www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.1.2

УДК 004.056.5:004.738.5
ББК 32.973я73

ОТДЕЛЬНЫЕ РЕЗУЛЬТАТЫ ПРИМЕНЕНИЯ ПРОГРАММНОГО СРЕДСТВА АУТЕНТИФИКАЦИИ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Юлия Денисовна Ермишева

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
ibb-191_442563@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Татьяна Александровна Омельченко

Старший преподаватель, кафедра информационной безопасности,
Волгоградский государственный университет
omelchenko.tatiana@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Процесс аутентификации пользователей в различных системах заслуживает особого внимания, когда речь идет о необходимости достоверного подтверждения прав доступа субъектов доступа к объектам доступа. Скорость распространения информационных потоков в современном обществе, переход к удаленному подключению к информационным системам и их использование во всех сферах жизни человека побуждают злоумышленников к поиску способов обхода методов, позволяющих отличать нужных пользователей системы от всех остальных. А значит, актуальной является задача повышения уровня надежности процесса аутентификации в предприятиях и организациях, за основу полноценного функционирования которых отвечает возможность предоставления удаленного доступа пользователей в информационные системы. Проведенный анализ существующих способов и методов аутентификации показал, что аутентификация, проводимая исключительно по единичному признаку не все-

гда может в достаточной степени подтвердить подлинность субъектов информационной системы, а значит, необходимо рассмотреть возможность построения модели двухфакторной аутентификации. В рамках проводимого исследования принято решение о разработке программного средства, реализующего модель двухфакторной аутентификации по парольной, как самой простой и распространенной, и биометрической (гарантирующей наиболее высокую точность по сравнению с другими существующими способами проверки идентичности) составляющим. Среди рассматриваемых методов биометрической аутентификации особое внимание было уделено клавиатурному мониторингу, направленному на решение задачи распознавания клавиатурного почерка и позволяющему способствовать построению подсистемы защиты информации в компьютерных системах при проведении процедур идентификации и аутентификации пользователей. Основным результатом, полученным при проведении экспериментального исследования применения разработанного программного средства, является ограничение возможности получения несанкционированного доступа к корпоративной информации за счет более точного распознавания аутентификационных признаков субъектов информационных систем.

Ключевые слова: биометрическая аутентификация, идентификация, клавиатурный почерк, защита информации, информационная система.

Предотвращение несанкционированного доступа в систему является важным элементом при поддержании целостности, доступности и конфиденциальности информации. Система защиты выполняет проверку подлинности на основе определенной уникальной информации, содержащей индивидуальные характеристики конкретного пользователя. Этот процесс получил название аутентификации [2].

Существует несколько методов аутентификации. Каждый предполагает свои ключевые особенности. Рассмотрим основные из них.

Парольная аутентификация подразумевает собой процедуру контроля подлинности пользователя, сравнивая введенный пароль (для соответствующего логина) с паролем, хранящимся в массиве данных. Основными плюсами парольной аутентификации являются простота и большая степень распространенности. Однако по совокупности характеристик этот вид аутентификации считается самым уязвимым средством проверки подлинности. По данным исследований Positive Technologies [3] большинство пользователей используют простые пароли, подробная статистика об используемых символах представлена в таблице.

Следующим методом аутентификации рассмотрим аутентификацию с помощью внешних носителей ключевой информации. Этот метод предполагает подключение к компьютеру носителя ключевой информации при каждой попытке авторизации в системе. Операционная система считывает с него идентификатор пользователя и соответствующий ему ключ. В таком случае идентификатор пользователя используется в качестве логина, а ключ – в качестве пароля.

Отдельный класс в иерархии методов аутентификации занимает аутентификация по биометрическим характеристикам. Проверка проходит по характеристикам присущим человеку, таким как отпечаток пальца, сканиро-

Суммарная статистика по используемым наборам символов в паролях

Набор используемых символов	Доля, %
Только цифры (numeric)	52,73
Символы английского алфавита в нижнем регистре (loweralpha)	17,96
Символы английского алфавита в нижнем регистре и цифры (loweralpha-numeric)	17,51
Символы английского алфавита в разных регистрах и цифры (mixalpha-numeric)	3,4
Символы английского алфавита в разных регистрах (mixalpha)	1,63
Символы английского алфавита в верхнем регистре и цифры (alpha-numeric)	1,35
Символы русского алфавита в нижнем регистре (loweralpha-rus)	1,12

вание сетчатки глаза, клавиатурному почерку, тембру голоса [1].

