Министерство науки и высшего образования Российской Федерации
Университетский колледж
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»

Отделение информационных технологий

Р.Н. Гилязова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах

Оренбург
2018

002.56:681 (075.32)
32.97 Я723
С16

Рецензент – кандидат педагогических наук, доцент кафедры АСОИиУ ИУРиКБ ОГАУ Панасюк К.А.

Гилязова, Р. Н.
С16 Информационная безопасность : методические указания/Р. Н. Гилязова; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2018.

Основное содержание: реализовать простейший генератор паролей, обладающий основными требованиями к парольным генераторам и стойкостью к взлому; составить программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля; составить программу шифрования методом контрольных сумм и методом хеширования с применением метода гаммирования.

Методические указания по курсу «Информационная безопасность» предназначены для обучающихся в колледжах по образовательным программам среднего профессионального образования специальности 09.02.03 Программирование в компьютерных системах.

Содержание

Введение

Дисциплина «Информационная безопасность» является вариативной частью профессионального цикла очной формы обучения по специальности 09.02.03 Программирование в компьютерных системах в 6 семестре.

В результате освоения дисциплины студент должен:

иметь представление:

- о количественной оценке стойкости парольной защиты;
- о методах парольной защиты;
- о технологии аутентификации пользователя на основе пароля;
- о технологии закрытия информации электронно-цифровой подписью и приемами хеширования;
- о методах контрольных сумм и наложения кодов – гаммирование;

знать:

- основные задачи, которые могут решаться с использованием определения стойкости пароля;
- основные требования к выбору пароля;
- определения аутентификации, идентификации в информационных системах, авторизации пользователя;
- функции электронно-цифровой подписи;
- этапы формирования электронно-цифровой подписи;
- хеш - значение документа, хеш-функциию;

уметь:

- реализовывать простейший генератор паролей, обладающий основными требованиями к парольным генераторам;
- составлять программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля;
- реализовывать простейший генератор паролей, обладающий требуемой стойкостью к взлому;
- составлять программу шифрования методом контрольных сумм;
- составлять программу шифрования методом хеширования с применением гаммирования.

Предшествующие курсы, на которых непосредственно базируется дисциплина «Информационная безопасность»:

- информационные технологии;
- теория алгоритмов;
- основы программирования;
- технические средства информатизации;

- основы объектно-ориентированного программирования.

Вместе с тем дисциплина Информационная безопасность устанавливает базовый уровень знаний для освоения междисциплинарных курсов 03.01 Технология разработки программного обеспечения, 02.02 Разработка и защита баз данных, производственных практик (по профилю специальности) по профессиональному модулю 03 Участие в интеграции программных модулей.

Курс рассчитан на 60 часов лекций, 62 часа лабораторно-практических занятий. Промежуточная оценка знаний и умений студентов проводится с помощью контрольных работ, которые включают в себя основные проблемы курса. Итоговый контроль в виде экзамена предусмотрен на третьем курсе.

1 Лабораторная работа № 1. Реализация простейшего генератора паролей

Цель работы: получение основных теоретических сведений и практических навыков по оценке стойкости парольной защиты.

1.1 Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу-генератор паролей.
3. Составить отчет по проделанной работе.
4. Защитить работу.

1.2 Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.
4. Постановка задачи.
5. Листинг программы.
6. Результат выполнения программы.

1.3 Теоретическая справка

Стойкость к взлому подсистемы парольной идентификации (аутентификации) во многом определяется тем, насколько правильно были сформированы пароли пользователей. При несоблюдении ряда требований к выбору паролей, данная стойкость в значительной степени уменьшается, и подсистема идентификации (аутентификации) становится достаточно уязвима при правильно построенной атаке.

Ниже перечислены основные требования, которые должны быть учтены при выборе пароля пользователя:

1 Минимальная длина пароля должна быть не менее 6 символов. Сокращение длины пароля во многом повышает вероятность успешной атаки полным их перебором.

2 Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.). Использование одной конкретной группы символов при формировании пароля в значительной степени повышает вероятность успешной атаки по маске.

3 В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д. Использование в качестве паролей конкретных слов, имен в значительной степени повышает вероятность успешной атаки по словарю.

Иногда, генераторы паролей могут использовать при данном генерировании элементы, входящие в идентификатор пользователя (отдельные его символы, количество символов и т.д.). В отдельных вариантах, пароль может формироваться даже целиком из идентификатора на основе некоторого алгоритма. В последнем случае, заданному идентификатору пользователя ставится в соответствие единственный пароль, который формируется на основе идентификатора.

1.4 Задание к лабораторной работе № 1

Реализовать простейший генератор паролей, обладающий основными требованиями к парольным генераторам.

Программа должна выполнять следующие действия:

1. Ввод идентификатора пользователя с клавиатуры. Данный идентификатор представляет собой последовательность символов $a_1, a_2, \ldots a_N$, где N – количество символов идентификатора (может быть любым), a_i – i-ый символ идентификатора пользователя.

2. Формирование пароля пользователя $b_1, b_2, \ldots b_M$ для данного идентификатора, где M – количество символов пароля, соответствующее Вашему варианту и вывод его на экран. Алгоритм получения символов пароля b_i указан в перечне требований для Вашего варианта (таблица 1).

