


ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»



УТВЕРЖДАЮ

Заместитель директора по УМР

 Е.Ю. Кузнецов

« 26 » июня 20 20 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ
ПО ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ
СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ
СРЕДСТВАМИ

по специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 4

« 25 » июня 20 20 г.

Председатель ПЦК  /Л.И.Логинова/

Разработчики: Пекунов Андрей Ананьевич, преподаватель, доцент кафедры ИВС ФГБОУ ВО «Поволжский государственный технологический университет»; Глозштейн Даниил Александрович, преподаватель первой квалификационной категории Высшего колледжа «Политехник».

Методические рекомендации предназначены для обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и направлены на оказание практической помощи при выполнении внеаудиторной самостоятельной работы по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ
2. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
3. ТЕМАТИКА И СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ
4. КОНТРОЛЬ САМОСТОЯТЕЛЬНОЙ РАБОТЫ И КРИТЕРИИ ЕЕ ОЦЕНКИ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. ВВЕДЕНИЕ

Самостоятельная работа является основным средством овладения обучающимися учебного материала в свободное от аудиторных учебных занятий время, средством углубления и упрочения знаний, полученных на лекциях, а также инструментом формирования навыков самостоятельного поиска дополнительных знаний. Как вид деятельности самостоятельная работа является неотъемлемой составляющей процесса изучения учебной дисциплины. Этот вид работы осуществляется при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа обучающегося заключается в индивидуальном, распределенном во времени выполнении комплекса заданий при консультативно-координирующей помощи преподавателя, ориентированной на самоорганизацию деятельности обучающихся.

Цель самостоятельной работы обучающихся заключается в овладении знаниями, профессиональными умениями и навыками деятельности по специальности.

Задачи организации самостоятельной работы с обучающимися:

- формирование и развитие способности самостоятельно работать и принимать решения;
- мотивация к самообразованию;
- развитие способности планировать и распределять свое время;
- развитие умения обрабатывать и анализировать информацию из разных источников;
- стимулирование к творческим видам деятельности;
- повышение уровня мотивации студентов и ответственности за качество освоения образовательной программы.

Самостоятельная работа обучающихся осуществляется в следующих формах:

- работа с литературными источниками;
- работа с информационными базами;
- работа в сети Internet (поиск и обработка необходимой информации, работа со специализированными сайтами);
- подготовка обзоров по теме занятия.

Самостоятельная работа заключается в самостоятельном изучении части учебного материала по определенным темам (вопросам) и в установленных объемах часов.

2. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания направлены на организацию и реализацию самостоятельной работы по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Основной задачей самостоятельной работы по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами является развитие общих компетенций, умений приобретать знания, умения и навыки путем индивидуальной работы, формирование активного интереса к творческому самостоятельному подходу в учебной и практической работе.

Самостоятельная работа складывается из изучения учебной и специальной литературы, как основной, так и дополнительной, нормативного материала, конспектирования источников, подготовки устных и письменных сообщений, решения задач.

Методические рекомендации по выполнению самостоятельной внеаудиторной работы разработаны в соответствии с рабочей программой ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

При выполнении самостоятельной работы у обучающихся формируются следующие компетенции:

- ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
- ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
- ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
- ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
- ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
- ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
- ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
- ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
- ОК 09. Использовать информационные технологии в профессиональной деятельности.
- ОК 10. Пользоваться профессиональной документацией на государственном

и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

При выполнении самостоятельной работы обучающийся должен уметь:

- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

- применять программные и программно-аппаратные средства для защиты информации в базах данных;

- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

- применять математический аппарат для выполнения криптографических преобразований;

- использовать типовые программные криптографические средства, в том числе электронную подпись;

- применять средства гарантированного уничтожения информации;

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

3. ТЕМАТИКА И СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

МДК.02.01. Программные и программно-аппаратные средства защиты информации.

| № п/п | Самостоятельная работа обучающихся | Количество часов |
|-------|---|------------------|
| 1 | Изучение новых технологий хранения информации | 5 |
| 2 | Статистика и анализ крупных утечек информации за год | 5 |
| 3 | Поиск информации о новых видах атак на информационную систему | 5 |
| 4 | Обзор современных программных и программно-аппаратных средств защиты | 5 |
| 5 | Сравнительный анализ современных программных и программно-аппаратных средств защиты | 8 |
| Итого | | 28 |

Самостоятельная работа № 1

Тема: Изучение новых технологий хранения информации.

