ОБЗОР ХАРАКТЕРИСТИК И ПРИЗНАКОВ, ОПРЕДЕЛЯЮЩИХ ПОВЕДЕНИЕ ПОЛЬЗОВАТЕЛЯ ПК

Байдун Д.Р.

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

Насуро Е.В. – к.т.н., доцент каф. ЭВМ

Проблема надежной аутентификации пользователя компьютерной системы актуальна во всех сферах человеческой деятельности. Особое место среди средств аутентификации занимают биометрические методы, основанные на уникальности биометрической информации каждого человека. В данной работе рассматриваются характеристики и признаки уникальные для каждого отдельного пользователя компьютерной системы.

Любая система требует надежной защиты, и если от попыток взлома через интернет имеется богатый спектр антивирусных программ, то от взлома физического нас защищают пароли. Но существует шанс, что злоумышленник смог узнать пароль и тогда компьютер и все его данные остаются полностью беззащитными. Однако, каждый человек уникален – имеет свой темперамент, привычки и навыки. В связи с этим, биометрические данные каждого пользователя компьютерной системой будут различаться, как и используемое периферийное оборудование. Далее представлены характерные признаки, основываясь на которых, можно составить биометрический профиль каждого пользователя.

Характеристики и признаки:

1. Распознавание лица. Используя веб-камеру, можно сравнить картинку с камеры с сохраненной ранее.
2. Пароль. Проверка подлинности введенного пароля, количество неправильных попыток, скорость ввода пароля.
3. Действия пользователя при запуске системы. Например, сочетание запущенных программ, открытие определенных файлов и т.п.
4. Сочетания клавиш. Используются ли пользователем сочетания клавиш (например, ctrl+c или ctrl+v), либо используется только мышь/тачпад для выполнения команд. Аналогично с использованием клавиш панели NumLock.
5. Среднее время активности. Например, если это рабочий компьютер и среднее время его работы приходится на промежуток времени с 09.00 до 18.00, то будет подозрительна активность данного устройства в нерабочее время.
6. Отключение алгоритмов защиты компьютера (антивирусные программы, брандмауэр и т.п.).
7. Активность пользователя. Подразумевается время активности пользователя как в отдельно взятых программах, так и в определенных областях программ (например, хранилище паролей в браузерах).
8. Работа с программным обеспечением. Количество единовременно открытых копий программ, количество загруженных файлов из интернета и область работы данных файлов.
9. Внешние периферийные устройства. Название устройства, активность, область применения, мониторинг файлов, измененных данной активностью.
10. Клавиатурный почерк. Под данным термином, подразумевается несколько признаков присущих каждому пользователю: количество ошибок при наборе, интервалы между нажатиями клавиш, время удержания клавиш, число перекрытий между клавишами, степень аритмичности при наборе, скорость набора.
11. Жесты. Определенные движения мышью на рабочем столе и в отдельных программах.
12. Работа с мышью/тачпадом. Скорость и ритм клика в каждой отдельно взятой программе.

Представленные выше характеристики и признаки можно собрать у каждого пользователя ПК и хранить наравне с паролями. Подобная система не затребует дополнительного оборудования. Однако, для более высокой точности идентификации пользователя и минимизации ложных срабатываний, необходимы дальнейшие исследования и сбор информации для создания системы приоритетов для каждого отдельно взятого признака, для поиска возможной синергии и диссинергии между отдельными характеристиками, а также для создания самой системы защиты.

Список использованных источников:

1. А.В. Соколов. Защита информации в распределенных корпоративных сетях и системах / Соколов А.В., Шаньгин В.Ф. М.: ДМК Пресс, 2002. – 656 с.

2. Технологии биоидентификации и биометрический рынок / А. Евангели // PC Week/RE 2003, № 7. -- С. 24—25.

3. А.В. Еременко. Идентификационный потенциал клавиатурного почерка с учетом параметров вибрации и силы нажатия клавиши/ А.В. Еременко и др.. М.: Синергия, 2017. - 16 с.