Информационные процессы, Том 1, № 1, 2001, стр. 1–10.

НАЗВАНИЕ РАЗДЕЛА, ГДЕ ПРЕДСТВАЛЯЕТСЯ СТАТЬЯ

Идентификация в компьютерных системах цифровой экономики

А.В. Бродский[*], В.А. Горбачев[**], О.Э. Карпов[***], В.А. Конявский[****], Н.А. Кузнецов[****], А.М. Райгородский[‡], С. А. Тренин[§]

[*] *ПАО Сбербанк, г. Москва*
[**] *ФГУП ГНЦ РФ, МФТИ, г. Москва*
[***] *НХМЦ им. Пирогова, г. Москва*
[****] *МФТИ, г. Долгопрудный*
[‡] *МФТИ, г. Долгопрудный, Кавказский математический центр Адыгейского госуниверситета, Республика Адыгея, г. Майкоп*
[§] *МГТУ им. Баумана, Москва*

Поступила в редколлегию 26.11.2018

Аннотация—Предложен новый способ интерактивной идентификации – доверенной идентификации человека с использованием недоверенных устройств (например, смартфонов, планшетов и т.д.). Показано, что статичные, неизменяемые или почти неизменяемые биометрические признаки можно применять в криминалистике, но нецелесообразно для компьютерных систем цифровой экономики. В качестве признаков малоэффективно использование отпечатков пальцев, радужной оболочки и сетчатки глаза, рисунка сосудистого русла и аналогичных. Напротив, необходимо использовать динамические характеристики, имманентно присущие человеку, отражающиеся, например, в рефлексах. В качестве таковых могут использоваться движения глаз при чтении и/или слежении за стимулом, саккады, пульсовая волна и другие. Для принятия решения предложено использовать искусственные нейронные сети.

КЛЮЧЕВЫЕ СЛОВА: Цифровая экономика, цифровая трансформация, идентификация, аутентификация, защита информации, биометрия, биометрическая идентификация, нейронные сети, искусственный интеллект, доверенная идентификация, интерактивная идентификация.

«Системы ИИ должны учитывать
сложность мира, а не уменьшать ее»
М. Мински

1. ВВЕДЕНИЕ. ИДЕНТИФИКАЦИЯ ДЛЯ ЗАЩИЩЕННОСТИ И БЕЗОПАСНОСТИ

Приемы идентификации существенно зависят от целей, которые могут характеризоваться как криминалистические и технологические.

Криминалистическая идентификация выполняется как правило на доверенном оборудовании, без сотрудничества с идентифицируемым объектом. Идентификация в технической защите информации выполняется в предположении, что субъект готов к сотрудничеству.

Все исследования в области технической защиты информации до последнего времени проводились с учетом того, что мы работаем с корпоративными системами, границы которых точно известны. В этих границах всегда можно обеспечить достаточный уровень защищенности, базирующийся на доверенности СВТ, включенных в состав системы. В открытых же системах ставить вопрос об обеспечении доверенности всех средств вычислительной техники

просто невозможно. Так, мобильные средства доступа пользователей ни при каких условиях нельзя сделать доверенными.

В этих условиях можно развивать систему в двух направлениях – перенести всю тяжесть защиты на центр и отказаться от использования надежной криптографической защиты при доступе к сервисам (например, банка) с мобильных устройств пользователей, или/и строить распределенную, «иммунную» систему защиты, обеспечивающую приемлемый уровень защищенности клиентских транзакций даже при недоверенном оборудовании.

Первое направление очевидно, и многие идут по этому пути, полагая, что риски пока невелики и такими же останутся в дальнейшем. Очевидно, что это не так. Брешь в защите всегда находится и эксплуатируется преступниками. Брешей в защите следует избегать.

Второе направление еще ждет своих исследователей. Основой эффективных решений могут стать системы обнаружения вредоносной активности, построенные по принципу мультиагентных систем [1], а также системы мультимодальной биометрической идентификации с использованием динамики рефлекторных реакций. Статья посвящена рефлекторной идентификации как методу и средству применения недоверенных клиентских терминалов в доверенных информационных системах цифрового общества.

Безопасность (и защищенность) всегда базируется на сложности и избыточности [2]. Так, электронный документ для фиксации волеизъявления автора дополняют электронной подписью (избыточность), а конфиденциальность обеспечивается криптографическими методами (сложность решения обратной задачи).

