**Министерство образования Республики Беларусь**

**Учреждение образования**
**«Белорусский государственный университет информатики и радиоэлектроники»**

**Кафедра защиты информации**

# ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ ДАННЫХ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

**к практическим занятиям по дисциплине**
**«Методология информационной безопасности»**

**для студентов специальности**
**1-98 01 02 «Защита информации в телекоммуникациях»**

**Минск 2021**

# ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7
# «ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ ДАННЫХ»

**Цель занятия:** изучение особенностей построения систем парольной защиты данных информационных систем, требований предъявляемых к паролю и получения практические навыков оценки стойкости парольной защиты данных.

## 1 Краткие теоретические сведения

Информация распространение и (или) предоставление которой ограничено, как известно, подлежит защите. Такая информация обрабатывается в информационных системах.

**Информационная система** - совокупность *банков данных*, информационных технологий и комплекса (комплексов) программно-технических средств.

**Банк данных** - организационно-техническая система, включающая одну или несколько *баз данных* и систему управления ими.

**База данных** – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях.

Для контроля доступа пользователей информационной системы к такой информации необходимо выполнить проверку прав доступа пользователя (субъекта доступа) и на основании наличия или отсутствия таких прав, разрешить или запретить им доступ (принять решение) к информации. Система, которая реализует такую процедуру, называется **системой авторизации пользователей**.

**Авторизация** – предоставление прав доступа субъекту доступа к информации, обрабатываемой в информационной системе.

Любую информационную систему можно представить как совокупность субъектов и объектов и отношений между ними (рисунок 1). **Объект** – пассивный компонент системы, который хранит в себе информацию (примером такого объекта является файл). **Файл** - структурированная по определенным правилам информация, представляющая собой блок данных имеющий определенное наименование (имя). **Субъект** – активный компонент системы, который получая доступ к объектам системы, является причиной потока информации от одного объекта к другому (например, копирование информации из одного файла в другой).


Рисунок 1. – Схематичное изображение компонентов информационной системы

Субъектом в информационной системе является человек, но он непосредственно не взаимодействует с объектами (файлами), так как они не могут быть непосредственно им прочитаны, как например информация, содержащаяся на бумаге. Поэтому человеку необходимо использовать соответствующие программно-технические средства, которые предоставят ему информацию, содержащуюся в объектах (файлах) в таком виде, который он сможет воспринимать. Именно поэтому **субъектом доступа** в информационной системе является не человек, а программно технический комплекс (например, персональный компьютер), с помощью которого человек осуществляет доступ к информационной системе и информации хранимой в ней.

В рамках информационных систем информация хранится в виде файлов размещаемых на машинных носителях. Субъект доступа может получить следующие права доступа к информации (файлам):

- ***чтение*** - позволяет открыть файл и ознакомиться с его содержанием (применимо к текстовым и исполняемым файлам);

- ***запись*** - позволяет открыть файл и ознакомиться с его содержанием и изменить его (применимо к текстовым и исполняемым файлам);

- ***исполнение*** – позволяет выполнить код, содержащийся в этом файле (применимо к исполняемым файлам).

Для того чтобы можно было провести авторизацию пользователя информационной системы необходимо каким-то образом его опознать. Для этого существует процедура идентификации.

**Идентификация** – процесс присвоения уникального (неповторимого) признака (идентификатора) субъекту доступа, по которому он впоследствии будет опознан.

Выделяют следующие виды идентификаторов:

1. Идентификатор, который известен только субъекту доступа. Такой подход предполагает, что идентификатор необходимо запомнить. Примером является пароль.

2. Идентификатор может быть записан на некоторое устройство, которое гарантирует противодействие угрозе сохранности идентификатора. Примером являются специализированные устройства обеспечивающие сохранность информации и подключаемые к персональному компьютеру через разъем USB. Они имеют внешнее сходство с картой флеш памяти, которая имеет разъем USB. Применение таких идентификаторов сопряжено с проблемами связанными с потерей таких устройств (человек нашедший такое устройство сможет с его помощью авторизоваться от имени владельца устройства) и случаями, когда такие устройства владелец забывает отключить от персонального компьютера и оставляет без его контроля (человек который получит физический доступ к такому компьютеру сможет авторизоваться от имени владельца).

