УДК 004.056.5

DOI: http://doi.org/10.25728/pu.2022.3.4

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ОПЕРАТОРОВ В ПРОМЫШЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ[1]

В.Г. Промыслов, К.В. Семенков, Н.Э. Менгазетдинов

Аннотация. Рассматривается проблема аутентификации операторов в автоматизированных системах управления технологическими процессами (АСУ ТП) промышленными объектами критической информационной инфраструктуры на примере АСУ ТП атомных электростанций (АЭС). Проведен обзор применяемых в информационных системах общего назначения методов аутентификации – парольного, токена и биометрических – и анализируется их применимость для типовых условий работы оператора АСУ ТП. Анализ включает как экспериментальное тестирование парольного и биометрического методов аутентификации, так и экспертную оценку преимуществ и недостатков методов аутентификации в АСУ ТП. В ходе тестирования все исследуемые методы показали несколько худшие значения ошибок первого рода по сравнению с характеристиками, известными из доступных источников. Наилучшие результаты показал метод биометрической аутентификации по овалу лица. Однако и для него процент ошибок первого рода значителен, что может повлиять на доступность функции управления для легитимного пользователя. Сделан вывод о перспективности реализации в АСУ ТП многофакторной аутентификации на основе токена или парольной защиты в качестве блокирующего метода аутентификации с дополнительным биометрическим методом аутентификации по овалу лица с неблокирующей политикой безопасности.

Ключевые слова: аутентификация, биометрия, токен, пароль, АСУ ТП, оператор.

ВВЕДЕНИЕ

Для современных производств, в том числе опасных, например, атомных станций, транспорта, предприятий химической промышленности и т. д., характерна зависимость от цифровых автоматизированных систем управления. В контуре управления таких систем чаще всего присутствует человек (оператор), который воздействует как на сам объект управления, так и на систему управления через компьютеры, входящие в состав АСУ ТП.

В промышленных системах при решении задачи допуска доверенного оператора к управлению технологическим объектом возникают вопросы аутентификации. В частности, задачу аутентификации необходимо решать при наделении оператора правами на выполнение определенных действий с объектом управления, что в информационных технологиях принято называть авторизацией. Аутентификацию можно определить как «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» [1].

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

Неавторизованные действия оператора могут не только к нарушить основные свойства информационной безопасности (целостность, доступность и конфиденциальность), но нанести экономический ущерб или 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 аутентифи-

[1] Исследование (п. 2.3–2.5) выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-29-06044.

кации даже в рутинных операциях в цифровых системах управления.

Решение задачи аутентификации операторов АСУ ТП критических объектов имеет особенности, связанные как с объектом управления, так и с политикой информационной безопасности [2]. Это отличает аутентификацию операторов АСУ ТП от аутентификации в информационных системах общего пользования. Перечислим основные из этих особенностей:

- наличие контролируемой физической зоны безопасности для доступа на объект снижает угрозу со стороны внешнего нарушителя в задаче аутентификации персонала; однако это не устраняет опасность, связанную с действиями внутреннего нарушителя, когда человек, допущенный в зону безопасности, но не имеющий полномочий оператора, пытается получить доступ к функциям операторского управления;
- приоритет доступности над другими свойствами информационной безопасности приводит к тому, что в задаче аутентификации ставятся жесткие ограничения на длительность процесса аутентификации и на вероятность ошибки первого рода (ошибочной негативной аутентификации объекта);
- в работе оператора могут возникнуть стрессовые ситуации (например, техногенная авария), отчего человек может забыть очевидные вещи, у него могут поменяться функциональные и внешние характеристики (задрожать руки, измениться тембр голоса, он может вспотеть и т. д.);
- из-за изменений внешней среды могут появиться помехи аутентификации; помеха – это некоторое изменение внешней среды, которое не приводит к разрушению объекта и немедленному отказу функций в АСУ ТП или на самом объекте, но вызывает неудобство для оператора, например, частичный выход из строя системы освещения, задымление, срабатывание системы пожаротушения, землетрясение и т. д.

Задачи аутентификации для промышленных систем, как и для обычных информационных систем, включают в себя и аутентификацию оператора (пользователя) на компьютере (цифровом устройстве), и аутентификацию самих компьютеров. Для информационных систем общего пользования задача аутентификации между компьютерами хорошо проработана [3, 4], но для промышленных систем, где применяются контроллеры и промышленные компьютеры, часто используются протоколы со слабыми механизмами аутентификации или даже вообще без аутентификации. Однако проблема обеспечения надежной аутентификации «компьютер – компьютер» в промышленных системах является скорее проблемой конкретных реализаций, чем научного исследования.

Протоколы, используемые для задачи аутентификации пользователей, гораздо менее безопасны, чем протоколы аутентификации между компьютерами, так как имеют дело с людьми и их лимитированными возможностями и слабостями [5]. В области информационной безопасности люди часто являются слабым звеном в защите.

