Информатика и вычислительная техника
Informatics and computer engineering

Научная статья
УДК 62; 004; 007
DOI: 10.14529/ctcr220301

ПРИМЕНЕНИЕ МЕТОДА ИДЕАЛЬНОЙ ТОЧКИ ДЛЯ ПОИСКА НАИЛУЧШЕГО СПОСОБА АУТЕНТИФИКАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

О.В. Логиновский[1], *loginovskiyo@mail.ru*
М.Е. Коваль[1], *kovalmax06@gmail.com*
А.А. Шинкарев[2], *sania.kill@mail.ru*

[1] *Южно-Уральский государственный университет, Челябинск, Россия*
[2] *ООО «Софтмаст-ИТ», Челябинск, Россия*

Аннотация. В современном мире все популярнее становятся различные информационные системы, в том числе и корпоративные. Многие из таких систем хранят конфиденциальные данные своих пользователей. В основном эти данные защищены только логином и паролем, которые на сегодняшний день уже не могут обеспечить высокий уровень безопасности и гарантировать сохранность эти данных. Одновременно с развитием информационных систем развиваются методы и инструменты, с помощью которых злоумышленники могут завладеть конфиденциальной информацией. Довольно часто появляются новости о том, что какая-либо из крупных компаний допустила утечку личных данных пользователей. И для того чтобы минимизировать возможности для компрометации пользовательских данных, стоит более тщательно подходить к выбору способа аутентификации пользователей в системе. **Цель исследования.** Используя математический подход, определить наиболее подходящий способ аутентификации в корпоративных информационных системах с учетом определенных критериев. **Материалы и методы.** Рассматриваются такие виды аутентификации, как: аутентификация на основе многоразового пароля, TOTP (Time-based one-time password authentication), аутентификация на основе SMS, аутентификация на основе биометрии, OpenID, SAML (Security Assertion Markup Language). Используется метод построения множества Парето и определение с помощью метода идеальной точки наиболее предпочтительного для реализации метода аутентификации. **Результаты.** В статье авторами приводится описание рассматриваемых способов аутентификации, описание алгоритма их работы и диаграммы взаимодействия. С помощью метода идеальной точки было определено, что наиболее подходящим способом аутентификации является SAML.

Ключевые слова: аутентификация, корпоративные информационные системы, TOTP, SAML, SMS-аутентификация, биометрия, метод идеальной точки, множество Парето

Для цитирования: Логиновский О.В., Коваль М.Е., Шинкарев А.А. Применение метода идеальной точки для поиска наилучшего способа аутентификации в корпоративных информационных системах // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2022. Т. 22, № 3. С. 5–18. DOI: 10.14529/ctcr220301

Original article
DOI: 10.14529/ctcr220301

USING THE IDEAL POINT METHOD TO SEARCH THE BEST AUTHENTICATION METHOD IN CORPORATE INFORMATION SYSTEMS

O.V. Loginovskiy[1], *loginovskiyo@mail.ru*
M.E. Koval[1], *kovalmax06@gmail.com*
A.A. Shinkarev[2], *sania.kill@mail.ru*
[1] *South Ural State University, Chelyabinsk, Russia*
[2] *LLC "Softmast-IT", Chelyabinsk, Russia*

Abstract. Nowadays, various information systems, including enterprise ones, are becoming increasingly popular. Many of these systems store sensitive data of their users. Basically, this data is protected only by a login and a password, which today can no longer provide a high level of security and guarantee the safety of the data. Along with the development of information systems, methods and tools that attackers can use to get hold of confidential information are also evolving. It is not uncommon to hear news that some of the large companies have leaked its users' personal data. So, in order to minimize the risk of compromising user data, it is worth taking a more careful approach to selecting a method of authenticating users in the system. **Aim.** To determine the most appropriate method of authentication in enterprise information systems with the help of a mathematical approach and taking into account certain criteria. **Materials and methods.** The following types of authentication were considered: reusable password authentication, TOTP (Time-based one-time password authentication), SMS-based authentication, biometric authentication, OpenID, SAML (Security Assertion Markup Language). The Pareto set method and the ideal point method were used to determine the most preferable authentication method to implement. **Results.** In the article, the authors describe the authentication methods considered, the algorithm of their work, and diagrams of their interaction. Using the ideal point method, SAML was determined to be the most appropriate authentication method.

Keywords: authentication, enterprise information systems, TOTP, SAML, SMS authentication, biometrics, ideal point method, Pareto set

For citation: Loginovskiy O.V., Koval M.E., Shinkarev A.A. Using the ideal point method to search the best authentication method in corporate information systems. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2022;22(3):5–18. (In Russ.) DOI: 10.14529/ctcr220301

Введение

В настоящее время информационные технологии стали неотъемлемой частью жизни людей. Распространены социальные сети, облачные хранилища, интернет-магазины, мессенджеры и другие онлайн-сервисы, которые так или иначе хранят персональные данные пользователей. Можно выделить такие чувствительные к утечкам персональные данные, как имя, номер телефона, адрес, дату рождения и банковские реквизиты. С ростом количества информационных сервисов, которым пользователи доверяют персональные данные, растет и риск того, что эти данные будут украдены, ведь они дублируются в нескольких местах, на каждое из которых можно осуществлять хакерскую атаку. Поэтому сегодня на первый план выходит вопрос обеспечения безопасности персональных данных, равно как и их прозрачности размещения. Кража информации грозит серьезными последствиями как для компании, которая предоставляет сервис, так и для пользователей, чьи данные были украдены. Для компаний ситуация с компрометированием персональных данных скорее всего обернется судебными разбирательствами, финансовыми издержками и подрывом репутации, а для пользователей тем, что злоумышленники смогут воспользоваться, например, банковскими данными и перевести денежные средства пользователя на свои счета.