Так как однофакторная аутентификации обеспечивает низкий уровень защиты данных пользователей, рассмотрим наиболее сложный вариант аутентификации - двухфакторную аутентификацию. Подтверждение личности пользователя происходит путем проверки двух условий разных типов. Используем сочетание наиболее распространенной парольной аутентификации с биометрической, в качестве биометрической аутентификации рассмотрим клавиатурный почерк [5].

Клавиатурный почерк представляет собой динамику работы на клавиатуре, учитывая различные особенности работы с клавиатурой. Для аутентификации в системе разработаем программное средство, которое будет сочетать в себе два различных метода аутентификации [4].

Для обеспечения доступа к базе данных пользователей PhpMyAdmin подключен сервер, созданный при помощи программного обеспечения MAMP (рис. 1 и 2).

На следующем этапе разработки спроектированы формы для регистрации и авторизации в системе (см. рис. 3 и 4).

При регистрации считываются особенности работы на клавиатуре, запускается кейлоггер, пароль и логин заносятся в соответствующую базу данных. Аутентификация происходит по двум методам: сверки пароля и логина пользователя и проверки соответствия характеристик работе с клавиатурой, таких

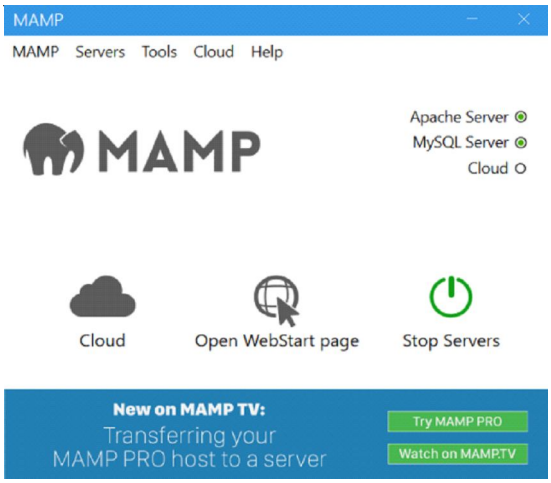

Рис. 1. Программное обеспечение MAMP для работы с локальным сервером базы данных

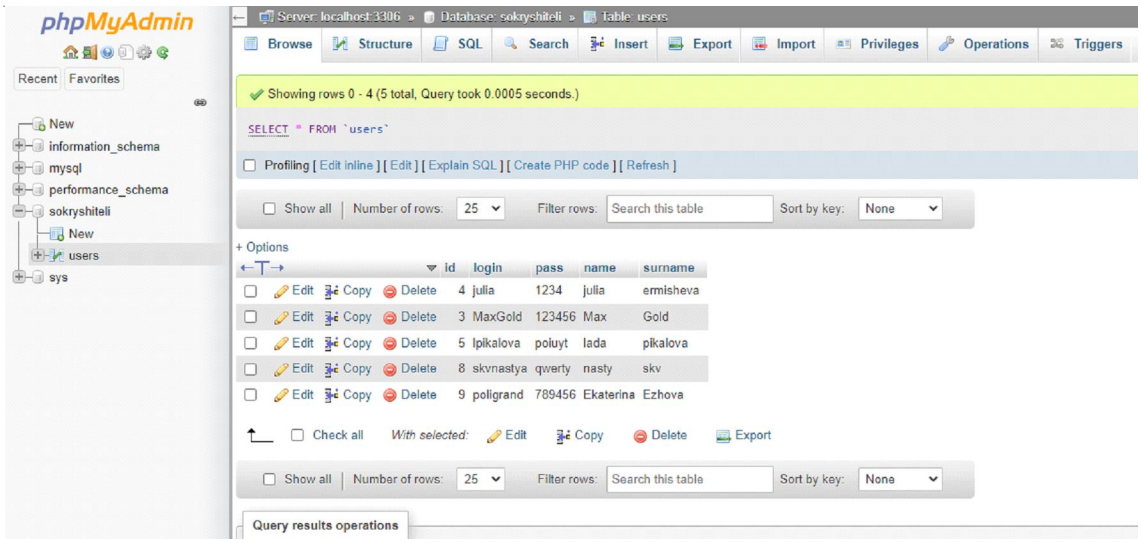

Рис. 2. База данных в web-режиме

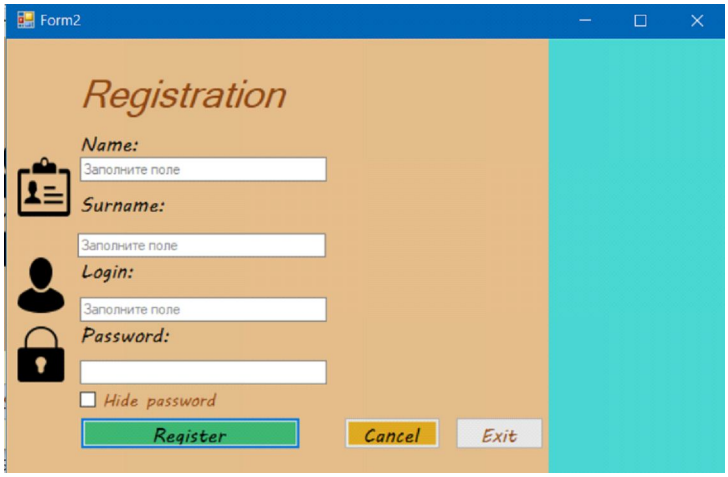

Рис. 3. Окно регистрации

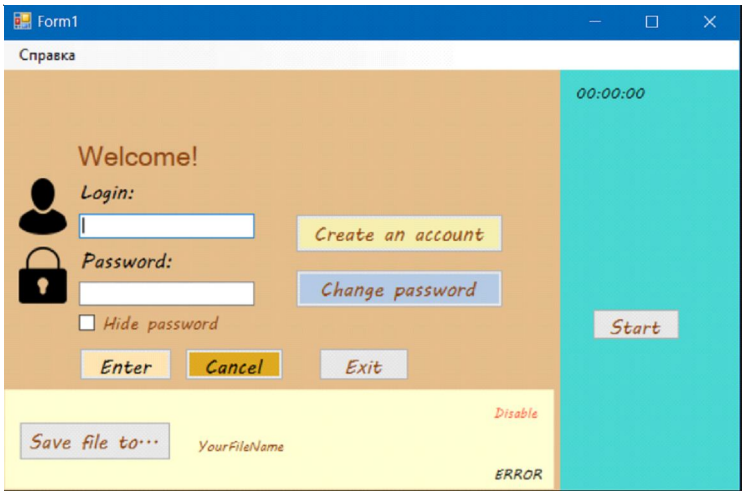

Рис. 4. Окно авторизации

как использование системных клавиш, скорость печати, а также отслеживается количество использований клавиши Backspace.

