DOI: 10.25728/mlsd.2022.1074

ОЦЕНКА ПРИМЕНИМОСТИ МЕТОДОВ АУТЕНТИФИКАЦИИ ОПЕРАТОРОВ В ПРОМЫШЛЕННЫХ СИСТЕМАХ[1]

Промыслов В.Г., Семенков К.В., Тимофеев М.Ю.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва ул. Профсоюзная д.65
v1925@mail.ru, semenkovk@mail.ru, timof-1964@mail.ru

Аннотация: В работе рассматривается проблема аутентификации операторов автоматизированных систем управления промышленными объектами критической информационной инфраструктуры на примере атомных электростанций. Также проведен обзор методов аутентификации. В работе делается вывод о перспективности реализации многофакторной аутентификации на основе токена или парольной защиты.

Ключевые слова: Аутентификация, биометрия, токен, пароль, АСУ ТП.

Введение

В промышленных системах управления при решении задачи допуска доверенного оператора к управлению объектом с учетом возможных угроз несанкционированного доступа возникают вопросы аутентификации.

Аутентификация, согласно нормативным документам [ГОСТ Р 58833-2020], определяется следующим образом: «действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации».

Аутентифицирующий субъект выполняет проверку, сопоставляя некоторый идентификатор личности, например, общий секрет, который был заранее оговорен во время регистрации пользователя. Это может делаться с целью создания доверенных коммуникаций между сторонами или для наделения правами доступа к коммуникационным и вычислительным ресурсам системы в ходе авторизации.

При личном общении аутентификация, вообще говоря, не является сложной задачей, так как абоненты лично контактируют и могут по внешнему виду или другим признакам идентифицировать друг друга. Но в эпоху появления удаленных средств связи, а особенно в цифровую эпоху проблема аутентификация изменилась. Теперь нельзя «видеть» абонента на удаленном конце сети (или, по крайней мере, полностью доверять тому, что видишь). Пользователь может быть, как добропорядочным, так и злоумышленником. А в процессе коммуникации возможен обмен личной информацией, такой как финансовые данные или данные о здоровье, которые желательно сохранить втайне от третьей стороны.

Эпоха цифровых технологий поставила задачу аутентификации не только при удаленной коммуникации абонентов для сохранения конфиденциальности. Современные производства, в том числе опасные, например, атомные станции, транспорт, химические предприятия и т.д., зависят от цифровых автоматизированных систем управления технологическим процессом (АСУ ТП). В контуре управления таких систем чаще всего присутствует человек (оператор), который воздействует как на сам объект управления, так и систему управления через компьютеры, входящие в состав АСУ ТП. Неавторизованные действия оператора могут не только нарушить основные свойства информационной безопасности (целостность, доступность и конфиденциальность), но и привести к экономическому ущербу, нанести вред здоровью людей. Дополнительно существует проблема отслеживания решений по управлению объектом, т.е. обеспечение неотказуемости от совершенных ранее действий. В целом данные проблемы вынуждают использовать более формальные методы аутентификации даже в рутинных операциях в цифровых системах управления.

Задачи аутентификация для промышленных систем, как и для обычных информационных систем, включают и аутентификацию оператора (пользователя) на компьютере (цифровом устройстве), и аутентификацию самих компьютеров.

Протоколы, используемые для задачи аутентификации пользователей, гораздо менее безопасны, чем протоколы аутентификации между компьютерами, так как имеют дело с людьми и их ограничениями и слабостями [1]. Традиционно, в информационной безопасности часто слабым звеном в защите являются люди.

[1] *Исследование (раздел 2) выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-29-06044.*

Поэтому в нашей работе внимание уделено анализу существующих методов и протоколов аутентификации пользователей и исследованию их применимости для задачи аутентификации операторов АСУ ТП. Анализ проводится с учетом особенностей функционирования промышленных объектов и задачи аутентификации. В качестве примера промышленной системы управления для исследований выбрана разработанная в ИПУ РАН система верхнего блочного уровня АСУ ТП АЭС [2]. Будем предполагать, что условия работы оператора на объекте и степень воздействия физических полей на людей и оборудование близки к нормальной офисной среде. Данное предположение для части промышленных объектов может нарушаться, но учет этих факторов лежит за рамками выполненной работы.

1 Задачи и методы аутентификации в АСУ ТП

Рассмотрим основные методы аутентификации пользователей и сравним их эффективность с точки зрения применимости для АСУ ТП.

Методы аутентификации пользователей можно разделить на классы, основываясь на трех основных вопросах [3]:

- Что вы знаете?
- Что у вас есть?
- Кто вы?

Часто три метода аутентификации ассоциируются с их характерными представителями: паролем, токеном и биометрическим признаком

1.1 Парольные методы аутентификации

Пароль – это секретное слово, которое знает пользователь и возможно компьютер, с которым пользователь аутентифицируется. Мы говорим, что компьютер «возможно» знает пароль, потому что чаще всего на компьютере хранится не сам пароль, а его хеши, и сравниваются не пароли, а их хеш-функции.