Нельзя забывать и о том, что зачастую пользователи информационных систем (ИС) имеют низкую грамотность в вопросе информационной безопасности данных. Пользователи не знают, как и где хранятся их данные, например информация об оплате онлайн-покупок хранится на сто-

роне банка и онлайн-магазин не имеет к ней доступа. Еще одной проблемой, которая объясняется низкой информационной грамотностью, является использование одного пароля для аккаунтов в различных системах. Если у пользователя везде одинаковый пароль, злоумышленник, украв пароль и логин от почты, получает доступ ко всем сервисам пользователя и может совершать противоправные действия, например покупки или переводы денежных средств. В таком случае непричастность пользователя к этим действия будет довольно сложно доказать для возврата собственных денег. Тяжело отследить и продажу данных в даркнете. Все это делает необходимым повышение уровня безопасности систем, хранящих личные данные.

В связи с возрастающей ценностью персональных данных на черном рынке и расширением возможностей по извлечению из них выгоды злоумышленниками необходимо обеспечить информационную безопасность. Обеспечить информационную безопасность ИС – создать такую систему защиты, которая позволит защитить доступ к секретной информации системы и исключить возможные попытки взлома злоумышленниками. Для повышения защиты информационной системы пользователю требуется пройти идентификацию, аутентификацию и авторизацию.

На сегодняшний день существует большое количество способов аутентификации в информационных системах. К ним относятся аутентификация с использованием многоразового пароля, аутентификация по SMS, аутентификация на основе географического положения, аутентификация на основе биометрических данных, SAML, TOTP, OpenID и другие. В данной статье будет рассмотрено 6 наиболее распространенных подходов:

1) аутентификация на основе многоразового пароля;
2) TOTP (Time-based one-time password authentication);
3) аутентификация на основе SMS;
4) аутентификация на основе биометрии;
5) OpenID;
6) SAML (Security Assertion Markup Language).

1. Понятие аутентификации и ее факторы

Для минимизации возможности компрометации персональных и коммерческих данных и обеспечения их конфиденциальности требуется ограничить к ним доступ. Другими словами, требуется использование механизмов, которые бы позволяли однозначно понять, кто запросил доступ к информации, и определить, что это именно тот пользователь, за которого он себя выдает. Такие механизмы называются идентификация и аутентификация соответственно. Идентификация – это процедура распознавания пользователя по его личному идентификатору (например, логину). Эта функция выполняется при попытке пользователя войти в сеть. Аутентификация – процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор [1].

С развитием информационных систем происходит и развитие способов для осуществления несанкционированного доступа к данным, поэтому требуется постоянное улучшение механизмов аутентификации для ее защиты.

В любой системе аутентификации обычно можно выделить несколько элементов:

1) субъект (subject), который будет проходить процедуру аутентификации;
2) характеристика субъекта (subject characteristic) – отличительная черта;
3) владелец системы аутентификации (authentication system owner), несущий ответственность и контролирующий её работу;
4) механизм аутентификации (authentication mechanism), то есть принцип работы системы;
5) механизм управления доступом (access control mechanism), предоставляющий определенные права доступа субъекту.

Все субъекты обладают определенным характеристиками, использование которых в системе зависит от требуемой надежности, защищенности и стоимости внедрения. В зависимости от используемых характеристик субъекта выделяют три фактора аутентификации:

1) нечто, что нам известно, например, какая-либо секретная информация;
2) нечто, чем мы обладаем, например, какой-либо уникальный физический объект;
3) нечто, что является неотъемлемой частью нас самих – биометрика.

Существует однофакторная и многофакторная аутентификация (MFA, Multi Factor Authentication) на основе двух и более факторов. Многофакторная аутентификация, осуществляется с использованием двух и более факторов. При этом следует разделять факторы и шаги аутентификации. Шаги аутентификации являются составными частями факторов, например, если для аутентификации необходимо ввести два пароля, то это аутентификации на основе одного фактора. На примере методов аутентификации, рассматриваемых в данной статье, выявляются различия между шагами и факторами аутентификации.

Например, метод на основе SMS следует относить к однофакторной аутентификации, но с двумя шагами, поскольку пароль для SMS генерируется на стороне сервера. TOTP, с другой стороны, относится к двухфакторной, так как генерация пароля происходит при помощи специального приложения на смартфоне пользователя, что усложняет задачу доступа злоумышленников к этой информации. В этом заключаются различия в понятиях фактора и шага аутентификации [2–4].

2. Типы аутентификации

2.1. Аутентификация на основе многоразового пароля

Почти в любой информационной системе необходимо пройти процедуру идентификации. Обычно для этого используются логин и пароль. Во время процедуры аутентификации сопоставляются пароль, введенный пользователем, и значение, которое хранится на сервере. Аутентификация при помощи паролей – наиболее распространенный вид аутентификации. Главный недостаток этого типа аутентификации состоит в том, что если злоумышленник владеет чужим паролем, то может выдавать себя за другого пользователя. На рис. 1 изображена схема аутентификации пользователя на основе пароля на сервере [5–6].

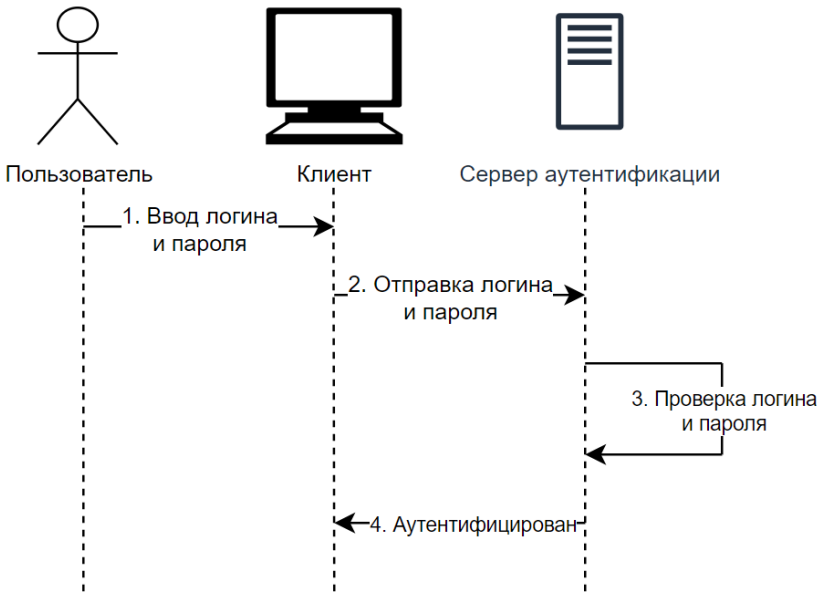

Рис. 1. Схема аутентификации на основе многоразового пароля
Fig. 1. Authentication scheme based on a reusable password

2.2. TOTP (Time-based one-time password algorithm)

TOTP – алгоритм создания одноразовых паролей для защищенной аутентификации. Является алгоритмом односторонней аутентификации – сервер удостоверяется в подлинности клиента.

