Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

DOI: 10.37943/AITU.2020.89.25.011

B. Sultanova
Candidate of Pedagogical Sciences, Professor of the Department of Information and Computing Systems
bk.sultanova@mail.ru, orcid.org/0000-0003-1587-650X
Karaganda Technical University, Kazakhstan.

A. Chsherbov
Master student of the Department of Information Technology and Security
alexandr.chsherbov@gmail.com, orcid.org/0000-0003-4238-6389
Karaganda Technical University, Kazakhstan.

USING OF ADDITIONAL METHODS OF USER AUTHORIZATION

Abstract: The article considers the methods of additional authorization of users of information systems, their advantages, and disadvantages, typical examples of usage. Multifactor authentication is becoming a standard tool for verifying the identity and access rights of information systems, from banking operations to access to enterprise databases. With the expansion of the spheres of use of various information systems, applications, and services, users of the systems get new opportunities, convenience, and mobility. But at the same time, there is a problem of secure and controlled access, authorization and identification of the user, confirmation of his authority. The options under consideration cannot be limited to service delivery alone: mechanisms could and should be used in various combinations. In addition to the analysis, experiments were carried out on implementing and testing additional authorization mechanisms, and feedback from end users was collected. Each of the methods was evaluated from many angles: ease of implementation, ease of use by the end user, availability, and adequacy of use. At the same time, there is no way to identify the optimal and universal method of additional authorization, since various service sectors have their own requirements for accessibility, reliability, and security. One can single out corporate services that provide data exchange, data processing or analytics, or remote management services industrial network management as the most promising areas for implementation. The authors analyzed the various methods most widely used in the security market, their capabilities, advantages, and disadvantages. The authors did not set the goal of nominating one selected mechanism as a priority; therefore, no recommendations are given to use a particular method.

Keywords: Internet, encryption key, certificate, authorization.

DOI: 10.37943/AITU.2020.89.25.011

Султанова Б.К.
Кандидат педагогических наук, профессор кафедры информационно-вычислительных систем
bk.sultanova@mail.ru, orcid.org/0000-0003-1587-650X
Карагандинский Технический Университет, Казахстан.

Щербов А.С.
Магистрант кафедры информационных технологий и безопасности
alexandr.chsherbov@gmail.com, orcid.org/0000-0003-4238-6389
Карагандинский Технический Университет, Казахстан.

ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ МЕТОДОВ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Аннотация: Статья рассматривает методы дополнительной авторизации пользователей информационных систем, их достоинства и недостатки, типичные примеры использования. Мульти (много) факторная авторизация становится стандартным инструментом для подтверждения личности и прав доступа информационных систем, от банковских операций, до доступа к базам данных предприятия. С расширением сфер использования различных информационных систем, приложений и сервисов, пользователи систем получают новые возможности, удобство и мобильность. Но в то же время, возникает проблема безопасного и контролируемого доступа, авторизация и идентификация пользователя, подтверждение его полномочий. Авторы проанализировали различные методы, наиболее широко распространённые на рынке безопасности, их возможности, преимущества и недостатки. Рассматриваемые варианты не могут относиться только к одной лишь сфере предоставления услуг: механизмы могут и должны быть использованы в различных комбинациях. Помимо анализа, были проведены опыты по внедрению и тестированию механизмов дополнительной авторизации, собраны отзывы конечных пользователей. Каждый из методов был оценён со множества сторон: лёгкость внедрения, простота использования конечным пользователем, доступность и адекватность применения. В то же время нет возможности выявить оптимальный и универсальный метод дополнительной авторизации, поскольку различные сферы услуг предъявляют собственные требования к доступности, надёжности и безопасности. Как наиболее перспективные направления для внедрения, можно выделить корпоративные сервисы, которые предоставляют обмен данными, их обработку или аналитику или сервисы удалённого управления, в частности управления промышленными сетями. Авторы не ставили целью выдвижение одного выделенного механизма как приоритетного, поэтому и не даются рекомендации по использованию отдельного взятого метода.

Ключевые слова: Интернет, ключ шифрования, сертификат, авторизация.