В качестве пароля в задаче аутентификации также могут рассматриваться фразы и персональные идентификационные номера (ПИН-коды), а также другие тщательно охраняемые секреты.

Рассмотрим для примера расширенный стандарт шифрования (AES – Advanced Encryption Standard) [4]. AES относится к протоколам симметричного шифрования с закрытым ключом, максимальная длина ключа AES составляет 256 бит. Если злоумышленник хочет угадать ключ, то на это может потребоваться в среднем более 10^{76} попыток, что займет слишком много времени даже с помощью компьютеров в обозримом будущем. Однако длина ключ в 256-бит слишком велика для большинства людей, поэтому на практике этот ключ хранится в компьютерном файле, защищенном более запоминающимся (коротким) паролем. Проблема протоколов аутентификации с участием пользователя состоит в том, что люди часто выбирают такой пароль, который другой человек или компьютер может легко угадать. Основная уязвимость парольной защиты состоит в том, что запоминающийся пароль может быть угадан или найден злоумышленником, а длинный, случайный, меняющийся пароль трудно запомнить, и в этом случае его могут записать и хранить в открытом виде.

Этих недостатков парольного метода аутентификации можно избежать, используя методы иных классов, где процессе аутентификации человек становится не субъектом, а объектом. Это методы на основе токенов и биометрические методы.

1.2 Методы аутентификации с применением токенов

Токен – это физическое устройство, которое выполняет или помогает провести аутентификацию. Например, википедия его определяет так: «Токен, (также аппаратный токен, USB-ключ, криптографический токен) – это компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т. д. Как правило, это физическое устройство, которое используется для упрощения аутентификации. Также этот термин может относиться и к программным токенам, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам» [5].

Токены могут быть как пассивными, так и активными (например, предоставляющими одноразовые коды доступа, либо изменяющимися синхронно с мастером на хосте и т.д.).

В общем случае токен можно рассматривать как секретный ключ, аналогичный паролю, за исключением того, что он сгенерирован машиной или сохранен машиной, поэтому он может быть длиннее, более случайным и, возможно, меняться во времени.

1.3 Биометрические методы

Биометрия или биометрические персональные данные – это некоторая измеримая индивидуальная характеристика человеческого тела, достаточная для того, чтобы ее можно было использовать для аутентификации пользователя.

К биометрическим данным относятся, в частности: отпечатки пальцев, глаза (радужная оболочка и сетчатки глаза), лицо, рука, голос и подпись, а также другие менее явные или футуристические биометрические данные, такие как походка, запах или моргание [6, 7, 8].

Детальные требования к биометрическим методам аутентификации приведены в различных нормативных документах, например, в стандарте ГОСТ Р 52633.0-2006 «Требования к средствам высоконадежной биометрической аутентификации». Биометрия призвана неразрывно связать аутентификатор (признак) и владельца аутентификационного признака, что в случае пароля и токена сделать нельзя (последнее сейчас уже не совсем верно, токен можно вживить в человека), так как их можно одолжить или украсть. Такая неразрывная связка признака аутентификации с носителем признака позволила бы обеспечить свойство неотказуемости. Напомним, что неотказуемость — это свойство, которое обеспечивает доказательство сделки таким образом, что вовлеченные стороны не могут впоследствии отклонить транзакцию, как несанкционированную или заявить, что не участвовали в сделке. Однако биометрические характеристики, как и пароли, можно скопировать или подделать с большим или меньшим уровнем затрат и, впоследствии, использовать для получения несанкционированного доступа. В целом, биометрия на текущем техническом уровне не может гарантировать свойство «неотказуемости».

Биометрические данные, используемые для аутентификации, обычно классифицируются на физические и поведенческие типы.

Физический тип включает биометрию, основанную на стабильных характеристиках тела, таких как отпечатки пальцев, лицо, радужная оболочка и форма руки и др. Поведенческий тип включает в себя умения, приобретенные в процессе обучения, такие как рукописная подпись, динамика работы с клавиатурой, походка. Речь обычно классифицируется как поведенческий тип данных, потому что она является продуктом усвоенного поведения. Биометрический метод аутентификации, как и прочие методы, может приводить к ошибкам. Однако психологическое отношение пользователя к ошибкам в том и другом случае различаются. Пользователь может забыть или неправильно ввести пароль, может потерять токен. Эти ошибки неудобны, но пользователь осознает, что виноват он сам. В случае ошибки аутентификации с использованием биометрического метода пользователь не виноват и не может сам устранить проблему. Биометрическая ошибка может возникнуть по разным причинам:

- грязный сканер;
- плохое освещение;
- система, возможно, изначально запомнила неправильный шаблон BT для сравнения;
- система может плохо приспосабливаться к изменению окружающей среды (холод, дождь, солнечные блики, сухость и т. д.) или к естественному изменению биометрических характеристик пользователя (прическа, борода, порезанный палец и т.п.);

Детальные требования к биометрическим методам аутентификации приведены в различных нормативных документах, например, в стандарте ГОСТ Р 52633.0-2006 «Требования к средствам высоконадежной биометрической аутентификации».