Таблица 1 – Варианты заданий на лабораторную работу № 1

Вариант	M	Перечень требований
1	2	3
1	6	b_1, b_2 – случайные заглавные буквы английского алфавита; $b_3 = N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10); b_4 – случайная цифра; b_5 – случайный символ из множества {!,”,#,$,%,&,’,(,),*}; b_6 – случайная малая буква английского алфавита
2	7	b_1, b_2, b_3 – случайные малые буквы английского алфавита; b_4, b_5 – случайные заглавные буквы английского алфавита; $b_6 b_7$ – двузначное число, равное $N^4 \bmod 100$ (Если остаток – однозначное число, то $b_6 = 0$)
3	8	b_1, b_2, b_3 – случайные цифры; b_4, b_5 – случайные символы из множества {!,”,#,$,%,&,’,(,),*}; b_7 – случайная заглавная буква английского алфавита; b_8 – P-ая по счету малая буква английского алфавита, где $P = N^2 \bmod 26$
4	9	$b_1, \ldots, b_{1+Q}$ – случайные символы из множества {!, ”, #, $, %, &, ’,(,),*}, где $Q = N \bmod 5$. Оставшиеся символы пароля, кроме b_9, – случайные малые буквы английского алфавита; b_9 – случайная цифра
5	10	$b_{10-Q}, \ldots, b_{10}$ – случайные цифры, где $Q = N \bmod 6$; b_1, b_2 – случайные большие буквы английского алфавита; $b_3, \ldots b_{10-Q-1}$ – случайные малые буквы английского алфавита
6	11	b_1, b_2 – случайные цифры; $b_3, \ldots, b_{3+Q}$ – случайные большие буквы английского алфавита, где $Q = N \bmod 8$; $b_{4+Q}, \ldots, b_{11}$ – случайные символы из множества {!,”,#,$,%,&,’,(,),*}
7	11	b_1, b_2 – случайные цифры; $b_3, \ldots, b_{3+Q}$ – случайные малые буквы русского алфавита, где $Q = N \bmod 8$; $b_{4+Q}, \ldots, b_{11}$ – случайные символы из множества {!,”,#,$,%,&,’,(,),*}
8	12	$b_1, \ldots, b_{1+Q}$ – случайные малые буквы английского алфавита, где $Q = N^3 \bmod 5$; $b_{1+Q1}, \ldots b_{1+Q1+P}$ – случайные заглавные буквы английского алфавита, где $P = N^2 \bmod 6$. Оставшиеся символы пароля – случайные цифры
9	12	$b_1, \ldots, b_{1+Q}$ – случайные малые буквы русского алфавита, где $Q = N^3 \bmod 5$; $b_{1+Q1}, \ldots b_{1+Q1+P}$ – случайные заглавные буквы русского алфавита, где $P = N^2 \bmod 6$. Оставшиеся символы пароля – случайные цифры

Продолжение таблицы 1

1	2	3
10	10	$b_{10-Q},...b_{10}$ – случайные цифры, где $Q=N \bmod 5$; b_1,b_2 – случайные большие буквы русского алфавита; $b_3,...b_{10-Q-1}$ – случайные малые буквы русского алфавита
11	9	$b_1,b_2..b_{1+Q}$ – случайные символы из множества {!, ”, #, $, %, &, ’,(,), *}, где $Q=N \bmod 5$. Оставшиеся символы пароля, кроме b_9, - случайные малые буквы русского алфавита; b_9 – случайная цифра
12	8	b_1,b_2,b_3 – случайные цифры; b_4,b_5 – случайные символы из множества {!,”,#,$,%,&,’,(,),*}; b_7 – случайная заглавная буква русского алфавита; b_8 – P-ая по счету малая буква русского алфавита, где $P=N^2 \bmod 32$
13	7	b_1,b_2,b_3 – случайные малые буквы русского алфавита; b_4,b_5 – случайные заглавные буквы русского алфавита; b_6b_7 – двузначное число, равное $N^4 \bmod 100$(Если остаток – однозначное число, то $b_6 = 0$)
14	6	b_1,b_2 – случайные заглавные буквы русского алфавита; $b_3=N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10); b_4 – случайная цифра; b_5 – случайный символ из множества {!,”,#,$,%,&,’,(,),*}; b_6 – случайная малая буква русского алфавита
15	6	b_1,b_2 – случайные заглавные буквы английского алфавита; $b_3=N^2 \bmod 10$ (где mod 10 – остаток от деления числа на 10); b_4 – случайная цифра; b_5 – случайный символ из множества {!,”,#,$,%,&,’,(,),*}; b_6 – случайная малая буква русского алфавита

1.5 Пример реализации лабораторной работы

Входным параметром здесь является произвольный идентификатор. Далее, в соответствии с перечнем требований, происходит генерация пароля.

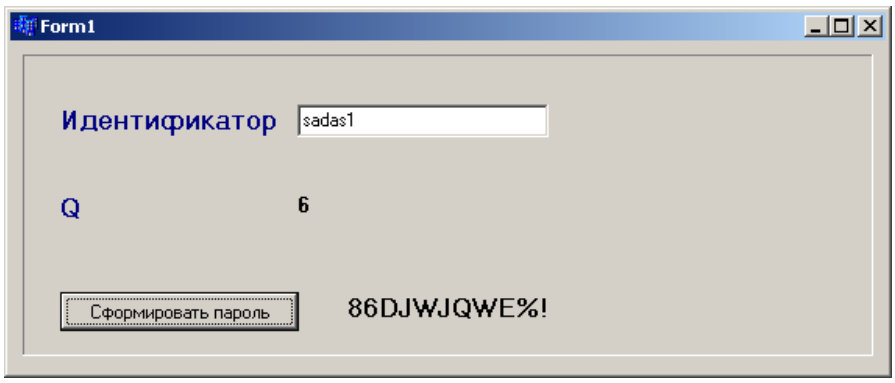

Рисунок 1 – Результат работы программы, реализующей простейший генератор паролей с заданными требованиями

1.6 Контрольные вопросы

1. Дать определение стойкости пароля к взлому. Написать формулу.
2. Дать определение мощности алфавита паролей.
3. Перечислить основные задачи, которые могут решаться с использованием определения стойкости пароля.
4. Перечислить основные требования к выбору пароля.

