстановки и в более сложных системах шифрования Виженера. Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26x26=676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Шифр Плейфера использует матрицу 5x5 (для латинского алфавита, для русского алфавита необходимо увеличить размер матрицы до 6x6), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ "Q", чтобы уменьшить алфавит, в других версиях "I" и "J" объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом составляет матрицу 5x5 и является ключом шифра.

Для того, чтобы зашифровать сообщение необходимо разбить его на биграммы (группы из двух символов), например « Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем руководствуясь следующими 4 правилами зашифровываем пары символов исходного текста:

Если два символа биграммы совпадают, добавляем после первого символа «X», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «X» используется «Q».

Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «X» (или «Q») , если они не несут смысла в исходном сообщении.

Лабораторная работа 3
РОССИЙСКИЙ СТАНДАРТ ХЭШ-ФУНКЦИИ ГОСТ Р 34.11-94

1. **Цель работы**: изучение основных принципов функционирования хеш-функций и особенностей российского стандарта хеш-функции ГОСТ Р 34.11-94.

2. **Задачи работы:**
   - Изучение основных понятий и определений в области криптографии.
   - Ознакомление с основными свойствами и характеристиками хэш-функций.
   - Изучение основных положений и требований, предъявляемых к хэш-функциям по ГОСТ Р 34.11-94.
   - Анализ структуры и особенностей алгоритма хэширования, описанного в стандарте ГОСТ Р 34.11-94.
   - Изучение основных методов атак на хэш-функции и анализ устойчивости ГОСТ Р 34.11-94 к различным атакам.
   - Ознакомление с примерами использования хэш-функции ГОСТ Р 34.11-94 в различных областях применения, таких как электронная подпись, защита информации и т.д.
   - Проведение практических экспериментов по использованию хэш-функции ГОСТ Р 34.11-94 и анализ полученных результатов.

Студент должен:
Иметь практический опыт:
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

4. **Задание**
   Провести сравнение ГОСТ Р 34.11-94 и ГОСТ 34.311-95. Результаты представить в виде доклада.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;
   7. ответы на контрольные вопросы.

Лабораторная работа 4
КРИПТОСИСТЕМА RSA

1. **Цель работы**: изучить криптосистему RSA и реализовать алгоритм шифрования и расшифрования сообщений.
2. **Задачи работы:**
   - Изучить теоретические основы криптосистемы RSA.
   - Написать программу на выбранном языке программирования, реализующую алгоритм генерации ключей.
   - Написать программу, реализующую алгоритм шифрования сообщения.
   - Написать программу, реализующую алгоритм расшифрования сообщения.
   - Проверить корректность работы программы на тестовых данных.
   - Оценить стойкость криптосистемы RSA.

Студент должен:
Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Используя ключ {3,11}зашифровать слова:

1. Текст
2. Шифр
3. Ответ
4. Корреляция
5. Информация

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. ход выполнения работ;
   5. выводы по работе;
   6. ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
   1. Какие бывают методы шифрования?
   2. Какие ключи используются в RSA?
   3. Назовите алгоритм шифрования RSA.

Приложение 1

Краткие сведения из теории

В зависимости от структуры используемых ключей методы шифрования подразделяются на

- симметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации — ключа, одинакового для отправителя и получателя сообщения; Примеры: DES, 3DES, AES, Blowfish, Twofish, ГОСТ 28147-89
- асимметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, и, возможно открытый ключ, но неизвестен закрытый ключ, известный только получателю. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), а так же SSH, PGP, S/MIME и т. д. Российский стандарт, использующий асимметричное шифрование - ГОСТ Р 34.10-2001.

На данный момент асимметричное шифрование на основе открытого ключа RSA (расшифровывается, как Rivest, Shamir and Aldeman - создатели алгоритма) использует большинство продуктов на рынке информационной безопасности.

Его криптостойкость основывается на сложности разложения на множители больших чисел, а именно - на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа. Наиболее криптостойкие системы используют 1024-битовые и большие числа.

Рассмотрим алгоритм RSA с практической точки зрения.

Для начала необходимо сгенерировать открытый и секретные ключи:

Возьмем два больших простых числа p and q.

Определим n, как результат умножения p on q (n= p*q).

Выберем случайное число, которое назовем d. Это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме 1) с результатом умножения (p-1)*(q-1).

Определим такое число e, для которого является истинным следующее соотношение (e*d) mod ((p-1)*(q-1))=1.

Назовем открытым ключем числа e и n, а секретным - d и n.

Для того, чтобы зашифровать данные по открытому ключу {e,n}, необходимо следующее:

разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа M(i)=0,1,2..., n-1(т.е. только до n-1).

зашифровать текст, рассматриваемый как последовательность чисел M(i) по формуле C(i)=(M(I)^e)mod n.