2 Протоколы аутентификации и их применение в АСУ ТП

Все основные протоколы аутентификации обеспечивают создание аутентифицированных ключей (authenticated key establishment) для защиты передаваемой информации на основе некоторого другого секрета. Базовый протокол аутентификации обеспечивает разделение некоторого секрета между абонентами, который служит доказательством для одной или каждой из сторон подлинности абонента.

В контексте задачи аутентификации пользователя мы будем рассматривать самый общий протокол аутентификации [9], в котором пользователь обменивается с компьютером ключом ($Password$), возможно в виде хеш-функции $h(Password)$, который сервер сравнивает с известным ему образцом ($StoredHash$). Протокол аутентификации при использовании парольного метода приведен в таблице 1. Для других методов аутентификации протокол легко модифицируется подстановкой вместо пароля ключа, содержащегося в токене или биометрического шаблона.

Таблица 1. Базовый протокол парольной аутентификации

Клиент	**Сервер**
$User \rightarrow Password \rightarrow$	
	$h(Password) == StoredHash\,?$
	← Да /Нет

Для информационных систем общего пользования популярными вариантами протокола аутентификации являются протокол «оклик-отзыв» [10] и варианты протоколов многофакторной аутентификацию, обеспечивающие необходимую стойкость базового протокола.

2.1 Протокол «оклик-отзыв»

Протокол «оклик-отзыв» (challenge-response), позволяет проверить, что протокольное сообщение не является воспроизведением старого сообщения, для чего реализуется механизм, который проверяет личность, требуя предоставления верной аутентификационной информации в ответ на непредсказуемый вызов.

Применение протокола для парольного метода аутентификации ограничено из-за требований обеспечения доступности. Также ограничения накладываются использованием отдельных сценариев работы оператора, которые связаны с критичными функциями системы. Тем не менее, применение протокола возможно, например, для доступа к функции перепрограммирования цифрового устройства.

2.2 Многофакторная аутентификация

В реальных системах протоколы аутентификации для достижения высокого уровня защиты и обеспечения ее эшелонирования могут объединять несколько разных методов аутентификации. Такая аутентификация называется многофакторной. Многофакторная аутентификация реализует алгоритм логического “И”, когда для успешной аутентификации необходимо, чтобы аутентификация всеми методами прошла успешно. Связка физический токен – пароль составляет подавляющее большинство текущих реализаций многофакторных аутентификаций [11, 12]. Совместное применение пароля и биометрического идентификатора используют редко, потому что биометрические данные обычно включаются для удобства, чтобы не запоминать пароль.

Многофакторная аутентификация, сочетающая все три фактора, не нашла широкого применения, хотя такая реализация может потребоваться для доступа к функциям, где необходим высокий уровень защиты. Таблица 2 содержит сводку основных преимуществ и недостатков некоторых методов многофакторной аутентификации, а также экспертную оценку их пригодности для задач аутентификации оператора АСУ ТП по качественной шкале: Плохо-Удовлетворительно-Хорошо.

Таблица 2. Многофакторная аутентификации пользователя для получения более сильной защиты

Комбинация методов аутентификации	**Преимущества**	**Недостатки**	**Пример**	**Степень применимости для АСУ ТП**
Что вы знаете + Что у вас есть	Потеря токена не приводит к его немедленной компрометации, так как он защищен паролем	Необходимо иметь токен и помнить пароль	Банковская карта + ПИН	Удовлетворительно
Что у вас есть + Кто вы	Потеря токена не приводит к его немедленной компрометации, так как он защищен вашей уникальностью	Необходимо иметь токен. Может приводить к ложному отказу при аутентификации из-за несовершенства биометрических методов	Пропуск с чипом и фотографией	Хорошо
Что вы знаете + Кто вы	Подмена вашего идентификатора (использование двойника) не приведет к ложной аутентификации	Может приводить к ложному отказу при аутентификации из-за несовершенства биометрических методов	Пароль + датчик отпечатка пальца на компьютере	Удовлетворительно

Комбинация методов аутентификации	Преимущества	Недостатки	Пример	Степень применимости для АСУ ТП
Что вы знаете + Что у вас есть + Кто вы	Все три метода работают последовательно	Надо иметь токен и помнить пароль. Может приводить к ложному отказу при аутентификации из- за несовершенства биометрических методов	Доступ на критический объект	Плохо

Основные протоколы аутентификации легко модифицируются для случая многофакторной аутентификации. Однако для политик безопасности с высокими требованиями доступности, характерными для АСУ ТП, введение дополнительной транзакции и сложности в протокол может быть вредным.