2 Лабораторная работа № 2. Методы парольной защиты. Разработка программной парольной защиты

Цель работы: Изучение технологии аутентификации пользователя на основе пароля.

2.1 Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля.
3. Составить отчет по проделанной работе.
4. Защитить работу.

2.2 Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.
4. Постановка задачи.
5. Листинг программы.
6. Результат выполнения программы.

2.3 Теоретическая справка

Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства, например:

- проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей;
- подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
- проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация — установление тождественности неизвестного объекта известному на основании совпадения признаков; опознание.

Идентификация в информационных системах — присвоение субъектам и объектам идентификатора и/ или сравнение идентификатора с перечнем присвоенных идентификаторов. Например, идентификация по штрихкоду.

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Аутентификацию не следует путать с авторизацией (процедурой предоставления субъекту определённых прав) идентификацией (процедурой распознавания субъекта по его идентификатору).

Авторизация – процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

2.4 Задание к лабораторной работе № 2

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля:

1. В качестве информационного ресурса использовать любой файл или приложение.
2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе.
3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.
4. Пользователь должен иметь возможность поменять пароль (таблица 2).

Таблица 2 – Варианты заданий к лабораторной работе № 2

Номер варианта	Длина пароля (количество символов)	Используемые символы	Дополнительные средства защиты
1	2	3	4
1	6	Латиница (строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов
2	7	Кириллица (строчные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)
3	8	Цифры	Применение метода аутентификации на основе одноразовых паролей: каждый следующий пароль=предыдущий пароль+5
4	5	Цифры, знаки арифметических операций	При смене пароля: проверка на отсутствие повторяющихся символов
5	8	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (храниться в системе) в формате дд.мм.гг или дд/мм/гг
6	10	Латиница (прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: при каждой следующей попытке входа в систему последняя буква пароля меняется на следующую по алфавиту
7	11	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с фамилией пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)

Продолжение таблицы 2

1	2	3	4
8	10	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (храниться в системе) в формате дд.мм.гггг или дд/мм/гггг
9	7	Цифры	Применение метода аутентификации на основе одноразовых паролей: к первой цифре каждого следующего пароля прибавляется 1
10	8	Кириллица (прописные и строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов
11	5	Латиница (строчные и прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля к нему добавляется «случайная» величина, такая же величина добавляется к паролю, который хранится в системе, после чего производится сравнение.(в качестве «случайной» величины использовать «Abc»)
12	9	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с отчеством пользователя
13	10	Цифры	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: xxxxxxxxxx
14	7	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий месяцев)
15	6	Латиница (строчные и прописные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов

Продолжение таблицы 2

1	2	3	4
16	7	Кириллица (строчные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля в его начало добавляется «случайная» величина, такая же величина добавляется к паролю, который хранится в системе, после чего производится сравнение (в качестве «случайной» величины использовать «АБВ»)
17	4	Цифры	При смене пароля: проверка на совпадение пароля с годом рождения пользователя
18	5	Цифры	Применение односторонней (хэш) функции: сложение всех цифр пароля. Такая же функция должна быть применена к паролю, который хранится в системе. Затем проводится сравнение паролей
19	9	Кириллица (строчные буквы)	Шифрование пароля (В качестве алгоритма шифрования применить метод перестановки: поменять местами первую и последнюю букву пароля). Тот же алгоритм должен быть применен к паролю, который хранится в системе. Затем проводится сравнение паролей
20	10	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с местом рождения пользователя
21	13	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: xxx-xxx-xx-xx
22	6	Латиница (строчные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий дней недели)
23	7	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя, записанным в обратном порядке

Продолжение таблицы 2

1	2	3	4
24	8	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с текущей датой в формате дд.мм.гг или дд/мм/гг
25	5	Цифры	Применение односторонней (хэш) функции: перемножение всех цифр пароля. Такая же функция должна быть применена к паролю, который хранится в системе. Затем проводится сравнение паролей
26	6	Цифры	Шифрование пароля (В качестве алгоритма шифрования применить метод замены: к каждой цифре пароля прибавить по цифре из даты рождения пользователя соответственно) Тот же алгоритм должен быть применен к паролю, который хранится в системе. Затем проводится сравнение паролей
27	10	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив из любых 10 слов, длиной в 10 символов)
28	4	Кириллица (строчные и прописные буквы)	При смене пароля: проверка на совпадение пароля с месяцем рождения пользователя
29	10	Цифры, знаки препинания	При смене пароля: проверка на совпадение пароля с текущей датой в формате дд.мм.гггг или дд/мм/гггг
30	9	Цифры	При смене пароля: проверка на отсутствие повторяющихся символов

2.5 Пример реализации лабораторной работы

Примерный интерфейс программы представлен на рисунках 2, 3, 4.

