



Асяев Г. Д., Рагозин А. Н.

ОПРЕДЕЛЕНИЕ МИНИМАЛЬНОГО НАБОРА ВХОДНЫХ ДАННЫХ ДЛЯ КОРРЕКТНОЙ АУТЕНТИФИКАЦИИ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

В статье проводится обзор биометрических динамических характеристик человека, параметров по которым будет происходить аутентификация по клавиатурному почерку. Экспериментальным образом определяется тип нейронной сети, который оптимально проводит операцию аутентификации по клавиатурному почерку, проводится экспериментальное исследование минимального количества входных данных на основе произвольного текста для корректного распознавания зарегистрированного пользователя. Определены границы параметров системы идентификации и их обоснование при практической реализации, выбран алгоритм распознавания на основе нейронной сети.

Ключевые слова: Безопасность, аутентификация, парольное слово, клавиатурный почерк, аудит, ошибки второго рода.

DETERMINATION OF THE MINIMUM SET OF INPUT DATA FOR CORRECT KEY-BASED AUTHENTICATION USING A NEURAL NETWORK

The article reviews the biometric dynamic characteristics of a person whose parameters will be used to authenticate using the keyboard handwriting. The type of the neural network is determined experimentally which optimally performs the authentication operation using the keyboard handwriting, an experimental study of the minimum amount of input data on the basis of arbitrary text is performed to correctly recognize the registered user. The boundaries of the parameters of the identification system and their justification for practical implementation are determined, and the recognition algorithm based on the neural network is chosen.

Keywords: Security, authentication, password, keyboard handwriting, audit, errors of the second kind.

Отождествление пользователя ЭВМ является первостепенной задачей при обеспечении информационной безопасности объекта. Это можно сделать как при помощи традиционной парольной защиты, так и при помощи проверки физических и психофизических параметров человека. В данной статье рассмотрена биометрическая система аутентификации, анализирующая динамический образ, который в свою очередь построен на анализе клавиатурного почерка.

Клавиатурный почерк - динамическая биометрическая характеристика, которую описывают: динамика и скорость ввода, частота возникновения ошибки. В ходе выполнения исследования было разработано программное обеспечение, которое регистрирует все характеристики, описанные выше. В качестве парольной фразы могут быть как несвязные по смыслу буквы (20 - 42), так и произвольно генерируемый текст. Данная система может находиться в 3 этапах: получение информации, обработка информации, разрешение или запрет на получение ресурсов пользователю на основе аутентификации. В ходе проведения эксперимента было написано программное обеспечение, которое регистрирует временные интервалы между нажатиями клавиш и направляет выходные данные программы на вход нейронной сети.

Использование нейронной сети для аутентификации было выбрано в связи с обла-

данием ряда преимуществ по сравнению с обычными статистическими моделями:

1. В силу физической и психической особенности человека невозможно получить одни и те же параметры клавиатурной аутентификации при одинаковых условиях. Именно применение нейронной сети делает систему устойчивой к отклонениям входных данных. Отсутствует необходимость в проведении предварительной обработки шумов входных данных.

2. В силу психического состояния человека нейронная сеть способна адаптироваться к изменениям в поведении и темпу набора парольной фразы на клавиатуре.

3. Нейронные сети обладают высоким быстродействием из-за параллелизма обработки информации.

Во время исследования рассматривалось 4 типа нейронной сети:

1. Нейронная сеть с прямым распространением сигнала и обратным распространением ошибки¹. В результате эксперимента выяснилось, что сеть успешно распознала всех пользователей. Неточность в определении пользователя определяется недостаточным выбором метрики нейронной сети с прямым распространением сигнала и обратным распространением ошибки и, как следствие, неправильное вычисление весовых коэффициентов. Данный тип нейронной сети корректно работает при количестве зарегистрированных пользователей до 20.

2. Самоорганизующаяся карта Кохонена¹. В ходе эксперимента выяснилось, что данный подход имеет существенный недостаток: аутентификация по клавиатурному почерку с помощью нейронной сети Кохонена возможна при обязательном использовании парольной защиты, либо другой аутентификации, исключающей доступ к ЭВМ незарегистрированных лиц. Исходя из этого основным применением данной сети является скрытый мониторинг информационных систем безопасности.

3. Иерархическая сеть. Максимальное количество пользователей при котором возможна корректная аутентификация, вследствие подчинённости иерархии, составило 50 человек.

