ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»**

**Факультет безопасности информационных технологий**

**Дисциплина:**
**«Теория информационной безопасности и методология защиты информации»**

# ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6
## Разграничение доступа. Идентификация и аутентификация

**Выполнил:**
Студент гр. N3253
Пастухова А.А.

**Проверил:**
Якимова С.А.

Санкт-Петербург
2022г.

*Цель:*разработка подсистемы идентификации и аутентификации субъектов.

*Задачи:*

1. Составить алгоритм для реализации выбранной подсистемы.
2. Составить полную схему компьютерной системы со встроенной в нее подсистемой идентификации и аутентификации.

*Ход работы:*

1. Изучить документ https://drive.google.com/file/d/1Inhho7b5ik_aE98vmEpoaMc6KWEGvnMz/view?usp=sharing
2. Выбрать одну из подсистем, описанных в документе, и детально ознакомиться с ней (использование дополнительной литературы приветствуется).
3. Составить краткий конспект (1-2 стр.): основные принципы реализации выбранной подсистемы, достоинства, недостатки(уязвимости).
4. Составить алгоритм (можно в виде блок схемы) для реализации выбранной подсистемы учитывая все требования по безопасности.
5. Составить полную схему компьютерной системы со встроенной в нее подсистемой идентификации и аутентификации (включая базы данных, описать модель безопасности, с мониторами безопасности объектов и субъектов).
6. Сделать вывод: насколько надежным является совокупность выбранной вами модели безопасности и подсистемы аутентификации и идентификации, ее достоинства и недостатки.

Ход работы:

Мною был выбран метод парольных систем идентификации/аутентификации, так как он является наиболее распространенным на данные момент.

Парольная защита — это программные средства, позволяющие обеспечить защиту от несанкционированного доступа и защиту самих паролей. Под паролем подразумевается набор символов, вводимый пользователем с клавиатуры, который необходим для того, чтобы подтвердить личность пользователя, либо его полномочия на доступ к данным или в систему, используя метод разграничения доступа. Парольная защита применяется с целью защиты от несанкционированного доступа. Обычно при входе в систему у пользователя запрашивается его идентификатор (логин), а также аутентификатор, которым чаще всего является пароль.

Кроме того, многие существующие информационные системы должны соответствовать требованиям регуляторов (например, ФСТЭК России) для прохождения аттестации.

Использование стандартной политики требований сложности задаваемых паролей в операционных системах, в значительной степени затрудняет компрометацию учетных записей удаленным злоумышленником с использованием словарей.

*Достоинства:*

Главным достоинством такой системы является ее простота. Пользователю достаточно просто знать пароль и правильно ввести его, чтобы получить беспрепятственный доступ к ресурсу, который ему нужен. Поэтому парольная аутентификация является наиболее часто используемой. Кроме того, парольная система используется очень давно, появившись раньше, чем все прочие методы, позволяет применять его в большом количестве разнообразных компьютерных программ.

*Недостатки:*

Любая парольная система является в определенной степени уязвимой отдельные ее элементы могут быть расположены в местах, открытых для

доступа потенциальному злоумышленнику (в том числе и база данных учетных записей пользователей).

В связи с этим, парольные системы становятся одним из наиболее привлекательных для злоумышленника объектов атаки. Основными типами угроз безопасности парольных систем являются следующие.

1. Перебор паролей в интерактивном режиме.
2. Подсмотр пароля.
3. Преднамеренная передача пароля его владельцем другому лицу.
4. Кража базы данных учетных записей с дальнейшим ее анализом, подбором пароля.
5. Перехват вводимого пароля путем внедрения в КС программных закладок (клавиатурных шпионов); перехват пароля, передаваемого по сети.
6. Социальная инженерия.

*Пути устранения недостатков:*

Вне зависимости от уровня защищенности информационной системы и требуемого уровня защищенности персональных данных в системе должны выполняться меры по идентификации и аутентификации, в том числе и для уменьшения деструктивного влияния человеческого фактора. В случае, когда в информационной системе используются пароли как средство аутентификации, они должны соответствовать определенным критериям:

1. Задание минимальной длины пароля для затруднения подбора пароля злоумышленником «в лоб» (полный перебор, brute-forcing) и подсмотра.
2. Использование в пароле различных групп символов для усложнения подбора злоумышленником пароля «в лоб».
3. Проверка и отбраковка пароля по словарю для затруднения подбора пароля злоумышленником с использованием словарей.