Для АСУ ТП и других объектов с приоритетом доступности может быть реализована многофакторная аутентификация по сценарию логического «ИЛИ». В этом случае аутентификация считается выполненной, если хотя бы один из методов многофакторной аутентификации дал утвердительный ответ.

2.3 Модель обмена данными в каналах протокола аутентификации и атаки в канале

Рассмотри обобщенную модель канала аутентификации между пользователем и удаленным сервером с применением различных методов аутентификации [3]. Модель можно описать в виде трех схем:

1) Пользователь отправляет пароль или биометрический шаблон через клиентский компьютер к серверу для аутентификации.
2) Пользователь аутентифицируется у посредника на клиентской машине (таким посредником может быть считыватель токенов, биометрический сопоставитель или программа хранения паролей), а пароль отправляется на сервер с указанием результата аутентификации.
3) Пользователь отправляет аутентификатор через клиентскую машину на промежуточный сервер аутентификации, с которого пароль отправляется на сервер с указанием результата аутентификации.

Вторая и третья схема аналогичны и отличаются только размещением среды, где проводиться аутентификация (локально или удаленно).

В соответствии с моделью можно видеть, что при наличии в АСУ ТП внутреннего нарушителя аутентификаторы могут быть атакованы в трех местах: на машине клиента, в канале передачи (промежуточном сервере) и на сервере. Основные типы атак на методы аутентификации на стороне клиента и сервера приведены в таблице 3.

Таблица 3. Потенциальные атаки на методы аутентификацию

Атака	Метод аутентификации	Пример атаки	Типовые методы защиты, которые можно реализовать в АСУ ТП
Атака на стороне клиента	Пароль	Угадывание пароля, взлом перебором. Кража (подглядывание) пароля	Политика управления паролями с мерами по обеспечению достаточной энтропии ключа. Диагностический сигнал для офицера безопасности
	Токен	Кража токена	Физические меры безопасности.
	Биометрия	Ложное срабатывание	Многофакторная аутентификация
Атака на стороне сервера	Пароль	Угадывание пароля, взлом перебором	Политика управления паролями с мерами по обеспечению достаточной энтропии ключа. Одноразовые пароли. Политика безопасности сервера, учитывающая данную угрозу
	Токен	Угадывание пароля, взлом перебором	Политика управления паролями с мерами по обеспечению достаточной энтропии ключа. Одноразовые пароли. Политика безопасности сервера

Атака	Метод аутентификации	Пример атаки	Типовые методы защиты, которые можно реализовать в АСУ ТП
	Биометрия	Угадывание биометрического шаблона, взлом перебором	Политика управления паролями с мерами по обеспечению достаточной энтропии ключа. Политика безопасности сервера

Легко заметить, что в контексте политики безопасности АСУ ТП возможности для атак не равнозначны. Если на предприятии имеется постоянно действующая система обнаружения вторжений (IDS, intrusion detection system) и существуют лица ответственные за компьютерную безопасность, то атаки перебором должны легко обнаруживаться, после чего должны приниматься соответствующие меры. В то же время, атаки, связанные с кражей токена или пароля, особенно последние, весьма вероятны, учитывая высокую степень доверия, которая обычно устанавливается между пользователями, допущенными в зону безопасности на промышленном объекте.

Для АСУ ТП, мы полагаем, желательно применение неблокирующих методов защиты от многих атак, связанных с попытками обойти процедуру аутентификации. Неблокирующие методы защиты прежде всего призваны привлечь внимание офицера по безопасности к нештатной ситуации, оставляя на усмотрение человека принятие мер в ответ на событие безопасности.

3 Анализ и сравнение методов аутентификации

3.1 Принципы сравнения

Попробуем сравнить три основных метода аутентификации для их применимости в АСУ ТП, по их характерным представителям. Мы будем сравнивать методы по следующим признакам: стойкость, достоинства (удобство) и недостатки, качество распознавания. Сравнение будет в большинстве случаев качественным, и в значительной мере основанным на практическом (экспертном) опыте, который может иметь субъективный характер; набор показателей для сравнения взят из работы [3].

В таблице 4 приведены основные атрибуты трех методов аутентификации.

Таблица 4. Три основных метода аутентификации пользователя и их атрибуты

Методы аутентификации	Что вы знаете?	Что у вас есть?	Кто вы?
Реализации метода	Пароль	Токен	Биометрия
На чем основана аутентификация	Знание секрета	Владение нужным объектом	Характерные признаки субъекта
Защита	Сохранение тайны	Физическая безопасность	Уникальность субъекта
Примеры уязвимости	Можно подсмотреть или угадать	Можно потерять, может быть украден	Можно подделать, трудно сменить, если скомпрометирован

3.2 Практическая энтропия ключа

Для оценки стойкости методов аутентификации, то есть различные метрики, по которым можно сравнивать процедуры аутентификации, но главный из них – энтропия ключа, используемого в протоколе аутентификации. Определим пространство ключа: $k_p = c^n$, где

$c -$ символ,

$n -$ длина секрета.