Чтобы расшифровать эти данные, используя секретный ключ {d,n}, необходимо выполнить следующие вычисления: M(i) = (C(i)^d) mod n. В результате будет получено множество чисел M(i), которые представляют собой исходный текст.

Следующий пример наглядно демонстрирует алгоритм шифрования RSA:

Зашифруем и расшифруем сообщение "CAB" по алгоритму RSA. Для простоты возьмем небольшие числа - это сократит наши расчеты.

Выберем p=3 and q=11.

Определим n= 3*11=33.

Найдем (p-1)*(q-1)=20. Следовательно, d будет равно, например, 3: (d=3).

Выберем число e по следующей формуле: (e*3) mod 20=1. Значит e будет равно, например, 7: (e=7).

Представим шифруемое сообщение как последовательность чисел в диапозоне от 0 до 32 (незабывайте, что кончается на n-1). Буква A =1, B=2, C=3.

Теперь зашифруем сообщение, используя открытый ключ {7,33}
C1 = (3^7) mod 33 = 2187 mod 33 = 9;
C2 = (1^7) mod 33 = 1 mod 33 = 1;
C3 = (2^7) mod 33 = 128 mod 33 = 29;
Теперь расшифруем данные, используя закрытый ключ {3,33}.
M1=(9^3) mod 33 =729 mod 33 = 3(C);
M2=(1^3) mod 33 =1 mod 33 = 1(A);
M3=(29^3) mod 33 = 24389 mod 33 = 2(B);

Лабораторная работа 5
ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

1. **Цель работы**: изучить принцип формирования и способы использования электронной цифровой подписи.

2. **Задачи работы:**
   - Создание ключевой пары для электронной цифровой подписи с использованием инструментов, таких как OpenSSL или GPG.
   - Создание электронной цифровой подписи для файла или сообщения с использованием созданной ключевой пары.
   - Проверка электронной цифровой подписи для убеждения в том, что подпись была создана с использованием правильного ключа и что подписываемое содержимое не было изменено после создания подписи.
   - Изучение и понимание протоколов, используемых для обмена подписанными сообщениями или документами.
   - Оценка преимуществ и ограничений электронной цифровой подписи по сравнению с другими методами аутентификации и защиты информации.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.
Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   - создать электронную подпись для текстового файла с использованием инструментов GPG или OpenSSL, проверить этой подписи

- создать подпись для сообщения, отправленного по электронной почте, и проверить ее с помощью открытого ключа получателя

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое ЭЦП?
2. Назовите этапы подписания документа.
3. Перечислите виды ЭП.

Приложение 1

Краткие сведения из теории

Электронная цифровая подпись — это устройство со сложной технической составляющей.

Электронная подпись состоит из двух основных частей:

Открытый ключ, он же сертификат.

Закрытый ключ — криптографическая часть.

Эти составные части выполняют разные функции: с помощью закрытого ключа, доступного только владельцу, документ шифруется, а с помощью сертификата, доступного для всех, документ дешифруется. Таким образом, достигается цель использования ЭЦП — подтверждается то, кем был подписан документ, и заверяется его неизменность с момента подписания.

Закрытый ключ не содержит в себе ничего, кроме механизма, с помощью которого он может шифровать документы. Сертификат же несёт в себе такую полезную информацию, как сведения о владельце, сведения об удостоверяющем центре, срок действия цифровой электронной подписи и т.д. Сертификат выступает в роли главного носителя информации о ЭЦП.

С ЭЦП не получится работать сразу. Чтобы шифровать и подписывать документы, недостаточно только иметь сертификат и закрытый ключ, для работы нужно устанавливать специальные программы. С помощью этих программ, которые работают по определённому стандарту шифрования (в России — ГОСТ 34.10-2018), обеспечивается связь закрытого и открытого ключа с документами.

Электронная подпись работает по асимметричному принципу шифрования. То есть документ зашифровывается с помощью закрытого ключа, а расшифровывается с помощью открытого.

Подписание документа производится в несколько этапов:

1. Хеш документа шифруется с помощью закрытого ключа.
2. Полученная подпись добавляется к документу.
3. К документу прикрепляется сертификат проверки.

Так как сертификаты, выдаваемые удостоверяющим центром, тоже подписываются с помощью электронной подписи, подменить сертификат невозможно. На сайте удостоверяющего центра, как правило, можно скачать открытый ключ проверки, хеш которого должен совпадать с хешем открытого ключа владельца. Таким образом доказывается его достоверность.

Существует три вида ЭП, которые используют для различных ситуаций. Рассмотрим, какой может быть электронная подпись, понятие, виды и применение.

