ЛАБОРАТОРНАЯ РАБОТА №3

Парольная аутентификация. Оценка стойкости парольной защиты. Генераторы паролей

Цель – исследование парольных подсистем аутентификации пользователей. Реализация генератора паролей, обладающего требуемой стойкостью ко взлому.

Теоретический материал

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы). Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Идентификация пользователя – присвоение ему некоторого несекретного идентификатора, который он должен предъявить системе защиты информации (СЗИ) при осуществлении доступа к объекту. В качестве идентификатора может быть использован, логин, физическое устройство и т.д.

Аутентификация – подтверждение пользователем своего идентификатора, проверка его подлинности. Данный этап необходим для устранения фальсификации идентификатора, предотвращения несанкционированного доступа в случае утери пользователем идентификатора.

Авторизация – это предоставление доступа к какому-либо ресурсу на основе результатов идентификации и аутентификации пользователя.

Рис.1. Идентификация, аутентификация и авторизация

Стойкость подсистемы идентификации и аутентификации (И/А) пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

По используемому методу подсистемы И/А делят на четыре группы:

- основанные на некоторой секретной информации, например, пароля;
- основанные на использовании уникального предмета, смарт-карты, жетона, ключа iButton и проч.;
- основанные на измерении биометрических параметров человека – физиологических или поведенческих атрибутах (отпечатки пальцев, почерк, голос, геометрия лица/руки и проч.);
- основанные на информации, ассоциированной с пользователем, например, с его координатами.

Парольные системы идентификации/аутентификации получили самое широкое распространение в СЗИ в силу их простоты и прозрачности. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю. При вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения

паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные системы аутентификации по степени изменяемости паролей делятся на:

- методы, использующие постоянные пароли;
- методы, использующие одноразовые пароли.

Разумеется, с точки зрения безопасности предпочтительными являются одноразовые пароли – взломать их значительно сложнее. Но в таких системах встает вопрос об удобстве хранения таких паролей. Поэтому получили распространение комбинированные методы идентификации и аутентификации, требующие, помимо знания пароля, наличие карточки (e-token) – специального устройства, подтверждающего подлинность субъекта. Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двукомпонентной аутентификацией.

Парольная аутентификация пользователя является, как правило, передним краем обороны СЗИ. В связи с этим, модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель злоумышленника в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя являются наиболее простыми методами аутентификации и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми. Как правило, любая процедура идентификации предполагает ввод пользователем своего логина (login) и пароля (password). В зависимости от особенностей функционирования системы пароль выбирается самим пользователем либо назначается администратором (или же иногда его генерирует сама система).

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

Пароль должен быть таким, чтобы его нельзя было легко раскрыть. Для этого при выборе и использовании пароля рекомендуется руководствоваться следующими правилами:

1) пароль не должен содержать личных данных пользователя (таких, как фамилия, имя, серия или номер паспорта либо другого документа, удостоверяющего личность, дата рождения, адрес и т. п.);
2) пароль не должен быть словом из какого-либо словаря (входить в какой-либо тезаурус), так как перебор слов заданного словаря – технически достаточно простая задача;
3) пароль не должен быть слишком коротким (подобрать сочетание символов в этом случае также не представляет сложности);
4) пароль не должен состоять из повторяющихся букв или фрагментов текста;
5) пароль не должен состоять из символов, соответствующих подряд идущим клавишам на клавиатуре (например, «QWERTY» –образец недопустимого пароля);
6) желательно включать в пароль символы в разных регистрах (прописные и строчные буквы, кириллицу и латиницу), знаки препинания, цифры и др.;

Меры предосторожности, которые необходимо соблюдать при использовании пароля:

1) старайтесь сохранять пароль в тайне (лучше всего его запоминать, а не записывать;
2) периодически (при регулярном обращении к системе — не реже одного раза в месяц) заменяйте пароль на новый, но он не должен выдаваться пользователю в конце сеанса работы. Заметим, что в разное время могут применяться различные пароли;
3) в паспорте пользователя пароль должен храниться в зашифрованном виде. Наиболее подходящими для этих целей являются методы необратимого шифрования (при которых обратное преобразование невозможно). Введенный пользователем пароль тоже должен шифроваться, а уже затем сравниваться с хранящимся.

Несоблюдение вышеперечисленных правил ведет к раскрытию пароля и к угрозе несанкционированного доступа к информационной системе и данным, хранящимся в ней.