3. В качестве идентификатора могут быть использованы биометрические характеристики человека (поведенческие и физиологические). Использование таких идентификаторов сопряжено с ошибками идентификации, которые обусловлены тем, что эти характеристики варьируются в течение суток в некоторых пределах, так как человек является живым объектом. Кроме того, если к такому идентификатору получит доступ нарушитель и его скопирует, то изменить такой идентификатор у человека не возможно в отличие, например от изменения пароля.

В информационных системах наиболее широко используют такой идентификатор как пароль. Это обусловлено рядом его преимуществ:

- выбрать его может сам пользователь информационной системы;
- при компрометации его можно достаточно легко сменить;
- сложность и стоимость системы не высока.

Таким образом, процедура идентификации пользователя (субъекта доступа) заключается в выдаче пользователю уникального идентификатора. Для того чтобы субъект доступа получил доступ к информации необходимо реализовать еще одну процедуру – аутентификации. **Аутентификация** – процесс проверки подлинности субъекта доступа по его идентификатору.

Система, реализующая контроль доступа к ней по паролю состоит из трех основных компонентов (рисунок 2):

1. Рабочее место пользователя (например, персональный компьютер) на котором установлено прикладное программное обеспечение (например,

браузер). Такое рабочее место в терминологии компьютерных сетей называется клиентом.

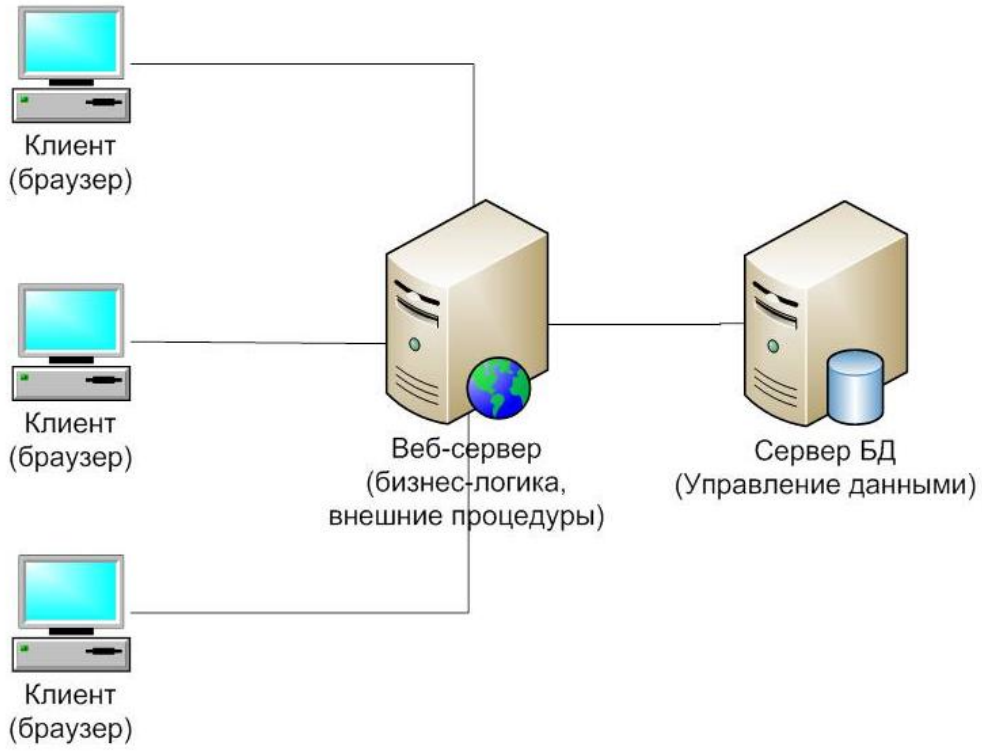


Рисунок 2. – Схематичное изображение информационной системы реализующей функцию аутентификации субъекта доступа

2. Сервер, который способен принять запрос от субъекта доступа, и по предоставленной ему информации проверить его подлинность.