Введение

Современные информационные системы не могут существовать изолированно и всё больше сервисов становятся доступными для пользователей. Широкое распространение Интернет и подключенных мобильных устройств, дают предпосылки для вывода сервисов во внешние сети Интернет. Каждый из нас, использует эти методы повседневно, не вникая в технические детали процесса. Яркими примерами могут послужить приложения KASPI.KZ, HOMEBANK, EGOV.KZ. Пользователи систем высоко оценили удобство и вариативность методов авторизации, простоту использования. Но простота, в свою очередь, вынуждает

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

и обязывает компании использовать дополнительные методы проверки пользователя, запросившего доступ. Существует множество методов дополнительной авторизации пользователей, но стоит сразу отметить, что дополнительная авторизация не даёт 100% защиты от несанкционированного доступа к вашим данным, поскольку механизм позволяет только идентифицировать удалённого пользователя, как участника системы, а не подтвердить его личность. И, наверное, это один из самых слабых аргументов для внедрения механизмов многофакторной авторизации. Ведь помимо удобства клиентов и пользователей, это финансовые затраты на внедрение, обслуживание и контроль системы. С точки зрения имиджа и безопасности компании, использование дополнительной авторизации в системах повышает инвестиционную и потребительскую привлекательность организации, что приводит к повышению финансовой стабильности.

Во время проведения исследования и тестовых внедрений многофакторной авторизации, авторы руководствовались техническими регламентами, нотами и инструкциями производителей и интеграторов сервисов. Существует множество публикаций, обзорных и технических, но не описывающих именно техническую реализацию и внедрение методов в продуктивное использование. К примеру, корпорации Google и Microsoft имеют подробное описание внедрения многофакторной авторизации, но техническая документация ссылается на разделы администрирования коммерческой подписки пользователя, что не даёт возможности, не имея платной подписки, проводить тестовые внедрения. Такая же ситуация и с физическими устройствами для обеспечения авторизации: можно получить техническое описание и документацию, но требуется наличие физического устройства для проведения тестирования. В период исследования, авторы, получили полный набор управляющих функций и устройств для проведения тестирования и оценки возможностей каждого из методов.

Целью исследовательской работы было тестирование и определение оптимальной комбинации методов проведения идентификации пользователя.

Дополнительные методы авторизации пользователей

Авторизация (англ. authorization «разрешение; уполномочивание») – предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Согласно определению, для предоставления доступа к данным, система должна авторизовать пользователя, с целью определения уровня полномочий и возможности подключения к информационной системе. Что можно отнести к информационной системе? Это банковский клиент-приложение на устройстве, портал услуг, системы коллективной работы. Специалистами по безопасности давно установлено, что использование связки пользователь - пароль, не является надёжным и может быть легко скомпрометировано. Для дополнительной проверки пользователя необходимо использовать методы расширенной авторизации. Это может быть как действие со стороны пользователя, так и программные компоненты, автоматически подтверждающие полномочия пользователя.

Для правильной авторизации пользователя необходимо использовать многофакторную авторизацию персоны, запрашивающей доступ к информационной системе.

Немаловажным фактором, при внедрении, является механизм обратной связи с пользователем. Именно он будет определять возможности и интерактивность сервиса. Так, сервис SMS может помочь в организации большинства механизмов многофакторной авторизации, но вместе с тем, он же один из самых неустойчивых и зависящий от множества внешних факторов.

Самое время перейти к рассмотрению механизмов дополнительной авторизации более подробно.

DOI: 10.37943/AITU.2020.89.25.011

OTP (One Time Password*)* – метод выдачи пароля / ПИН-кода по запросу пользователя. К этому методу можно отнести SMS сообщение или PUSH сообщение от системы в момент запроса доступа. Система генерирует случайную комбинацию, которая передаётся пользователю. Как правило, имеет ограниченный срок действия от нескольких минут, до нескольких часов. Широко применяется в банковском секторе, а также на сайтах услуг, порталах самообслуживания.

Достоинства:

- достаточно простой метод для внедрения;
- быстрый ответ пользователя/приложения.

Недостатки:

- SMS может быть не доставлен вовремя, или, в случае роуминга, может быть не доставлен;
- SMS признан не безопасным, и существуют рекомендации по прекращению его использования;
- нет идентификации пользователя. Украденное устройство может использоваться мошенниками для доступа к системам.

Подтверждение по электронной почте – при запросе доступа отправка почтового сообщения. Широко применяется на сайтах электронного обучения, торговли.