Как правило, для помощи администратору безопасности в формировании паролей подчиненных ему пользователей, удовлетворяющих перечисленным требованиям к паролям, используются особые программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации, единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (*brute forcing*). В данном случае, количественная оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

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 А.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

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

$$P = \frac{V * T}{S} = \frac{V * T}{A^L} \qquad (1)$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи:

Задача. 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 следующей формуле

$$S* = \left\lceil \frac{V * T}{P} \right\rceil \qquad (2)$$

где $\lceil\ \rceil$ - 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 (2).

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

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Необходимо отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

*Пример. Исходные данные – $P=10^{-6}$, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю.*

Тогда, $S^* = \left[\frac{100800 * 1}{10^{-6}}\right] = 1008 * 10^8$.

Условию $S^* \le A^L$ *удовлетворяют, например, такие комбинации A и L, как A=26, L=8 (пароль состоит из 8 малых символов английского алфавита), A=36, L=6 (пароль состоит из 6 символов, среди которых могут быть малые латинские буквы и произвольные цифры).*

Задание для практической работы

1. В табл.1 найти для Вашего варианта (выбирается исходя из последних двух цифр номера зачетной книжки) значения характеристик *P, V, T,* а также группы символов, используемых при формировании пароля. Вычислить мощность алфавита паролей A, соответствующую Вашему варианту. Вычислить по формуле (1) нижнюю границу S^* для заданных *P, V, T*. Зная мощность алфавита паролей A, вычислить минимальную длину пароля L, при котором выполняется условие (2).

2. Реализовать на языке программирования программу, реализующую генератор паролей с характеристиками, соответствующими Вашему варианту. Программа должна формировать случайную последовательность символов длины L, должны использоваться символы из тех групп, которые выданы Вашему варианту.

Таблица 1

Варианты заданий для выполнения лабораторной работы №4

Вариант	***P***	***V***	***T***	***Используемые группы символов пароля***
1.	10^{-4}	15 паролей/мин	2 недели	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
2.	10^{-5}	3 паролей/мин	10 дней	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
3.	10^{-6}	10 паролей/мин	5 дней	1. Русские прописные буквы (А-Я) 2. Специальные символы.

4.	10^{-7}	11 паролей/мин	6 дней	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
5.	10^{-4}	100 паролей/день	12 дней	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
6.	10^{-5}	10 паролей/день	1 месяц	1. Русские строчные буквы (а-я) 2. Специальные символы.
7.	10^{-6}	20 паролей/мин	3 недели	1. Цифры (0-9) 2. Русские строчные буквы (а-я)
8.	10^{-7}	15 паролей/мин	20 дней	1. Латинские строчные буквы (a-z) 2. Латинские прописные буквы (A-Z)
9.	10^{-4}	3 паролей/мин	15 дней	1. Русские прописные буквы (А-Я) 2. Русские строчные буквы (а-я)
10.	10^{-5}	10 паролей/мин	1 неделя	1. Цифры (0-9) 2. Специальные символы.
11.	10^{-6}	11 паролей/мин	2 недели	1. Цифры (0-9) 2. Русские прописные буквы (А-Я)
12.	10^{-7}	100 паролей/день	10 дней	1. Латинские строчные буквы (a-z) 2. Русские прописные буквы (А-Я)
13.	10^{-4}	10 паролей/день	5 дней	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
14.	10^{-5}	20 паролей/мин	6 дней	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
15.	10^{-6}	15 паролей/мин	12 дней	1. Русские прописные буквы (А-Я) 2. Специальные символы.
16.	10^{-7}	3 паролей/мин	1 месяц	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
17.	10^{-4}	10 паролей/мин	3 недели	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
18.	10^{-5}	11 паролей/мин	20 дней	1. Русские строчные буквы (а-я) 2. Специальные символы.
19.	10^{-6}	100 паролей/день	15 дней	1. Цифры (0-9) 2. Русские строчные буквы (а-я)
20.	10^{-7}	10 паролей/день	1 неделя	1. Латинские строчные буквы (a-z)

				2. Латинские прописные буквы (A-Z)

Также предусмотрите возможность расчета времени взлома сгенерированного пароля. В отчет включите скриншоты работы Вашей программы.

Рассчитайте надежность сгенерированного в программе пароля с использованием сервиса из п.2 списка используемых ресурсов. Сравните время, полученное по Вашим расчетам, и с помощью сервиса. Есть ли разница? Почему? Какое значение более точное?