Особое место в последовательности операций занимают именно операции идентификации и аутентификации [3], так как еще до начала всех операций нужно понимать, с кем начинается взаимодействие – с партнером или хакером. Результат информационного взаимодействия фиксируется применением электронной подписи, придающей записи свойства документа. При использовании недоверенных клиентских терминалов (телефонов) ключи подписи должны быть отчуждены, и храниться защищенным образом. Уровень доверенности результата идентификации должен быть достаточным для доступа к отчужденным ключам подписи, что позволит обеспечить возможность применения электронной подписи, и с этим юридически значимых облачных сервисов в целом.

В рамках корпоративных систем нет проблемы обеспечить всех участников сертифицированными идентификаторами и выполнять операции по аутентификации в доверенной среде. В открытой же системе этого добиться невозможно. Обращаясь за госуслугами, телемедицинскими консультациями, услугами банков, услугами в секторе B2C граждане всегда будут пользоваться смартфонами, о доверенности которых говорить не приходится. Такой доступ всегда будет самой «легкой добычей» для всех видов атак с использованием вредоносного ПО. Поэтому решение проблемы применения облачной подписи с использованием недоверенных терминалов за счет рефлекторной идентификации является актуальной научно-технической задачей.

2. ИДЕНТИФИКАЦИЯ В ОТКРЫТЫХ СИСТЕМАХ

Естественным механизмом идентификации (аутентификации) для открытых систем представляется биометрическая идентификация. Биометрические параметры неотъемлемы от человека, и поэтому соблазн использовать их объясним. Об эффективности биометрии свидетельствует огромный опыт применения для идентификации самых разных модальностей – радужной оболочки глаза, папиллярного узора, рисунка сосудистого русла, формы лица, ладони, голоса, состав генома и другие. Эти биометрические модальности хотя и избыточны, но предельно просты – они или статичны, или условно статичны. Более того – если снимаемые

приборами характеристики не инвариантны[1], то исследователи зачастую пытаются свести их к инвариантам[2] [4] в попытке упростить последующий анализ.

В силу простоты и статичности эти модальности легко воспроизводятся и моделируются, что не только не снижает риски ошибочной идентификации, но и позволяет влиять на ее результаты. Традиционные (инвариантные) биометрические модальности не обеспечивают и не могут обеспечить достаточный уровень доверия к результатам идентификации на недоверенном устройстве. Успешный же опыт применения биометрии связан не с визуальной и/или приборной идентификацией, а только с криминалистической – предполагается, что в базах данных никто отпечатки не подменит, гражданин не наденет при регистрации отпечатков перчатку и не передаст ее потом злоумышленнику, а средства идентификации, используемые полицией – доверенные[3].

Таким образом:

- биометрические характеристики применяются для идентификации и аутентификации в силу своей инвариантности к внешним факторам, полной или частичной;
- исследования по применению биометрических механизмов явно или неявно основываются на предположении о доверенности технических средств обработки.

В нашем случае предположение во втором пункте явно неверно, и именно это требует изменения подхода к биометрическим характеристикам как к инвариантам.

Действительно, любые результаты идентификации, если они будут получены на недоверенных (обычных) устройствах (смартфонах, планшетах) легко подделать (подменить), что дискредитирует саму идею применения биометрии в юридически значимом информационном взаимодействии. Работаем ли мы с измерениями, полученными непосредственно датчиками (микрофоном, камерой и т.д.), или это данные, уже подменённые злоумышленником — понять это и есть основная задача, решение которой необходимо для достижения характеристик идентификации, достаточных для обеспечения юридической значимости и доступа к удаленным (отчужденным) криптографическим ключам при использовании недоверенных клиентских устройств.

Простота подделки статических биометрических модальностей сегодня осознана[4], и операторов идентификации на основе биометрических данных начинает интересовать вопрос: «А нельзя ли повысить достоверность идентификации за счет использования не одной, а нескольких биометрических характеристик»? – то есть за счет мультимодальности на этапе принятия решения.

3. МУЛЬТИМОДАЛЬНОСТЬ

Для независимых модальностей вероятности ошибок (как первого, так и второго рода) перемножаются, что объясняет целесообразность многофакторных (мультимодальных) решений и позволяет обеспечить достаточный уровень доверенности. Независимость при этом понимается как независимость факторов и независимость каналов [5].