Целью настоящей работы является выбор и обоснование методов и протокола аутентификации для применения их в задаче аутентификации операторов АСУ ТП. В работе анализируются основные методы и протоколы аутентификации пользователей и проводится их экспериментальное тестирование и анализ с учетом особенностей функционирования промышленных объектов и используемых политик информационной безопасности. В качестве примера промышленной системы управления для исследований выбрана разработанная в ИПУ РАН система верхнего блочного уровня АСУ ТП АЭС [6].

При проведении экспериментальных исследований предполагалось, 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 данной работы.

1. ПРОТОКОЛЫ 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 [7]:

– Что вы знаете?

– Что у вас есть?

– Кто вы?

Часто три метода аутентификации ассоциируются с их характерными представителями: паролем, токеном и биометрическим признаком. Поэтому, описывая каждый из методов, мы будем приводить ссылку на их конкретные реализации. Во всех случаях объектом аутентификации является человек.

1.1. Парольные методы аутентификации

Пароль – это секретное слово, которое знает пользователь и, возможно, компьютер, на котором пользователь аутентифицируется. Это слово связано с ключом, по которому происходит аутентификация. В теории парольный метод аутентификации может быть весьма стойким: например, в случае применения расширенного стандарта шифрования [8] максимальная длина ключа составляет 256 бит, и чтобы угадать ключ, злоумышленнику в среднем потребуется более 10^{76} попыток, что займет слишком много времени и сейчас, и в обозримом будущем. В случае непосредственной зависимости пароля и ключа, используемого для аутентификации, для обеспечения высокой стойкости ключа необходим пароль сравнимой длины, а такое количество символов слишком велико для запоминания человеком. Поэтому на практике этот ключ хранится, например, в файле, защищенном более запоминающимся (то есть коротким) паролем. Основная уязвимость парольной защиты состоит в том, что запоминающийся пароль может быть угадан или найден злоумышленником [5, 9], а длинный, случайный, меняющийся пароль трудно запомнить, и тогда его могут записать и хранить в открытом виде. Считается [10, 11], что около 20 % пользователей из всех возможных сочетаний паролей используют не более пяти тысяч. Следовательно, пространство поиска для взлома системы снижается, и злоумышленник часто может сосредоточиться на этих пяти тысячах сочетаний.

Недостатков парольного метода аутентификации можно избежать, используя методы иных классов, в соответствии с которым в 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. Также этот термин может относиться и к программным токенам, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам. Токены могут быть как пассивными, так и активными (например, предоставляющими одноразовые коды доступа либо изменяющимися синхронно с мастером на хосте и т. д.) Безопасность токена обеспечивают различные средства защиты, например, футляр или специальное аппаратное обеспечение, которое отключает токен, если он скомпрометирован или если количество неудачных попыток аутентификации превысит выбранный порог.

В общем случае токен можно рассматривать как секрет, 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

Для человека как пользователя биометрия – наиболее удобный и простой способ аутентификации, поскольку она является продолжением естественных способов установления личности.

Биометрия, или биометрические персональные данные, – это некоторая измеримая индивидуальная характеристика человеческого тела, достаточная для того, чтобы ее можно было использовать для аутентификации пользователя. Стандарт [1] определяет биометрические персональные данные как сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность.

Биометрия призвана неразрывно связать аутентификатор (признак) и владельца аутентификационного признака, что в случае пароля и токена принципиально сделать нельзя, 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 такие доказательства выполнения определенных действий, что вовлеченные стороны не могут впоследствии отклонить транзакцию как несанкционированную или заявить, что не выполняли этих действий. Однако биометрические характеристики, как и пароли, можно скопировать или подделать с бо́льшим или меньшим уровнем затрат и 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. К физическому типу относят биометрию, основанную на стабильных характеристиках тела: отпечатках пальцев,

лице, радужной оболочке глаза, форме руки и др. К поведенческому типу относятся 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 [12–14].

Биометрический метод аутентификации, как и прочие методы, может приводить к ошибкам [15], однако отношение пользователя к ошибкам при разных методах аутентификации различается. Пользователь может забыть или неправильно ввести пароль, может потерять токен. Эти ошибки неудобны, но пользователь осознает, что виноват он сам. В случае ошибки биометрической аутентификации пользователь не виноват и не может сам устранить проблему.

Биометрическая ошибка может возникнуть по разным причинам, например:

– грязный сканер,

– плохое освещение,

– система изначально запомнила неправильный шаблон 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.).

Один из последних примеров проблем биометрии связан с необходимостью носить маски в связи с пандемией.

Детальные требования к биометрическим методам аутентификации приведены в различных нормативных документах, например, в стандарте [16].

1.4. Протоколы аутентификации и их применение в АСУ ТП

В контексте задачи аутентификации пользователя мы будем рассматривать самый общий протокол аутентификации [17], устанавливающий правила обмена, которые необходимо применять для обеспечения аутентификации на основе двусторонне согласованной секретной информации.