4. Нейронная сеть, у которой количество входов равняется количеству выходов. В ходе проведённого эксперимента выяснилось, что она обладает достаточной устойчивостью и оптимально распознаёт зарегистрированных пользователей. Большим плюсом является большое количество пользователей при котором возможна корректная аутентификация.

В качестве алгоритма для идентификации пользователя применим нейронную сеть, у которой количество входов равняется количеству выходов. Функцией активации была выбрана единичная функция активации с жёстким ограничением. Она передаёт "1" на выход нейронной сети, который соответствует входным параметрам пользователя.

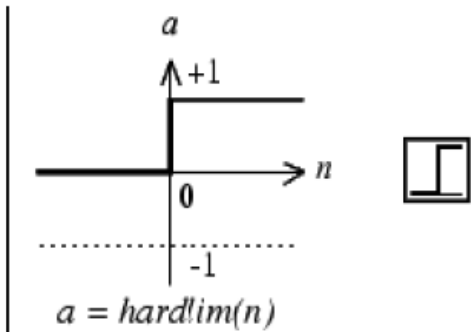


Рис. 1. Функция активации с жестким ограничением

Вычисление коэффициентов осуществляется по следующему принципу:

$$X_i = W X_i, \text{ где} \tag{1}$$

X_i – запомненные образы;

Весовые коэффициенты настраиваются один раз и больше не изменяются. Именно,

когда матрица весов удовлетворяет условию, описанному выше, X_i становится максимально устойчивым, что позволяет сети при попадании в такое состояние там и остаться².

Алгоритм работы сети³:

1. Каждое значение элемента вектора входа умножается на вес этого вектора W_{ij} ;
2. Полученные взвешенные элементы суммируются и подаются на вход функции активации;
3. Если на вход функции активации поступило $n > 0$, то нейрон возвращает 1;
4. Если на вход функции активации поступило $n < 0$, то нейрон возвращает 0.

Упрощённая модель нашей схемы представлена на рисунке.

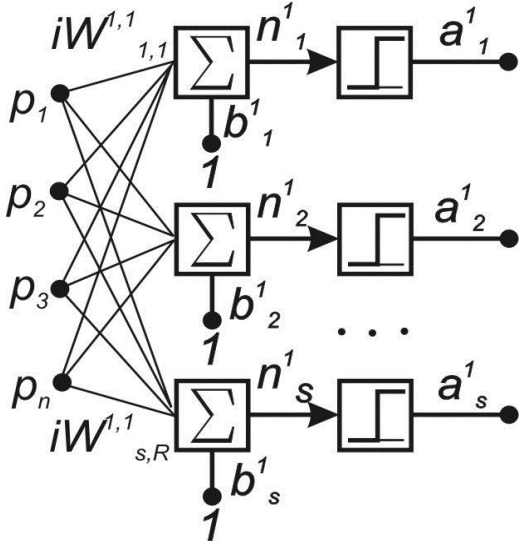


Рис.2. Упрощенная структура схемы

Каждому пользователю отведён свой выходной слой. Это позволяет исключить ошибки второго рода. Из каждого набора входных слоёв выбирается ровно один вектор, который и характеризует данный слой. При этом чем больше количество повторений временных интервалов для каждого субъекта при обучении, тем корректнее работает данная сеть². Вследствие того, что каждому входу соответствует ровно один выход, то количество зарегистрированных пользователей может быть больше 60. Данный тип нейронной сети хорошо применим для организаций с большим штатом сотрудников. Для данного алгоритма данные о количестве нажатий составляют 60% от общего массива данных, что является недопустимым для реализации в конечном программном продукте. Очевидно, что при уменьшении количества нажатий корректность идентификации будет умень-

шаться. Основной же задачей исследования является определить минимальное количество входных данных при котором пользователь будет корректно распознаваться для данной модели алгоритма с заданной точностью – 95%. Остальные 5% - психофизическое состояние человека. Параметры, влияющие на корректность идентификации:

1. Количество нажатий на клавиши;
2. Временной интервал между нажатиями клавиш;
3. Количество ошибок при наборе произвольного текста.

рода. При размере входных данных составляющем 13 символов – 25%, возникали ошибки второго рода. При размере входных сигналов составляющих 16 символов из 8 попыток идентификации все 8 были успешны.