Как правило, включает в теле письма ссылку на сайт и сгенерированным хэшем пароля или сессии. Обычно, имеет срок действия от нескольких часов, до нескольких дней.

Достоинства:

- легко в использовании для конечного пользователя.

Недостатки:

- легко перехватить сообщение с кодом;
- может быть задержка с доставкой электронного сообщения;
- из-за некорректной работы браузера или почтового приложения, пользователь может не получить доступ.

ЭЦП (Электронно-Цифровая Подпись) – на самом деле, это сертификат, выданный пользователю авторизованным центром сертификации. Является комбинацией шифрованного хранилища и пароля пользователя. Может быть как физическим устройством (USB HASP ключ), так и файлом на устройстве пользователя. Применяется в системах самообслуживания, к примеру EGOV.KZ.

Достоинства:

- ключ как правило выдаётся пользователю с проверкой дополнительных данных;
- может применяться на множестве устройств.

Недостатки:

- как правило, использует приложения на языке Java;
- легко передаётся другому пользователю.

Телефонный ответ системы – один из методов, когда система инициирует звонок на заранее утверждённый в системе телефон пользователя и просит подтвердить действия последовательностью клавиш. Как пример, службы Microsoft O365 используют такой метод, как альтернативный, для авторизации пользователя в системе.

Достоинства:

- лёгок для пользователя.

Недостатки:

- могут возникнуть проблемы в роуминге;
- украденное устройство может авторизоваться в системе.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Ответы на дополнительные секретные вопросы – многие порталы предлагают такой метод для онлайн авторизации пользователя. При первичной регистрации пользователя предлагается задать несколько секретных вопросов, которые будут использоваться для дополнительной проверки. Например, «имя домашнего животного», «в каком году вы поступили в университет». Или последние цифры телефона, указанного при регистрации.

Достоинства:

- не требует дополнительных технических средств;
- лёгок для использования.

Недостатки:

- пользователи зачастую забывают ответы;
- при достаточном изучении пользователя, ответы можно подобрать.

Аппаратный токен ключ – достаточно редко встречающийся метод. Специализированное устройство, которое генерирует цифровую комбинацию для получения доступа. Должно иметь обратную связь с устройством/сервером и приложением на устройстве. Не даёт уверенности, что человек, который имеет на данный момент ключ, является авторизованным пользователем.

Достоинства:

- сложен для взлома и перехвата.

Недостатки:

- физическое устройство может выйти из строя;
- устройство, выполняющее проверку, должно иметь криптографический модуль.

Биометрическая идентификация – всё более популярный метод авторизации. Развитие технологий, позволяет проводить авторизацию по отпечатку пальца, сканирование лица. Широко применяется для приложений на мобильных устройствах.

Достоинства:

- доступно да большинстве мобильных устройств;
- множество параметров (например, несколько отпечатков).

Недостатки:

- может не работать в некоторых условиях окружающей среды;
- метод с распознаванием лица может давать сбои и произвести ошибочную авторизацию;
- сложно для применения на компьютерах, требуется дополнительное оборудование.

Дополнительными факторами могут служить также время доступа – контроль действий и полномочий пользователя в зависимости от времени получения доступа; геолокация – определение местоположения пользователя GPS или GEO-IP, например если IP адрес из запрещённого списка, заблокировать доступ или GPS координаты указывают на запрещённое местоположение.

Возможно, есть и другие методы, которые не удалось рассмотреть, но основные и широко используемые механизмы были проверены и протестированы в тестовом окружении. В качестве результата приведены таблице 1.

DOI: 10.37943/AITU.2020.89.25.011

Таблица 1. Результаты тестирования и анализа методов авторизации

Метод авторизации	Простота внедрения	Ограничения	Безопасность	Надежность
OTP (One Time Password	Просто	Может быть задержка при сбоях сотовой сети	Может использоваться на украденном устройстве	Средняя
Подтверждение по электронной почте	Просто	Нужно учитывать кодировку, SPAM базы, доступность сервера отправки	Может быть перехвачено.	Средняя
ЭЦП (Электронно-Цифровая Подпись)	Требует подписанный сертификат. Разработка приложения	Требует дополнительных компонентов для работы	Безопасен. Но может быть передан/ украден сторонними лицами	Высокая
Ответы на дополнительные секретные вопросы	Просто	Вопросы должны быть типовыми. Как правило 20-30	Может быть взломан путём подбора.	Средняя
Аппаратный токен ключ	Сложно	Требует аппаратной и программной составляющей	Высокая	Высокая
Биометрическая авторизация	Сложно	Требует аппаратной и программной составляющей	Высокая	Высокая

Как и следовало ожидать, решения, сложные для внедрения, одновременно являются самыми надёжными. Но требуют значительных финансовых и человеческих ресурсов.