Для информационных систем общего пользования популярными вариантами протокола аутентификации являются протокол «оклик – отзыв» [18]. Варианты протокола «оклик – отзыв» лежат в основе протоколов аутентификации Unix с модулями PAM [19] и MS Windows [20] и в их составе могут использоваться для аутентификации оператора АСУ ТП. Опыт авторов показывает, что применение протокола для парольного метода аутентификации ограничено из-за требований обеспечения доступности и сценариев работы оператора при выполнении критичных функций системы. Тем не менее, применение протокола возможно, например, для доступа к функции перепрограммирования цифрового устройства.

В реальных системах протоколы аутентификации для достижения высокого уровня защиты и обеспечения ее эшелонирования могут объединять несколько разных методов аутентификации [21]. Такая аутентификация называется многофакторной. Многофакторная аутентификация реализует алгоритм логического «И», когда для успешной аутентификации необходимо, чтобы аутентификация всеми методами прошла успешно. В настоящее время в подавляющем большинстве случаев при многофакторной аутентификации используется связка «физический токен – пароль» [22, 23]. Совместное применение пароля и биометрического идентификатора используют редко, потому что биометрию обычно применяют 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. В табл. 1 сведены основные преимущества и недостатки некоторых методов многофакторной аутентификации, а также экспертная оценка их пригодности для задач аутентификации оператора АСУ ТП по качественной шкале «плохо» – «удовлетворительно» – «хорошо».

Основные протоколы аутентификации легко модифицируются для применения в многофакторной аутентификации. Однако для реализации политики безопасности с высокими требованиями к доступности, характерными для АСУ ТП, введение дополнительной транзакции и сложности в протокол может привести к негативным последствиям.

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. АНАЛИЗ И СРАВНЕНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ

2.1. Принципы сравнения

Сравним три основных метода аутентификации с точки зрения их применимости в АСУ ТП на примере их характерных представителей. Сравнение будем проводить 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 [7].

В табл. 2 приведены основные атрибуты трех методов аутентификации.

Таблица 1

Сравнение методов многофакторной сильной защиты аутентификации пользователя для получения более сильной защиты в АСУ ТП

Комбинация методов аутентификации	Преимущества	Недостатки	Пример	Оценка 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 уникальностью его владельца	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 идентификатора пользователя (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
«Что вы знаете?» + «Что у вас есть?» + «Кто вы?»	Все три метода работают последовательно	Нужно иметь токен и помнить пароль. Может приводить к ложному отказу при аутентификации из-за несовершенства биометрических методов	Аутентификация для доступа на критически важный объект, включающая пропуск с чипом и фотографией, на входе в объект, биометрический сканер по отпечатку пальца для доступа в помещение и пароль для доступа к компьютеру	Плохо

Таблица 2

Три основных метода аутентификации пользователя и их атрибуты

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

2.2. Практическая энтропия ключа

Сравнение стойкости различных методов аутентификации – непростая задача, так как в зависимости от реализации метода аутентификации используемый в протоколе ключ может иметь различную связь с исходными данными, предоставляемыми методом. Например, для парольного метода ключ может просто представлять собой хранимую копию пароля, или его хеш-код, или проверочные значения, которые зависят от паролей, но не могут быть непосредственно использованы злоумышленником для аутентификации. Для других методов аутентификации вместо пароля может использоваться некоторое значение, полученное от токена или устройства биометрии.

Поэтому для оценки стойкости методов аутентификации воспользуемся метрикой, основанной на энтропии ключа, который может быть непосредственно получен из исходных данных (пароля, информации хранимой в токене, или биометрических данных). Исследования энтропии ключей, полученных на основе паролей, проведенные в крупных IT-компаниях, имеющих большой объем персональных данных (Yahoo, Google) [5], показывают, что энтропия ключа составляет 10–20 бит. Причем отмечается, что применение хеш-кода уменьшает энтропию ключа, который скорее ближе к левой границе (т. е. к 10 битам), так как хеш-код оптимизирован для обеспечения быстродействия, что уменьшает стойкость ключа. Хотя, например, реализации алгоритмов хеширования SHA1 (*Secure Hash Algorithm* 1) [24] являются настраиваемыми и могут быть весьма стойкими.

Ранние исследования [5] показывали, что энтропия ключа и, следовательно, стойкость метода для биометрического и парольного видов защиты примерно одинакова, но более поздние работы свидетельствуют о том, что биометрические методы позволяют получить степень защиты в два-три раза лучшую, чем парольные [25].

Специальные исследования по стойкости парольного метода для операторов АСУ ТП авторам неизвестны. Однако представляется целесообразным 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, получаемого на основе данных и содержащегося в токене, может быть весьма большой при использовании алгоритмов, аналогичных методам аутентификации «компьютер – компьютер». Например, в работе [26] приведены значения энтропии ключа до 128 бит. Однако нужно учитывать вероятность кражи токена, которая может оказаться значительной, особенно при наличии злого умысла.