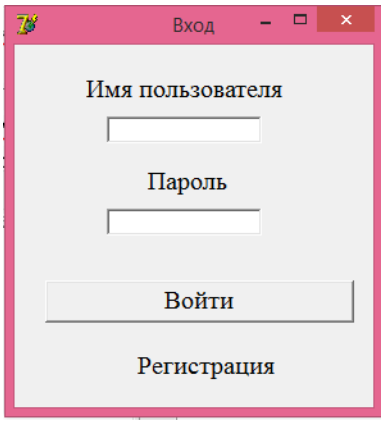

Рисунок 2 – Форма авторизации пользователя

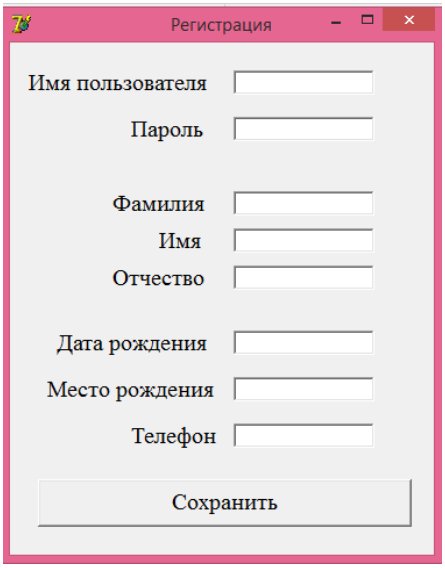

Рисунок 3 – Форма регистрации пользователя

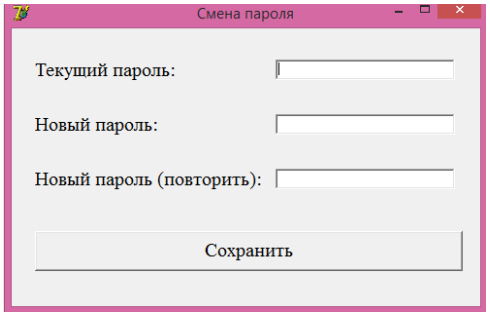

Рисунок 4 – Форма смены пароля

2.6 Контрольные вопросы

1. Дать определение аутентификации. Привести примеры.
2. Дать определение идентификации в информационных системах.
3. Дать определение авторизации пользователя.
4. Дать определение пароля.

3 Лабораторная работа № 3. Количественная оценка стойкости парольной защиты

Цель работы: получение основных теоретических сведений и практических навыков по оценке стойкости парольной защиты.

3.1 Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Реализовать простейший генератор паролей, обладающий требуемой стойкостью к взлому.
3. Составить отчет по проделанной работе.
4. Защитить работу.

3.2 Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.
4. Постановка задачи.
5. Листинг программы.
6. Результат выполнения программы.

3.3 Теоретическая справка

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то $A = 26$).

L – длина пароля.

$S = A^L$ - число всевозможных паролей длины L, которые можно составить из символов алфавита A.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течении срока его действия V определяется по формуле 1:

$$P = \frac{VT}{S} = \frac{VT}{A^L}. \quad (1)$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи: определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V, T, P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле 2:

$$S^* = \left[\frac{VT}{P}\right], \quad (2)$$

где [] – целая часть числа, взятая с округлением вверх.

После нахождения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось неравенство (формула 3):

$$S^* \le S = A^L. \quad (3)$$

При выборе S, удовлетворяющего неравенству (формула 3), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Необходимо отметить, что при осуществлении вычислений по формулам (2) и (3), величины должны быть приведены к одним размерностям.

3.4 Задание к лабораторной работе № 3

В таблице 3 найти для Вашего варианта значения характеристик P, V, T.

1. Вычислить по формуле (2) нижнюю границу S^* для заданных P,V,T.
2. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (3).
3. Реализовать программу – генератор паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.

Таблица 3 – Варианты заданий на лабораторную работу № 3

Вариант	P	V	T
1	2	3	4
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя

Продолжение таблицы 3.

1	2	3	4
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

3.5 Пример реализации лабораторной работы

На рисунке 5 показан пример реализации программы по генерированию паролей с заданными требованиями. Входными параметрами являются:

- вероятность подбора пароля злоумышленником;
- скорость перебора пароля;
- срок действия пароля;
- используемый алфавит.

На выходе получаем сгенерированный пароль, обладающий требуемой стойкостью к взлому.

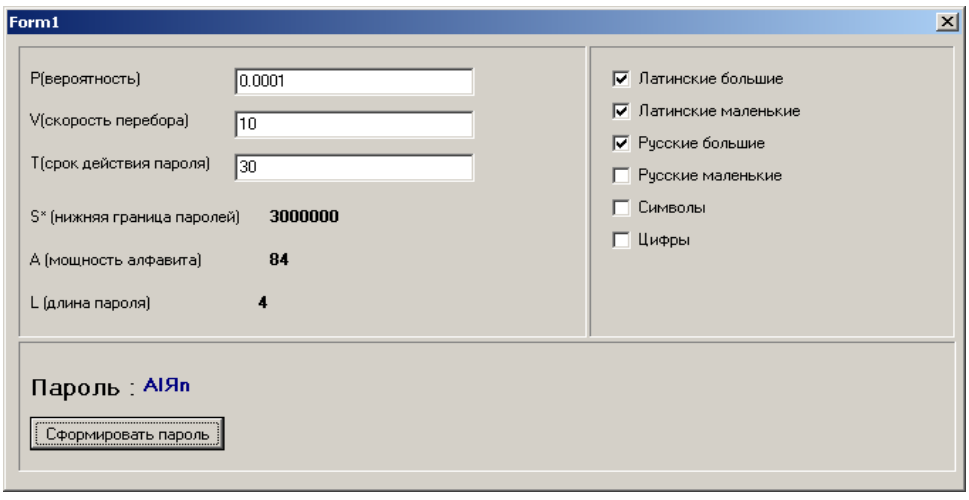

Рисунок 4 – Результат работы программы, реализующей простейший генератор с заданными требованиями

3.6 Контрольные вопросы

1. Дать определение стойкости пароля к взлому. Написать формулу.
2. Дать определение мощности алфавита паролей.
3. Перечислить основные задачи, которые могут решаться с использованием определения стойкости пароля.
4. Перечислить основные требования к выбору пароля.

4 Лабораторная работа № 4. Электронно-цифровая подпись и приемы хеширования

Цель: овладеть практическими навыками закрытия информации электронно-цифровой подписью и приемами хеширования, рассмотрение хеширования методом контрольных сумм и методом наложения кодов – гаммированием.

4.1 Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу шифрования методом контрольных сумм.
3. Составить программу шифрования методом хеширования с применением гаммирования.
4. Составить отчет по проделанной работе.
5. Защитить работу.

4.2 Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.
4. Постановка задачи.
5. Листинг программы.
6. Результат выполнения программы.