Но как авторизовать нового пользователя в системе? Ведь его данных нет в базе данных и невозможно его идентифицировать. В подавляющем ряде случаев первичная регистрация необходима при физическом присутствии пользователя для его идентификации и получении данных для регистрации. В Казахстане, каждый совершеннолетний и дееспособный гражданин имеет ИИН (индивидуальный идентификационный номер), уникальный номер, который является общим для идентификации человека в базах всех государственных органов и банковского сектора. Именно ИИН даёт свободу использования сервисов и нивелирует необходимость физического присутствия в месте получения услуги. К примеру, сервисы KASPI.KZ позволяют провести регистрацию имея только номер телефона и ИИН в руках.

На первый взгляд всё выглядит достаточно просто, за этим стоит работы множества людей и связанных систем. В общем, процесс авторизации можно представить в виде блок-схемы (Рисунок 1).

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Рис. 1. Обобщённая схема применения многофакторной аутентификации

Приведём пример внедрения механизма двухфакторной аутентификации пользователя на основе Microsoft MFA. Пользователь запрашивает доступ к облачному хранилищу, находясь в офисе – в этом случае, пользователь находится в доверенной сети, предварительно настроенной администратором как «доверенная зона», дополнительно, можно использовать механизм SSO для получения информации о пользователе. Таким образом все согласования авторизации абсолютно прозрачны для конечного пользователя и как результат, пользователь получает доступ к облачному хранилищу без ввода дополнительных данных. Тот же пользователь, запрашивает доступ находясь вне офиса – сеть теперь не доверенная и система запрашивает имя пользователя для проверки, после ввода имени пользователя, запрашивается пароль пользователя. В целях безопасности и исключения работы роботов, эти данные вводятся в различных окнах. После согласования связки пользователь + пароль, система отправляет SMS на номер телефона, который указан в свойствах MFA пользователя, для подтверждения открытия сессии. Как резервный вариант, можно указать альтернативный вариант: вызов на указанный телефонный номер. Во время звонка, в зависимости от настроек сложности, нужно набрать комбинацию цифр, с нажатием # в конце, для подтверждения завершения ввода. Если администратор настроил сохранение сессии для пользователя, то появится запрос на сохранение данных для последующих входов в систему.

Стоит отметить, что на практике, такой способ достаточно действенный и лёгок как для внедрения, так и для использования, но вызывает сложности, к сожалению, в использовании у персонала компаний среднего и старшего возраста.

DOI: 10.37943/AITU.2020.89.25.011

Как ещё один интересный пример можно привести использование двухфакторной аутентификации в системах охраны. Карточный доступ в офисные помещения и здания стал уже нормой в нашей жизни. Работники прикладывают электронный пропуск к считывателю, проходит верификация пропуска, разрешается вход. Это типовая реализация и работает в тысячах офисов по всему миру. Но возможна ситуация, когда пропуск может быть утерян или намеренно передан неуполномоченному лицу. Что делать в этом случае. Да, охрана, как правило, знает постоянных работников в лицо, в силу каждодневных встреч, но, если работников несколько тысяч, а ведь есть ещё и посетители. Как возможный вариант дополнительной верификации – использование биометрических средств проверки работников. Есть два возможных и доступных метода: верификация отпечатков пальцев и верификация лица. Сканеры отпечатков пальцев – это сильная проверка, поскольку подделать рисунок капилляров нереально, но сканер может не срабатывать на грязных пальцах, при минусовых температурах; мы уже не говорим о гигиене – считыватель может стать рассадником заболеваний при недостаточной и своевременной его обработке санитарными средствами, особенно это критично в период пандемии COVID-19. Второй метод – анализ лица или фото идентификация. Эталонное фото в базе данных системы контроля доступа, при считывании номера пропуска, сравнивается с полученным изображением с видеокамеры, анализируется по опорным точкам, например, линия подбородок – скула – надбровная дуга, система принимает решение о совпадении полученного изображения с оригиналом в базе и разрешает или запрещает проход. В промышленной эксплуатации система ITV Face-Интеллект на базе процессора Tevian позволила проводить верификацию и проверку личности работников с точностью 95% – что достаточно серьёзный результат.