3. База данных и система управления ею. База данных хранит идентификаторы всех зарегистрированных в информационной системе субъектов доступа.

Аутентификация субъекта доступа происходит следующим образом. Субъект доступа подключается к информационной системе и та ему предлагает ввести логин и пароль (идентификатор) демонстрируя окно авторизации (рисунок 3). Человек вводит логин и пароль. Браузер передает эти данные веб-серверу, которые получив их, формирует запрос к системе управления сервера баз данных (БД). Система управления, получив логин и пароль пользователя анализируя содержимое базы данных на предмет наличия такого идентификатора. В случае если он найден в базе данных, то система управления базой данных передает на веб-сервер информацию, что результат аутентификации пользователя положительный и пользователь получит доступ к

массиву данных, в противном случае в доступе субъекту доступа будет отказано.


Рисунок 3. – Внешний вид окна авторизации

**Система парольной защиты** – программно-аппаратный комплекс, реализующий на основе одноразовых или многоразовых паролей процессы идентификации, аутентификации и авторизации субъектов доступа информационной системы.

**Пароль пользователя** – информация, известная только пользователю и хранимая в парольной системе, которая должна сохраняться в секрете и может быть предъявлена им для прохождения процедуры аутентификации. Одноразовый пароль дает возможность субъекту доступа однократно пройти аутентификацию, после чего пароль аннулируется. Многоразовый пароль может быть использован для проверки подлинности субъекта доступа повторно.

Совокупность логина и пароля пользователя образуют его **учетную запись**.

Рассмотрим основные пути реализации угроз в отношении систем парольной защиты.

1. Определение параметров учетной записи через:

– их подбор в интерактивном режиме;

– подсматривание при вводе пользователем;

– преднамеренную передачу пароля его владельцем другому лицу;

– захват базы данных системы парольной защиты (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или расшифрование);

– перехват переданной по сети информации в процессе аутентификации субъекта доступа;

– хранение пароля в доступном для нарушителя месте.

2. Вмешательство в функционирование компонентов системы парольной защиты через:

– внедрение вредоносной программы;

– обнаружение и использование ошибок, допущенных на стадии разработки системы;

– выведение из строя системы за счет создания условий, при которых реализуется в ней программный или технический сбой.

Пароль состоит из некоторого алфавита с некоторым числом символов в нем (A) и имеет определенную длину с количеством символов (L). Число всевозможных паролей (S) длиной L, которые можно составить из символов алфавита A определяется следующим выражением:

$$S = A^{L}$$

Одна из распространенных атак позволяющих подобрать пароль называется brute force (грубая сила). Она заключается в переборе всевозможных комбинаций пароля при известной его длине.

Стойкость пароля к подобным атакам определяется его энтропией (степенью не определенности). Чем выше энтропия пароля, тем больше времени потребуется нарушителю для его подбора. Энтропия пароля определяется в соответствии со следующим выражением:

$$H = L \times \frac{\log A}{\log 2}$$

В соответствии с выражением, можно утверждать, что энтропия пароля, а соответственно и его стойкость будет в большей степени определяться его длиной.

Перебор паролей нарушитель проводит с использованием средств вычислительной техники, которые характеризуются некоторой производительностью. Чем больше производительность – тем меньше времени необходимо для подбора пароля. Кроме того пароль можно с некоторой периодичностью менять, что также будет влиять на сложность подбора его нарушителем.

В результате чего можно рассчитать вероятность подбора нарушителем пароля:

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

где V - скорость подбора пароля нарушителем;

T - максимальный срок действия пароля.