3. С использованием одного из языков программирования высокого уровня составить программу, которая выполняет действия, указанные в таблице с номером вашего варианта (выбирается исходя из последних двух цифр номера зачетной книжки).

Задание	**Алгоритм**
Вариант №1	
Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a». 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен

	или неверен?
Вариант №2	
Пусть на экран выведены следующие три слова: «scleroses», «scoliosis», «paradantoz». Составить программу, которая записывает пароль следующим образом	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом первого слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует предпоследней букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся предшественником среднего символа третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах плюс 1 символ; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №3	
Пусть на экран выведены следующие три слова: «computer», «maus», «scanner». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся последним символом первого слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите следует за буквой, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует через пять позиций за буквой, являющейся средним символом третьего

	слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в третьем и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №4	
Пусть на экран выведены следующие три слова: «mathematic», «physic», «hemi». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. Если первое слово содержит нечетное количество букв, то в качестве первого символа в строку *<результат>* записать букву, которая в алфавите следует через три позиции за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же первое слово содержит четное количество символов, то в качестве первого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов первого слова; если это буква «a», записать «z». 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. В качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся первым символом третьего слова на экране; если это буква «z», записать «a». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 1 символ; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.

Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №5	
Пусть на экран выведены следующие три слова: «pero», «ruchka», «bumaga». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся третьим символом первого слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся первым символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Ввести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №6	
Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard».	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым от конца символом первого слова на экране; если это буква «z», записать «a».

Составить программу, которая записывает пароль следующим образом	2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует через две позиции за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах плюс 2 символ; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №7	
Пусть на экран выведены следующие три слова: «Kats», «milk», «smitten». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом третьего слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся первым символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует

	букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 2 символ; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №8	
Пусть на экран выведены следующие три слова: «dog», «zaps», «budge». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом второго слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся предпоследним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, которая предшествует среднему символу третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением

аутентификации	вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №9	
Пусть на экран выведены следующие три слова: «pipers», «hauls», «polios». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом третьего слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся вторым символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся последним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах плюс 3 символа; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №10	
Пусть на экран выведены следующие три слова: «student», «pedagogy», «buck».	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся третьим символом третьего слова на экране; если это буква «z», записать «a».

Составить программу, которая записывает пароль следующим образом	2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся предпоследним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся первым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 3 символа; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №11	
Пусть на экран выведены следующие три слова: «basic», «compilation», «programs». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку *<результат>* в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом с конца первого слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите следует за буквой, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов

	третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №12	
Пусть на экран выведены следующие три слова: «gourd», «speckle», «capote». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку *<результат>* в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a». 2. В качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся предпоследним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся предпоследним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве четвертого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве пятого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах плюс 4 символа; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Ввести полученную строку.
Дополнить полученную программу средствами	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением

аутентификации	вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №13	
Пусть на экран выведены следующие три слова: «worship», «outreach», «luck». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку *<результат>* в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом второго слова на экране; если это буква «z», записать «a». 2. В качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся пятым символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся третьим символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве четвертого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве пятого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах минус 4 символа; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №14	
Пусть на экран выведены следующие три слова: «starved», «carp», «shuck».	Исходные данные — строковые константы 1. В строку *<результат>* в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом

Составить программу, которая записывает пароль следующим образом	третьего слова на экране; если это буква «z», записать «a». 2. В качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся третьим символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся четвертым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве четвертого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве пятого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №15	
Пусть на экран выведены следующие три слова: «Mark», «Shark», «Dark». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку *<результат>* в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a». 2. В качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся третьим символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся четвертым символом третьего слова; если это буква «z», записать «a». Если же третье слово

	содержит четное количество символов, то в качестве четвертого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №16	
Пусть на экран выведены следующие три слова: «9DOLLAR0», «Cheby», «Homework». **Составить программу, которая записывает пароль следующим образом**	Исходные данные — строковые константы 1. В строку *<результат>* в качестве 2-х первых символов записать буквы, которые в алфавите следуют за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся третьим символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве четвертого символа записать букву, которая в алфавите следует за буквой, являющейся четвертым символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве четвертого символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве пятого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и втором словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.