При использовании для двухфакторной аутентификации метода на основе TOTP одноразовый пароль генерируется на стороне пользователя через приложение для смартфона. Это значит, что пользователь всегда имеет доступ к одноразовому паролю. А также избавляет сервер от необходимости отправлять текстовое сообщение при каждом входе в систему. Также стоит отметить, что сгенерированный пароль через определенный промежуток времени меняется, что делает его, по сути, одноразовым [7, 8].

Для реализации двухфакторной аутентификации с использованием TOTP необходимо учитывать основное требование – пароль должен создаваться на стороне пользователя, а также по-

стоянно изменяться. На рис. 2 изображена диаграмма, демонстрирующая процесс аутентификации на основе TOTP.

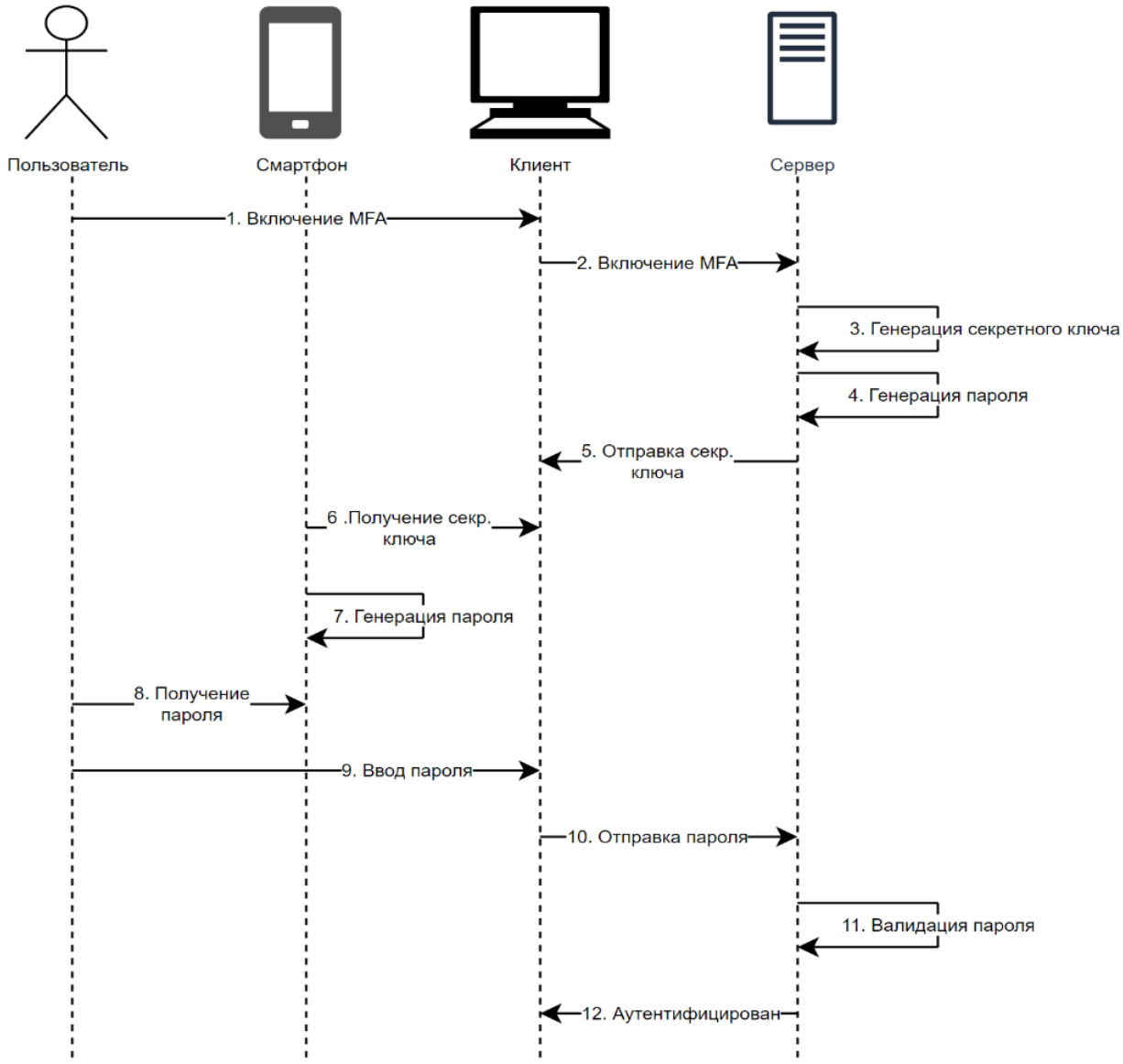

Рис. 2. Аутентификация с использованием TOTP
Fig. 2. Authentication using TOTP

Шаги такого типа аутентификации выглядят так.

1. Пользователь включает многофакторную аутентификацию (MFA) в системе.
2. Клиент передает запрос на включение MFA серверу.
3. Сервер создает секретный ключ для конкретного пользователя.
4. Сервер генерирует пароль на основе времени и секретного ключа.
5. Сервер передает секретный ключ пользовательскому клиенту.
6. Секретный ключ добавляется в телефонное приложение.
7. Телефонное приложение генерирует одноразовый пароль, используя ключ и время.
8. Пользователь получает пароль из приложения.
9. Пользователь вводит пароль.
10. Клиент передает введенный пароль на сервер.
11. Сервер сравнивает введенный пароль со сгенерированным.
12. Если пароли совпадают, то пользователь считается аутентифицированным.