Хотелось бы повторить, что использование только лишь пароля для доступа к системам, не обеспечивает должной безопасности и надёжной аутентификации пользователя. Для должного обеспечения безопасности данных, как системы, так и персонально пользователя, необходимо задействовать максимально возможный и допустимый набор методов дополнительной верификации лица, запрашивающего доступ. Ниже представлена схема (Рисунок 2), которая наглядно показывает зоны относительной надёжности проверки пользователя, с использованием многофакторной аутентификации.

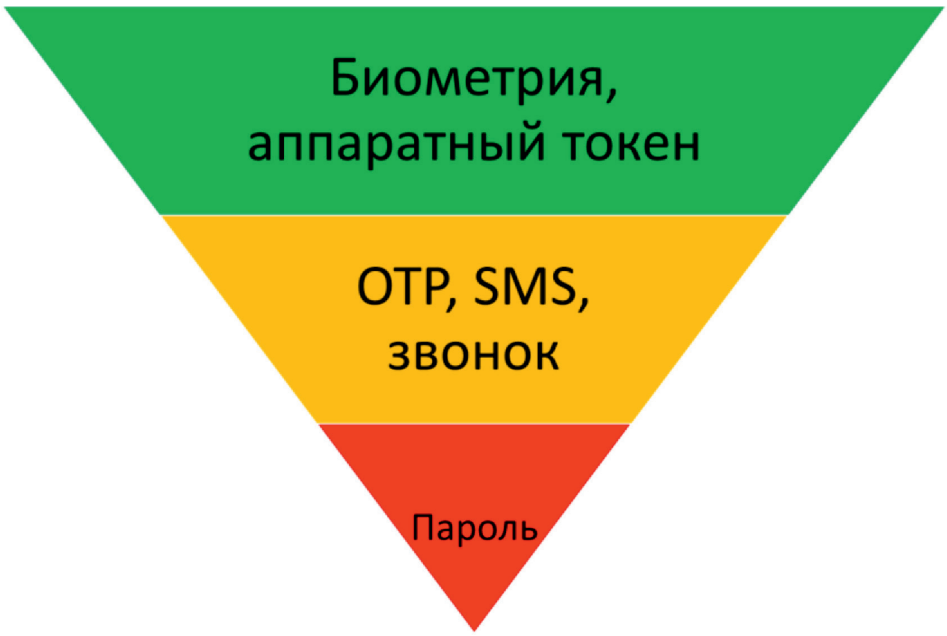

Рис. 2. Обобщённая схема надёжности многофакторной аутентификации

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Анализ методов

В ходе исследования, внедрения и использования методов многофакторной аутентификации был произведён анализ методов, их областей применения и рисков, связанных с их использованием. В ходе работ производилось множество коммуникаций с различными организациями, для выявления самих используемых методов и сложностей с их применением в продуктивной среде. Исходя из результатов обратной связи, были получены следующие результаты, которые объедены в таблице 2. Банки – это область банковских услуг и сервисов. Промышленность – системы, находящиеся в периметре предприятия, например, сенсоры отпечатков пальцев для доступа в серверные помещения. Сайты – сервисы, доступные пользователям через Интернет, либо корпоративные порталы. Системы безопасности – любые системы, ограничивающие доступ к системе или помещению.

Таблица 2. Таблица применения методов многофакторной аутентификации в разрезе областей применения, %

Сфера	Банки	Промышленность	Сайты	Системы безопасности
OTP	45	10	35	10
Биометрия	35	10	10	45
TOKEN	65	15	10	10
Электронная почта	10	5	80	5
ЭЦП	60	5	30	5
Звонок	5	0	90	5
Секретные вопросы	30	5	60	5

Более показательным будет представление этих данных в виде графической диаграммы (Рисунок 3):