2.3. Основные характеристики качества распознавания

Для оценки качества распознавания традиционно используются 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 решении о положительной аутентификации. Чем лучше система, тем при одинаковых значениях FAR меньше значение FRR. Параметр FAR имеет смысл приводить только для биометрического метода аутентификации, так как для остальных методов аутентификации значение отражает способности человека (набор и запоминание парольной фразы) или надежность аппаратной реализации.

У любого метода аутентификации есть некоторая доля ошибок, связанная с отказом аппаратуры, например, считывателя токена или клавиатуры, однако, как показывает практика, она пренебрежимо мала. Качество биометрической аутентификации является наиболее неустойчивой характеристикой, так как существенно зависит от конкретного человека. В табл. 3 содержатся типовые характеристики различных способов биометрического метода аутентификации, найденные авторами в литературе. Типовые характеристики демонстрируют только тенденцию, сравнение реализаций и алгоритмов для биометрического метода выходит за рамки настоящей работы.

Таблица 3

Типовые параметры ошибок для биометрического метода

Тип биометрии	FAR	FRR	Размер выборки (согласно работе [27])	Источник
Распознавание по отпечатку пальца	10^{-3}	10^{-2}	$5 \cdot 10^6$	[27]
Распознавание по овалу лица	0,058		$12 \cdot 10^6$	[27]
Распознавание по сетчатке глаза	0,059		$500 \cdot 10^3$	[27]

Чтобы исследовать практические аспекты применимости коммерчески доступных устройств для биометрической аутентификации операторов АСУ ТП, мы провели дополнительное тестирование, в ходе которого имитировались некоторые характерные условия работы оператора АСУ ТП. Результаты приведены в п. 3.4.

2.4. Практическое тестирование пригодности методов аутентификации для операторов АСУ ТП

Авторами были проведены испытания 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 они стабильны в процессе эксплуатации.

В табл. 4 приведены используемые коммерческие устройства и тип биометрической аутентификации, доступный на устройстве. Использовались устройства, официально поставляемые в Российскую Федерацию и не имеющие лицензионных ограничений на момент написания статьи. Для тестирования биометрических методов аутентификации выбирались устройства и алгоритмы, доступные массовому потребителю, 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. Как показывает опыт авторов, именно массовые продукты в основном применяются в реализации технических мер защиты для промышленных систем.

Для каждого из методов проводилось не менее 50 тестов. Каждый тест проводила группа из двух испытателей, один (оператор) по команде другого испытателя делал попытку аутентифицироваться с применением одного из методов аутентификации.

Таблица 4

Устройства, используемые в ходе тестирования

Устройство	Тип аутентификации
HONOR 10. Android version 10	Распознавание по отпечатку пальца; распознавание по овалу лица
MI 5S Plus. Android version 8. MIUI Global 10.2	Распознавание по отпечатку пальца
Персональный компьютер с мембранной клавиатурой	Парольная защита

В ходе тестирования испытатели в группе периодически менялись ролями. В каждом тесте измерялось время, за которое была проведена аутентификация, и число затраченных попыток до удачной аутентификации. Тесты проводились как в обычных, нормальных внешних условиях, так и при наличии помех, осложняющих аутентификацию (табл. 5).

Таблица 5

Типы вводимых при тестировании помех

Обозначение помехи	Описание
Помеха 1	Нагретые руки
Помеха 2	Чехол на сенсоре
Помеха 3	Вода тонким слоем на пальце
Помеха 4	Охлаждение пальца
Помеха 5	Маска на лице
Помеха 6	Изменение угла между камерой и лицом объекта
Помеха 7	Изменение освещенности
Помеха 10	Ввод пароля стоя
Помеха 11	Ввод пароля в перчатках
Помеха 12	Ввод пароля «вслепую»
Помеха 13	Ввод пароля при физической помехе (один из испытателей подталкивал другого)

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

Результаты испытаний приведены в табл. 6.