2.3. Аутентификация на основе СМС

Из названия данного типа аутентификации ясно, что при таком способе используется одноразовый пароль, который пользователь получает по СМС на свой телефон. На рис. 3 изображена диаграмма процесса аутентификации на основе СМС.

Рис. 3. Аутентификация на основе СМС
Fig. 3. SMS-based authentication

Данный способ осуществляется с помощью таких шагов.

1. Пользователь вводит свой номер телефона.
2. Номер телефона передается на сервер.
3. Сервер генерирует одноразовый пароль.
4. Сервер отправляет пароль на телефон пользователя в СМС.
5. Пользователь вводит полученный пароль на сайте.
6. Пароль передается на сервер.
7. Сервер сравнивает созданный им пароль с пришедшим.
8. Если пароли совпадают, то пользователь считается аутентифицированным.

Этот способ удобен тем, что пользователю не нужно придумывать и запоминать сложный пароль, снижаются трудозатраты на разработку системы аутентификации, так как не нужно реализовывать методы валидации пароля, а также способы восстановления пароля.

Однако такой подход имеет и значительные минусы с точки зрения безопасности. Во-первых, установленным на смартфон пользователя вредоносным ПО может перехватить сообщение с кодом. Во-вторых, имели место случаи с подкупом сотрудника салона сотовой связи с целью выпуска новой sim-карты с номером телефона жертвы. Наконец, код из SMS можно просто подсмотреть и передать злоумышленнику [9, 10].

2.4. Аутентификация на основе OpenID

OpenID – открытый стандарт децентрализованной системы аутентификации, предоставляющей пользователю возможность создать единую учетную запись для аутентификации на множестве не связанных друг с другом интернет-ресурсов, используя услуги третьих лиц. Это означает,

что системы могут проверять подлинность пользователей от имени приложения через такие сервисы, как Google, Microsoft, Facebook, Twitter, ВКонтакте и т. д.

Есть множество преимуществ такой системы аутентификации: многие пользователи уже имеют профили в различных социальных сетях, пользователи могут использовать двухфакторную аутентификацию, и вы не должны управлять учетными записями пользователя в приложении.

Если говорить коротко, OpenID позволяет входить на множество сайтов, используя один аккаунт провайдера, например профиль в социальной сети Facebook или Google. Например, когда пользователь заходит на сайт, как показано на рис. 4, ему предоставляется выбор провайдера, после чего он перенаправляется на сайт этого провайдера и вводит свои учетные данные. Если он успешно проходит аутентификацию у провайдера, провайдер возвращает сайту успешный OpenID пользователя и после этого его аутентифицируют в своем приложении [11, 12].

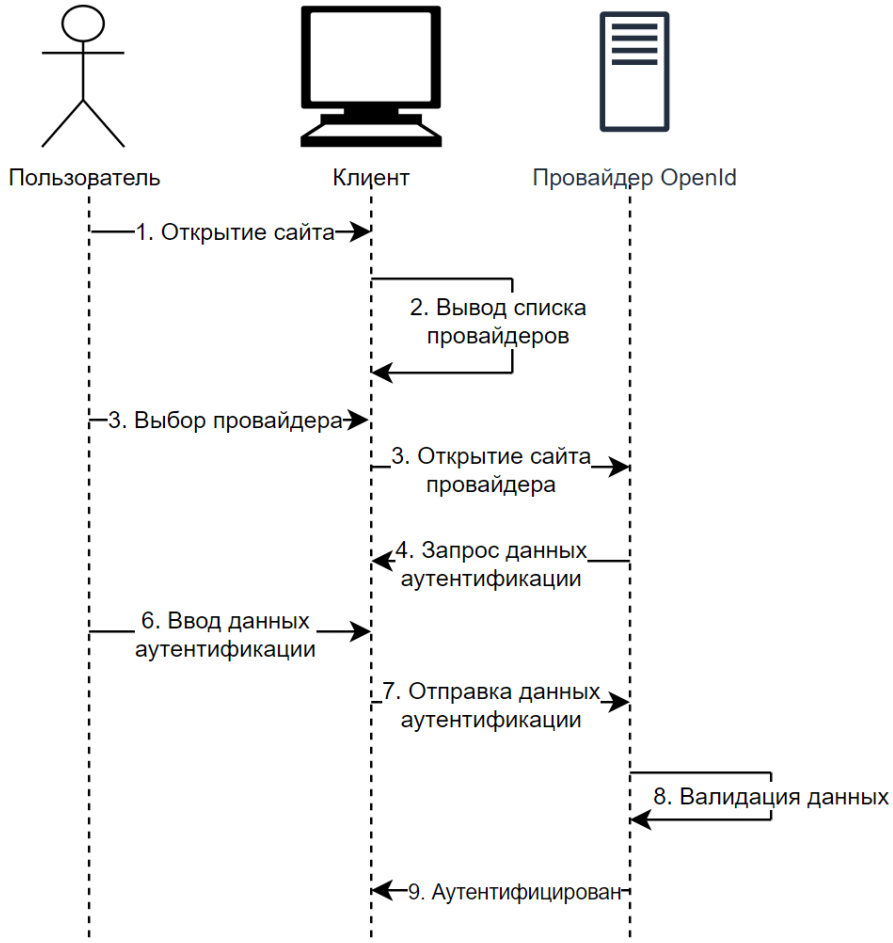

Рис. 4. Аутентификация на основе OpenID
Fig. 4. OpenID-based authentication

При OpenID-аутентификации выполняются следующие шаги.

1. Пользователь открывает сайт в браузере (клиент).
2. На сайте отображается форма с возможностью выбора провайдера для аутентификации (например, Google или VK).
3. Пользователь выбирает провайдера.
4. Открывается сайт провайдера аутентификации с формой.
5. Пользователь заполняет форму с необходимыми данными для аутентификации.
6. Клиент отправляет данные аутентификации провайдеру.
7. Провайдер проверяет корректность введенных данных (например, логин и пароль).
8. Если данные валидны, то пользователь считается аутентифицированным.