4. Установление максимального срока действия пароля для затруднения подбора пароля злоумышленником «в лоб», в том числе и в режиме «off-line» при взломе предварительно похищенной базы данных учетных записей пользователей.

5. Применение эвристического алгоритма, бракующего «плохие» пароли для усложнения подбора пароля злоумышленником «по словарю» или с использованием эвристического алгоритма.

6. Ограничение числа попыток ввода пароля для предотвращения интерактивного подбора пароля злоумышленником.

7. Использование задержки при вводе неправильного пароля для предотвращения интерактивного подбора пароля злоумышленником.

8. Поддержка режима принудительной смены пароля пользователя для эффективности реализации требования, ограничивающего максимальный срок действия пароля.

9. Запрет на выбор пароля самим пользователем и автоматическая генерация паролей для затруднения использования злоумышленником эвристического алгоритма подбора паролей.

Еще одним важным параметром парольной системы является оценка ее стойкости для того, чтобы сделать вывод о возможности и целесообразности ее взлома, ведь время взлома может быть настолько велико, что знание парольной информации может потерять ценность.

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля). Например, если при составлении пароля могут быть использованы только малые английские буквы, то A=26.

L – длина пароля.

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

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

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

$$P = \frac{V*T}{S} = \frac{V*T}{A^L}$$

Алгоритм для реализации парольной подсистемы, учитывая все требования по безопасности:

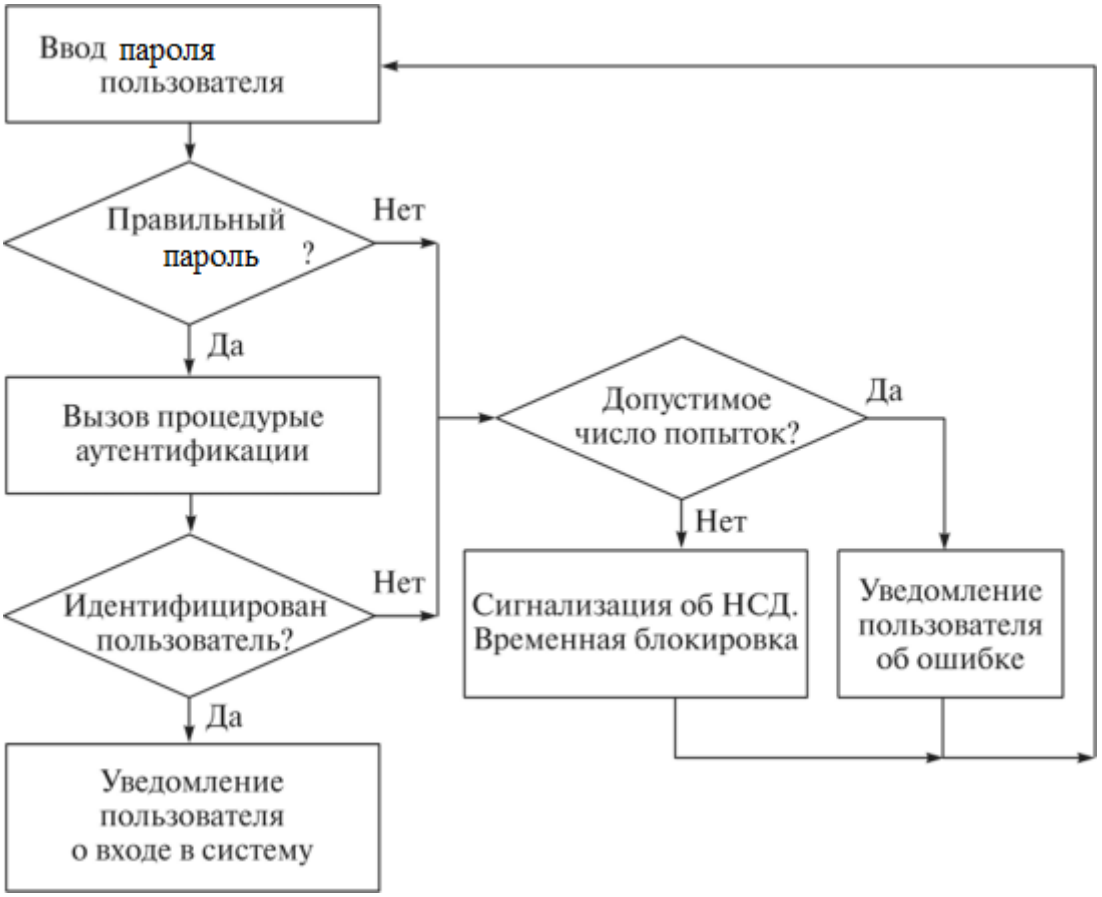
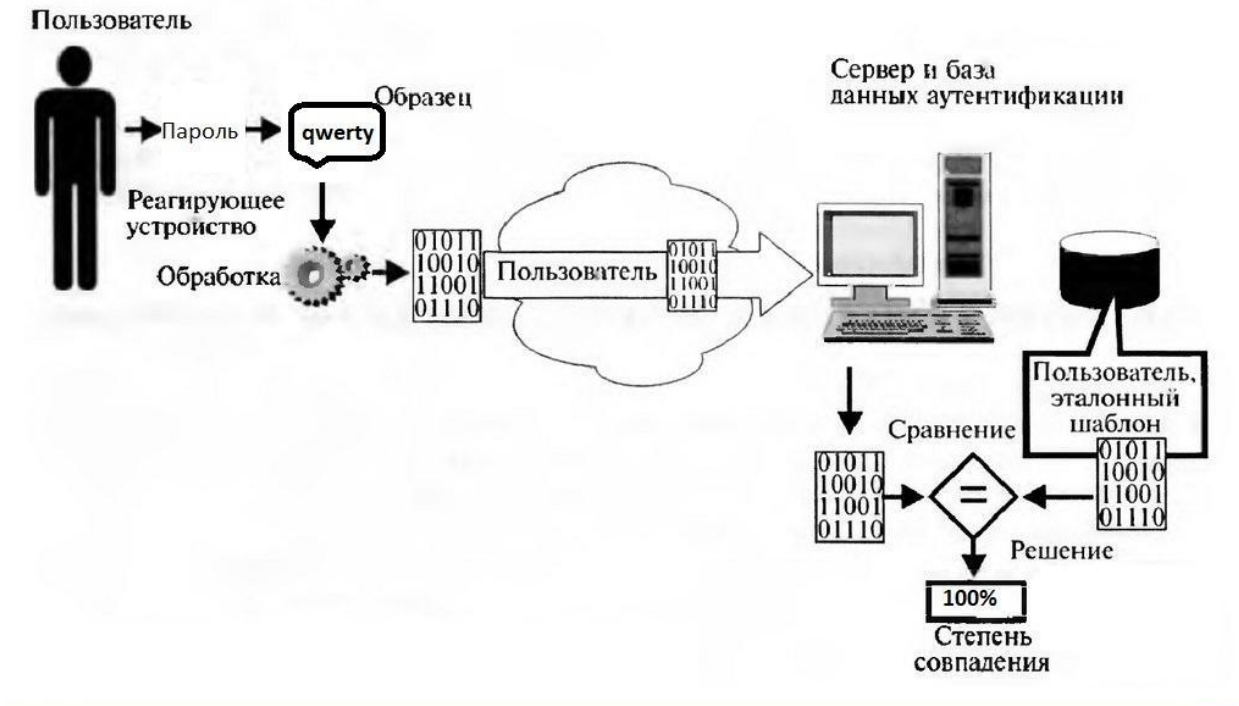



Схема компьютерной системы со встроенной в нее подсистемой идентификации и аутентификации с использованием пароля:




*Вывод*:

Парольная система может считаться относительно надежной, если выполнен ряд обязательных условий. Кроме того, такая подсистема идентификации и аутентификации считается простой в реализации, но нужно учитывать, что информация, подтверждающая подлинность пользователя должна храниться в секрете, лучше – на внешнем аппаратном устройстве, максимально защищенном от НСД.

*Использованная литература*:

https://studme.org/179760/informatika/parolnye_sistemy_autentifikatsii

https://safe-crypto.me/c1/soft/ataki-na-parolnie-sistemi.php

https://www.anti-malware.ru/security/passwords