4.3 Теоретическая справка

Любая подпись (или иной способ подтверждения подлинности документа), будь то обычная или электронная, всегда выполняет, по крайней мере, три функции:

1) функцию авторизации — подтверждение того, что подписавшийся действительно является тем, за кого мы его принимаем;

2) обеспечение того, что подписавшийся не может отказаться от документа, который он подписал;

3) подтверждение того, что отправитель подписал именно тот документ, который отправил, а не какой-либо иной.

Первые две функции обеспечивают защиту лица, для которого документ предназначен (адресат), а третья — интересы подписавшегося (корреспондента). Во всех случаях проявляется свойство подписи, называемое аутентичностью (подлинностью). Свойство аутентичности подписи переносится на весь документ в целом.

При выработке электронной цифровой подписи (ЭЦП) и ее расшифровании получателем корреспондент и адресат пользуются методом несимметричного шифрования.

В упрощенном виде ЭЦП формируется следующим образом:

1. Корреспондент *X* по специальному алгоритму обрабатывает документ, предназначенный для отправки адресату *У*. В результате применения этого алгоритма, вырабатывается некоторый параметр, характеризующий документ в целом. Объем памяти, занимаемый выработанным параметром, значительно меньше, чем объем всего документа (1, 2, 4 байта).

2. Затем *X* с помощью секретной части ключа шифрует полученный параметр. Полученный таким образом шифр является ЭЦП корреспондента *X*.

3. Корреспондент *X* отправляет адресату *У* документ и свою электронную цифровую подпись.

4. Адресат *У* реализует на полученном документе тот же алгоритм, которым пользовался корреспондент *X*.

5. Затем *У* дешифрует электронную цифровую подпись, полученную от *X*, пользуясь открытой частью ключа, предоставленной ему корреспондентом *X*.

6. Окончательно адресат *У* сравнивает значение параметра, полученного на четвертом этапе, с расшифрованным значением ЭЦП. Если эти значения совпадают, то подпись подлинная и документ при передаче не был изменен. В противном случае – либо документ искажен, либо подпись подделана, либо и то и другое.

Применение ЭЦП не предполагает обязательного засекречивания (шифрования) самого передаваемого документа. Шифруется только некоторая

интегральная характеристика этого документа. Если документ при передаче по каналу связи будет изменен злоумышленником, то, естественно, изменится и его интегральная характеристика, а это сразу заметит адресат при расшифровании ЭЦП. В связи с этим встает вопрос, каким должен быть алгоритм получения интегральной характеристики документа (не слишком большого параметра, характеризующего документ в целом).

Значение интегрального параметра называют хеш - значением документа, а способ (алгоритм) получения хеш-значения — хеш-функцией. Получение хеш-значения с помощью хеш-функции называют сворачиванием (хешированием) текста документа в более короткий текст (интегральный параметр).

Обратимся к важному вопросу хеширования данных. Предположим, что имеется некоторый текст *P* – последовательность знаков некоторого алфавита – и некоторый алгоритм *A,* преобразующий *P* в некоторый текст *M* меньшей длины (формула 4):

$$M = A(P). \qquad (4)$$

Ясно, что алгоритм хеширования *A* должен быть таким, чтобы при случайном равновероятном выборе двух текстов *P1* и *P2*, из множества возможных, соответствующие тексты *M1* и *M2* с высокой вероятностью были бы различны. Поскольку текст *P* длиннее (содержит значительно большее количество двоичных разрядов при двоичном кодировании) хеш-значения *M,* то, вообще говоря, существует много текстов *P* с одним и тем же хеш-значением *M.* Однако алгоритм *A* организуется так, что невозможно однозначно по хеш-значению *M* восстановить сам текст. В этом проявляется отсутствие свойства взаимной однозначности между множеством исходных текстов *{P}* и множеством хеш-значений *{M}*. Кроме того, сложность алгоритма *A* должна обеспечить невозможность осмысленного изменения текста *P* с сохранением того же самого хеш-значения *M.*

Рассмотрим некоторые способы хеширования.

Метод контрольных сумм.

Исторически это самый первый и самый простой способ хеширования, который использовался для проверки правильности ввода программ и данных еще в ЭВМ первого поколения.

Под контрольной суммой понимается некоторое значение, рассчитанное путем сложения всех чисел (кодов символов), соответствующих данному тексту. Если сумма всех таких чисел *K* превышает максимально допустимое значение *(MaxVal),* заданное заранее, то величина контрольной суммы полагается равной остатку от деления полученной суммы на максимально возможное значение контрольной

суммы, увеличенное на единицу. Таким образом, контрольную сумму можно записать в следующем виде (формула 5):

$$KSumm = \begin{cases} K & \text{при} \quad K \le MaxVal \\ K \bmod (MaxVal + 1) & \text{при} \quad K > MaxVal \end{cases} \qquad (5)$$

Пример. Допустим, что документ, который следует подписать ЭЦП, представляет собой следующий текст из романа Ф. М. Достоевского «Идиот»:

«Смиренный игумен Пафнутий руку приложил.»

В соответствии с системой кодирования ASCII написанное предложение (вместе с последней точкой) представляет собой последовательность целых чисел, записанных в десятичной системе счисления:

145 172 168 224 165 173 173 235 169 32 168 163 227 172 165 173

32 143 160 228 173 227 226 168 169 32 224 227 170 227

32 175 224 168 171 174 166 168 171 46

Сумма всех кодов *K = 6625.* Задав значения *MaxVal = 3776,* получаем *KSumm = 2848 (*вычислили остаток от деления *K* на *3777).*

Затем полученную контрольную сумму *KSumm* = 2848 шифруем с помощью открытой части ключа и посылаем адресату.