Цель: ознакомиться с современными способами хранения информации.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 5

Порядок работы:

Задание 1. Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?

Задание 2. Изучить технологический процесс обработки информации. Перечислить и охарактеризовать технологические процессы процесса обработки информации. В чем заключается различие между централизованным и децентрализованным способами обработки информации? Какие режимы обработки информации вам известны?

Задание 3. Изучить технологии передачи и представления информации. Описать, как происходит передача данных.

Задание 4. Опишите облачные технологии хранения информации. Выберите один из популярных облачных сервисов и составьте онтологию работы его информационной системы.

Самостоятельная работа № 2

Тема: Статистика и анализ крупных утечек информации за год.

Цель: Исследовать масштаб и тематическое распределение крупных утечек информации.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 5

Порядок работы:

Задание 1. Соберите информацию из открытых источников о 20 крупнейших утечках информации за последние три года.

Задание 2. Классифицируйте утечки по предметной области атаки, ценности, типу активов, используемой уязвимости, нанесенному ущербу.

Задание 3. Соберите информацию о затратах на информационную безопасность за год в представленных предметных областях. Сделайте вывод о целесообразности затрат на информационную безопасность.

Самостоятельная работа № 3

Тема: Поиск информации о новых видах атак на информационную систему.

Цель: Изучить новые виды атак и способы их обнаружения.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

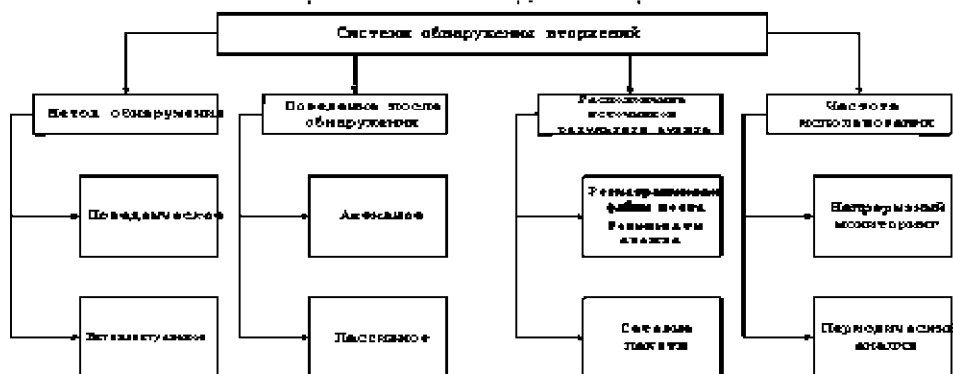
Количество часов: 5

Порядок работы:

Задание 1. Опишите один из методов обнаружения вторжений:

- сигнатурный анализ;
- использование статистики Байеса;
- продукционные (экспертные) системы;
- анализ перехода системы из состояния в состояние и сети Петри;
- статистический анализ;
- относительная частота последовательностей;
- модель среднего значения и среднеквадратичного отклонения;
- операционная модель;
- модель временных серий.

Задание 2. Поясните классификацию систем обнаружения вторжений.



Задание 3. Проанализируйте открытые источники информации и выявите сетевые атаки, появившиеся за последние три года.

Задание 4. Приведите примеры систем обнаружения вторжений. Охарактеризуйте одну из систем обнаружения вторжений.

Самостоятельная работа № 4

Тема: Обзор современных программных и программно-аппаратных средств защиты.