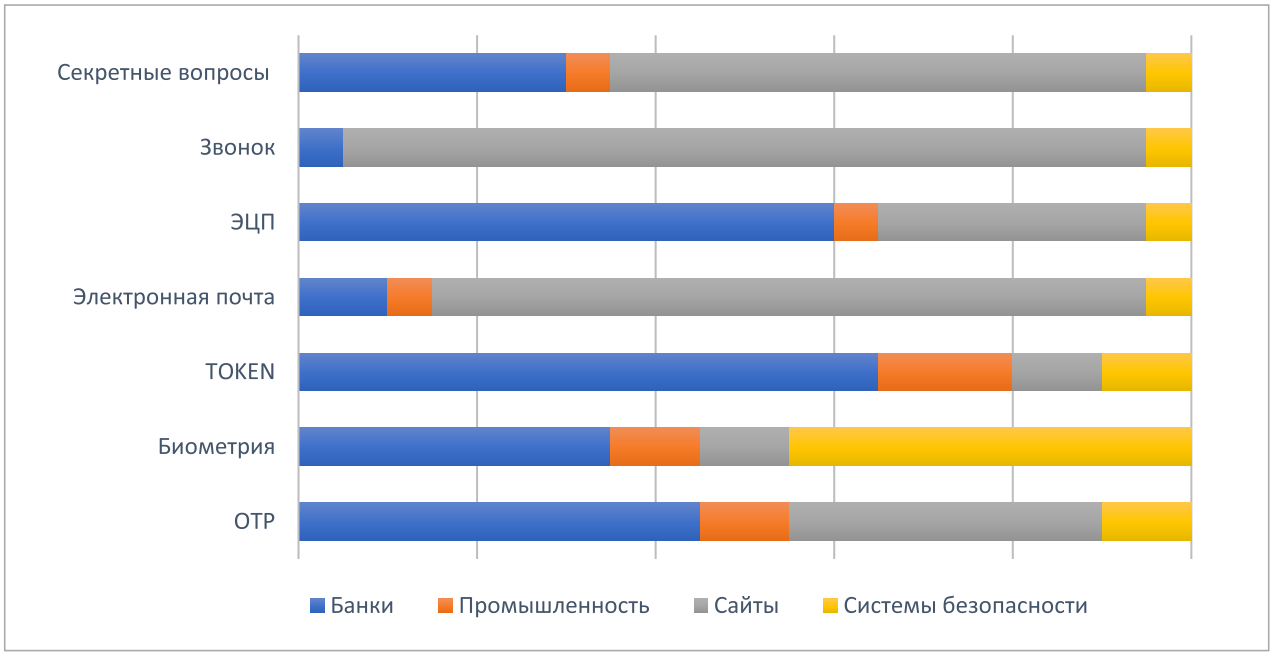

Рис. 3. Графическое отображение применения методов многофакторной аутентификации в разрезе областей применения

DOI: 10.37943/AITU.2020.89.25.011

Сложности, которые возникли у организаций при внедрении многофакторной аутентификации:

- OTP/SMS – базовый PIN, было установлено 4 символа. Данное решение было признано не безопасным, после чего было установлено значение 6-8 числовых символов.
- ЭЦП – требовал сертифицированного центра подписи сертификатов. Есть только несколько мировых центров, авторизованных для данных операций. В Казахстане, эту функцию выполняет Национальный Удостоверяющий Центр (https://pki.gov.kz/). Долгая процедура подтверждения.
- Обратный звонок – не получил широкого распространения для большинства сфер. Связано с расходами на международную связь. Только большие компании могут позволить использование данного метода. Дополнительно, законодательные и правовые ограничения не позволяют использование этого механизма в некоторых странах.
- Электронная почта – как показала практика, достаточно проста для взлома и не может обеспечить должного уровня безопасности. Безопасное внедрение требует значительных затрат и постоянного обслуживания, и контроля. В основном используется для возможностей первичной регистрации или смены данных.
- Биометрия – по отзывам, самый надёжный и мощный метод. Однако требует значительных мощностей для аналитики; поддерживаемого устройства у пользователя. Вместе с тем при неправильной настройке алгоритма распознавания, может авторизовать другую персону. Примером может служить ошибка Apple Face ID при запуске проекта – приложение могло авторизовать по фотографии, а не живого человека. Или при не достаточном освещении, система не может распознать темнокожих людей. То есть, при внедрении необходимо прорабатывать смежную инфраструктуру.
- Секретные вопросы – часто используются как дополнительный фактор для аутентификации пользователя. Множество общедоступных сайтов, например, Mail.ru, Yandex.ru используют этот метод для проверки пользователя или восстановления доступа к системе. Сервис EDGE F5 VPN также использует этот механизм для аутентификации пользователя. Сложность в том, что пользователи забывают ответы на пароли, либо отвечают неверно: к примеру, имя кота было написано на английском при формировании ответов, а пользователь набирает на русском.
- TOKEN – помимо очень сложной имплементации, нет проблем с данным методом. Требует для внедрения аппаратных средств как для системы, так и для аналитики. И достаточно дорог для внедрения.

