# ПРИЗНАКИ И КРИТЕРИИ НЕСТАНДАРТНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ

*Байдун Д.Р.*

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

*Насуро Е.В. – канд. техн. наук, доцент*

Различные способы идентификации пользователей дают неравнозначные уровни защиты от несанкционированного доступа в систему. Использование комбинаций признаков, полученных при анализе действий пользователя, позволят повысить безопасность систем. Доклад содержит информацию о доступных для анализа характеристиках действий пользователя, сбор которых не требует установки дополнительного оборудования и основан на уже имеющихся аппаратных средствах. Методы машинного обучения позволяют получать персонализированные признаки, характерные для одного пользователя, которые невозможно подделать, так как их сбор проводится неявно в фоновом режиме.

**Признаки и характеристики.**

Ниже представлены признаки, которые рассматриваются в качестве значимых параметров при отслеживании действий пользователя для выявления аномального поведения.

1. Распознавание лица. Используя камеру устройства, можно сравнить изображение, сохраненное ранее с изображением, полученным в режиме реального времени [1].
2. Имя пользователя и пароль. Проверка подлинности введенного пароля. Надежность этого метода можно повысить, сократив количество неправильных попыток. Дополнительным критерием может выступать скорость ввода пароля [2].
3. Среднее время и расписание активности. Например, рабочие аккаунты, при необходимости, можно привязывать к режиму работы сотрудника. В остальное время использование служебных учетных записей можно ограничить.
4. Активность пользователя. Подразумевается время активности пользователя как в отдельно взятых программах, так и в определенных областях программ (например, хранилище паролей в браузерах, поисковые запросы, отключение алгоритмов защиты компьютера – антивирусных программ, брандмауэра). Например, операционные системы ведут наблюдения и предоставляют некоторую статистику [3]. Кроме того, можно использовать специализированные программы.
5. Работа с программным обеспечением. Пользователь зачастую имеет устоявшиеся привычки, касающиеся выбора определенных программ, количества единовременно открытых копий программы, количества и типа загруженных из интернета файлов и область работы данных файлов. Кроме того, начало работы характеризуется определенным набором действий – сочетанием запущенных программ, открытием определенных файлов и т.п.
6. Внешние периферийные устройства. Чтобы исключить внесение изменений в систему и средства защиты при помощи внешних устройств отслеживается ряд параметров: название устройства, активность, область применения, а также – мониторинг файлов, измененных при помощи периферийных устройств.
7. Клавиатурный почерк [4]. 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, привычные комбинации клавиш. Кроме того, сюда можно включить особенности работы с мышью/тачпадом. Скорость и ритм клика в каждой отдельно взятой программе.

**Коэффициенты критичности.**

В связи с разнородностью собираемых данных, а также, с учетом вариабельности некоторых характеристик, необходимо установить коэффициенты критичности критериев и определить уровень ошибок пользователя, при котором будет срабатывать система защиты. Кроме того, нужно предусмотреть разные способы идентификации пользователя при получении тревожных сигналов от системы защиты. В зависимости от комбинации допущенных пользователем ошибок, можно разработать разные реакции алгоритма – от повторного введения пароля или возвращения пользователя в область видимости камеры до полной блокировки системы и учетной записи пользователя с последующим обращением в службу безопасности предприятия.

***Список использованных источников:***

*[1] Face Recognition Performance Role of Demographic Information. IEEE Transactions On Information Forensics And Security, Vol. 7, No. 6, December 2012*

*[2] Electronic Authentication Guideline. National Institute of Standards and Technology, USA [Электронный ресурс] / Nist. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-63/ver-102/archive/2006-04-30. Дата доступа: 10.02.2021.*

*[3] Журнал действий Windows 10 и конфиденциальность [Электронный ресурс] / Microsoft. – Режим доступа: https://support.microsoft.com/ru-ru/windows/. Дата доступа: 19.01.2021.*

*[4] Нейросетевая идентификация типа личности человека по клавиатурному почерку. Т.В. Жашкова, О.М. Шарунова, Э.Ш. Исянова. Международный студенческий научный вестник. 2015. №3 Ч.1. С. 144-1462.*