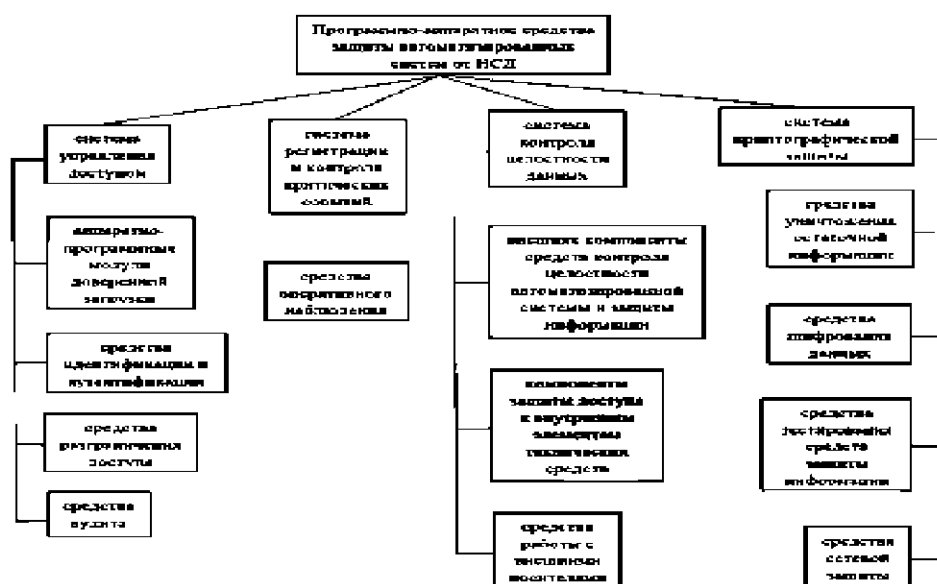
Цель: ознакомиться с современными программными и программно-аппаратными средствами защиты от НСД.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 5

Порядок работы:

Задание 1. Охарактеризуйте программно-аппаратные средства защиты автоматизированных систем от НСД.



Задание 2. В качестве примеров отдельных программ, повышающих защищенность от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др. Опишите одно из программных средств, повышающих защищенность от НСД.

Самостоятельная работа № 5

Тема: Сравнительный анализ современных программных и программно-аппаратных средств защиты.

Цель: Изучить технико-экономические характеристики современных программных и программно-аппаратных средств защиты информации.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 8

Порядок работы:

Задание 1. Выполните анализ существующих российских программных и программно-аппаратных средств защиты. Опишите 3 из них.

Задание 2. Выполните анализ существующих зарубежных программных и программно-аппаратных средств защиты. Опишите 3 из них.

Задание 3. Составьте сравнительную характеристику вышеописанных средств защиты по основным техническим и экономическим характеристикам в форме таблицы.

МДК.02.02. Криптографические средства защиты информации

| № п/п | Самостоятельная работа обучающихся | Количество часов |
|-------|--|------------------|
| 1 | История развития криптографии | 2 |
| 2 | Программная реализация классических шифров | 4 |
| 3 | Оптимизация методов частотного анализа моноалфавитных шифров. | 2 |
| 4 | Методы механизации шифрования | 4 |
| 5 | Цифровое представление различных форм информации | 4 |
| 6 | Анализ современных симметричных криптоалгоритмов | 2 |
| 7 | Анализ современных асимметричных криптоалгоритмов | 2 |
| 8 | Программная реализация современных криптоалгоритмов | 2 |
| 9 | Сравнительный анализ функций хеширования | 2 |
| 10 | Аутентификация сообщений | 2 |
| 11 | Законодательство в области криптографической защиты информации | 4 |
| 12 | Перспективные направления криптографии | 2 |
| Итого | | 32 |

Самостоятельная работа № 1

Тема: История развития криптографии.

Цель: изучить основные вехи становления криптографии как отдельной сферы прикладных наук.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание 1: Изучите начальный этап развития криптографии. Опишите квадрат Полибия, шифр Цезаря, шифр Тритемия, шифр Виженера.

Задание 2: Изучите этап "черных кабинетов". Опишите блочное шифрование Джефферсона, гаммирование, криптопреобразования при помощи электрического тока ("Энигма").

Задание 3: Изучите доклад К. Шеннона "Математическая теория криптографии". Перечислите основные инновационные концепции в этой работе.

Задание 4: Изучите новейший этап развития криптографии. Изложите основные концепции стандарта DES, RSA шифрсистемы, ГОСТ 28147-89.

Самостоятельная работа № 2

Тема: Программная реализация классических шифров.

Цель: изучение способов кодирования информации.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 4

Порядок работы:

Вариант 1

В Средние века для шифрования перестановкой применялись и магические квадраты. Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток.

Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила.

Пример магического квадрата и его заполнения сообщением «Прилетаю восьмого» показан ниже (рисунок 3).