Энтропия $H_{max} = log_2 k_p$.

Исследования энтропии паролей, проведенные на основе данных крупных IT-компаний (yahoo, google) [1], показывают, что энтропия составляет 10-20 бит. Если же говорить о хеш-функциях (взлом на уровне сервера аутентификации), то энтропия скорее ближе к левой границе (т.е. к 10 битам), т.к. хеш-функции оптимизированы для обеспечения быстродействия, что уменьшает их стойкость. Хотя, например, реализации алгоритмов хеширования SHA1 (Secure Hash Algorithm 1) [RFC 3174] являются настраиваемыми и могут быть весьма стойкими.

Ранние исследования [3] показывают, что энтропия ключа, следовательно, и стойкость метода для биометрической и парольной защиты примерно одинакова, но более поздние работы говорят, что

биометрические методы позволяют получить в два три раза лучшую степень защиты чем парольные [13].

Специальные исследования по стойкости паролей для операторов АСУ ТП нам не известны. Однако мы склоняемся к тому, чтобы принять значение стойкости используемых паролей ближе к нижней границе (простые пароли). Хотя политика безопасности промышленного объекта может и должна содержать требования к стойкости паролей и процедуру управления ими, применение слишком сложного (стойкого) пароля невозможно из-за требований к доступности системы и наличия стрессовых ситуаций в работе оператора.

Энтропия ключа, содержащегося в токене, может быть весьма большой, при использовании алгоритмов аналогичных методам аутентификации Компьютер-Компьютер. Например, в работе [14], приведены значения энтропии ключа до 128 бит. Однако, нужно учитывать вероятность кражи токена, которая может оказаться существенной, особенно при наличии злого умысла.

3.3 Основные характеристики качества распознавания

Для оценки качества распознавания традиционно используется две основные характеристики: ошибки первого и второго рода, часто обозначаемые английскими аббревиатурами FRR (False Rejection Rate) и FAR (False Acceptance Rate).

Первое число характеризует вероятность отказа в доступе человеку, имеющему допуск. Второе - это вероятность принятия ложного решения о положительной аутентификации. Чем лучше система, тем при одинаковых значениях FAR меньше значение FRR. Параметр FAR имеет смысл приводить только для биометрического метода аутентификации, т.к. для остальных методов аутентификации значение отражают способности человека (набор и запоминание парольной фразы) или надёжность аппаратной реализации.

Типовые характеристики демонстрируют только тенденцию, сравнение реализаций и алгоритмов для биометрического метода выходит за рамки нашей работы, однако, чтобы исследовать практические аспекты применимости коммерчески доступных устройств для биометрической аутентификации операторов АСУ ТП, мы провели дополнительное тестирование, где имитировались некоторые характерные условия работы оператора АСУ ТП. Результаты приведены в разделе 3.4.

3.4 Практическое тестирование пригодности методов аутентификации для операторов АСУ ТП

Нами приведены тестовые испытание парольных и некоторых реализаций биометрических методов аутентификации в типичных сценариях работы оператора АСУ ТП на промышленном объекте. Тестирование метода аутентификации с токеном не проводилось, так как предполагалось, что его свойства определяются возможностями, заложенными при проектировании и изготовлении токена и стабильны в процессе эксплуатации.

Для тестирования биометрических методов аутентификации использовались устройства и алгоритмы, доступные массовому потребителю и применяемые для аутентификации в мобильных устройствах. Для тестов парольной аутентификации использовались типовые клавиатуры для персональных компьютеров, которые также используются на рабочих местах операторов АСУ ТП.

Для каждого из методов проводилось не менее 50 тестирований.

Каждый тест проводила группа из двух испытателей, один (оператор) по команде другого испытателя делал попытку аутентифицироваться с применением одного из методов аутентификации. В ходе каждого из тестов измерялось время, за которое была проведена аутентификация и число затраченных попыток до удачной аутентификации. Во время испытаний для каждого из тестов изменялись в пределах типовых рабочих условий внешние параметры среды, освещенность, уровень шума.

Для биометрических методов моделировалась изменения в соответствующем биометрическом сигнале введением периодической помеховой нагрузки для испытателя.

Для парольных методов аутентификации после каждых 10 тестов менялся пароль в соответствии с выбранным уровнем сложности.

Для парольного метода получена относительно высокая $\sim 10^{-1}$ ошибка первого рода: вероятность отказа в доступе человеку имеющего право доступа при наличии помех.

Это может быть основанием отказа от парольной защиты в пользу токенов, биометрических методов или организационных и физических мер аутентификации и их комбинации.