Таблица 6

Тестирование методов аутентификации

Тест (Условия)	Результат	
	Время максимальное, минимальное и среднее, с	Максимальное число попыток для успешной аутентификации
Простой пароль (5 символов; базирующийся на словарном слове; нормальные условия)	2,63; 1,82; 2,1	1
Простой пароль (5 символов; базирующийся на словарном слове; помеха 8)	6,34; 2,1; 2,3	2
Простой пароль (5 символов; базирующийся на словарном слове; помеха 9)	9,29; 1,68; 4,2	3
Простой пароль (5 символов; базирующийся на словарном слове; помеха 10)	12,64; 2,37; 5,62	4
Простой пароль (5 символов; базирующийся на словарном слове; помеха 11)	20,33; 2;06; 6,12	6
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; нормальные условия)	24,5; 5,33; 9,1	3
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 10)	11,59; 5,98; 6,6	1
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 11)	49,03; 9,1; 12;6	3
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 12)	95,31; 7,8; 23,4	11
Сложный пароль (не менее 9 символов; большие и маленькие буквы, цифры; помеха 13)	46,39; 8,1; 24,3	4
Отпечаток пальцев (нормальные условия)	3,92; 0,99; 1,44	2
Отпечаток пальцев (помеха 1)	1,23; 1,09; 1,2	1
Отпечаток пальцев (помеха 2)	2,69; 1,09; 1,82	3
Отпечаток пальцев (помеха 3)	9,48; 1,05; 3,61	6
Отпечаток пальцев (помеха 4)	3,59; ,2,1; 1,7	3
Овал лица (нормальные условия)	2,87; 1,85; 1,91	1
Овал лица (помеха 5)	4,23; 1,7; 2,64	2
Овал лица (помеха 6)	5,42; 1,64; 3,26	2
Овал лица (помеха 7)	2,09; 0,99; 1,2	1

Для парольного метода получена относительно высокая ($\sim 10^{-1}$) вероятность отказа в доступе человеку, имеющему право доступа, при наличии помех. Вероятность ошибки первого рода возрастает при увеличении сложности пароля. Большая вероятность ошибки оператора при вводе пароля, особенно сложного, при наличии помехи приводит к тому, что оператор вынужден неоднократно (в тестах это значение достигало 11 раз) вводить пароль для успешной аутентификации. Время аутентификации в этом случае вырастает на порядок при типовом значении около двух-трех секунд для простого пароля и около пяти секунд для сложного пароля.

В АСУ ТП такие задержки могут быть критическими. Это может стать основанием для 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 овалу лица. Для биометрических методов аутентификации проводилось дополнительное тестирование с це-

лью выявить возможность ложной аутентификации. Ни по одному из используемых биометрических методов не удалось добиться ложной аутентификации в пределах средств, доступных обычному пользователю ($FAR = 0$). Это не означает, что биометрическая аутентификация в условиях работы оператора АСУ ТП свободна от ошибок второго рода и что полученные данные противоречат типовым значениям, приведенным в предыдущем разделе. Причинами могут быть как ограниченность используемой выборки, так и то, что обход систем защиты требует знания как особенностей реализаций используемых алгоритмов для сравнения биометрического шаблона, так и, возможно, специального реквизита.

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.

2.5. Анализ применимости методов аутентификации в АСУ ТП

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

- Аутентификаторы, основанные на знаниях («Что вы знаете?»), включают в себя секретную информацию (пароль), но такая информация является не столько секретной, сколько «неизвестной». Данной информации можно дать приблизительно такое определение – «скрытая от большинства людей». Недостатком секретов является то, что при каждом их использовании для аутентификации они становятся все менее секретными. К тому же «большинство людей» часто означает «большинство честных людей», а для злоумышленника при некотором усилии (например, путем применения средств социальной инженерии) такая информация перестает быть закрытой. Для систем управления АСУ ТП характерен высокий уровень доверия между пользователями, возникающего как в результате отбора персонала, так и в ходе производственной деятельности, 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.

- 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 нашел, может обойти систему защиты. В этом смысле слабости объектных аутентификаторов аналогичны парольной защите: злоумышленник может использовать потерянный или украденный токен. Как и при парольной защите, пользователи АСУ ТП склонны доверять друг другу. Однако, в отличие от парольной защиты, при утере физического объекта владелец узнает об этом при первом обращении к нему и сможет принять меры для скорейшей нейтрализации угрозы.

- 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 радужной оболочки, голосовой отпечаток или подпись. Биометрический метод аутентификации имеет сравнительно высокую степень защиты в части копирования и подделки и очевидно не может быть утерян [28].

Суммируя вышесказанное, можно заключить, что ни один из этих методов аутентификации не идеален, они имеют некоторый набор «врожденных» недостатков. В табл. 7 приведены характерные уязвимости различных методов аутентификации применительно к задачам АСУ ТП.

Легко заметить, что в контексте политики безопасности АСУ ТП возможности для атак на систему аутентификации неравнозначны. Если на предприятии имеется постоянно действующая система обнаружения вторжений и есть должностные 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, по мнению авторов, 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.

Таблица 7

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	Информирование пользователя 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	
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	Неблокирующая политика безопасности с нотификацией офицера по безопасности
Ложная аутентификация	Пароль, токен, биометрия	Атака с повторной передачей сообщений	Протокол «оклик – отзыв»
	Пароль	Атака перебором	Блокирующая политика безопасности при некотором числе неудачных попыток аутентификации

2.6. Качественный анализ и сравнение методов аутентификации для АСУ ТП

Для сравнения методов аутентификации можно предложить различные показатели. Рассмотрим три высокоуровневых показателя, которые традиционно используются для сравнения методов аутентификации [5]:

– удобство использования,

– удобство развертывания,

– безопасность.