Предположительно, биометрические характеристики человека нельзя считать независимыми уже хотя бы потому, что они принадлежат одному человеку. Во всяком случае, независимость не доказана и, скорее всего, не изучалась. Уже в связи с этим гипотеза о повышении

[1] Например, голос существенно зависит от состояния мягких тканей – то есть при насморке может сильно измениться.

[2] Например, к зависимости только от твердых тканей – добиваясь инвариантности, но уменьшая информативность (сложность).

[3] http://www.papillon.ru/rus/38/

[4] http://gvv.mpi-inf.mpg.de/files/TOG2016/PersonalizedFaceRig.pdf

уровня доверия при использовании мультимодальностей не очевидна и требует серьезного изучения.

Еще более наглядной является необходимость в независимости каналов – а в нашем случае канал один – он формируется клиентским терминалом (смартфоном) и интернетом. Конечно, ни о какой независимости здесь даже не может идти речь.

Таким образом, использование статических параметров для повышения достоверности идентификации с использованием недоверенного устройства практически нецелесообразно.

Одним из решений проблемы подделки (подмены) статических (инвариантных) биометрических параметров является проверка активности и разумности субъекта в дополнение к проверке биометрических показателей. Такая проверка могла бы отсечь случаи полностью автоматизированной подмены параметров. Традиционным способом проверки того, что субъект не является алгоритмом или компьютерной программой, является т.н. тест Тьюринга, или CAPTCHA. Пользователю предлагается распознать текст, звук, изображение, или решить арифметическую или логическую задачу. Работоспособность такой методики обосновывается тем, что указанные задачи для их решения требуют применения интеллекта человека. Однако последние успехи в области машинного обучения хоть и не позволяют построить «сильный» искусственный интеллект (подобный человеческому), но позволяют решить множество частных задач, которые, как ранее считалось, может решить только человек (то есть создать «слабый» искусственный интеллект). К таким задачам относятся распознавание речи и образов, перевод на разные языки, обработка запросов на естественном языке, текстовое описание изображений и видео. Поэтому такой подход не применим для описанной выше проблемы. Во-первых, алгоритмы искусственного интеллекта совершенствуются с каждым днём, а во-вторых, на недоверенном устройстве злоумышленник-человек может пройти тесты, контролирующие интеллект, а биометрические характеристики подменить.

Другие способы проверки активности субъекта – проверка подвижности зрачков глаз при сличении рисунка радужной оболочки, проверка температуры лица при идентификации по лицу, или проверка наличия пульса при анализе отпечатков пальцев – обладают аналогичными недостатками: могут быть подделаны либо подменены на недоверенном считывающем устройстве.

Сравним **задачи, средства и данные**, необходимые для решения задачи идентификации в криминалистике и в цифровой экономике.

Идентификация в рассматриваемом контексте может упрощенно трактоваться как установление личности. Это так и для криминалистики, и для процессов цифровой экономики. Видимо, такая упрощенная трактовка и привела к имеющейся путанице. Рассмотрим теперь понятия более глубоко.

Нулевая гипотеза идентификации может быть сформулирована субъектом так: «Идентифицируемый объект – тот, за кого он себя выдает (за кого его принимает субъект)».

Криминалистика, как правило, имеет дело с людьми, не ориентированными на сотрудничество. Ее обычный объект – это труп, подозреваемый или преступник. Цель анализа – доказать факт совершившегося доступа объекта – к орудию и/или месту преступления, установление личности потерпевшего и так далее. И, конечно, объект обычно совсем не заинтересован в правильной идентификации.

Активное противодействие здесь, если оно есть, направлено на нарушение идентификации – доказать, что там не был, не участвовал, не нарушал.

Другими словами, противодействие (со стороны субъекта, или сообщников, или трудности, связанные с недостатком данных) направлено для достижения ошибки «false positive» – ошибки первого рода.

Цель противодействия (бездействия) – отклонить нулевую гипотезу при том, что она верна.

Используемые технические средства при этом – доверенные. Они специально разрабатываются, защищаются сертифицированными средствами, проходят регламентные процедуры контроля и так далее.

В цифровой экономике – объект идентификации вполне живой и добропорядочный участник экономической деятельности. Пример его потребности –получить доступ к некоторым ресурсам. Он готов к сотрудничеству, готов выполнить некоторые действия, чтобы после успешной идентификации получить нужную ему услугу. Он заинтересован в правильной идентификации.