Среди биометрических методов идентификации наилучшие результаты во время тестирования были получены для идентификации по лицу.

Полученная в практических условиях ошибка первого рода для биометрического метода приблизительно на порядок превышает типовые значения, что в основном связано с наличием помех. Данные результаты следует учитывать при использовании биометрических методов для АСУ ТП.

3.4 Анализ применимости методов аутентификации в АСУ ТП

Проанализируем основные проблемы, связанные с применением каждого метода для типовых условий работы оператора промышленной системы управления:

1) Аутентификаторы, основанные на знаниях («что вы знаете?»), включают секретную информацию (пароль), но такая информация является не столько секретной, сколько «неизвестной». Данной информации можно дать приблизительно следующее определение – «скрытая от большинства людей». Недостатком секретов является то, что каждый раз, когда они используются для аутентификации, то становятся все менее секретными. К тому же «большинство людей» часто означает «большинство честных людей», а для злоумышленника при некотором усилии (например, средствами социальной инженерии) такая информация перестает быть закрытой. Для систем управления АСУ ТП характерен высокий уровень доверия между пользователями. Доверие устанавливается как результат отбора персонала, так и определяется производственной деятельностью, когда люди выполняют в течении долгого времени общую работу. Поэтому у злоумышленника, проникшего в изолированный коллектив, упрощается задача получения знаний, включая секретные (пароли), от других членов этого коллектива.

2) Аутентификаторы-объекты («что у вас есть?») – это материальные объекты, наиболее характерный пример – токен. Основной недостаток аутентификатора-объекта тот же, что и у предметов, которые непосредственно им предшествовали – физических ключей. Если ключ утерян, то любой, кто его нашёл, может обойти систему защиты. В этом смысле слабости объектных аутентификаторов аналогичны парольной защите: злоумышленник может использовать потерянный или украденный токен. Аналогично парольной защите, пользователи АСУ ТП склонны доверять друг другу. Однако в отличие от парольной защиты при утере физического объекта владелец узнает это при первом обращении к нему и сможет принять меры для скорейшей нейтрализации угрозы.

3) Аутентификаторы на основе идентификаторов («кто вы?») – привязаны к одному человеку, они уникальны. Данная категория включает в себя все биометрические методы аутентификации, такие как отпечаток пальца, сканирование глаз и радужная оболочка, голосовой отпечаток или подпись. Биометрический метод аутентификации имеет сравнительно высокую степень защиты в части копирования и подделки и очевидно не может быть утерян.

Суммируя вышесказанное, можно заключить, что ни один из этих методов аутентификации не идеален, они имеют некоторый набор «врожденных» недостатков. В таблице 5 приведены характерные уязвимости различных методов аутентификации применительно к задачам АСУ ТП.

Таблица 5. Компрометация свойств безопасности при различных методах аутентификации

Компрометируемое свойство безопасности	**Метод аутентификации**	**Пример атаки**	**Типовые методы защиты**
Неопровержимость	Пароль, токен	Потеря или кража токена	Персональная ответственность пользователя за потерю (административная мера защиты)
	Биометрия	Подделка	Многофакторная аутентификация
Обнаружение компрометации	Пароль, биометрия	Подделка, кража	Информация пользователю об использовании аутентификатора (last login)
	Токен		Обнаружение пропажи пользователем
Подмена пользователя при начальной идентификации пользователя	Пароль	Передача данных неавторизованному лицу. Пароль по умолчанию	Личная явка пользователя. Политика управления паролями
	Токен	Передача токена неавторизованному лицу	Личная явка пользователя
	Биометрия	Замена пользовательских биометрических данных	Личная явка пользователя

Компрометируемое свойство безопасности	Метод аутентификации	Пример атаки	Типовые методы защиты
Утечка данных при обновлении идентификатора	Пароль	Передача данных неавторизованному лицу. Пароль по умолчанию	Политика управления паролями. Многофакторная аутентификация
	Токен	Передача токена неавторизованному лицу	Личная явка пользователя и сдача токена если он сломан, а не утерян
	Биометрия	Замена пользовательских биометрических данных при компрометации	Политика управления персональной информацией
Отказ в обслуживании	Пароль, Токен, Биометрия	Многократные неудачные попытки для блокирования доступа	Не блокирующая политика безопасности с нотификацией офицера по безопасности.
Ложная аутентификация	Пароль, Токен, Биометрия	Атака с повторной передачей сообщений	Протокол «оклик отзыв»

3.5 Качественный анализ и сравнение методов аутентификации для АСУ ТП

Для сравнения методов аутентификации можно предложить различные м показатели. Рассмотрим три высокоуровневых показателя, которые традиционно используются для сравнения методов аутентификации [O'Gorman 200]:

- удобство использования,
- удобство развертывания,
- безопасность.