Для входа в систему проверяется соответствие логина и пароля, а также идентификация клавиатурного почерка пользователя, при успешной попытке входа получаем сообщение о прохождении аутентификации (рис. 5).

В противном случае пользователю будет отказано в доступе (см. рис. 6).

Основной результат, который достигается при использовании предложенного метода аутентификации, сочетающего в себе парольную и биометрическую составляющие, заключается в ограничении возможности получения несанкционированного доступа к корпоративной информации в случае компрометации логина и пароля злоумышленником за счет более точного распознавания аутентификационных признаков субъектов информационных систем.

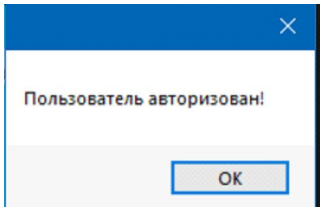

Рис. 5. Сообщение об успешной аутентификации

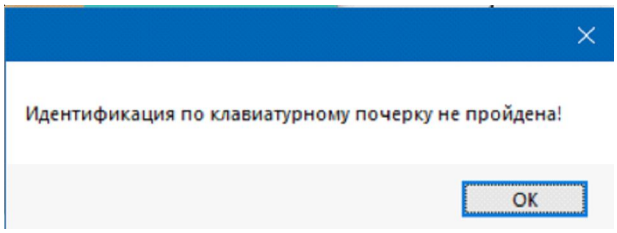

Рис. 6. Сообщение об ошибке при входе в систему

СПИСОК ЛИТЕРАТУРЫ

1. Биометрическая идентификация и аутентификация. Методы и технологии // Techportal.ru: Медийный портал отрасли безопасности. – Электрон. текстовые дан. – Режим доступа: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

2. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения // Электронный фонд правовой и нормативно-технической информации docs.cntd.ru. – Электрон. текстовые дан. – Режим доступа: https://docs.cntd.ru/document/1200172576

3. Евтеев, Д. Анализ проблем парольной защиты в Российских компаниях / Д. Евтеев // Positive Technologies – Vulnerability Assessment, Compliance Management and Threat Analysis Solutions. – Электрон. текстовые дан. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Metrics-Passwords-2009.pdf

4. Сидоркина, И. Г. Три алгоритма управления доступом к КСИИ на основе распознавания клавиатурного почерка оператора / И. Г. Сидоркина, А. Н. Савинов // Вестник Чувашского университета. – 2013. – № 3. – С. 293–301.