В каждом из наборов высокоуровневых показателей выделим набор показателей более низкого уровня. Значения всех показателей в наборе будут оцениваться по ранговой шкале: «хорошо» – 2, «удовлетворительно» – 1, «плохо» – 0. Значение высокоуровневого показателя вычислим как сумму отдельных показателей в наборе.

Рассмотрим группы показателей «удобство использования» (табл. 8) и «удобство развертывания» (табл. 9). В табл. 10, в свою очередь, представлен набор показателей из группы «безопасность» в контексте того, какие виды атак может предотвратить метод аутентификации.

Таблица 8

Показатели из группы «удобство использования» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Легкость взаимодействия со схемой аутентификации для пользователя	Удовлетворительно	Хорошо	Удовлетворительно
Простота обучения: пользователи, не знакомые с методом, могут понять его и освоить 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
Простое восстановление после компрометации	Хорошо. Преимущество паролей – их легко сбросить	Удовлетворительно	Плохо
Необходимость что-то иметь при себе	Хорошо	Плохо	Хорошо
Сумма	8	8	7

Таблица 9

Показатели группы «удобство развертывания» для различных методов аутентификации для применения в АСУ ТП

Показатель	Пароль	Токен	Биометрия
Простота внедрения метода 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

См. окончание табл. 9

Окончание табл. 9

Показатель	Пароль	Токен	Биометрия
Доступность. Наличие ограничений на использование в зависимости от конкретного индивидуума	Хорошо	Хорошо	Плохо Доступность метода может меняться в зависимости 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 смене присутствует временный персонал, не прошедший медицинский отбор, аналогичный тому, который проходят операторы
Возможность обновления	Удовлетворительно	Хорошо. При условии административной поддержки	Плохо. Биометрия меняется очень медленно (голос, лицо) или не меняется совсем (отпечатки пальцев)
Сумма	9	9	3

Таблица 10

Показатели группы «безопасность» для различных методов 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 несколько раз наблюдает за его аутентификацией путем повторения наблюдения более, допустим, 10–20 раз. Атаки включают в себя серфинг через плечо, видеосъемку клавиатуры, запись звуков нажатия клавиш или телевизионное изображение клавиатуры и т. д.	Хорошо	Хорошо
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 со стороны субъектов внутри компьютерной системы	Удовлетворительно. Зависит от длины пароля	Хорошо	Удовлетворительно. Биометрические методы, как и пароль, имеют невысокую энтропию и длину ключа
Сумма	4	8	7

В табл. 11 приведены суммарные оценки методов аутентификации по всем группам показателей. Результаты проведенного анализа демонстрируют, что токен может быть наиболее сбалансированным методом, если он используется в качестве единственного метода аутентификации.

Таблица 11

Суммарная оценка каждого из методов по всем группам показателей

	Пароль	Токен	Биометрия
Сумма	21	25	17

ЗАКЛЮЧЕНИЕ. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Подчеркнем, что в задачу данной работы входило не собственно исследование известных на сегодняшний момент методов аутентификации, а рассмотрение особенностей их применения для решения задачи аутентификации оператора АСУ ТП.

Был учтен накопленный опыт использования методов аутентификации для информационных систем общего назначения. Обзор доступных источников показывает, что на данный момент степени защиты, предоставляемые каждым из методов, сравнимы. Общая проблема заключается в том, что, если аутентификатор неудобен, им либо не пользуются, либо пользуются недолжным образом, что может привести к уязвимости. На практике это означает, что если для доступа к разным рабочим местам или для выполнения разных операций операторам АСУ ТП будет нужно запоминать несколько паролей, то они будут выбирать простые пароли или пароли, связанные простой зависимостью. В политике безопасности предприятия могут предъявляться определенные требования к паролям (например, длина, использование специальных символов) для увеличения энтропии. Однако мы полагаем, что такие требования к паролям редко приводят к увеличению энтропии ключа. Компетентный взломщик может учесть ограничения паролей, накладываемые политикой безопасности, при составлении таблиц хеш-кодов, используемых для взлома системы, либо, что еще проще, может просто подсмотреть пароль, так как сложный пароль оператор будет записывать на бумаге и носить с собой.

Проведенные 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 должно учитываться влияние ошибок первого рода на свойство доступности в системе, что автоматически ограничивает как частоту смены пароля, так и его сложность.