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид ОИРМ ЕОСЮ ВТАЬ ЛГОП.

| | | | |
|----|----|----|----|
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

| | | | |
|---|---|---|---|
| О | И | Р | М |
| Е | О | С | Ю |
| В | Т | А | Ь |
| Л | Г | О | П |

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3×3 (если не учитывать его повороты). Количество магических квадратов 4×4 составляет уже 880, а количество магических квадратов 5×5 – около 250000.

Пользуясь изложенным способом создать программу, которая:

а) зашифрует введенный текст и сохранит его в файл;

б) считает зашифрованный текст из файла и расшифрует данный текст.

Вариант 2

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рисунке. Если считать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее: ТЮАЕ ООГМ РЛИП ОБСВ.

| | | | | |
|---|---|---|---|---|
| | 4 | 1 | 3 | 2 |
| 3 | П | Р | И | Л |
| 1 | Е | Т | А | Ю |
| 4 | В | О | С | Ь |
| 2 | М | О | Г | М |

Исходная
таблица

| | | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 3 | Р | Л | И | П |
| 1 | Т | Ю | А | Е |
| 4 | О | Ь | С | В |
| 2 | О | О | Г | М |

Перестановка
столбцов

| | | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 1 | Т | Ю | А | Е |
| 2 | О | О | Г | М |
| 3 | Р | Л | И | П |
| 4 | О | Ь | С | В |

Перестановка
строк

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

- для таблицы 3×3 – 36 вариантов;
- для таблицы 4×4 – 576 вариантов;
- для таблицы 5×5 – 14400 вариантов.

Пользуясь изложенным способом создать программу, которая:

- а) зашифрует введенный текст и сохранит его в файл;
- б) считает зашифрованный текст из файла и расшифрует данный текст.

Самостоятельная работа № 3

Тема: Оптимизация методов частотного анализа моноалфавитных шифров.

Цель: Используя частотный анализ, дешифровать криптограмму зашифрованную методом моноалфавитных подстановок.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание: Ознакомиться с теоретическим материалом. Для дешифровки криптограммы, зашифрованной моноалфавитной подстановкой, необходимо

произвести замену символов. Учесть, что замена символов производится в соответствии с значениями частот букв русского языка, а также частоты встречаемости символов для данной криптограммы.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Введение

Шифр моноалфавитной подстановки - это один из самых древних шифров. Частным случаем этого шифра для закрытия секретных сообщений пользовался еще Гай Юлий Цезарь. Данная лабораторная работа посвящена изучению криптоанализа моноалфавитных подстановок.

Рассмотрим, как используют этот шифр. Прежде всего, выбирается нормативный алфавит, т.е. набор символов, которые будут использоваться при составлении сообщений, требующих зашифровки. Допустим, это будут прописные буквы русского алфавита (исключая буквы “Ё” и “Ъ”) и пробел. Таким образом, наш нормативный алфавит состоит из 32 символов. Затем выбирается алфавит шифрования и устанавливается взаимно однозначное соответствие между символами нормативного алфавита и символами алфавита шифрования. Алфавит шифрования может состоять из произвольных символов, в том числе и из символов нормативного алфавита. Чтобы зашифровать исходное сообщение, необходимо каждый символ открытого текста заменить соответствующим ему символом алфавита шифрования (таблица 1).

Таблица 1 – Соответствие символов исходного и шифрующего алфавитов

| | | | | | | | | | |
|---------------------|---|---|---|---|---|---|---|---|------|
| Нормативный алфавит | А | Б | В | Г | Д | Е | Ж | З | |
| Алфавит шифрования | И | К | А | Л | Э | Т | П | И | |

Зашифруем, например, слово “звезда”. Если использовать алфавиты, приведенные в таблице 1, то получится следующее (таблица 2):

Таблица 2. Пример шифрования

| | | | | | | |
|--------------------|---|---|---|---|---|---|
| Исходное сообщение | З | В | Е | З | Д | А |
| Шифрованный текст | И | А | Т | И | Э | Н |

Метод моноалфавитной подстановки можно представить как числовые преобразования символов исходного текста. Для этого каждой букве нормативного алфавита ставится в соответствие некоторое число, называемое числовым эквивалентом этой буквы. Например, для букв русского алфавита и пробела это выглядит так, как показано в таблице 3. Моноалфавитные подстановки можно описать выражением:

Таблица 3 – Числовые эквиваленты

| | | | | | | | | | | | | | | | | |
|----------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-----|
| Нормативный алфавит | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П |
| Числовые эквиваленты | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Нормативный алфавит | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ы | Ь | Э | Ю | Я | “_” |
| Числовые эквиваленты | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

где E_i , M_i - числовые эквиваленты символов алфавита шифрования и нормативного алфавита соответственно, S_i - коэффициент сдвига, L - мощность алфавита.