В каждом из наборов высокоуровневых показателей выделим набор показателей более низкого уровня. Все показатели в наборе будут оцениваться по ранговой шкале: Хорошо – (2), Удовлетворительно – (1), Плохо – (0). Значение высокоуровневого показателя вычислим как сумму отдельных показателей в наборе.

Рассмотрим набор показателей «удобство использования» см. таблицу 6.

Таблица 6. Показатель «удобство использования» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Насколько легко пользователям взаимодействовать со схемой аутентификации	Удовлетворительно	Хорошо	Удовлетворительно
Простота обучения: «Пользователи, не знакомые со схемой, могут понять ее и выучить без особых проблем»	Хорошо	Хорошо	Удовлетворительно
Нечастые ошибки: «Задача, которую пользователи должны выполнить для аутентификации, обычно завершается успешно, если ее выполняет законный и честный пользователь»	Удовлетворительно. Пользователи обычно успешно справляются, но при условии слабого пароля	Хорошо	Удовлетворительно
Масштабируемость для пользователей: «Использование схемы для сотен учетных записей не увеличивает нагрузку на пользователя»	Плохо. Люди часто повторно используют пароли или создают простую схему уникальности для каждого сайта для базового пароля	Удовлетворительно. Проблема выбора одного токена из множества имеющихся в наличии не всегда тривиальна	Хорошо

Показатель	Пароль	Токен	Биометрия
Простое восстановление после компрометации	Хорошо. Преимущество паролей – их легко сбросить	Удоволетворительно	Плохо
Нужно ли что ни будь носить с собой	Хорошо	Плохо	Хорошо
Сумма:	8	8	7

Рассмотрим набор показателей «удобство развертывания» см. таблицу 7**Ошибка! Источник ссылки не найден.**.

Таблица 7. Показатель «удобство развертывания» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Насколько просто внедрить метод аутентификации в реальные системы?	Хорошо	Хорошо	Удовлетворительно
Совместимость с сервером аутентификации	Хорошо. Серверы аутентификации изначально разработаны для парольных методов аутентификации	Хорошо. С точки зрения сервера ключ, полученный от токена не отличим от ключа, полученного через пароль	Удовлетворительно. Возможно необходимо внедрить защиту биометрической информации если того требует законодательство
Совместимость с клиентским компьютером	Хорошо. Клиенты аутентификации изначально разработаны для парольных методов аутентификации	Удовлетворительно. Требуется поддержка со стороны специальных устройств	Удовлетворительно. Требуется поддержка со стороны специальных устройств
Доступность Наличие ограничений на использование в зависимости от конкретного индивидуума	Хорошо	Хорошо	Плохо Доступность метода может меняться от состояния здоровья, наличия травм. Люди с ограниченными возможностями могут быть не способны использовать определенные методы биометрической аутентификации. Для операторов АСУ ТП это может быть актуально если в сменен присутствует временный персонал, не прошедший медицинского отбора аналогичного для операторов
Способность обновляться	Удовлетворительно	Хорошо. При условии административной поддержки.	Плохо. Биометрия меняется очень медленно (голос, лицо) или не меняется совсем (отпечатки пальцев).
Сумма:	9	9	3

Рассмотрим набор показателей «безопасность» в контексте какие виды атак может предотвратить метод аутентификации см. таблицу 8.

Таблица 8. Показатель «безопасность» различных метода аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Сопротивляемость наблюдению со стороны	Плохо. Злоумышленник может выдавать себя за пользователя после того, как он один или	Хорошо	Хорошо

Показатель	Пароль	Токен	Биометрия
	несколько раз наблюдает за его аутентификацией. путем повторения наблюдения более, скажем, 10–20 раз. Атаки включают в себя сёрфинг через плечо, видеосъемку клавиатуры, запись звуков нажатия клавиш или телевизионное изображение клавиатуры и т.д.		
Сопротивляемость методам социальной инженерии	Хорошо. Знакомому (или опытному хакеру) невозможно выдать себя за конкретного пользователя, используя знание личных данных (дата рождения, имена родственников и т. д.)	Хорошо	Хорошо
Сопротивляемость простому угадыванию	Удовлетворительно. Зависит от длины пароля.	Хорошо	Хорошо
Сопротивляемость атакам от субъектов внутри компьютерной системы	Удовлетворительно. Зависит от длинны пароля	Хорошо	Удовлетворительно. Биометрические методы, как и пароль, имеют не высокую энтропию и длину ключа
Сумма:	4	8	7

Общая сумма по всем наборам показателей для каждого из методов:

	Пароль	Токен	Биометрия
Сумма	21	25	17

Анализ показывает, что токен может быть наиболее сбалансированным методом аутентификации, если он используется в качестве единственного метода аутентификации.

Заключение

Обзор доступных источников показывает, что на данный момент степень защиты, предоставляемая каждым из методов, сравнима. Общая проблема заключается в том, что, если аутентификатор неудобен, им либо не будут использоваться, либо не будут пользоваться должным образом, что может привести к уязвимости.