Если весь текст необходимо сжать (хешировать) в параметр длиной в один байт, то можно в качестве *KSumm* взять остаток от деления *K* на 256. В приведенном примере при этом получаем *KSumm* = 225.

Контрольную сумму можно вычислить и по-другому. Представим все коды символов документа в виде двоичных слов. Каждое такое слово имеет длину 8 битов (1 байт). Например, в приведенной фразе (цитата из Ф. М. Достоевского) символы кодируются двоичными словами:

10010001 - 145 10101100 - 172 10101000 - 168

……

10101011 - 171 00101110 - 46

Контрольную сумму можно составить как поразрядную сумму по модулю 2 (⊕) всех двоичных кодов текста *P.* В нашем примере получается: *KSumm* = 10011011.

Метод контрольных сумм впервые был применен для тестирования правильности ввода данных в ЭВМ, т. е. для контроля работы технических устройств. Поскольку сбои в работе устройств ЭВМ нецеленаправленны

(случайны), метод контрольных сумм давал надежный результат. Иная ситуация в случае с ЭЦП. Человек (злоумышленник) будет стараться изменить документ в свою пользу так, чтобы контрольная сумма не изменялась.

Недостаток метода контрольных сумм (в обоих вариантах) заключается в том, что хотя несовпадение значений этих сумм служит верным признаком того, что документ подвергся изменению, но равенство значений еще не дает гарантии, что информация осталась неизменной. Можно произвольным образом изменить порядок следования букв, цифр или слов и фраз в документе, при этом контрольная сумма сохранит прежнее значение. Так предложениям «казнить нельзя, помиловать» и «казнить, нельзя помиловать» соответствуют одни и те же контрольные суммы, а их содержание прямо противоположное. И что еще хуже — можно изменить отдельные числа в документе и подогнать остальные так, что контрольная сумма останется той же самой. Например, вместо суммы в 1000005 рублей написать 1500000 рублей и получить ни за что половину миллиона рублей.

Внесение небольших изменений в получение контрольной суммы.

Этот метод позволяет преодолеть названные недостатки. Изменение состоит в том, что, прежде чем вычислять контрольную сумму, на каждый код текста накладывается специальный код. Совокупность этих кодов в теории шифрования носит название гаммы шифра, метод наложения кодов – гаммированием. Опишем этот метод.

Пусть каждому символу документа (открытого текста) соответствует восьмибитовое двоичное слово X_i. Таким образом, исходный документ представляется в виде последовательности восьмибитовых двоичных слов: $X_1, X_2, \ldots, Xp$.

Затем выработаем последовательность псевдослучайных чисел t_i по рекуррентной формуле (6):

$$t_{i+1} = (a \bullet t_i + b) \mod c, \qquad (6)$$

где i = 0, 1, …, p – 1;

a, b, t_0 – заданные числа;

p — количество символов в тексте.

При $c = 2^n$. Если взять $n = 8$, то двоичные представления чисел t_i не будут превышать восьми двоичных знаков.

Далее каждое число t_i представим в виде восьмибитового двоичного слова. Получаем последовательность двоичных слов: $T_1, T_2, \ldots, T_p$.

Двоичные числа X_i и T_i, сложим поразрядно по модулю 2. Получим новую последовательность двоичных слов:

$Y_1 = X_1 \oplus T_1, Y_2 = X_2 \oplus T_2, \ldots, Y_p = X_p \oplus T_p$

Каждое двоичное слово, рассматриваемое как двоичное число, переведем в десятичную систему, при этом получим последовательность чисел: $y_1, y_2, \ldots, y_p$.

Полученная последовательность целых чисел суммируется по модулю *MaxVal* + 1 (если $n = 8$, то *MaxVal* = 255).

4.4 Задание к лабораторной работе № 4

Составить программу шифрования методом контрольных сумм и методом хеширования с применением гаммирования.

Варианты заданий к лабораторной работе № 4.

Вариант№ 1.

Пусть $a = 17$, $b = 11$, $c = MaxVal + 1 = 256$, $t_0 = 172$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = '0123456789', *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* = '9876543210', *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = '1000005', *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = '1500000', *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 2.

Пусть $a = 13$, $b = 19$, $c = MaxVal + 1 = 256$, $t_0 = 155$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = '0123456789', *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P ='* 9876543210', *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000005', *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1500000', *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 3.

Пусть $a = 23$, $b = 7$, $c = MaxVal + 1 = 256$, $t_0 = 131$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = '0123456789', *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P ='* 9876543210', *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000005', *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1500000', *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 4.

Пусть $a = 19$, $b = 3$, $c = MaxVal + 1 = 256$, $t_0 = 101$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = '02468', *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P ='* 86420', *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000009', *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1900000', *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 5.

Пусть $a = 17$, $b = 3$, $c = MaxVal + 1 = 256$, $t_0 = 191$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 013579 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P ='* 975310 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000006 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1600000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 6.

Пусть $a = 31$, $b = 5$, $c = MaxVal + 1 = 256$, $t_0 = 121$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 001133557799 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P ='* 997755331100 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000008 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1800000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 7.

Пусть $a = 37$, $b = 11$, $c = MaxVal + 1 = 256$, $t_0 = 221$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 021135579 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P ='* 975531120 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000097 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1970000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 8.

Пусть a = 9, b = 11, c = *MaxVal* + 1 = 256, t_0 = 201. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 021345 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 543120 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 1000999 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 1999000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 9.

Пусть a = 23, b = 19, c = *MaxVal* + 1 = 256, t_0 = 235. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 0000123456 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 6543210000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 10000001 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 11000000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 10.

Пусть a = 31, b = 7, c = *MaxVal* + 1 = 256, t_0 = 126. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 00009999 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 99990000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 10000001 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 11000000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 11.

Пусть a = 41, b = 9, c = *MaxVal* + 1 = 256, t_0 = 192. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 11115555 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 55551111 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 10000001 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 11000000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 12.