Биометрические методы аутентификации на практике при типовых условиях и помехах для работы оператора показали значения ошибок первого рода в несколько раз хуже теоретических ($\leq 10^{-2}$). Основываясь на результатах приведенного тестирования, наиболее перспективным из исследованных биометрических методов представляется контроль по овалу лица. Однако даже он имеет высокий процент ошибок, поэтому его не рекомендуется объединять с блокирующей политикой безопасности. Предлагается использовать его при многофакторной аутентификации вместе с парольным методом или токеном. Выбирая методы многофакторной аутентификации, стоит 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 носитель, 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. Операторы АСУ ТП, как правило, работают в помещении с контролируемым физическим доступом. Исходя из этого, в пределах контролируемой зоны безопасности можно установить процедуру доступа на основе токенов с дополнительным видеоконтролем со стороны службы безопасности. По мнению авторов, перспективной является двухфакторная аутентификация с блокирующей политикой безопасности для токена и неблокирующей для биометрического метода распознавания по овалу лица.

ЛИТЕРАТУРА

1. *ГОСТ* Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения. [*GOST* R 58833-2020. Zashchita informacii. Identifikaciya i autentifikaciya. Obshchie polozheniya. (In Russian)]
2. *Исхаков С.Ю.,* Шелупанов А.А., Исхаков А.Ю. Имитационная модель комплексной сети систем безопасности // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 2(32). – С. 82–86. – EDN SEBGNR. [*Iskhakov, S.Yu., Shelupanov, A.A., Iskhakov, A.Yu.* Imitacionnaya model' kompleksnoj seti sistem bezopasnosti // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. – 2014. – No. 2(32). – P. 82–86. – EDN SEBGNR.
3. *Dierks, T. and Rescorla, E.* The Transport Layer Security (TLS) Protocol Version 1.1. – RFC 4346, 2006.
4. *Conte de Leon, D., Makrakis, G.M., Kolias, C.* "Cybersecurity," in Resilient Control Architectures and Power Systems. – IEEE, 2022. – P. 89–111. – DOI: 10.1002/9781119660446.ch7.
5. *Hu, G.* On Password Strength: A Survey and Analysis. – Springer International Publishing, 2018. – DOI: 10.1007/978-3-319-62048-0_12.
6. *Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г.* и др. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУ ТП ДЛЯ АЭС

«БУШЕР» на основе отечественных технологий. – М.: ИПУ РАН. – 2013. – 95 с. [*Mengazetdinov, N.E., Poletykin, A.G., Promyslov, V.G.* i dr. Kompleks rabot po sozdaniyu pervoj upravlya-yushchej sistemy verhnego blochnogo urovnya ASUTP DLYA AES «BUSHER» na osnove otechestvennyh tekhnolo-gij. – M.: IPU RAN. – 2013. – 95 s. (In Russian)]