В ходе проведения эксперимента был написан алгоритм распознавания пользователей по временному интервалу между нажатиям клавиш, определён минимальный набор входных данных при котором пользователь будет корректно распознаваться для нейронной сети у которой количество входов равняется количеству выходов. Исходя из результатов экспери-

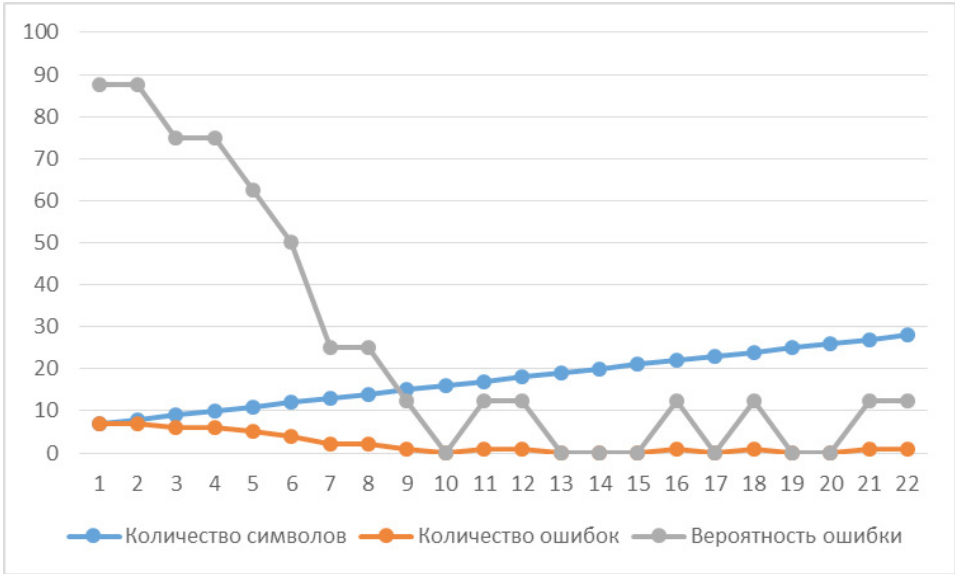


Рис. 3. График зависимости количества введенных символов от вероятности ошибки

В ходе проведения эксперимента было зарегистрировано 8 пользователей. Знаки пунктуации в произвольном тексте были исключены. При входном наборе равным 6 символов вероятность ошибки составила 87,9%, возникали ошибки как первого, так и второго

мента 16 символов парольной фразы является оптимальным количеством для успешной аутентификации. При меньшем наборе входных данных наблюдались ошибки первого и второго рода, а при количестве символов больше 16 наблюдается избыточность входных данных.

Примечания

1. Мищенко Е. Ю., Соколов А. Н. Количественный анализ процедуры обезличивания персональных данных. Метод перемешивания // Вестник УрФО. Безопасность в информационной сфере / № 3(21) / 2016, с. 30–37.
2. Хайкин С. Нейронные сети: полный курс. – М.: Вильямс, 2006. – С. 1104.

References

1. Mishchenko E. Yu., Sokolov A. N Quantitative analysis of the depersonalization procedure. Method of mixing//.Bulletin of the Ural Federal District Security in the Sphere of Information No. 3(21) / 2016, p. 30–37.
2. Haykin S. Neural networks: a full course. – М.: Williams, 2006. – P. 1104.

АСЯЕВ Григорий Дмитриевич, студент высшей школы электроники и компьютерных наук, кафедры “Защита информации” Южно-Уральского Государственного Университета. Россия, 454080, г.Челябинск, проспект Ленина, д 76. E-mail: asyaev1996@mail.ru

РАГОЗИН Андрей Николаевич, научный рук., кандидат технических наук, доцент кафедры «Защита информации», доцент кафедры инфокоммуникационных технологий ФГАОУ ВО «Южно-Уральский Государственный Университет» (Национальный исследовательский университет). Россия, 454080, г. Челябинск, проспект Ленина, д 76. E-mail: asyaev1996@mail.ru

ASYAEV Grigoriy Dmitrievich, Higher School of Electronics and Computer student of the Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: asyaev1996@mail.ru

RAGOZIN Andrey, scientific chief, Ph.D., Candidate of Technical Sciences, assistant professor of information security, assistant professor of information and communication technologies FGAOU «South Ural State University» (National Research University). Russia, 454080, Chelyabinsk, Prospekt Lenina, 76. E-mail: asyaev1996@mail.ru