Шифр Цезаря

Простейшим примером моноалфавитных подстановок является шифр Цезаря. В этом шифре каждый символ открытого текста заменяется третьим после него символом в алфавите, замкнутом в кольцо, т.е. после пробела следует буква “А”. Таким образом, шифр Цезаря описывается так:

где S - коэффициент сдвига, одинаковый для всех символов. Цезарь использовал величину сдвига $S=3$, но, конечно, можно использовать любое целое S : $1 \leq S \leq (L-1)$. Зашифруем, например, текст “ШИФР_ЦЕЗАРЯ”, используя коэффициент сдвига $S=2$ (Таблица 4).

Таблица 4 – Пример шифрования

| | | | | | | | | | | | |
|-------------------|---|---|---|---|---|---|---|---|---|---|---|
| Открытый текст | Ш | И | Ф | Р | _ | Ц | Е | З | А | Р | Я |
| Шифрованный текст | Ы | К | Ц | Т | Б | Ш | З | Й | В | Т | А |

Частотный анализ

Все естественные языки имеют характерное частотное распределение символов. Например, буква “О” - встречается в русском языке чаще других, а буква “Ф” - самая редкая (см. таблицу 5).

Таблица 5 – Частотные характеристики символов

| Символ | Вероятность | Символ | Вероятность | Символ | Вероятность |
|--------|-------------|--------|-------------|--------|-------------|
| Пробел | 0.175 | К | 0.028 | Ч | 0.012 |
| О | 0.089 | М | 0.026 | Й | 0.010 |
| Е | 0.072 | Д | 0.025 | Х | 0.009 |
| А | 0.062 | П | 0.023 | Ж | 0.007 |
| И | 0.062 | У | 0.021 | Ю | 0.006 |
| Н | 0.053 | Я | 0.018 | Ш | 0.006 |
| Т | 0.053 | Ы | 0.016 | Ц | 0.004 |
| С | 0.045 | З | 0.016 | Щ | 0.003 |
| Р | 0.040 | Ь | 0.014 | Э | 0.003 |
| В | 0.038 | Б | 0.014 | Ф | 0.002 |
| Л | 0.035 | Г | 0.013 | | |

Моноалфавитные подстановки обладают важным свойством: они не нарушают частот появления символов, характерных для данного языка. Это позволяет криптоаналитику легко получить открытый текст при помощи частотного анализа. Для этого нужно сопоставить частоты появления символов шифра с

вероятностями появления букв используемого алфавита (в данном случае русского). После этого наиболее частые символы криптограммы заменяются наиболее вероятными символами алфавита, остальные замены производятся на основе вероятных слов и знания синтаксических правил используемого языка.

Самостоятельная работа № 4

Тема: Методы механизации шифрования.

Цель: изучить методы механизации шифрования.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 4

Порядок работы:

Задание 1. Изучите историю шифра Виженера и его разрешения. Опишите работу механизма, использовавшего эту задачу.

Задание 2. Опишите устройство и принцип работы шифровального диска.

Задание 3. Опишите устройство и принцип работы шифровальной машины "Энигма". Сравните эффективность "Энигмы" и современных алгоритмов шифрования.

Самостоятельная работа № 5

Тема: Цифровое представление различных форм информации.

Цель: изучить способы представления текстовой, графической, звуковой информации и видеоинформации.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 4

Порядок работы:

Задание 1: Изучите способы кодирования и декодирования информации.

Задание 2: Изучите способы кодирования векторных и растровых изображений.

Задание 3: Изучите способы двоичного кодирования звуковой информации.

Задание 4: Изучите устройство и принципы работы аналого-цифровых и цифро-аналоговых преобразователей.

Самостоятельная работа № 6

Тема: Анализ современных симметричных криптоалгоритмов.

Цель: ознакомиться с современными симметричными шифрами.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание 1. Представьте алгоритм работы российского стандарта шифрования ГОСТ 28147-89.