Пусть a = 51, b = 13, c = *MaxVal* + 1 = 256, t_0 = 102. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 12121212 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 21212121 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 90000009 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 99000000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 13.

Пусть a = 61, b = 5, c = *MaxVal* + 1 = 256, t_0 = 212. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 191919 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 919191 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 10000009 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 19000000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

Вариант№ 14.

Пусть a = 71, b = 13, c = *MaxVal* + 1 = 256, t_0 = 144. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 100009 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 900001 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 100009 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 190000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

Вариант№ 15.

Пусть a = 17, b = 7, c = *MaxVal* + 1 = 256, t_0 = 152. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (*KSumm*) и методом хеширования с применением гаммирования (*SummKodBukvOtkr*):

а) *P* = ' 100009 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

б) *P* =' 900001 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

д) *P* = ' 100009 ' , *KSumm* = ?, *SummKodBukvOtkr -?*;

е) *P* = ' 190000 ' , *KSumm* = ?, *SummKodBukvOtkr -?*.

4.5 Контрольные вопросы

1. Назвать три функции ЭЦП.
2. Перечислить этапы формирования ЭЦП.
3. Что шифруется при применение ЭЦП?
4. Что называется хеш - значением документа?
5. Что называется хеш-функцией?
6. Что называется сворачиванием (хешированием) документа?
7. В чем заключается метод контрольных сумм?
8. Перечислить этапы метода хеширования с применением гаммирования?
9. Недостаток метода контрольных сумм?

5 Лабораторная работа № 5. Организационно-правовое обеспечение программного обеспечения

Цель работы: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

5.1 Ход работы

1. Изучить литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации).
2. Ответить на контрольные вопросы.
3. Оформить отчет, содержащий краткую информацию по контрольным вопросам.
4. Защитить практическую работу преподавателю (защита в виде опроса).

5.2 Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.

4. Ответы на контрольные вопросы.
5. Вывод по теме.

5.3 Задание к лабораторной работе № 5

Вариант 1. Тема: Законодательство РФ в области информационной безопасности.

Контрольные вопросы:

1. Охарактеризуйте информацию и ее основные показатели.
2. Какие существуют подходы к определению понятия «информация».
3. В чем заключается двуединство документированной информации с правовой точки зрения.
4. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
5. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
6. Назовите основные виды конфиденциальной информации.
7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
8. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
9. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
10. Назовите основные цели государства в области обеспечения информационной безопасности.
11. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
12. Какой закон определяет понятие «официальный документ»?
13. Какой закон определяет понятие «электронный документ»?
14. В тексте какого закона приведена классификация средств защиты информации?
15. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?

Вариант 2. Тема: Законодательство РФ в области информационной безопасности.

Контрольные вопросы:

1. Назовите основные положения Доктрины информационной безопасности РФ.
2. Назовите составляющие правового института государственной тайны.
3. В каких случаях нельзя относить информацию к государственной тайне?
4. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
5. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.
6. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
7. Что в соответствии с законодательством РФ представляет собой засекречивание информации.
8. Перечислите основные принципы засекречивания информации.
9. Что понимается под профессиональной тайной?
10. Какие виды профессиональных тайн вам известны?
11. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?
12. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?
13. Что представляет собой электронная цифровая подпись?
14. Каковы основные особенности правового режима электронного документа?
15. Назовите основные ограничения на использование электронных документов?

Вариант 3. Тема: Изучение положений о государственном лицензировании деятельности в области защиты информации.

Контрольные вопросы:

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.

5. Права и обязанности лицензиатов.

6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.

7. Назовите случаи приостановления или прекращения действия лицензии.

8. В каких случаях предприятию отказывают в выдаче лицензии?

Вариант 4. Тема: Изучение положений о государственном лицензировании деятельности в области защиты информации.

Контрольные вопросы:

1. Какие документы предоставляются для получения лицензии?

2. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

3. Какие средства относятся к шифровальным?

4. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

5. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

6. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

7. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

8. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Вариант 5. Тема: Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.

Контрольные вопросы:

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.

2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.

3. Назовите виды и схемы сертификации средств защиты информации.

4. Каковы функции ФСТЭК в области сертификации средств защиты информации?

5. Каковы функции органов сертификации средств защиты информации?

6. Каковы функции испытательных лабораторий (центров).

7. Каковы функции заявителей?

8. Общий порядок проведения сертификации средств защиты информации.

9. Виды контроля в области сертификации средств защиты информации.

10. Чем определяются сроки проведения сертификационных испытаний?

11. На какой срок выдается сертификат?

12. Назовите причины приостановления или аннулирования действия сертификата.

Вариант 6. Тема: Система сертификации средств криптографической защиты информации.

Контрольные вопросы:

1. Организационная структура системы сертификации средств криптографической защиты информации.

2. Назовите виды и схемы сертификации средств криптографической защиты информации.

3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств криптографической защиты информации?

4. Особенности порядка подготовки и проведения сертификации средств криптографической защиты информации.

5. Виды контроля в области сертификации средств криптографической защиты информации.

6. На какой срок выдается сертификат?

7. Назовите причины приостановления или аннулирования действия сертификата.

8. Какие средства относятся к шифровальным?

9. Что относится к закрытым телекоммуникационным системам и комплексам?

Вариант 7. Тема: Изучение положения о сертификации средств вычислительной техники и связи.

Контрольные вопросы:

1. Организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.

2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.

3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?

4. Особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.

5. Виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.

6. На какой срок выдается сертификат?

7. Назовите причины приостановления или аннулирования действия сертификата.

8. Назовите показатели защищенности.

9. Сколько классов защищенности существует?

10. Сформулируйте требования к показателям защищенности.

Вариант 8. Тема: Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.

Контрольные вопросы:

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.