5. Яндиев, И. Б. Исследование временных характеристик клавиатурного почерка для быстрой аутентификации личности / И. Б. Яндиев // Молодой ученый. – 2017. – № 14 (148). – С. 154–158. – URL: https://moluch.ru/archive/148/41543/

REFERENCES

1. Biometricheskaja identifikacija i autentifikacija. Metody i tehnologii [Biometric Identification and Authentication. Methods and Technologies]. *Techportal.ru: Medijnyj portal otrasli bezopasnosti* [Techportal.ru: Security Industry Media Portal]. URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

2. GOST R 58833-2020 Zashhita informacii. Identifikacija i autentifikacija. Obshhie polozhenija [GOST R 58833-2020 Information Protection. Identification and Authentication. General Provisions]. *Elektronnyj fond pravovoj i normativno-tehnicheskoj informacii – docs.cntd.ru* [Electronic Legal and Regulatory Technical Information Fund – docs.cntd.ru]. URL: https://docs.cntd.ru/document/1200172576

3. Evteev D. Analiz problem parolnoj zashhity v Rossijskih kompanijah [Analysis of Password Protection Problems in Russian Companies]. *Positive Technologies – Vulnerability Assessment, Compliance Management and Threat Analysis Solutions*. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Metrics-Passwords-2009.pdf

4. Sidorkina I.G., Savinov A.N. Tri algoritma upravlenija dostupom k KSII na osnove raspoznavanija klaviaturnogo pocherka operatora [Three Algorithms for Controlling Access to KSII Based on Recognition of the Operator's Keyboard Handwriting]. *Vestnik Chuvashskogo universiteta* [Bulletin of the Chuvash University], 2013, no. 3, pp. 293-301.

5. Yandiev I.B. Issledovanie vremennyh harakteristik klaviaturnogo pocherka dlja bystroj autentifikacii lichnosti [Research of the Time Characteristics of Keystroke Dynamics for Quick Person Authentication]. *Molodoj uchenyj* [Young Scientist], 2017, no. 14 (148), pp. 154-158. URL: https://moluch.ru/archive/148/41543/

SEPARATE RESULTS OF THE APPLICATION OF THE SOFTWARE AUTHENTICATION TOOL BY KEYSTROKE DYNAMICS

Yulia D. Ermisheva

Student, Department of the Information Security,
Volgograd State University
ibb-191_442563@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Tatyana A. Omelchenko

Senior Lecturer, Department of the Information Security,
Volgograd State University
omelchenko.tatiana@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The process of user authentication in various systems deserves special attention when it comes to the need for reliable confirmation of access rights of access subjects to access objects. The speed of the spread of information flows in modern society, the transition to remote connection to information systems and their use in all spheres of human life encourage attackers to search for ways to bypass methods that allow distinguishing the right users of the system from all others. This means that the task of increasing the reliability of the authentication process in enterprises and organizations is urgent, the basis for the full functioning of which is the possibility of providing remote access to information systems for users. The analysis of existing authentication methods and processes has shown authentication has been carried out exclusively on a single basis cannot always sufficiently confirm the authenticity of the information system subjects, which means that it is necessary to consider the possibility of building a two-factor authentication model. Within the ongoing research, we decided to develop a software tool that implements a two-factor authentication model using a password (the simplest and most common method) and biometric (guaranteeing the highest accuracy compared to the other existing methods of identity verification) components. Among the considered methods of biometric authentication, special attention has been paid to keyboard monitoring, aimed at solving the problem of recognizing keystroke dynamics and allowing to contribute to the construction of a subsystem for information protection in computer systems during user identification and authentication procedures. The main result obtained during the experimental study of the application of the developed software tool is to limit the possibility of obtaining unauthorized access to corporate information due to a more accurate identification of the authentication of the subjects of information systems.

Key words: biometric authentication, identification, keystroke dynamics, data protection, information system.