Активное противодействие системе может осуществлять хакер (или просто злоумышленник), добиваясь в свою пользу ложной идентификации. Противодействие направлено на достижение ошибки «false negative» – ошибки второго рода.

Цель противодействия – выдать себя за другого. Вынудить субъекта принять нулевую гипотезу при том, что она ложна.

Технические средства – произвольные. Это обычные планшеты и смартфоны, ничем не защищенные от внедрения вредоносного ПО.

Для наглядности сведем в таблицу характеристики и установки объекта процесса идентификации (табл. 1). Вырожденные случаи (труп) не рассматриваем.

Таблица 1. Субъект идентифицирует объект. Цели объекта.

Сфера применения	Объект идентификации	Заинтересованность объекта в подтверждении гипотезы	Желательный результат
Криминалистика	Добропорядочный гражданин (подозреваемый)	Нет	Верный
	Преступник	Нет	Ошибка 1 рода
Цифровая экономика	Добропорядочный гражданин	Да	Верный
	Преступник	Да	Ошибка 2 рода

Мы видим полностью противоположные характеристики.

Не менее менее наглядны и отличия в позициях субъекта идентификации (табл. 2).

Таблица 2. Субъект идентифицирует объект. Характеристики процесса.

Характеристики процесса для субъекта	Криминалистика	Цифровая экономика
Гипотеза	Объект – тот, за кого его принимает субъект	
Доверенность среды идентификации и контролируемость инструмента	Да	Нет
Значимость того, жив ли объект	Нет	Да
Значимость согласия объекта на идентификацию	Нет	Да
Значимость согласия объекта с результатами	Нет	Да

Таким образом, процессы идентификации в криминалистике и цифровой экономике при заданной гипотезе полностью различны.

Не совпадают:

- объекты идентификации;
- их одушевленность/неодушевленность;
- заинтересованность объекта идентификации в ошибке;
- желательный для объекта идентификации результат;

– характер участия объекта в процессе идентификации.

При этом противоположными являются:

– контролируемость инструмента субъектом;
– доверенность среды идентификации;
– значимость того, жив ли объект идентификации;
– значимость согласия объекта идентификации с результатом идентификации;
– заинтересованность объекта идентификации в подтверждении гипотезы субъекта.

4. НОВАЯ БИОМЕТРИЯ. ЗАМЫСЕЛ ЗАЩИТЫ

Для устранения уязвимостей, связанных с простотой подмены измерений на недоверенных устройствах, необходимо от статических показателей перейти к динамическим типа «стимул-реакция» со сложной динамикой связи. Динамическим звеном, чрезвычайно сложным на сегодняшний день для моделирования, являются нервная и вегетативная системы человека и связанные с этим особенности физиологии движений. В частности, индивидуальными оказываются непроизвольные реакции на внешние стимулы (в частности, аудио и видео раздражители).

Предположительно реакция на стимулы может быть зафиксирована датчиками клиентского устройства, обработана с помощью методов искусственного интеллекта, например, искусственных нейронных сетей [6], что позволит определить источник потоков данных и повысить достоверность идентификации.

Совокупность нескольких биометрических модальностей нужно дополнить анализом хотя бы одной физиологической (рефлекторной) реакции, что повысит достоверность биометрической идентификации и обеспечит решение задачи виталентности.

На недоверенном клиентском терминале не сложно подделать голос, лицо, подменить отпечатки пальцев и рисунок сосудистого русла, сымитировать движение глаз, но если в качестве биометрического признака использовать реакцию на раздражитель — то изменения этих модальностей при реальном источнике должны быть согласованными, и поэтому подделать потоки данных будет почти невозможно, так как для согласования поддельных данных нужна модель реакций конкретного человека, что нереально ввиду высокой сложности такой модели.

Таким образом, сформировалось и осознано противоречие между потребностью общества в доверенной идентификации человека с использованием недоверенных клиентских терминалов и отсутствием обоснованных подходов к решению этой задачи. Разрешение этого противоречия возможно путем использования рефлекторных реакций человека на внешние раздражители, что и позволяет считать исследования в данном направлении актуальными.