7. *O'Gorman, L.* Comparing Passwords, Tokens, and Biometrics for User Authentication / Proceedings of the IEEE. – 2003. – Vol. 91, no. 12. – P. 2021–2040. – DOI: 10.1109/JPROC.2003.819611.
8. *Dworkin, M., Barker, E., Nechvatal, J.,* et al. Advanced Encryption Standard (AES). – Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 2001. – DOI: 10.6028/NIST.FIPS.197.
9. *Jobusch, D.L., Oldehoeft, A.E.* A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 1 // Computers & Security. – 1989. – Vol. 8, iss. 7. – P. 587–604. – DOI: 10.1016/0167-4048(89)90051-5.
10. *The 200 Worst* Passwords of 2021 Are Here and Oh My God. – https://gizmodo.com/the-200-worst-passwords-of-2021-are-here-and-oh-my-god-1848073946 (дата обращения 7.03.2022).
11. *Most* Common Passwords of 2021. – https://nordpass.com/most-common-passwords-list/ (дата обращения 7.03.2022).
12. *Köhler, D., Klieme, E., Kreuseler, M.,* et al. 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. – P. 22–31. – DOI: 10.1109/CSP51677.2021.9357504.
13. *Alanezi, N.A., Alharbi, N.H., Alharthi, Z.S., and Alhazmi, O.H.* POSTER: A Brief Overview of Biometrics in Cybersecurity: A Comparative Analysis / 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH). – 2020. – P. 257–258. – DOI: 10.1109/SMART-TECH49988.2020.00067.
14. *Антонова В.М., Балакин К.А., Гречишкина Н.А., Кузнецов Н.А.* Разработка системы аутентификации с использованием верификации диктора по голосу / Информационные процессы. – 2020. – Т. 20, № 1. – С. 10–21. [*Antonova, V.M., Balakin, K.A., Grechishkina, N.A., Kuznetsov, N.A.* Development of an authentication system using voice announcer verification / Informacionnye processy. – 2020. – Vol. 20, no. 1. – P. 10–21. (In Russian)]
15. Machine Learning Masters the Fingerprint to Fool Biometric Systems: https://engineering.nyu.edu/news/machine-learning-masters-fingerprint-fool-biometric-systems (дата обращения 12.07.2022)
16. *ГОСТ* Р 52633.0-2006. Требования к средствам высоконадежной биометрической аутентификации. [*GOST* R 52633.0-2006. Trebovaniya k sredstvam vysokonadezhnoj biometricheskoj autentifikacii. (In Russian)]
17. *Mao B.* Современная криптография: теория и практика. Пер. с англ. – М.: Издательский дом «Вильямс». – 2005. – 768 с. [*Mao, V.* Sovremennaya kriptografiya: teoriya i praktika. Per. s angl. – M.: Izdatel'skij dom «Vil'yams». – 2005. – 768 s. (In Russian)]
18. *Burrows, M., Abadi, M., and Needham, R.M.* A Logic for Authentication / DEC System Research Center Technical Report. – 1989. – No. 39.
19. *Krawczyk, H., Bellare, M., Canetti, R.* HMAC: Keyed-Hashing for Message Authentication. – RFC 2104, 1997.
20. *Agorithms* for Challenge/Response Authentication. – https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/4d1a2cb0-0951-462a-8582-121fd1afe28e (дата обращения 7.03.2022).
21. *Исхаков А.Ю.* Система двухфакторной аутентификации на основе QR-кодов / Безопасность информационных технологий. – 2014. – Т. 21. – № 3. – С. 97–101. – EDN TRZJLN. [*Iskhakov, A.Y.* Two-Factor Authentication System Based on QR-Codes / IT Security (Russia). – 2014. – Vol. 21, no. 3. – P. 97–101. (In Russian)]
22. *Giri, D., Sherratt, R.S., Maitra, T., and Amin, R.* Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices / IEEE Transactions on Consumer Electronics. – 2015. – Vol. 61, no. 4. – P. 491–499. – DOI: 10.1109/TCE.2015.7389804.
23. *Razaque, K.K. Myrzabekovna, S.Y. Magbatkyzy, M.,* et al. Secure Password-Driven Fingerprint Biometrics Authentication / 2020 Seventh International Conference on Software Defined Systems (SDS). – 2020. – P. 95–99. –DOI: 10.1109/SDS49854.2020.9143881.
24. *Eastlake, D., Jones, P.* US Secure Hash Algorithm 1 (SHA1). – RFC 3174, 2001.
25. *Dinca, L. and Hancke, G.* User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks // Entropy. – 2017. – Vol. 19, no. 2. – DOI: 10.3390/e19020070.
26. *Fouque, P.-A., Pointcheval, D., Zimmer, S.* HMAC is a Randomness Extractor and Applications to TLS / Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security (ASIACCS '08). – Tokyo, Japan, 2008. – P. 21–32.
27. *Jain, A.K., Deb, D., and Engelsma, J.J.* Biometrics: Trust, but Verify / IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2021. – DOI: 10.1109/TBIOM.2021.3115465.
28. *Alsellami, B., Deshmukh, P.D., Ahmed, Z.A.T.* Overview of Biometric Traits / 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA). – 2021. – P. 807–813. DOI: 10.1109/ICIRCA51532.2021.9545069.

Статья представлена к публикации членом редколлегии А.О. Калашниковым.

Поступила в редакцию 6.05.2022,
после доработки 30.06.2022.
Принята к публикации 11.07.2022.

Промыслов Виталий Георгиевич – канд. физ.-мат. наук,
✉ vp@ipu.ru,

Семенков Кирилл Валерьевич – канд. физ.-мат. наук,
✉ semenkovk@ipu.ru,

Менгазетдинов Надыр Энверович – ст. науч. сотрудник,
✉ mengazne@mail.ru,

Институт проблем управления им. В.А. Трапезникова РАН,
г. Москва.

ASSESSMENT OF OPERATOR AUTHENTICATION METHODS IN INDUSTRIAL CONTROL SYSTEMS

V.G. Promyslov[1], K.V. Semenkov[2], N.E. Mengazetdinov[3]

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

[1]✉ vp@ipu.ru, [2]✉ semenkovk@mail.ru, [3]✉ mengazne@mail.ru

Abstract. This paper considers the authentication of operators in instrumentation and control (I&C) systems for industrial facilities. The main emphasis is on such systems for critical facilities, on an example of nuclear power plants (NPPs). Authentication methods known for public information systems (password, token, and biometrics) are surveyed, and their applicability in typical operating conditions of an I&C operator is analyzed. The analysis includes experimental testing of password and biometric authentication methods and an expert assessment of their advantages and disadvantages for I&C systems. According to the testing results, all the methods under consideration have somewhat worse values of the false rejection rate (FRR) compared with the known characteristics from available sources. The best results are shown by biometric identification by the face oval. However, the percentage of FRR for this method is significant, which can affect the availability of the control function for a legitimate operator. As concluded, a promising approach for industrial control systems is to implement multi-factor authentication: token or password protection for blocking authentication jointly with biometric authentication by the face oval with a non-blocking security policy.

Keywords: authentication, biometrics, token, password, industrial control system, I&C, operator.

Funding. This work (Sections 2.3–2.5) was supported in part by the Russian Foundation for Basic Research, project no. 19-29-06044.