2.5. Аутентификация на основе биометрических данных

Для пользователей такой тип аутентификации особенно удобен, так как не требуется запоминать пароли и так далее. Биометрические системы аутентифицируют пользователей, используя их анатомические данные.

В настоящее время методы биометрической аутентификации делятся на два класса:

1) статические методы, основанные на физиологических характеристиках человека, находящихся при нём в течение всей его жизни, и которые нельзя потерять, украсть и скопировать;

2) динамические методы, основанные на поведенческих характеристиках людей.

В процессе биометрической аутентификации эталонный образец биометрических данных и пользовательский сравнивают с учетом установленной ранее погрешности. Погрешность подбирается для установления оптимального соотношения двух основных характеристик биометрической аутентификации:

1) FAR (False Accept Rate) – коэффициент ложного принятия;

2) FRR (False Reject Rate) – коэффициент ложного отказа.

FAR и FRR измеряются в процентах и должны быть минимальны. Биометрическая система аутентификации должна позволять настроить коэффициент FAR до 0,01–0,001 % при FRR около 3–5 %.

В общем виде данный тип аутентификации схож с аутентификацией на основе многоразового пароля, только в роли пароля здесь выступают биометрические данные пользователя.

Биометрическая аутентификация имеет свои плюсы и минусы. Например, использование отпечатков пальцев наиболее удобно для пользователей, но существует вероятность подделки отпечатка пальца. Еще одним недостатком такого типа аутентификации является высокая стоимость необходимого оборудования. Стоит отметить, что биометрию чаще используют для идентификации, а аутентифицируется пользователь с помощью пароля [13, 14].

2.6. Аутентификация на основе SAML

SAML – сокращение от Security Assertion Markup Language (язык разметки декларации безопасности). Этот подход позволяет проходить процедуру аутентификации только с одним набором нужных данных. SAML производит обмен аутентификационной информацией в определенном формате между системой управления доступами и веб-приложением.

SAML обменивается пользовательской информацией между системой управления доступами и поставщиком услуг. Это упрощает и увеличивает уровень безопасности аутентификации, так как пользователю необходимо только единожды пройти аутентификацию. Таким образом, когда пользователь запрашивает доступ к сайту, SAML передает аутентификационные данные поставщику услуг, который впоследствии предоставляет доступ пользователю [15, 16].

Процесс аутентификации SAML изображен на рис. 5.

Для SAML-аутентификации необходимо выполнение следующих этапов.

1. Пользователь открывает браузер (клиент).
2. Клиент запрашивает требуемый сайт.
3. Сервер приложения отвечает SAML-запросом.
4. Браузер передает SAML-запрос системе управления доступами.
5. Система управления доступами (СУД) обрабатывает SAML-запрос.
6. Система управления доступами запрашивает логин, пароль или какой-либо другой фактор аутентификации.
7. Введенные данные отправляются на сервер системы управления доступами.
8. Система управления доступами проверяет корректность введенных данных.
9. Система управления доступами генерирует SAML-ответ.
10. СУД отправляет SAML-ответ обратно в браузер пользователя.
11. Браузер отправляет сгенерированный SAML-ответ серверу сайта для проверки.
12. Сервер проверяет ответ.
13. Если проверка прошла успешно, веб-приложение предоставляет доступ пользователю.