Отсюда можно выразить значение нижней границы всевозможных паролей при соответствующих известных значениях:

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

Это значение позволяет определить длину пароля и его алфавит, при которых вероятность подбора пароля будет равна заданной.

Предположим, что $P=10^{-6}$, T=7 дней, V=10 паролей/минуту. Перед расчетом необходимо привести исходные данные, касающиеся времени к единой временной единице. Поэтому V=10 паролей/минуту = 10*60*24*7=100800 паролей в неделю. Тогда:

$$S^* = \frac{100800 \times 1}{10^{-6}} = 1008 * 10^8 \text{ комбинаций паролей}$$

Учитывая, что

$$S^* \leq S = A^L$$

Требования к алфавиту следующие A=26, L=8. Указанному числу символов соответствует латинский алфавит, состоящий из малых букв.

Необходимо помнить, что одно из важнейших требований, предъявляемых к паролю это хранение его в секрете. Это означает, что пароль должен быть таким, чтобы с одной стороны его мог запомнить пользователь, а с другой – он сохранял свою стойкость в пределах определенного временного интервала. В организациях требования к паролю определяются политикой парольной защиты, которая является внутриведомственным нормативным правовым актом.

## 2 Практическое задание

1. Определите минимальное количество символов в пароле и минимальную его длину, при заданных значениях вероятности его подбора,

скорость подбора пароля нарушителем и максимального срока его действия, в соответствии с вариантом задания (приложение) которое задается преподавателем. На основании полученных результатов расчета определить состав удовлетворяющего полученным данным алфавита.

2. Используя ресурс www.2ip.ru (меню «Стойкость пароля») определить время подбора пароля длиной 8 символов состоящего из:

- малых букв латинского алфавита;
- одинаковых букв латинского алфавита;
- малых букв русского алфавита;
- одинаковых букв русского алфавита.

Сделайте вывод по полученным результатам данного задания.

3. Используя ресурс www.2ip.ru (меню «Стойкость пароля») определите минимальную длину пароля, при котором его стойкость будет обеспечиваться не менее 1 года:

- для русского алфавита;
- для латинского алфавита.

4. Используя ресурс www.2ip.ru (меню «Стойкость пароля») и знания получены при выполнении задания 2, составить пароль, который имеет не меньшую стойкость, чем в задании 3, но имеющий меньшую длину:

- при условии, что основу его составляет русский алфавит;
- при условии, что основу его составляет латинский алфавит.

## 3 Контрольные вопросы

1. Что такое система авторизации?
2. Что такое субъект доступа?
3. Дайте характеристику всем видам идентификаторов?
4. Какие особенности реализации угроз в системах парольной защиты?
5. Какие требования предъявляются к паролю?

## 3 Приложение

| Вариант | P | V | T |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | $10^{-2}$ | 10 паролей/мин | 5 дней |
| 2 | $10^{-3}$ | 100 паролей/мин | 1 неделя |
| 3 | $10^{-4}$ | 1000 паролей/мин | 2 недели |
| 4 | $10^{-5}$ | 10000 паролей/мин | 3 недели |
| 5 | $10^{-6}$ | 11000 паролей/мин | 1 месяц |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| 6 | $10^{-7}$ | 10 паролей/сек | 2 месяца |
| 7 | $10^{-2}$ | 100 паролей/сек | 3 месяца |
| 8 | $10^{-3}$ | 1000 паролей/сек | 4 месяца |
| 9 | $10^{-4}$ | 10000 паролей/сек | 5 месяца |
| 10 | $10^{-5}$ | 11000 паролей/сек | 5 дней |
| 11 | $10^{-6}$ | 12000 паролей/сек | 1 неделя |
| 12 | $10^{-7}$ | 10 паролей/день | 2 недели |
| 13 | $10^{-2}$ | 100 паролей/день | 3 недели |
| 14 | $10^{-3}$ | 1000 паролей/день | 1 месяц |
| 15 | $10^{-4}$ | 10000 паролей/день | 2 месяца |