ПРИМЕНЕНИЕ АДАПТИВНОСТИ В СИСТЕМАХ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Мажейко А.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – к.т.н.,доцент

Статья представляет собой обзор проблемы классических систем аутентификации пользователей, а также рассматривает предмет использования адаптивной аутентификации пользователей в информационных системах. Приводится авторский взгляд на достоинства и недостатки обоих подходов в аутентификации.

Классическая система аутентификации построена на принципе предоставления средству контроля разграничения доступа секретного либо оригинального ключа. В данном случае предполагается, что секретный ключ знает только легитимный пользователь, либо этот же пользователь обладает артефактом доступа, не предполагающим возможность воспроизведения копий и изготовления подделки. Практика показывает ненадежность использования пароля по двум основным причинам: слабая устойчивость ко взлому и компрометация фразы пользователем.

Слабая устойчивость объясняется большим набором требований, предъявляемых к вновь создаваемому паролю. Пользователи дабы избежать случая забыть пароль используют простые фразы и комбинации. Ежегодно составляются рейтинги самых взламываемых паролей. Таким образом в открытый доступ попадают наиболее часто встречаемые секретные фразы. Автор книги [1] утверждает, что 4 % паролей попадают в первые 100 самых используемых паролей (рисунок 1).

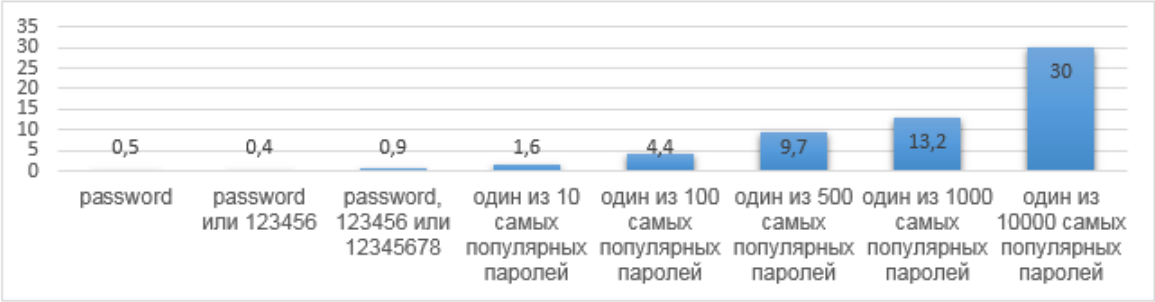

Рисунок 1 – Доли пользователей, использующих наиболее популярные пароли

Компрометация пароля также является частым явлением. В статистических данных [2] упоминается о нарушении правил конфиденциальности не менее чем у трети всех пользователей.

Разработчики систем защиты предлагают различные варианты решения данной проблемы. Один из способов – внедрение многофакторной аутентификации. По существу данный метод усложняет взлом системы, но не избавляет подход от ранее названных недостатков. Вводимые параметры как и ранее остаются статическими значениями. Поиск и внедрение динамических составляющих в процесс аутентификации представляется перспективным направлением развития.

В биометрии к динамическим параметрам относят поведенческие характеристики объекта. Здесь существует проблема повторного воспроизведения считываемых параметров. Неудачный выбор характеристик приведет к отказу в доступе. Доработка подобных систем привела исследователей к внедрению способности адаптации системы к считываемому субъекту.

Наиболее отличительной научной работой в данном направлении является диссертация Нестерука Ф.Г. [3]. Работа основана на применении нейронных сетей для аутентификации пользователя. В числе последних находится разработка система компании SABIGLOBAL. Компания позиционирует систему, обладающую самообучением на базе получаемого электромагнитного «отпечатка» структуры тела человека – реакции тела на излучение СВЧ- и КВЧ-диапазонов.

В соответствии с вышесказанным является перспективным разработка системы контроля доступа в виду необходимости подстройки механизма аутентификации под конкретного пользователя, отличающегося от существующих систем подходом считывания статических данных.

Список использованных источников:

14. XATO: Information Security by Mark Burnett[Электронный ресурс]. – Режим доступа: https://xato.net/10-000-top-passwords-6d6380716fe0. – Дата доступа: 24.06.2018.

15. Информационный портал ВЫБЕРИ!BY[Электронный ресурс]. – Режим доступа: https://viberi.by/news/banki/issledovanie_kazhdyj_tretij_polzovatel_seti_razglashaet_svoi_paroli. – Дата доступа: 12.01.2019.

16. Нестерук, Ф. Г. Разработка модели адаптивной системы защиты информации на базе нейро-нечеткихсетей :дис. канд. техн. наук : 05.13.19 / Ф.Г. Нестерук, – Санкт-Петербург, 2005. – 164 л.