2. Организационная структура системы объектов информатизации по требованиям безопасности информации.

3. Виды аттестации объектов информатизации по требованиям безопасности информации.

4. Какие объекты информатизации подлежат обязательной аттестации?

5. Каковы функции ФСТЭК в области аттестации объектов информатизации по требованиям безопасности информации?

6. Каковы функции органов по аттестации?

7. Каковы функции заявителей в области аттестации объектов информатизации по требованиям безопасности информации?

8. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

9. На основе каких сведений разрабатывается программа аттестационных испытаний?

10. Порядок проведения аттестационных испытаний.

Вариант 9. Тема: Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.

Контрольные вопросы:

1. Какая документация представляется органу по аттестации?
2. Что такое технический паспорт объекта информатизации и какие сведения о объекте он включает в себя?
3. В чем состоит содержание специального исследования аттестуемого объекта информатизации?
4. Цель и содержание специальных обследований и проверок.
5. Проведение измерения и оценка уровней защищенности.
6. Какие измерения дополнительно проводятся при использовании на объекте информатизации систем активной защиты?
7. Содержание заключения аттестационной проверки объекта информатизации.
8. Содержание протокола аттестационных испытаний объекта информатизации.
9. Содержание аттестата соответствия на объект информатизации.
10. Ответственность за выполнение установленных условий функционирования аттестованного объекта информатизации.

Вариант 10. Тема: Изучение особенностей аттестации помещений по требованиям безопасности информации.

Контрольные вопросы:

1. Дайте определение аттестации объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Какие помещения подлежат обязательной аттестации?
4. Порядок проведения аттестации помещений по требованиям безопасности информации.
5. Какая документация представляется органу по аттестации?
6. Содержание заключения аттестационной проверки помещения.
7. Содержание протокола аттестационных испытаний помещения.
8. Содержание аттестата соответствия на объект информатизации.

Вариант 11. Тема: Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации.

Контрольные вопросы:

1. Дайте определение аккредитации предприятия в качестве органа по сертификации средств защиты информации.
2. Дайте определение аккредитации предприятия в качестве испытательной лаборатории.
3. Порядок аккредитации предприятия в качестве органа по сертификации (испытательной лаборатории) средств защиты информации.
4. На какой срок выдается аттестат аккредитации?
5. Виды контроля за деятельностью аккредитованных предприятий.
6. Перечислите случаи, в которых аккредитация может быть досрочно аннулирована.

Вариант 12. Тема: Изучение типового положения об испытательной лаборатории.

Контрольные вопросы:

1. Кто осуществляет руководство деятельностью испытательной лаборатории?
2. Чем должна располагать испытательная лаборатория для проведения сертификационных испытаний?
3. Перечислите задачи испытательной лаборатории.
4. Перечислите функции испытательной лаборатории.
5. Какие документы готовит испытательная лаборатория по окончании сертификационных испытаний?
6. Какие права имеет испытательная лаборатория?
7. Перечислите обязанности испытательной лаборатории.
8. Какие требования предъявляются к сотрудникам испытательной лаборатории?
9. Какой документацией должна располагать испытательная лаборатория?
10. Какими помещениями должна располагать испытательная лаборатория?
11. Ответственность испытательной лаборатории.

Вариант 13. Тема: Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации.

Контрольные вопросы:

1. Перечислите объекты испытаний.
2. Назовите цели и задачи испытаний и проверок.
3. Каковы условия проведения испытаний?
4. Порядок проведения испытаний.
5. Перечислите общие методы испытаний.
6. В чем состоит суть испытаний объектов на соответствие организационно-техническим требованиям по защите информации?
7. Методы испытаний объектов на соответствие организационно-техническим требованиям по защите информации.
8. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН?
9. Виды испытаний объектов на соответствие требованиям по защите информации от утечки за счет ПЭМИН средств вычислительной техники (СВТ).
10. Методы испытаний объектов на соответствие требованиям по защите информации от утечки за счет ПЭМИН СВТ.
11. Виды испытаний объектов на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные цепи и оборудование.

Вариант 14. Тема: Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации.

Контрольные вопросы:

1. Методы испытаний объектов на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные цепи и оборудование.
2. Виды испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания.
3. Методы испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания.
4. Виды испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи.
5. Методы испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи.
6. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от НСД.

Вариант 15. Тема: Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации.

Контрольные вопросы:

1. Виды испытаний объектов на соответствие требованиям по защите информации от НСД.
2. Методы испытаний объектов на соответствие требованиям по защите информации от НСД.
3. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по акустическим каналам.
4. В чем состоит суть проверки выполнения требований по защите информации от течки за счет встроенных технических средств.
5. В чем состоит суть проверки правильности применения криптографических средств защиты информации.
6. Каким образом осуществляется оценка результатов испытаний и оформление отчетных материалов?

Список использованных источников

1. Домарев, В.В. Безопасность информационных технологий: Методология создания систем защиты /В.В. Домарев. – М.; СПб; Киев: «ТИД «ДИС»», 2002. – 688 с.
2. Мельников, В.П. Информационная безопасность: учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 4-е изд. – М: Академия, 2012. – 336 с.
3. Парытка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Парытка, И.И. Попов. – 5-е изд., перераб. и доп. – М.: Форум: НИЦ ИНФРА-М, 2014. – 432 с.: ил.
4. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов /П.Б. Хореев. – М.: Академия, 2005. – 256 с.
5. Амелин Р.В. Информационная безопасность. Электронный учебник. – **Режим доступа: http://nto.immpu.sgu.ru/sites/default/files/3/__77037.pdf**
6. Интернет-Университет Информационных Технологий: сайт. Басалова, Г.В. Основы криптографии: курс лекций [Электронный ресурс] / Басалова Г.В., 2011. – **Режим доступа: http://www.intuit.ru/**