Простая электронная подпись (ПЭП) — представляет из себя логин и пароль. Используется для авторизации и аутентификации пользователя в интернете или различных автоматизированных сервисах;

Неквалифицированная электронная подпись (НЭП) — подойдёт для внутреннего и партнёрского электронного документооборота. Чтобы работать с контрагентами, потребуется заключить дополнительное соглашение;

Квалифицированная электронная подпись (КЭП) — равнозначна рукописной, придаёт документам юридическую значимость, имеет высокую степень защиты информации. Для создания цифровой подписи используются средства криптографической защиты, которые соответствуют требованиям законодательства. Технические характеристики КЭП регулирует государство. Данный вид подписи подходит для сдачи электронной отчётности в государственные органы, участия в закупках по 223-ФЗ и 44-ФЗ и ЭДО с контрагентами без дополнительных соглашений.

Система подписания документов с помощью электронной подписи выглядит следующим образом:

1. Электронная подпись присоединяется не к цифровому документу. ЭП ставится на его сжатую версию — хэш. Таким образом, сокращается время шифрования, так как хэш файла весит меньше, чем сам файл.
2. Для создания хэша применяются криптографические хэш-функции. При данном способе объёмный текст файла не делится на отдельные модули и сохраняет свой порядок.
3. После создания хэша, закрытый ключ его шифрует и передаёт получателю вместе с сертификатом электронной подписи.
4. Открытый ключ ЭП адресата расшифровывает информацию и проверяет подлинность сертификата отправителя.

Лабораторная работа 6
РАЗРАБОТКА СХЕМЫ ПРОСТОГО ПАРОЛЯ

1. **Цель работы**: разработать схему простого пароля для защиты доступа к информации.
2. **Задачи работы:**
   - Изучить основы защиты информации и принципы работы с паролями.
   - Определить требования к паролю, которые будут использоваться в разработанной схеме.
   - Разработать схему простого пароля, учитывая требования к нему.
   - Протестировать разработанную схему на соответствие требованиям и эффективность защиты информации.
   - Подготовить отчет о выполненной работе.

Студент должен:
Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.
Подготовить бланк отчета

4. **Задание и порядок выполнения работы**

Разработать схему простого пароля для защиты доступа к компьютеру. Требования к паролю: длина не менее 8 символов, использование букв верхнего и нижнего регистра, цифр и специальных символов (например, !, @, #, $). Пароль должен быть легко запоминаемым для пользователя, но сложным для подбора. Проверить эффективность защиты информации при использовании разработанного пароля.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Лабораторная работа 7
РАЗРАБОТКА СХЕМЫ ДИНАМИЧЕСКОГО ПАРОЛЯ

1. **Цель работы**: изучение принципов и процесса разработки схемы динамического пароля, который позволяет повысить уровень безопасности доступа к защищенным ресурсам.
2. **Задачи работы:**
   - Изучение основных принципов динамического пароля.
   - Изучение существующих методов разработки динамического пароля.
   - Разработка собственной схемы динамического пароля.
   - Оценка безопасности разработанной схемы динамического пароля.
   - Тестирование разработанной схемы на прочность и эффективность.

Студент должен:
Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- возможные угрозы безопасности информации в ИТКС;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.
Подготовить бланк отчета

4. **Задание и порядок выполнения работы:**
   - Написать программу на любом языке программирования (например, Python), которая будет генерировать динамический пароль по разработанному алгоритму.
   - Реализовать интерфейс для программы, который будет позволять пользователю задавать параметры генерации пароля, например, длину пароля или возможность использования специальных символов.
   - Добавить в программу возможность сохранения сгенерированного пароля в зашифрованном виде с помощью алгоритма шифрования, например, AES.
   - Реализовать проверку правильности введенного пользователем пароля с использованием хэш-функции, например, SHA-256.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое АМ?
2. Какая основная характеристика АМ?
3. Что такое Глубина модуляции?

Лабораторная работа 8
СЕРТИФИКАТЫ ОТКРЫТОГО КЛЮЧА

1. **Цель работы**: Практическое применение знаний о сертификатах открытого ключа
2. **Задачи работы:**
   - Создать самоподписанный сертификат.
   - Установить созданный сертификат на сервер или на локальный компьютер.
   - Проверить установку сертификата.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета

4. **Задание**

Создание самоподписанного сертификата и его установка

5. **Порядок выполнения работы**

1. Открыть программу генерации сертификатов (например, OpenSSL).
2. Создать закрытый ключ, используя команду genrsa. Указать длину ключа, например, 2048 бит.
3. Создать запрос на сертификат, используя команду req. Указать информацию о субъекте сертификата (имя, организацию и т.д.).
4. Сгенерировать самоподписанный сертификат, используя команду x509. Указать даты действия сертификата и расширения (если нужно).
5. Установить созданный сертификат на сервер или на локальный компьютер. Для этого:
   - Сохранить закрытый ключ и сертификат в отдельных файлах.
   - Если это сервер, установить сертификат веб-сервером.
   - Если это локальный компьютер, установить сертификат в хранилище сертификатов операционной системы.
6. Проверить установку сертификата, перейдя по адресу, защищенному сертификатом,

в браузере. Браузер должен показать, что соединение защищено сертификатом.