На сегодняшний день психомоторные реакции человека исследуются, как правило, на сложном лабораторном медицинском оборудовании в контролируемых условиях. Однако исходя из параметров современных и перспективных технических средств (смартфонов), с их помощью среди динамических биометрических характеристик человека представляется возможным зафиксировать, по крайней мере, характеристики пульсовой волны, динамику изменения диаметра зрачка, динамику слежения взглядом за стимулом на экране. Для этого достаточно на смартфоне иметь камеру и вспышку (фонарик), а также сенсорный экран.

Перспективным является изучение движения глаз. Глаз не может быть неподвижным, клетки рецепторов «утомляются» и «подменяются» в процессе саккадических движений. Эти движения характеризуются высокой сложностью. Достаточно отметить, что движениями глаз управляют 7 мышц (!), и мышцы, ответственные за саккадические движения, являются са-

мыми быстрыми. Многообещающим представляется изучение рефлекторной составляющей саккад, а также (а может, и в первую очередь) процессы фиксации и регрессии при чтении.

Изучение пульсовой волны предположительно позволит выделить реакцию сердца – изучить вариабельность сердечного ритма. Это тем более важно, что для жизнедеятельности организма сердце важнее зрения, и регулирование осуществляется более «старыми» (и, таким образом, более стабильными) механизмами, в том числе ЦНС и вегетативной системой. При этом уровни регулирования могут меняться в зависимости от многих факторов, что позволяет считать механизм достаточно сложным для моделирования.

В качестве внешних раздражителей можно использовать имеющиеся у смартфона возможности – звук, цвет и свет, вибрацию, отображение текста (в том числе со случайным изменением числа пробелов).

Для движения по разработке данного подхода необходимо:

- проверить методом объективных измерений гипотезу о влиянии различных внешних раздражителей на рефлекторные реакции;
- создать алгоритмы сбора первичных данных на пользовательских устройствах (смартфонах);
- разработать искусственную нейронную сеть анализа данных, снимаемых средствами смартфона, либо применить другие адекватные задаче методы анализа.

Нужно сказать, что известны работы, в которых движение глаз рассматривалось в качестве биометрического признака [7, 8]. Фактически, полученные в них результаты можно рассматривать как подтверждение гипотезы о том, что в движении глаз имеется биометрическая информация (опосредовано – в движениях, связанных с рефлекторными реакциями). Опираясь на указанные результаты, нужно воспроизвести их, изучить требуемую разрешающую способность, и затем спроектировать алгоритмы идентификации на основе случайных стимулов, генерируемых удаленно, и удаленных же обработки и принятия решения. Клиентский терминал при этом будет только средством отображения и съема первичных данных, что никак не сможет повлиять на безопасность идентификации.

Отметим, что в известных работах снятие показателей производилось с помощью инфракрасной камеры и специальных калиброванных устройств, фиксирующих положение головы пользователя. Такой подход неприменим для широкого использования в реальных приложениях.

Таким образом, необходимо исследование возможностей снятия динамических показателей движения глаз в ответ на внешние стимулы с помощью массовых пользовательских устройств: бытовых видеокамер, встроенных камер планшетных устройств.

Ключевыми задачами являются исследование возможностей снятия указанных показателей с помощью RGB-камер (оптического диапазона) с низкой частотой кадров (30-60 к/с), и исследование возможностей геометрической калибровки системы «человек + камера» непосредственно перед измерениями или в процессе измерений.

5. ОБУЧЕНИЕ АЛГОРИТМА ИДЕНТИФАЦИИ

Одним из вариантов алгоритма идентификации могут быть нейронные сети. Искусственные нейронные сети получили огромное распространение в различных областях благодаря их возможности обучаться по данным и моделировать функцию практически любой степени сложности. Однако нейросетевые алгоритмы характеризуются огромным числом параметров и длительным обучением. Большой прогресс в области применения нейросетей произошёл в

относительно недавнее время после накопления больших коллекций данных и роста вычислительных мощностей.

При решении задач биометрической идентификации и аутентификации нейронные сети также применяются. В частности, когда биометрическим идентификатором является изображение, применяются свёрточные нейронные сети [9]. При этом традиционно используется сиамская архитектура сетей [10]. При такой архитектуре сеть применяется к поступающему изображению и изображению-эталону, и строит компактное векторное представление изображений. Решение о соответствии биометрического образца и эталона принимается либо на основе метрического сходства векторов описания, либо с помощью другой нейронной сети, принимающей на вход два полученных описания [10,11]. Удобство такой архитектуры заключается в том, что признаковые представления всех объектов из базы можно просчитать заранее и хранить в виде их компактных представлений, а обрабатывать только одно входящее. В случае динамических биометрических данных общая архитектура сети остаётся аналогичной.