Заключение

В данной статье мы не будем рассматривать обратную сторону внедрения этих методов – мониторинг и анализ событий информационной безопасности, работу систем SIEM, программистов и администраторов систем, но, необходимо принимать во внимание и эти факторы при внедрении многофакторной аутентификации.

Перечисленные в статье методы должны использоваться по отдельности или комбинированно для осуществления контроля доступа пользователя к информационной системе. Указанные методы могут только помочь в усилении механизма верификации, но не могут полностью гарантировать конфиденциальность и целостность данных. Каждый из методов имеет свои преимущества и недостатки, поэтому при внедрении необходимо также учитывать и уровень цифровой грамотности конечной категории пользователей. К примеру, внедрение биометрических считывателей в шахте или SMS уведомление для пастухов, не приведут к желаемому результату. В то же время, необходимо учитывать нормы законодательства страны, в которой планируется внедрение.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031
ISSN (E): 2707-904X

Литература

1. Комаров, А. (2008). Современные методы аутентификации: токен и это все о нем..!. *T-Comm-Телекоммуникации и Транспорт,* (6). [Электронный ресурс] // Режим доступа: https://www.aladdin-rd.ru/company/pressroom/articles/sovremennye_metody_autentifikacii_token_i_eto_vse_o_nem – Дата доступа 06.12.2020.
2. Скородумов, А. (2015). Многофакторная аутентификация – лучше меньше, да лучше, *«Information Security/ Информационная безопасность»*, (6) [Электронный ресурс] // Режим доступа: http://lib.itsec.ru/articles2/Oborandteh/mnogofaktornaya-autentifikatsiya-luchshe-menshe--da-luchshe – Дата доступа 08.12.2020.
3. Многофакторная (двухфакторная) аутентификация, [Электронный ресурс] // Режим доступа: https://www.tadviser.ru/index.php/Статья: Многофакторная_(двухфакторная)_аутентификация – Дата доступа 08.12.2020.
4. Marty Puranik, What is Two-Factor Authentication? The Tip of the Security Spear, [Электронный ресурс] // Режим доступа: https://www.securitymagazine.com/articles/91974-what-is-two-factor-authentication-the-tip-of-the-security-spear, March 23, 2020 – Дата доступа 21.12.2020.
5. Abhishek Shah, Multi-factor authentication, [Электронный ресурс] // Режим доступа: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:user-authentication-methods/a/multi-factor-authentication – Дата доступа 21.12.2020.
6. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography,* 2(1), 1.
7. Богданов, Д.С., & Клюев, С.Г. (2020). Классификация и сравнительный анализ технологий многофакторной аутентификации в Веб-приложениях. *Моделирование, оптимизация и информационные технологии,* 8(1), 17-18. [Электронный ресурс] //
8. Misha Ketchell, Can I still be hacked with 2FA enabled?, [Электронный ресурс] // Режим доступа: https://theconversation.com/can-i-still-be-hacked-with-2fa-enabled-144682, September 4, 2020, – Дата доступа 21.12.2020.
9. Misha Ketchell, Receiving a login code via SMS and email isn't secure. Here's what to use instead, [Электронный ресурс] // Режим доступа: https://theconversation.com/receiving-a-login-code-via-sms-and-email-isnt-secure-heres-what-to-use-instead-112767, March 6, 2019, – Дата доступа 18.12.2020.
10. Mike Betsko,Multifactor authentication critical as workplaces get more connected, [Электронный ресурс]. 14, 2020, – Дата доступа 18.12.2020. David Hald, 8 reasons you should turn to multi-factor authentication, [Электронный ресурс] // Режим доступа: https://techbeacon.com/security/8-reasons-you-should-turn-multi-factor-authentication, – Дата доступа 18.12.2020.