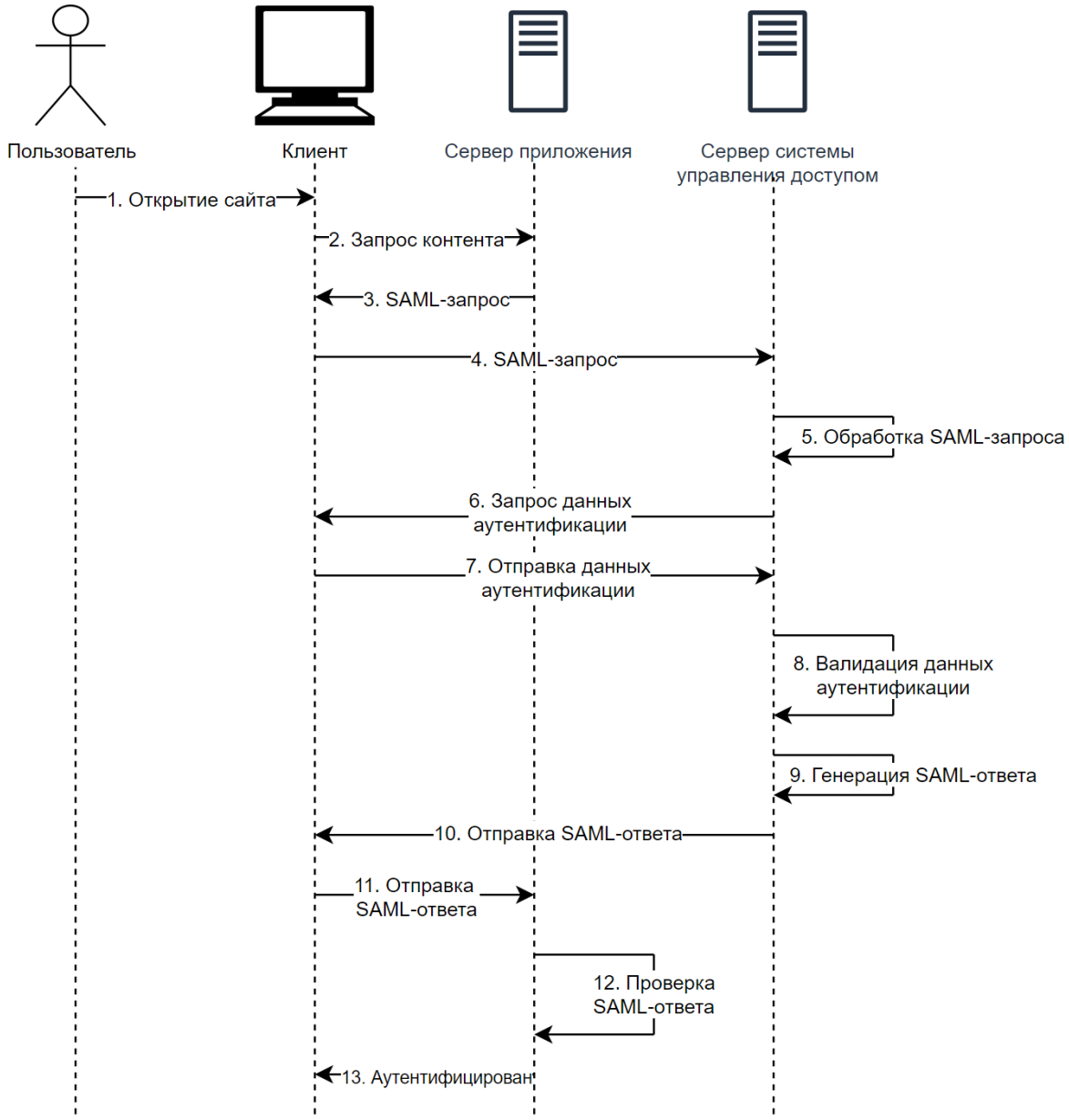

Рис. 5. Аутентификации на основе SAML
Fig. 5. SAML-based authentication

3. Анализ методов аутентификации по критериям и определение наиболее безопасных и рекомендуемых типов аутентификации

Для исследования типов аутентификации предлагается использовать следующие критерии.

1. Низкая стоимость внедрения (k_1) – включает в себя время и ресурсы, необходимые для внедрения аутентификации в систему.

2. Простота реализации (k_2) – отражает возможность интегрировать систему аутентификации в уже работающую информационную систему.

3. Уровень безопасности (k_3) – показатель, отражающий возможность взлома системы или использования чужих аутентификационных данных.

4. Возможность возникновения ошибок (k_4) – может ли система допустить ошибку при аутентификации, например, разрешить доступ злоумышленнику вместо реального пользователя.

5. Зависимость от сторонних сервисов (k_5).

6. Необходимость использования дополнительного оборудования (k_6).

В табл. 1 представлено сравнение способов аутентификации по выбранным критериям. Для простоты будем считать, что для оценки критериев k_1, k_2, k_3, k_4 была использована десятибалльная шкала. Так как для оценки критериев k_5 и k_6 не может быть использована такая шкала, применяются следующие значения: 0 – нет, 1 – да. При этом стоит учитывать, что для этих критериев 0 является более предпочтительным вариантом выбора.

Таблица 1

Сравнение способов аутентификации по выбранным критериям

Table 1

Comparison of authentication methods according to selected criteria

Способ аутентификации	Критерии оценки					
	k_1	k_2	k_3	k_4	k_5	k_6
Многоразовый пароль (f_1)	8	8	3	0	0	0
TOTP (f_2)	5	6	7	0	0	0
СМС (f_3)	2	7	6	1	0	1
Биометрия (f_4)	9	0	9	1	0	1
OpenID (f_5)	6	2	8	0	1	0
SAML (f_6)	8	3	8	0	1	0

Ввиду того, что ни один из рассматриваемых способов аутентификации не обладает только лишь высокими оценками по критериям, необходимо выбрать математические методы, применив которые к данным, можно получить наиболее предпочтительный для реализации способ аутентификации.

Поскольку необходимо на основе нескольких критериев выделить только один способ аутентификации, то эту задачу стоит относить к задачам многокритериального выбора. Ее решение заключается в отыскании множества Парето, которое может состоять из одного элемента, но в общем случае оно является подмножеством множества возможных решений. Если имеется конечное число альтернатив $f_1,...,f_6$, то для получения множества Парето необходимо вектор $C(f_i)$ сравнить с другим вектором $C(f_k)$, то есть определить справедливость неравенства $C(f_i) \geq C(f_k)$. Если это неравенство выполняется, то альтернатива f_k не может быть оптимальной по Парето [17, 18].

Проанализировав таким образом все возможные пары альтернатив и исключив альтернативы, которые не являются парето-оптимальными, получим множество Парето, из которого можно выбрать наиболее предпочтительный способ аутентификации.

1. Сравниваем f_1 с альтернативами $f_2,...,f_6$ по отношению $\geq$. Неравенство $C(f_1) \geq C(f_k)$ не выполняется ни для одной из альтернатив, поэтому на данном шаге ни одна из альтернатив не исключается.

2. Далее сравниваем f_2 с альтернативой f_1 и $f_3,...,f_6$. Неравенство $C(f_2) \geq C(f_k)$ не выполняет ни для одного из вариантов, поэтому на этом шаге также никакой вариант не исключается.

3. Сравниваем f_3 и другие альтернативы. Данная альтернатива не лучше остальных альтернатив по критерию k_1, поэтому невозможно исключить какой-либо вариант.

4. Сравниваем f_4 с остальными альтернативами. Для этой альтернативы неравенство $C(f_4) \geq C(f_k)$ не выполняется.

5. На этом этапе сравниваем альтернативу f_5. Для данной альтернативы условие $C(f_5) \geq C(f_k)$ не выполняется.

6. Последней сравниваем альтернативу f_6 с оставшимися альтернативами. В данном случае альтернатива f_6 более предпочтительна, чем альтернатива f_5.

Таким образом, после сравнения альтернатив получаем множество Парето из альтернатив f_1, f_2, f_3, f_4, f_6.

После того как было сформировано множество Парето, следует выделить наиболее предпочтительный вариант аутентификации, для этого можно использовать метод идеальной точки. Точка *a* называется идеальной, если она оптимальна сразу по всем критериям. Как правило, такой точки не существует, но для каждой реальной альтернативы можно определить расстояние до идеальной точки [19] и выбрать ту, для которой это расстояние минимально. Метод идеальной точки сводит исходную многокритериальную задачу к решению обычной однокритериальной задачи.

В нашем случае идеальным объектом следует считать альтернативу, которая имеет следующие оценки критериев: $k_1 = 10, k_2 = 10, k_3 = 10, k_4 = 0, k_5 = 0, k_6 = 0$. В табл. 2 отображены наиболее подходящие альтернативы, а также идеальный и наихудший по критериям объекты.