Примечания:

- Вместо OpenSSL можно использовать другие программы для генерации сертификатов.
- Установка сертификата может отличаться в зависимости от операционной системы и типа веб-сервера.
- В зависимости от цели задания, можно расширить его, например, создав несколько сертификатов и сравнивая их.

6. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

Лабораторная работа 9
НАСТРОЙКА И АДМИНИСТРИРОВАНИЕ ТОКЕНА

1. **Цель работы**: обеспечение безопасности при работе с информационными системами
2. **Задачи работы:**
   - обеспечения, настройка сетевых параметров и т.д.
   - Администрирование токена: управление пользователями, установка прав доступа, управление ключами и сертификатами, отслеживание использования токена.
   - Обеспечение безопасности: проверка подлинности пользователей, шифрование данных, контроль доступа и т.д.

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета

4. Порядок выполнения работы

1. Запустите программу КриптоПро CSP: (Пуск - Настройка - Панель управления - КриптоПро CSP или Пуск - Панель управления - КриптоПро CSP)
2. Для установки сертификата нажмите кнопку «Свойства»
3. Во вкладке «Общее» нажмите кнопку «Установить сертификат...»
4. Для подтверждения установки нажмите кнопку «Далее»

5. В окне «Хранилище сертификатов» выберите режим «Поместить сертификаты в следующие хранилище», нажмите кнопку «Обзор»
6. Затем выделите хранилище Личное (Личные) и нажмите кнопку «Ок»
7. После того, как в поле «Хранилище сертификатов» появится имя хранилища, нажмите кнопку «Далее», а затем «Готово»
8. Затем откроется окно «Импорт успешно выполнен» - это означает, что сертификат успешно установлен
9. Для завершения установки нажмите кнопки «Ок» - «Готово» - «Ок».

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Как понять, что сертификат в КриптоПро CSP успешно установлен?
2. Вопрос 2.
3. Вопрос 3.

Приложение 1

Краткие сведения из теории

сформулировать краткие теоретические понятия

Лабораторная работа 10
НАСТРОЙКА СЕРВИСОВ РУТОКЕН

1. **Цель работы**: научиться устанавливать и настраивать сервисы рутокен.

2. **Задачи работы:**

- установить и настроить сервисы рутокен.

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета

4. **Задание**

1. Скачайте актуальную версию драйверов.
2. Запустите программу установки и нажмите «Установить»
3. В окне с запросом на разрешение вносить изменения на компьютере нажмите Да. В результате запустится процесс установки.
4. Дождитесь завершения этого процесса и нажмите Закрыть.
5. Подключите Рутокен к компьютеру.
6. Запустите Панель управления Рутокен.
7. На вкладке Администрирование в раскрывающемся списке Подключенные Рутокен должно отображаться название подключенного устройства.
8. Если название устройства не отображается, то переподключите его.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое «Рутокен»?
2. Для чего используется Рутокен VPN?
3. На чем основывается Рутокен для Windows?

Приложение 1

Краткие сведения из теории

Рутокен — это вид ключевого носителя (токена). Он хранит электронную подпись и цифровой сертификат. В отличие от флешки, на токенах данные защищены паролем и дополнительными средствами безопасности. Рутокены имеют сертификацию ФСТЭК/ФСБ, что соответствует требованиям 63-ФЗ.

Устройства предназначены для использования ключа электронной подписи и ключа проверки электронной подписи. Разработаны на базе криптографических алгоритмов электронной подписи, а также имеют сертификацию ФСБ и ФСТЭК России. Все смарт-карты и токены Рутокен могут дополняться RFID-метками.

Рутокен VPN

Решение для безопасного удалённого доступа. Является комплексной разработкой для доступа к корпоративным ИТ-системам из любой точки мира, предназначенная для компаний малого и среднего бизнеса. Решение базируется на закрытых ключах, хранимых на борту USB-токена, благодаря чему обеспечивается безопасность при удалённой работе с файлами, почтой и программами 1С. В устройстве реализовано стойкое шифрование трафика. Для построения VPN-канала используются криптографические алгоритмы RSA 2048 и AES 256, а все важные операции выполняются «на борту» токенов.

Рутокен для Windows

Позволяет за короткий срок внедрить аппаратную аутентификацию пользователей и защиту электронной переписки в сетях на базе Microsoft Windows Server. Решение построено на применении встроенных инструментов безопасности Windows и устройств Рутокен в качестве носителей ключевой информации. Основа продукта — подробная документация по настройке продуктов Microsoft и применению в них шифрования и электронной подписи.