Для обработки последовательностей реакций можно использовать и обычные полносвязные сети, если будет построено низкоуровневое признаковое представление данных. Однако при наличии достаточного объёма обучающих данных можно пытаться исключить шаг «feature engineering» и подавать на вход сети необработанные данные. В таком случае для обработки последовательностей традиционно эффективно применяют рекуррентные нейронные сети, в частности LSTM [12] и GRU [13]. В этом случае потребуется больший объём данных, так как сеть будет содержать гораздо больше обучаемых параметров.

В случае изучения динамических реакций требуется поставить в соответствие паре «стимул-реакция» человека, для которого такие реакции характерны. Надо отметить, что задача достаточно сложна, так как предполагается, что стимулы не будут повторяться. Однако способность нейронных сетей к построению обобщений должна позволить выделять в стимулах общие элементы и оценивать степень сходства реакций в близких ситуациях, на основе этой информации и обучающей выборки неявно отражаемой в параметрах сети, определять для какого человека подобные реакции характерны. С другой стороны, в отличие от задачи моделирования нервной системы, в данном случае задача прогнозирования реакции человека на стимул не стоит. Определение схожести реакций является на порядок более простой, дескриминативной задачей, тогда как предыдущая является генеративной.

Технологически, для создания идентифицирующей нейросети нужно собраться коллекцию данных для обучения. Коллекция данных должна содержать пары стимул-реакция. Причём для каждого человека пар должно быть несколько. Ключевая задача по размеченным данным – обучить сеть строить представления для рефлекторных реакций. Представление должно быть таким, чтобы отображать реакции одного и того же человека в близкие точки, а разных людей – в далёкие. Этого можно добиться, например, применением т.н. триплетной функции потерь [11]. После обучения нейросети добавление или удаление новой записи в базу биометрических идентификаторов не потребует переобучения нейросети, а потребует только вычисления представления.

Сложность и количество параметров нейронной сети определяет и безопасность такого подхода. Так как потенциальный злоумышленник не знает какие параметры реакций анализирует нейросеть, то и подделать саму реакцию представляется крайне сложным. С другой стороны, если злоумышленник вдруг получит набор данных, по которым обучалась нейросеть, то это не приведёт к тому, что он сможет её воспроизвести. Даже в том случае если будет построена и обучена сеть аналогичной архитектуры, получаемое представление будет отлично от имеющегося. Результат обучения сети, характеристики нейронов выходных и низкоуровневых слоёв носят стохастический характер, определяется случайными начальными параметрами и порядком поступления данных. К примеру, перестановка выходных нейронов местами не изменит

точности работы сети, но принципиально изменит представление реакции, то есть идентификатор человека, который будет сравниваться на сервере с идентификаторами из базы.

6. ПОЧЕМУ ЭТО РАБОТВЕТ?

Основой нового подхода является гипотеза о том, что зависимость реакций человека на внешние стимулы существенно зависит от когнитивных и кинезиологических особенностей человека, носит динамический характер и отражается в измерениях в достаточной для анализа степени.

Принципиальными особенностями системы стимул-реакция является:

- наличие нервной системы человека как связующего звена между стимулом и реакцией. Если к симуляции интеллекта уже достаточно много подходов, то работ по симуляции нервной системы практически нет. Нервные системы людей крайне сильно отличаются между собой и сложны для моделирования. В отличие от интеллектуальных задач у нервной системы нет «правильного ответа», которому бы можно было научить машину.
- случайные, не повторяющиеся стимулы. Такой подход позволит принципиально исключить возможность воспроизведения ранее записанных реакций пользователя, то есть подлога первичных данных.
- обработка пары стимул-реакция может производиться на удалённом доверенном устройстве.

При этом:

1. Недоверенность клиентского терминала не влияет на результаты, так как генерация стимула и анализ реакции выполняется на отчужденных доверенных ресурсах, а искажение реакции не даст возможности злоумышленнику получить нужный для него результат
2. Перехватывать стимул нет смысла, так как зная стимул, невозможно сгенерировать реакцию в силу отсутствия модели человека
3. Извлечь параметры нейронной сети путем ее тестирования в заданных условиях невозможно, а акты идентификации постоянно уточняют параметры нейронной сети, и поэтому даже тотальное наблюдение не позволит в полной мере воспроизвести сеть.