Наши опыты показали достаточно высокий процент ошибок первого рода (неправильный набор пароля) при наличии помехи даже при достаточно простом пароле. Поэтому при определении политики безопасности парольной защиты должны учитываться влияние ошибки первого рода на свойство доступности в системе, что автоматически ограничивает как частоту смены пароля, так и его сложность.

Биометрические методы аутентификации при теоретических значения ошибок первого рода ($\leq 10^{-2}$), на практике при типовых условиях и помехах для работы оператора показали худшие в несколько раз результаты. Основываясь на результатах тестирования, наиболее перспективным из исследованных биометрических методов мы считаем контроль по овалу лица. Однако даже он имеет высокий процент ошибок, поэтому его не следует объединять с блокирующей политикой безопасности. Мы предлагаем использовать его при многофакторной аутентификации вместе с парольным методом или токеном. Выбирая методы многофакторной аутентификации, следует принимать во внимание то, что энтропия ключа для биометрической и парольной защиты приблизительно одинакова, но для пароля энтропия ограничена возможностями человеческой памяти, а для биометрии - текущей аппаратной реализацией сканеров и датчиков биометрии.

Применение токена устраняет проблему запоминания паролей, но пользователь должен иметь с собой физический объект, что иногда неудобно, так как токен можно украсть, скопировать или потерять.

Можно сделать вывод, что для аутентификации оператора АСУ ТП возможно построить систему защиты, использующую различные методы и их комбинации. Мы считаем перспективной двухфакторную аутентификацию с блокирующей политикой безопасности для токена и неблокирующей для биометрического метода распознавания по овалу лица.

Литература

1. *Hu, Gongzhu.* (2018). On Password Strength: A Survey and Analysis. DOI: 10.1007/978-3-319-62048-0_12.
2. *Poletikin A.G., Zharko E. F., Mengazetdinov N., Promyslov V.G.* A Conception of the New Generation of Upper Level Control Systems of NPP APCS / Proceedings of the 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017, Moscow). Moscow: IEEE, 2017. Vol. 1. C. 414-418.
3. *L. O'Gorman*. "Comparing passwords, tokens, and biometrics for user authentication," in Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, Dec. 2003, doi: 10.1109/JPROC.2003.819611.
4. *Dworkin M., Barker E., Nechvata J., Foti J. , Bassham, L. , Roback, E. and Dray, J.* (2001), Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.197 (Accessed March 8, 2022)
5. Wiki1. https://en.wikipedia.org/wiki/List_of_the_most_common_passwords. Доступ 7/03/2022.
6. *D. Köhler, E. Klieme, M. Kreuseler, F. Cheng and C. Meinel*. "Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords," 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 2021, pp. 22-31, doi: 10.1109/CSP51677.2021.9357504.
7. *Alanezi N. A., Alharbi N. H., Alharthi Z. S. and Alhazmi O. H.,* " A Brief Overview of Biometrics in Cybersecurity: A Comparative Analysis," 2020 First Inter-national Conference of Smart Systems and Emerging Technologies (SMARTTECH), 2020, pp. 257-258, doi: 10.1109/SMART-TECH49988.2020.00067. 8.
8. *Антонова В.М., Балакин К.А., Гречишкина Н.А., Кузнецов Н.А.* Разработка системы аутентификации с использованием верификации диктора по голосу. Информационные процессы, Том 20, № 1, 2020, с. 10–21.
9. *Мао В*. Современная криптография: теория и практика. :Пер. с англ. – М.: Издательский дом "Вильямс", 2005. –768 с.
10. *Burrows M., Abadi M. and Needham R.M.* "A Logic for Authentication," DEC System Research Center Technical Report No. 39, February 1989.
11. *Giri D., Sherratt R. S., Maitra T. and Amin R.,* "Efficient biometric and password based mutual authentication for consumer USB mass storage devices," in IEEE Transactions on Consumer Electronics, vol. 61, no. 4, pp. 491-499, November 2015, doi: 10.1109/TCE.2015.7389804.
12. *Razaque K. K., Myrzabekovna S. Y., Magbatkyzy M., Almiani B. A., Doszhanovna and Alnusair A.* "Secure Password-Driven Fingerprint Biometrics Authentication," 2020 Seventh International Conference on Software Defined Systems (SDS), 2020, pp. 95-99, doi: 10.1109/SDS49854.2020.9143881.
13. *Dinca Lavinia & Hancke Gerhard. (*2017). User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks. Entropy. 19. 70. 10.3390/e19020070.
14. *Pierre-Alain Fouque, David Pointcheval, Sébastien Zimmer*. HMAC is a Randomness Extractor and Applications to TLS. Proceedings of the 3rd ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS '08), 2008, Tokyo, Japon. pp.21-32.