УДК 004.056.53 **DOI: 10.18413/2518-1092-2024-9-1-0-4**

Храмов М.А.
Корнев Л.В.
Шабля В.О.

ФЕНОМЕНОЛОГИЧЕСКИЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ АУТЕНТИФИКАЦИИ

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
ул. Красина, 4, г. Краснодар, 350063, Россия

e-mail: khramov.m.a@yandex.ru

Аннотация
В статье рассмотрены методы аутентификации пользователей локальных вычислительных сетей и автоматизированных рабочих мест с целью определения наиболее актуальных способов противодействия внутренним нарушителям, использующих учетные данные других пользователей для входа в систему. Определяется угроза информационной безопасности, реализуемая внутренним нарушителем информационной безопасности различными способами, для последующего использования полученного доступа к учетным записям других пользователей, как плацдарма для реализации компьютерных атак. Методом экспертной оценки проведен сравнительный анализ методов аутентификации пользователей локальных вычислительных сетей и автоматизированных рабочих мест. Проведенный в работе сравнительный анализ позволяет сделать предположение, что противодействие вышеуказанной угрозе информационной безопасности, возможно за счет ввода в систему контроля и управления доступом операционной системы функциональных элементов, ответственных за выполнение процедуры аутентификации, с использованием методов биометрической аутентификации, основанной на динамике работы пользователя.
Ключевые слова: проблемы информационной безопасности; анализ средств защиты информации; биометрическая аутентификация
Для цитирования: Храмов М.А., Корнев Л.В., Шабля В.О. Феноменологический анализ существующих методов аутентификации // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 29-36. DOI: 10.18413/2518-1092-2024-9-1-0-4

Khramov M.A.
Kornev L.V.
Shablya V.O.

PHENOMENOLOGICAL ANALYSIS OF EXISTING AUTHENTICATION METHODS

Krasnodar Higher Military School named after Army General S.M. Shtemenko
4 Krasina str., Krasnodar, 350063, Russia

e-mail: khramov.m.a@yandex.ru

Abstract
The article discusses authentication methods for users of local area networks and automated workplaces in order to determine the most relevant ways to counter internal intruders using other users' credentials to log in. The threat to information security is determined, implemented by an internal information security violator in various ways, for subsequent use of the obtained access to the accounts of other users as a springboard for the implementation of computer attacks. A comparative analysis of authentication methods for users of local area networks and automated workplaces was carried out by the method of expert assessment. The comparative analysis carried out in the work suggests that countering the above-mentioned threat to information security is possible by introducing functional elements responsible for performing the authentication procedure into the operating system's access control and management system using biometric authentication methods based on the dynamics of the user's work.
Keywords: information security problems; analysis of information security tools; biometric authentication

For citation: Khramov M.A., Kornev L.V., Shablya V.O. Phenomenological analysis of existing authentication methods // Research result. Information technologies. – T. 9, №1, 2024. – P. 29-36. DOI: 10.18413/2518-1092-2024-9-1-0-4

ВВЕДЕНИЕ

В организациях, в которых принято решение о применении «Методики оценки угроз безопасности информации», утвержденной 5 февраля 2021 г. ФСТЭК России (далее – «Методика оценки угроз») для определения угроз безопасности информации, реализация которых возможна в информационных системах, определяются актуальные категории нарушителей, в зависимости от имеющихся прав и условий доступа к системам, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории: внутренних и внешних нарушителей. Выделяется тактика получения первоначального доступа к компонентам системы нарушителем, находящегося вне инфраструктуры, для использования их как плацдарма для дальнейших действий. Одной из техник достижения данной цели рассматривается несанкционированный доступ к защищаемым ресурсам за счет компрометации учетных данных легитимных пользователей [1, с. 67].

Противодействие угрозам безопасности информации, связанных с компрометацией учетных данных пользователей, осуществляется администраторами безопасности в соответствии с внутренними нормативными правовыми актами организации в области обеспечения безопасности информации. Методы борьбы с внутренними нарушителями, как правило, сводятся к выдаче долгосрочных паролей пользователям под личную подпись в соответствующем журнале учета выдачи, и к ознакомлению их с инструкцией по защите информации организации в вопросах, касающихся возложения на пользователей обязательств по неразглашению полученных учетных данных другим должностным лицам. Данный подход является организационным и позволяет обеспечить соблюдение принципа персональной ответственности пользователя за полученный им пароль, но не обеспечивает какого-либо предупреждения подобных случаев с технической стороны вопроса.