	5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №17	
Выберите пятую строку любимого произведения Лермонтова **Составить программу, которая записывает пароль следующим образом**	1. Замените заглавные буквы строчными, строчные – заглавными. 2. Буквы, стоящие в алфавите после М замените в строке соответствующими цифрами их порядкового номера в алфавите. 3. В качестве пароля выберите нечетные символы в строке.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №18	
Выберите десятую строку любимого произведения Пушкина **Составить программу, которая записывает пароль следующим образом**	1. Замените заглавные буквы строчными, строчные – заглавными. 2. Буквы, стоящие в алфавите до М замените специальными символами. 3. В качестве пароля выберите нечетные символы в строке.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №19	
Выберите шестую строку произведения Гумилева **Составить программу,**	1. Замените заглавные буквы строчными, строчные – заглавными. 2. Буквы, стоящие в алфавите до М замените специальными символами. 3. В качестве пароля выберите нечетные символы в

которая записывает пароль следующим образом	строке.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Вариант №20	
Выберите третью строку произведения Бальмонта **Составить программу, которая записывает пароль следующим образом**	1. Замените заглавные буквы строчными, строчные – заглавными. 2. Буквы, стоящие в алфавите после М замените в строке соответствующими цифрами их порядкового номера в алфавите. 3. В качестве пароля выберите нечетные символы в строке.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?

Предоставить скриншоты работы программы. Оцените аналогично п.2 надежность полученного пароля.

Контрольные вопросы

1. Дайте собственное определение понятиям «идентификация», «аутентификация», «авторизация». Приведите по 3 примера к каждому из них.

2. Какие еще правила выбора и использования пароля Вы бы предложили?

3. Какие еще признаки Вы бы предложили при двух- и многофакторной парольной аутентификации?

4. В какой момент должна производится процедура И/А в СЗИ компьютерной системы?

5. Как Вы считаете, насколько эффективна парольная аутентификация? Ответ обоснуйте.

Список используемых ресурсов:

1. Мифтахова Л.Х. Программно-аппаратные средства защиты информации / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников,

В.А. Богомолов, А.Д. Алехин // Учебное пособие. – СПб.: Изд-во «Интермедия», 2018. – 312 с.
2. How Secure Is My Password? – URL: https://howsecureismypassword.net/

Пример оформления отчета по лабораторной работе

ЛАБОРАТОРНАЯ РАБОТА №3

НАЗВАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

ВЫПОЛНИЛ: СТ. ГР. ….. ФИО

ВАРИАНТ № …

ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

P=…

V=…

T=…

S^*= (ПРИВЕСТИ ВЫЧИСЛЕНИЯ) = ….

В КАЧЕСТВЕ АЛФАВИТА СИМВОЛОВ, ИСПОЛЬЗУЕМЫХ ПРИ ГЕНЕРАЦИИ ПАРОЛЯ, БЫЛИ ИСПОЛЬЗОВАНЫ СЛЕДУЮЩИЕ НАБОРЫ _____. МОЩНОСТЬ ДАННОГО НАБОРА A =_____.

ПРИ МИНИМАЛЬНОМ ЗНАЧЕНИИ L=… ВЫПОЛНЯЕТСЯ УСЛОВИЕ $S^* \leq S = A^L$.

ТЕКСТ ПРОГРАММЫ ПО ЗАДАНИЮ П.2

ПРИМЕРЫ СГЕНЕРИРОВАННЫХ ПРОГРАММОЙ ПАРОЛЕЙ:

1) …..

2) …..

3) …..

4) …..

5) …..

СКРИНШОТЫ РАБОТЫ ПРОГРАММЫ

...

ОЦЕНКА НАДЕЖНОСТИ ПАРОЛЯ

ТЕКСТ ПРОГРАММЫ П ЗАДАНИЮ П.3

СКРИНШОТ СГЕНЕРИРОВАННОГО ПРОГРАММНОЙ ПАРОЛЯ

РЕЗУЛЬТАТ НЕПРАВИЛЬНОГО ВВОДА ПОЛЬЗОВАТЕЛЕМ ПАРОЛЯ

ОЦЕНКА НАДЕЖНОСТИ СГЕНЕРИРОВАННОГО ПАРОЛЯ

ОТВЕТЫ НА КОНТРОЛЬНЫЕ ВОПРОСЫ

1. ВОПРОС

ОТВЕТ

...

ВЫВОДЫ ПО РАБОТЕ

...