Нетрудно видеть, что основная особенность, обеспечивающая безопасность идентификации на недоверенном устройстве, состоит в интерактивности – ни клиентский терминал, ни центр сами по себе не выполнят идентификацию. Процедура существенно интерактивна, что и позволяет генерацию стимула и принятие решения отнести к доверенному центру, а съем информации осуществлять на принадлежащем клиенту персональном устройстве [14].

Конечно, полный анализ безопасности еще предстоит выполнить. Возможно, стоит поискать и альтернативный нейронной сети механизм принятия решений.

СПИСОК ЛИТЕРАТУРЫ

1. Лихтенштейн В.Е., Конявский В.А., Росс Г.В., Лось В.П. *Мультиагентные системы: самоорганизация и развитие.* М.: Финансы и статистика, 2018.

2. Конявский В.А., Гадасин В.А. *Основы понимания феномена электронного обмена информацией.* Минск: Беллитфонд, 2004.

3. Конявский В.А. Идентификация и применение ЭЦП в компьютерных системах информационного общества. *Безопасность информационных технологий*, 2010, №3, стр.6-13.

4. Сорокин В.Н., Макаров И.С. Обратная задача для голосового источника. *Информационные процессы*, 2006, том 6, №4. стр. 375-395.

5. Конявский В.А. *Управление защитой информации на базе СЗИ НСД «Аккорд»*. М.: Радио и связь, 1999.

6. LeCun, Y., Bengio, Y., and Hinton, G. (2015). *Deep learning*. Nature V 521, pp. 436–444.

7. Roman Bednarik, Tomi Kinnunen, Andrei Mihaila, Pasi Franti. *Eye-Movements as a Biometric*. H. Kalviainen et al. (Eds.): SCIA 2005, LNCS 3540, pp. 780–789.

8. Gary Bargary, Jenny M.Bosten, Patrick T.Goodbourn, Adam J.Lawrance-Owen, Ruth E.Hogg, J.D.Mollon. Individual differences in human eye movements: An oculomotor signature? *Vision Research*. Volume 141, December 2017, pp 157-169.

9. Krizhevsky, A., Sutskever, I. & Hinton, G. ImageNet classification with deep convolutional neural networks. In Proc. *Advances in Neural Information Processing Systems*, 2012, vol.25, pp. 1090–1098.

10. Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, Lior Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification *Conference on Computer Vision and Pattern Recognition (CVPR)*, Columbus, Ohio, USA, 2014, no. 6.

11. Florian Schroff, Dmitry Kalenichenko, James William Philbin FaceNet: A unified embedding for face recognition and clustering. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* Boston, MA, USA, 2015, no. 6.

12. Hochreiter, S. & Schmidhuber, J. Long short-term memory. *Neural Comput.* 1997, vol. 9, no. 3, 1735–1780.

13. Junyoung Chung, Caglar Gulcehre, Kyunghyun Cho, Yoshua Bengio Empirical evaluation of gated recurrent neural networks on sequence modeling. *NIPS 2014 Workshop on Deep Learning*, Montréal, Montréal Canada, 2014, no. 12.

14. Конявский В.А. Интерактивный способ биометрической аутентификации пользователя. *Патент на изобретение*, 2670648, 24.10.2018.

Identification in computer systems of digital economy.

A.V. Brodskiy, V.A. Gorbachev, O.E. Karpov, V.A. Konyavsky, N.A. Kuznetsov, A.M. Raigorodskii, S.A. Trenin

A new method of interactive identification is proposed-trusted identification of a person using untrusted devices (e.g. smartphones, tablets, etc.). It is shown that static, unchangeable or almost invariable biometric features can be used in criminology, but it is impractical for computer systems of digital economy. As signs of ineffective use of fingerprints, iris and retina, vascular pattern and similar. On the contrary, it is necessary to use the dynamic characteristics inherent in man, reflected, for example, in reflexes. As such, eye movements can be used when reading and/or tracking the stimulus, saccades, pulse wave and others. For decision-making it is offered to use artificial neural networks.

KEYWORDS: Digital economy, digital transformation, identification, authentication, information security, biometrics, biometric identification, interactive identification, neural networks, artificial intelligence, trusted identification.