Как следствие, можно сделать объективный вывод, что существующий подход предоставления доступа пользователям к защищаемым ресурсам не отвечает требованиям модели угроз безопасности информации, в которой рассматривается наличие внутренних нарушителей. Реализация тактики получения доступа к защищаемым ресурсам сводится к легко исполнимой технике компрометации паролей учетных записей пользователей. Инструменты защиты информации, способных выявить подобный несанкционированный доступ отсутствуют, а организационных мер недостаточно.

В данной работе предлагается оценить возможные подходы к решению данной проблемы, основываясь на выводах предыдущих исследований, а именно – для повышения доверия к среде функционирования взаимодействующих субъектов и объектов доступа операционной системы возможно использовать тот же подход, что и в отношении подсистем, выполняющих функции авторизации. Архитектура операционных систем реализует выполнение функции авторизации несколькими модулями. Предлагается ввести в систему дополнительный компонент, ответственный за выполнение процедуры аутентификации, как и диспетчер учетных записей безопасности операционных систем.

ФЕНОМЕНОЛОГИЧЕСКИЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Классифицировать методы аутентификации можно по факторам, используемых в методах аутентификации для проверки подлинности пользователя.

Выделяют следующие типы аутентификационной информации:

1. Фактор знания — наиболее распространенный вид аутентификации, который требует от пользователя знания некоторой информации.

1.1. Постоянные пароли — тип аутентификационной информации, который остаётся постоянным и не изменяется на протяжении определенного периода времени или до изменения пользователем.

1.2. Одноразовые пароли — временные и одноразовые пароли или коды, которые генерируются и используются для однократной аутентификации пользователя при входе в систему.

1.3. Графические пароли — тип аутентификационной информации, требующий от пользователя создать пароль не путем ввода символов или цифр, а путем выбора определенных изображений или паттернов на экране устройства.

1.4. Секретные вопросы — реализация фактора знания, характеризуемая тем, что при проверке подлинности пользователя, ему предъявляются определенные вопросы, на которые только он должен знать ответы [2, с. 2].

2. Фактор владения — вид аутентификации, который требует от пользователя иметь физическое устройство или объект, такой как ключ, смарт-карта, токен или мобильное устройство, для подтверждения своей подлинности. Так же необходимо наличие аппаратно-программные системы идентификации и аутентификации [2, с. 3].

2.1. Ключи и карты доступа — пользователь имеет физический объект, такой как ключ или карта доступа, который используется для получения доступа к системе или учетной записи.

2.2. Устройства аутентификации — это могут быть устройства типа токенов, смарт-карт, USB-ключей или мобильных устройств, которые генерируют одноразовые пароли или подтверждения для прохождения аутентификации.

2.3. Беспроводные устройства аутентификации — например, Bluetooth-устройства, которые автоматически аутентифицируют пользователя при нахождении в определенной зоне доступа.

2.4. Устройства с технологией NFC — такие устройства могут быть использованы для аутентификации пользователя на основе его физического присутствия и владения устройством.

3. Биометрический фактор — вид аутентификации, который использует уникальные физиологические или поведенческие характеристики пользователя.

3.1. Статические характеристики биометрической аутентификации — физиологические особенности или параметры, которые остаются постоянными у человека и могут быть использованы для его идентификации.

3.1.1 По отпечатку пальца — вид аутентификации, при котором индивидуальные физиологические особенности отпечатков пальцев пользователя используются для его аутентификации в системе.

3.1.2. По кисти руки — метод аутентификации пользователя с использованием уникальных биометрических характеристик руки, таких как геометрия ладони, длина пальцев, расстояния между суставами и другие особенности.

3.1.3. По сетчатке глаза — метод аутентификации человека на основе уникальных характеристик сосудистой сетчатки глаза. Уникальные особенности сетчатки, такие как узор сосудистой сетчатки и другие анатомические особенности, используются для создания уникального биометрического шаблона каждого человека.

3.1.4. По радужной оболочке глаза — метод аутентификации человека на основе уникальных особенностей радужной оболочки глаза. Используя особенности радужной оболочки, можно создать уникальный биометрический шаблон для аутентификации человека.

3.1.5. По форме лица — метод аутентификации человека на основе уникальных морфологических особенностей его лица. При данном методе биометрии сканируется лицо человека с помощью специальных камер или устройств, и на основе уникальных особенностей формы лица создается биометрический шаблон, который может быть использован для проверки пользователя.