Задание 2. Представьте алгоритм работы американского стандарта шифрования DES. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES.

Задание 3. Выполнить ручное шифрование исходного текста с помощью алгоритма DES, алгоритма ГОСТ 28147-89.

Задание 4. Опишите особенности алгоритма AES. Сравните алгоритмы шифрования ГОСТ 28147-89 и AES.

Задание 5. Охарактеризуйте программы симметричного шифрования сообщений. Результаты представьте в виде таблицы.

| Программа | Характеристики |
|------------------|----------------|
| Бесплатное ПО | |
| AES Free | |
| FineCrypt | |
| Dpccrypto | |

| | |
|------------------------------------|--|
| Платное ПО | |
| EasyCrypto Deluxe | |
| Crypto-Lock | |
| Iron Key | |
| SafeGuard PrivateCrypto | |

Самостоятельная работа № 7

Тема: Анализ современных асимметричных криптоалгоритмов.

Цель: ознакомиться с асимметричными алгоритмами.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание 1. Опишите асимметричные алгоритмы шифрования.

Задание 2. Изучите процедуру создания ключей в алгоритме шифрования RSA на примере.

| № п/п | Описание операции | Пример |
|-------|--|------------------------------------|
| 1 | Выбираются два простых числа ¹ p и q . | $p=7, q=13$ |
| 2 | Вычисляется произведение $n = p \cdot q$. | $n=91$ |
| 3 | Вычисляется функция Эйлера ² $\phi(n)$. | $\phi(n)=(7-1)(13-1)=91-7-13+1=72$ |
| 4 | Выбирается открытый ключ ³ e как произвольное число ($0 < e < n$) взаимно простое ⁴ с результатом функции Эйлера ($e \perp \phi(n)$) | $e=5$ |
| 5 | Вычисляется секретный ключ ⁵ d как обратное число ⁶ e по модулю $\phi(n)$ из соотношения $(e \cdot d) \bmod \phi(n) = 1$. | $(5 \cdot d) \bmod 72 = 1, d = 29$ |
| 6 | Публикуется открытый ключ (e, n) в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике) | |

Задание 3. Создайте открытый и секретный ключи для любой другой пары простых чисел.

Задание 4. Разработать алгоритм шифрования RSA.

Самостоятельная работа № 8

Тема: Программная реализация современных криптоалгоритмов.

Цель: ознакомиться с современными алгоритмами шифрования.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание: Изучите программные реализации криптографических алгоритмов md2/4/5/6, tiger, SHA-1/2/3, Ripemd, Haval, Rijndael, MMB, BAseking, NOEKEON, DFC, DECIM, MICKEY, SC2000, RC4-5, Rabbit, Salsa20, Trivium VMPC, NUSH e2 Twofish, Wake, Shark, Serpent, Seal. Составьте их рейтинг по применимости, распространенности и эффективности.

Самостоятельная работа № 9

Тема: Сравнительный анализ функций хеширования.

Цель: ознакомиться с различными функциями хеширования.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание 1. Опишите функции хеширования.

| Тип | Описание |
|-----------------------------|----------|
| MD2 | |
| MD4 | |
| MD5 | |
| SHA (Secure Hash Algorithm) | |

Задание 2. Опишите свойства хеш-функций.

Задание 3. Ознакомьтесь с алгоритмом работы хеш-функции MD5.

Задание 4. Программно реализовать алгоритм MD4 хеширования символьной строки. Хеш-код представить в виде 16-ричного числа.

Самостоятельная работа № 10

Тема: Аутентификация сообщений.

Цель: изучить принципы работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание 1. Опишите схему протокола Kerberos.



Задание 2. Объясните механизм работы протокола Kerberos.

Задание 3. Реализация Kerberos в ОС Windows Server.

Самостоятельная работа № 11

Тема: Законодательство в области криптографической защиты информации.

Цель: изучите нормативно-правовую базу РФ в области криптографической защиты информации.

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 4

Порядок работы:

Задание 1. Изучите основные положения ФЗ-390, ФЗ-5485, ФЗ "О ФСБ", связанные с криптографической защитой информации

Задание 2. Изучите законодательство в области ЭЦП. Опишите отличие между квалифицированной и неквалифицированной цифровой подписью.