Таблица 2

Множество Парето. Идеальный и наихудший объекты

Table 2

Lots of Pareto. Ideal and worst objects

Способ аутентификации	Критерии оценки					
	k_1	k_2	k_3	k_4	k_5	k_6
Многоразовый пароль (f_1)	8	8	3	0	0	0
TOTP (f_2)	5	6	7	0	0	0
СМС (f_3)	2	7	6	1	0	1
Биометрия (f_4)	9	0	9	1	0	1
SAML (f_6)	8	3	8	0	1	0
Лучшая альтернатива a^+	10	10	10	0	0	0
Худшая альтернатива a^-	0	0	0	1	1	1

Для сопоставления разнородных значений критериальных параметров разных альтернатив необходимо выполнить процедуру нормирования по формуле $x_{ij} = \frac{a_j^+ - a_{ij}}{a_j^+ - a_j^-}$, где a_j^+ – значение *j*-го критерия лучшей альтернативы, a_{ij} – исходное значение *j*-го критерия *i*-й альтернативы, a_j^- – значение *j*-го критерия худшей альтернативы. Нормированные значения критериев рассматриваемых альтернатив представлены в табл. 3.

Таблица 3

Нормированные значения критериев рассматриваемых альтернатив

Table 3

Normalized values of the criteria of the considered alternatives

Способ аутентификации	Критерии оценки					
	k_1	k_2	k_3	k_4	k_5	k_6
Многоразовый пароль (f_1)	0,2	0,2	0,7	0	0	0
TOTP (f_2)	0,5	0,4	0,3	0	0	0
СМС (f_3)	0,8	0,3	0,4	1	0	1
Биометрия (f_4)	0,1	0	0,1	1	1	1
SAML (f_6)	0,2	0,7	0,2	0	0	0

После нормировки значений критериев необходимо определить расстояние от каждой из альтернатив до идеальной альтернативы. Для этого воспользуемся формулой $L(f_i) = \sqrt{\sum_{j=1}^{n} a_{ij}^2}$, где

a_{ij} – исходное значение *j*-го критерия *i*-й альтернативы. В табл. 4 представлены расстояния альтернатив до идеального объекта.

Таблица 4

Расстояния альтернатив до идеального объекта

Table 4

Distances of alternatives to the ideal object

Альтернатива	f_1	f_2	f_3	f_4	f_6
Расстояние до идеального объекта	0,75	0,7	1,7	1,73	0,57

Как видно из табл. 4, кратчайшее расстояние до идеального объекта у альтернативы f_6, значит, в соответствии с проведенными расчетами наиболее предпочтительным типом аутентификации является аутентификация с использованием SAML-технологии.

Заключение

В современных условиях развития информационных технологий все больше сервисов и систем хранят личные данные пользователей, а значит, растет вероятность кражи этих данных злоумышленниками. Для обеспечения сохранности данных применяются механизмы аутентификации.

Наиболее популярные методы аутентификации, такие как аутентификация на основе многоразового пароля, TOTP, аутентификация на основе биометрии и другие, были рассмотрены и описаны в рамках данной статьи.

Каждый из рассмотренных методов имеет свои плюсы и минусы, поэтому затруднительно выбрать лучший метод. Для поиска наиболее предпочтительного метода аутентификации в информационных системах был предложен математический способ, основанный на определении множества Парето и применении метода идеальной точки. Был выделен набор критериев, по которым происходил отбор методов аутентификации. К этим критериям относятся: стоимость внедрения, сложность реализации, уровень безопасности, возможность возникновения ошибок, зависимость от сторонних сервисов, необходимость использования дополнительного оборудования.

После применения математической модели было установлено, что наиболее предпочтительным способом аутентификации является аутентификация на основе SAML. К плюсам такой аутентификации можно отнести высокий уровень безопасности, низкую возможность взлома, из минусов данного типа аутентификации можно выделить необходимость использования дополнительных сервисов и относительно высокое время на разработку. Но стоит обращать внимание на масштабы проекта, на уровень использования в нем чувствительных к краже данных, и исходя из этого выбирать способ аутентификации, который наиболее будет соответствовать требованиям системы.

Таким образом, в тех системах, которые хранят большие объемы персональных данных пользователей, рекомендуется применение аутентификации на основе SAML для обеспечения высокой степени защиты и снижения возможности компрометации персональных данных.

SAML – сокращение от Security Assertion Markup Language (Язык разметки декларации безопасности). Этот подход позволяет проходить процедуру аутентификации только с одним набором нужных данных. SAML производит обмен аутентификационной информацией в определенном формате между системой управления доступами и веб-приложением.

Список литературы

1. Chapman N., Chapman J. Authentication and Authorization on the Web. Edinburgh: MacAvon Media, 2012. 246 с.

2. Huang X., Robert J., Robert D. A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems // IEEE Transactions on Parallel and Distributed Systems. 2011. No. 22.

3. Lakshmi C. Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security // International Journal of Applied Engineering Research. 2018. No. 13.

4. Ometov A., Bezzateev S., Koucheryavy Y. Multi-Factor Authentication: A Survey // Cryptography. 2018. No. 2.

5. Teik Guan T., Szalachowski P., Zhou J. Securing Password Authentication for Web-based Applications // Networking and Internet Architecture. 2020. No. 1.

6. Fujita K., Hirakawa Y. A study of password authentication method against observing attacks // IEEE Xplore. 2008. No. 6.

7. Uymatiao M., Uymatiao Y. Time-Based OTP Authentication via Secure Tunnel (TOAST): A Mobile TOTP Scheme Using TLS Seed Exchange and Encrypted Offline Keystore // 2014 4th IEEE International Conference on Information Science and Technology. Shenzhen, 2014. P. 225–229.

8. Oluwakemi C. A Secured One Time Password Authentication Technique using Visual Cryptography Scheme // Journal of Physics. 2019. No. 8.

9. Balilo B., Vibar J. Authentication Key-Exchange Using SMS for Web-Based Platforms // Journal of Computer and Communications. 2020. No. 10.