3.1.6. По ДНК — метод идентификации человека на основе уникальной генетической информации, которая хранится в ДНК (дезоксирибонуклеиновой кислоте) каждого человека. ДНК содержит уникальные генетические характеристики, которые индивидуальны для каждого человека, за исключением идентичных близнецов. Используемые в настоящее время методы

получения и обработки ДНК – работают настолько долго, что такие системы используются только для специализированных экспертиз, в связи с чем, данный метод не будет рассматриваться в последующей анализе [3, с. 4].

3.2. Динамические характеристики биометрической аутентификации пользователя включают в себя физиологические или поведенческие аспекты, которые могут быть измерены и использованы для подтверждения аутентификации пользователя.

3.2.1. По рукописному почерку — метод аутентификации человека, основанный на уникальных особенностях его почерка, то есть стиля и способа написания текста от руки. Каждый человек имеет индивидуальные черты в своем почерке, такие как размер, форма и углы букв, интервалы между словами, давление пера и т. д., которые могут быть использованы для аутентификации личности.

3.2.2. По клавиатурному почерку — метод аутентификации пользователя на основе уникального образца нажатия клавиш на клавиатуре компьютера или устройства во время ввода текста.

3.2.3. По жестам управления на сенсорном экране — метод аутентификации человека на основе уникальных особенностей его жестов, совершаемых на сенсорном экране устройства.

3.2.4. По голосу — метод аутентификации личности на основе уникальных характеристик голоса человека.

3.2.5. С использованием системы акселерометров — метод аутентификации личности на основе уникальных характеристик движений и поведения пользователя, которые могут быть измерены с помощью акселерометра, устройства, способного измерять ускорение и изменения скорости движения объекта [4, с. 61].

3.2.6. С использованием биоэлектрических сигналов человека — метод аутентификации личности на основе уникальных электрических сигналов (электрокардиограмма, электроэнцефалограмма), которые генерируются человеческим организмом [5, с. 87].

4. Другие факторы.

4.1. С использованием поручителей — это метод аутентификации пользователей, при котором для подтверждения личности пользователя требуется участие третьей стороны, называемой поручителем или гарантом. Поручитель в данном случае является доверенным лицом или системой, которая выступает в качестве подтверждения личности пользователя [6, с. 114].

4.2. Аутентификация на основе блокчейна — метод аутентификации, который использует технологию блокчейна для проверки личности пользователя. Аутентификация на основе блокчейна основана на создании уникальной цифровой подписи, которая аутентификации пользователя. Пользователь создает свою цифровую подпись и сохраняет ее в блокчейне [7, с. 60].

4.3. Аутентификатор подлинности с использованием сертификатов, токенов и контрольных сумм [6, с. 112].

4.3.1. При аутентификации с использованием сертификатов, клиентский сертификат используется для подтверждения личности пользователя или устройства перед получением доступа к ресурсам.

4.3.2. При аутентификации с использованием токенов, пользователю может потребоваться ввести одноразовый код или использовать устройство для генерации токенов для подтверждения своей личности. Одним из преимуществ использования токенов, это возможность выдачи его пользователю на определенный срок или отзыв токена в связи с нарушением политики информационной безопасности.

4.3.3. При аутентификации с использованием контрольных сумм, сервер может сравнивать вычисленную контрольную сумму с ожидаемым значением для проверки целостности данных при передаче или хранении.

4.4. Цифровые отпечатки браузера — метод проверки подлинности пользователя, основанный на уникальных характеристиках и параметрах его веб-браузера. Каждый веб-браузер имеет уникальные характеристики, такие как версия браузера, операционная система, разрешение экрана,

установленные шрифты и т.д., которые могут быть использованы для создания цифрового отпечатка браузера [8, с. 103].

Объективно, аутентификационные данные, основанные на факторах «знания» и «владения» должны быть основой в вопросах допуска пользователей к защищаемым ресурсам информационных систем, что и соответствует текущему положению дел. Однако, все способы аутентификации, основанные на вышеуказанных факторах, не позволяют противодействовать внутреннему нарушителю требований информационной безопасности организации. У легитимного пользователя есть техническая возможность передать аутентификационные данные злоумышленнику.