Задание 3. Составьте перечень средств и услуг в области криптографической защиты информации, представленных на отечественном рынке.

Самостоятельная работа № 12

Тема: Перспективные направления криптографии

Цель: изучить современные тенденции развития криптографии

Форма самостоятельной деятельности: работа с информационными базами; работа в сети Internet.

Количество часов: 2

Порядок работы:

Задание 1. Изучите принципы криптографии на эллиптических кривых. Опишите основные принципы генерации цифровой подписи на стандарте ECDSA

Задание 2. Изучите спецификации SHA-256, SHA-384, SHA-512.

Задание 3. Изучите способы повышения надежности современных криптографических протоколов.

4. КОНТРОЛЬ САМОСТОЯТЕЛЬНОЙ РАБОТЫ И КРИТЕРИИ ЕЕ ОЦЕНКИ

Для проверки эффективности самостоятельной работы студента необходим ее контроль. К видам контроля относится - устный опрос, письменная работа.

Устный опрос позволяет оценить знания и кругозор студента, умение логически построить ответ, проявление коммуникативных навыков. Устный опрос ориентирован на оценку знаний. Устный опрос проводится в форме собеседования.

Письменная работа предназначена для проверки выполнения заданий самостоятельной работы, проводится на практических занятиях и направлена на оценку сформированных умений.

По итогам устных опросов и проверки письменных работ выставляется оценка по следующим критериям.

Критерии оценивания результатов самостоятельной работы, шкала оценивания

Критерии оценивания:

- умение самостоятельно выполнить работу (произвести расчеты, применить интеллектуальные и исследовательские приемы)
- качество выполнения работы и содержание информационного, расчетного, наглядного материала.
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала).
- соответствие требованиям оформления письменной части

Шкала оценивания:

Результаты оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, если работа выполнена самостоятельно, произведена самооценка, продемонстрированы навыки самостоятельного использования оборудования, дидактического материала, ТСО; отличается новизной, нестандартным, творческим подходом к теме, решению задачи, оформлению; выполнена своевременно, отличается четким и грамотным выполнением в соответствии с рекомендациями преподавателя.

Оценка «хорошо» выставляется обучающемуся, если выполнение работы, самооценка, навыки самостоятельного использования оборудования, дидактического материала, ТСО происходят с посторонней помощью, исполнение работы частично соответствует рекомендациям преподавателя по оформлению, структуре, аккуратности исполнения, сдана в срок.

Оценка «удовлетворительно» выставляется обучающемуся, если в работе отсутствуют установленные рекомендациями порядок и структура работы, работа выполнена не самостоятельно, сдана с опозданием обозначенного срока, объем информации незначительный, из ограниченного числа

источников

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Баричев, С. Г. Основы современной криптографии: учебное пособие/ С. Г. Баричев, В. В. Гончаров, Р. Е. Серов— Санкт-Петербург : Лань, 2020.- 175 с.
2. Основы информационной безопасности [Текст]: учебное пособие: [по направлению подготовки "Информационные системы и технологии"] / [Ю. Ю. Громов и др.]. - Старый Оскол: ТНТ, 2017. - 381 с.: ил.
3. Мельников, В.П. Методы и средства хранения и защиты компьютерной информации [Текст]: учебник: [по направлениям "Автоматизация технологических процессов и производств", "Конструкторско-технологическое обеспечение машиностроительных производств"] / В. П. Мельников, А. Г. Схиртладзе; под ред. В. П. Мельникова. - Старый Оскол: ТНТ, 2017. - 399 с.: ил.
4. Белов, Е.Б. Организационно-правовое обеспечение информационной безопасности/ Е.Б. Белов, В. Н. Пржегорлинский. –М.: Издательский центр «Академия». 2020 - 336 с.
5. Никифоров, С. Н. Методы защиты информации. Пароли, сккрытие, шифрование [Текст : Электронный ресурс]: учебное пособие для вузов / С. Н. Никифоров. - 3-е изд., стер. - Санкт-Петербург: Лань, 2020. - 124 с. – Режим доступа: <https://e.lanbook.com/reader/book/146885/#1>
6. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс]: 2018-06-07 / С. Н. Никифоров. - 1-е изд. - [Б. м.]: Лань, 2018. - 96 с. – Режим доступа: <https://e.lanbook.com/reader/book/107306/#1>