10. Gwonsang R., Kim S., Choi D. Implicit Secondary Authentication for Sustainable SMS Authentication // Sustainability. 2019. No. 11.

11. Ma W., Ma S., Bak P. OpenID Connect as a Security Service in Cloud-based Diagnostic Imaging Systems // SPIE. Medical Imaging 2015 (International Society of Optics and Photonics). Orlando, 2015.

12. Khan R., Ylitalo J., Ahmed A. OpenID authentication as a service in OpenStack // 7th Int. Conf. Information Assurance and Security (IAS). Melacca, 2011. P. 372–377.

13. Bhattacharyya D., Bhattacharyya R., Rahul A. Biometric Authentication: A Review // International Journal of u- and e-Service, Science and Technology. 2019. No. 2.

14. Carmel V., Akila D. A survey on biometric authentication systems in cloud to combat identity theft // Journal of Critical Reviews. 2020. No. No. 7.

15. Lewis J. Web single sign-on authentication using SAML // IJCSI International Journal of Computer Science Issues. 2009. No. 2.

16. Armando A., Carbone R., Compagna L. Formal analysis of SAML 2.0 web browser single sign-on // Formal Methods in Security Engineering. 2008. No. 6.

17. Панкратова Н.Д., Опарина Е.Л. Формирование множества Парето в задачах поиска рационального компромисса // SAEC. 2020. № 1.

18. Подиновский В.В., Ногин В.Д. Парето-оптималльные решения многокритериальных задач. М.: Наука, 1982. 256 с.

19. Ланнэ А.А., Улахович Д.А. Многокритериальная оптимизация. СПб.: ВАС, 1984. 146 с.

References

1. Chapman N., Chapman J. Authentication and Authorization on the Web. Edinburgh: MacAvon Media; 2012. 246 p.

2. Huang X., Robert J., Robert D. A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems*. 2011;22.

3. Lakshmi C. Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security. *International Journal of Applied Engineering Research*. 2018;13.

4. Ometov A., Bezzateev S., Koucheryavy Y. Multi-Factor Authentication: A Survey. *Cryptography*. 2018;2.

5. Teik Guan T., Szalachowski P., Zhou J. Securing Password Authentication for Web-based Applications. *Networking and Internet Architecture*. 2020;1.

6. Fujita K., Hirakawa Y. A study of password authentication method against observing attacks. *IEEE Xplore*. 2008;6.

7. Uymatiao M., Uymatiao Y. Time-Based OTP Authentication via Secure Tunnel (TOAST): A Mobile TOTP Scheme Using TLS Seed Exchange and Encrypted Offline Keystore. In: *2014 4th IEEE International Conference on Information Science and Technology*. Shenzhen; 2014. P. 225–229.

8. Oluwakemi C. A Secured One Time Password Authentication Technique using Visual Cryptography Scheme. *Journal of Physics*. 2019;8.

9. Balilo B., Vibar J. Authentication Key-Exchange Using SMS for Web-Based Platforms. *Journal of Computer and Communications*. 2020;10.

10. Gwonsang R., Kim S., Choi D. Implicit Secondary Authentication for Sustainable SMS Authentication. *Sustainability*. 2019;11.

11. Ma W., Ma S., Bak P. OpenID Connect as a Security Service in Cloud-based Diagnostic Imaging Systems. In: *SPIE. Medical Imaging 2015 (International Society of Optics and Photonics)*. Orlando; 2015.

12. Khan R., Ylitalo J., Ahmed A. OpenID authentication as a service in OpenStack. In: *7th Int. Conf. Information Assurance and Security (IAS)*. Melacca; 2011. P. 372–377.

13. Bhattacharyya D., Bhattacharyya R., Rahul A. Biometric Authentication: A Review. *International Journal of u- and e-Service, Science and Technology*. 2019;2.

14. Carmel V., Akila D. A survey on biometric authentication systems in cloud to combat identity theft. *Journal of Critical Reviews*. 2020;7.

15. Lewis J. Web single sign-on authentication using SAML. *IJCSI International Journal of Computer Science Issues*. 2009;2.

16. Armando A., Carbone R., Compagna L. Formal analysis of SAML 2.0 web browser single sign-on. *Formal Methods in Security Engineering*. 2008;6.

17. Pankratova N.D., Oparina E.L. Formation of the Pareto Set in Problems of Searching for a Rational Compromise. *SAEC*. 2020;1. (In Russ.)

18. Podinovsky V.V., Nogin V.D. *Pareto-optimall'nyye resheniya mnogokriterial'nykh zadach* [Pareto-optimal solutions of multicriteria problems]. Moscow: Nauka; 1982. 256 p. (In Russ.)

19. Lanne A.A., Ulakhovich D.A. *Mnogokriterial'naya optimizatsiya* [Multicriteria optimization]. St. Petersburg: VAS; 1984. 146 p. (In Russ.)

Информация об авторах

Логиновский Олег Витальевич, д-р техн. наук, проф., заведующий кафедрой информационно-аналитического обеспечения управления в социальных и экономических системах, Южно-Южно-Уральский государственный университет, Челябинск, Россия; loginovskiyo@mail.ru.

Коваль Максим Евгеньевич, магистрант, Южно-Уральский государственный университет, Челябинск, Россия; kovalmax06@gmail.com.

Шинкарев Александр Андреевич, канд. техн. наук, инженер-программист, ООО «Софтмаст-ИТ», г. Челябинск, Россия; sania.kill@mail.ru.

Information about the authors

Oleg V. Loginovskiy, Dr. Sci. (Eng.), Prof., Head of Department of Informational and Analytical Support of Control in Social and Economic Systems, South Ural State University, Chelyabinsk, Russia; loginovskiyo@mail.ru.

Maksim E. Koval, Master's Student, South Ural State University, Chelyabinsk, Russia; kovalmax06@gmail.com.

Aleksandr A. Shinkarev, Cand. Sci. (Eng.), Software engineer, LLC "Softmast-IT", Chelyabinsk, Russia; sania.kill@mail.ru.

Статья поступила в редакцию 15.03.2022
The article was submitted 15.03.2022