В вопросах борьбы с вышеописанными внутренними нарушителями особыми преимуществами обладают биометрические способы аутентификации, а именно: неподдельность, надежность, удобство, сложность реализации атак, долгосрочное использование аутентификационной информации. Так же существует и ограничение со стороны регулятора, а именно, необходимость использования биометрического фактора только совместно с другими факторами аутентификации [9, с. 13].

В связи с вышеизложенным, предлагается сравнить между собой методы биометрической аутентификации, с целью решения проблемы с отсутствием инструментов технического контроля пользователей на факт компрометации своих учетных данных.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ

Сравнение характеристик методов биометрической аутентификации проводится по пяти основных группам характеристик, актуальных в вопросах противодействия внутреннему нарушителю требований информационной безопасности. Для выбора рассматриваемых характеристик и ранжирования степени их проявления использовался метод экспертной оценки. Оценка каждой характеристики производилась независимо от совокупности используемых методов аутентификации. Каждой характеристике соответствующих методов аутентификации были присвоены значения исходя из степени проявления: 0 – низкая степень проявления; 0,5 – средняя степень проявления; 1 – высокая степень проявления.

Таблица

Сравнение характеристик методов биометрической аутентификации

Table

Comparison of characteristics of biometric authentication methods

Характеристики / Способы реализации	Стоимость реализации	Удобство использования	Мониторинг действий пользователя	Точность распознавания	Масштабируемость
Отпечатки пальцев	0,5	1	0	1	0,5
По кисти руки	0	1	0	1	0
По сетчатке глаза	0	0	0	1	0
По радужной оболочке глаза	0	0,5	0	1	0,5
По форме лица	0,5	1	0,5	1	0,5
По рукописному почерку	0,5	0,5	0,5	0,5	0,5
По клавиатурному почерку	1	1	1	0,5	1

Характеристики / Способы реализации	Стоимость реализации	Удобство использования	Мониторинг действий пользователя	Точность распознавания	Масштабируемость
По жестам управления на сенсорном экране	1	1	1	0,5	1
По голосу	0,5	0,5	0	0,5	0,5
С использованием системы акселерометров	0	1	0,5	0,5	0,5
С использованием биоэлектрических сигналов человека	0	0	0	0,5	0

Стоимость реализации биометрических методов аутентификации пользователей включает в себя все расходы, связанные с внедрением и использованием биометрических технологий для идентификации и аутентификации пользователей, и включает в себя: Стоимость оборудования, Стоимость программного обеспечения, техническую поддержку, настройку системы.

Удобство использования биометрических методов аутентификации пользователей характеризуется скоростью взаимодействия и отсутствием выполнения дополнительных действий со стороны пользователя.

Мониторинг действий пользователя при использовании биометрических методов аутентификации пользователей представляет собой процесс отслеживания и анализа поведения пользователей в системе, и является ключевым фактором выбора в работе наиболее подходящего метода противодействия внутреннему нарушителю.

Точность распознавания при использовании биометрических методов аутентификации пользователей отражает способность системы биометрической идентификации точно идентифицировать пользователя на основе его биометрических данных.

Масштабируемость при использовании биометрических методов аутентификации пользователей отражает сложность реализации метода на всех объектах организации, подлежащих защите.

Экспертной оценке подвергалось большинство перечисленных методов биометрической аутентификации, несмотря на неприменимость некоторых к использованию в системе защиты информации локальных вычислительных сетей и автоматизированных рабочих мест.

Исходя из оценки можно сделать вывод, что для работы со статической биометрической аутентификационной информацией требуется установка дополнительного оборудования, обеспечивающее однозначную аутентификацию пользователя. Однако, если рассматривать уже имеемую систему защиту информации в большинстве организаций и требования нормативных правовых актов в области информационной безопасности, большей актуальностью обладает стратегия внедрения способов биометрической аутентификации по поведенческим признакам человека, ввиду их доступности за счет программной реализации, и за счет ориентированности на постоянный мониторинг работы пользователя и подтверждение его соответствия заявленному идентификатору. Такими качествами обладает аутентификация по динамике работы пользователя с клавиатурой и сенсорным экраном.

В действительности, сенсорные экраны не являются основным способом взаимодействия пользователя с информационной системы, но, в свою очередь, аутентификация по динамике работы с клавиатурой обладает недостатками, а именно, она не дает один однозначный результат, в связи с тем, что зависит от многих свойств. Но, в качестве реализации многофакторной аутентификации пользователя, с фокусом на постоянный мониторинг легитимности пользователя, поведенческая

биометрическая аутентификация, основанная на анализе клавиатурного почерка пользователя, наиболее подходящий вектор развития системы аутентификации, как компонента системы контроля и управления доступом операционных систем локальных вычислительных сетей и автоматизированных рабочих мест.

ВЫВОДЫ

Сравнительный анализ методов аутентификации пользователей подтвердил преимущество методов биометрической аутентификации, основанных на динамических характеристиках пользователей, в системе защиты информации, где данные методы реализованы в качестве дополнительного фактора аутентификации, сфокусированных на обеспечении постоянного мониторинга действий пользователя и периодической проверки соответствия пользователя заявленной паре идентификатора и аутентификационной информации, предъявленной при авторизации в системе.

Необходимым свойством динамической биометрической аутентификации для построения данной модели системы защиты информации является невозможность компрометации аутентификационной информации пользователем, нарушающего требования безопасности информации организации, другим должностным лицам.

Проведенный в работе сравнительный анализ позволяет предположить, что для противодействия тактике реализации угроз информационной информации внутренних нарушителей, которая сводится к использованию чужих учетных данных, как плацдарма для реализации угроз в информационной системе, а именно, за счет ввода в систему контроля и управления доступом операционной системы функциональных элементов, ответственных за выполнение процедуры аутентификации, с использованием методов биометрической аутентификации, основанной на динамике работы пользователя.

Список литературы

1. Методический документ. Методика оценки угроз безопасности информации [Электронный ресурс]: утв. ФСТЭК России 05.02.2021 // URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g // (дата обращения: 03.03.2024).
2. Комеков Э.А. Системы аутентификации // Вестник науки и образования. 2022. № 1. С. 1-4.
3. Сидоркина И.Г. Классификация методов аутентификации человека // Вестник Волжского университета им. В.Н. Татищева. 2009. № 1. С. 1-6.
4. Корякова В.А. Аутентификация пользователя смартфона на основе данных, полученных с акселерометра // Прикаспийский журнал: управление и высокие технологии. 2023. № 61(1). С. 59-72.
5. Кураков В.И. Анализ уязвимостей биометрических методов аутентификации // Международный научный журнал «Вестник науки». 2022. № 5(50). С. 87-98.
6. Вишняков В.А. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2016. № 3(97). С. 111-114.
7. Посметухова К.Н. Обзор и краткий анализ современных методов аутентификации // Наука и реальность. 2023. № 2(14). С. 58-62.
8. Осин А.В. Обзор методов идентификации пользователя на основе цифровых отпечатков // Труды учебных заведений связи. 2023. № 5. С. 91-111.
9. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения.

References

1. Methodological document. Methodology for assessing information security threats [Electronic resource]: approved by FSTEC of Russia 05.02.2021 // URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g // (accessed: 03/03/2024).
2. Komekov E.A. Authentication systems // Bulletin of Science and Education. 2022. No. 1. pp. 1-4.

3. Sidorkina I.G. Classification of human authentication methods // Bulletin of the V.N. Tatishchev Volga State University. 2009. No. 1. pp. 1-6.

4. Koryakova V.A. Smartphone user authentication based on data obtained from the accelerometer // Caspian Journal: Management and high technologies. 2023. No. 61(1). pp. 59-72.

5. Kurakov V.I. Vulnerability analysis of biometric authentication methods // The international scientific journal "Bulletin of Science". 2022. No. 5(50). pp. 87-98.

6. Vishnyakov V.A. Models and means of user authentication in corporate management systems and cloud computing // Reports of the Belarusian State University of Informatics and Radioelectronics. 2016. No. 3(97). pp. 111-114.

7. Posmetukhova K.N. Review and brief analysis of modern authentication methods // Science and reality. 2023. No. 2(14). pp. 58-62.

8. Osin A.V. Review of user identification methods based on digital fingerprints // Proceedings of educational institutions of communications. 2023. No. 5. pp. 91-111.

9. GOST R 58833-2020 Information protection. Identification and authentication. General provisions.

Храмов Максим Андреевич, аспирант кафедры информационной безопасности
Корнев Лев Викторович, аспирант кафедры информационной безопасности
Шабля Владимир Олегович, аспирант кафедры информационной безопасности

Khramov Maxim Andreevich, postgraduate student of the Department of Information Security
Kornev Lev Viktorovich, postgraduate student of the Department of Information Security
Shablya Vladimir Olegovich, postgraduate student of the Department of Information Security