Устройство для формирования диэлектрических пленок содержит остов *1* токоввода, диэлектрическую пробку *2*, пружину *3*, токопроводящий зонд *4*, прижимное устройство *5*, концевое устройство *6*, образец *7* – пленки металла или полупроводника, нанесенного на изолирующую подложку *8*, корпус *9* устройства, ось *10* и диэлектрическую оболочку *11*.

Остов токоввода выполнен из жаростойкого вакуумного диэлектрика с оплавленным концом, в который введена ось *10*. Остов подвижно соединен с концевым устройством, позволяющим свободно поворачивать и перемещать остов токоввода на оптимальные расстояния в горизонтальной и вертикальной плоскостях. Концевое устройство жестко соединено с корпусом устройства.

Второй конец остова токоввода имеет чистую притертую поверхность. Диэлектрическая пробка, в которой закреплен токопроводящий зонд свободно плавает внутри остова токоввода.

Устройство работает следующим образом.

Требуемое давление токопроводящего зонда на поверхность полупроводникового образца *7* осуществляется пружиной. Диэлектрическая пробка притерта по отверстию остова токоввода и обеспечивает надежную его изоляцию и изоляцию пружины от кислородной плазмы. Выходящий из остова токоввода токопроводящий зонд *4* одет в диэлектрическую оболочку, которая плотно прилегает к стенкам остова токоввода. Прижимное устройство, жестко закрепленное на корпусе устройства, служит для получения нужного давления наконечника остова токоввода на поверхность окисляемого образца и для предотвращения смещения остова токоввода в горизонтальной плоскости.

Для получения диэлектрического окисного слоя на полупроводниковом образце последний подводится к окну плазменного генератора. Выходящая из генератора кислородная плазма омывает поверхность образца, подлежащую окислению, в результате чего происходит взаимодействие ионов полупроводника с кислородом, т.е. образуется и растет слой окисла, причем структура и толщина окисной пленки зависят от формовочного потенциала.

Выбором при помощи прижимного устройства и концевого устройства требуемого прилегания конца остова токоввода к окисляемому образцу можно получить высокую защиту контакта токопроводящего зонда 4 и образца от взаимодействия кислородной плазмы, что приведет к увеличению формовочного потенциала без переброса тлеющего разряда на остов токоввода, т. е. позволит увеличить толщину растущего диэлектрического слоя и улучшить его структуру.

Надежный контакт токопроводящего зонда с образцом обеспечивается в течение всего процесса окисления в плазме O_2 оптимальным выбором давления пружины.

В результате возможно получение диэлектрического подзатворного слоя заданной в пределах от 0,01 до 1 мкм толщины с однородной структурой и высокими электрическими свойствами.

Литература

1. Сычик В.А. Измерительные преобразователи излучений на основе полупроводниковых приборных структур. – Мн. : Выш. школа, 1991. – 179 с.

2. Колдун М.М. Солнечные элементы. – М. : Наука, 1987. – 190 с.

УДК 004.056

ВЫБОР ДОПОЛНИТЕЛЬНОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ДЛЯ БАНКОВСКИХ СИСТЕМ САМООБСЛУЖИВАНИЯ

Татаренков В.С., Рафиков А.Г.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. *В статье описаны существующие системы аутентификации. Показано, что использование одного ПИН-кода для аутентификации является небезопасным. Рассмотрены биометрические системы аутентификации, которые могут быть также использованы в АТМ. На основе математической модели, вычисленной по параметрам рассмотренных систем, сделан выбор для дополнения системы аутентификации банковских систем самообслуживания.*

Ключевые слова: банкомат, АТМ, аутентификация, биометрия, информационная безопасность.

Введение. Наше время – время развития информационных технологий и, как следствие, расцвета киберпреступности. По подсчетам к концу 2018 года ущерб экономике РФ от киберугроз может составить около 1,5 трлн. долларов США [1]. В связи с участившимися атаками на банкоматы и хищениями значительных денежных средств, банкиры всерьез озадачились повышением качества и надежности идентификации и аутентификации пользователей. На текущий момент в ряде банков запущены несколько проектов по совершенствованию аутентификации при удаленной идентификации и при использовании АТМ. Сбербанк создает собственную биометрическую систему – единую биометрическую систему (ЕБС), которую банк планирует использовать в процессах обслуживания своих клиентов. В основе лежит двухфакторная биометрическая аутенти-

фикация по голосу и лицу [1]. Банк Русский Стандарт начал собирать данные для передачи в ЕБС. Идентификация по голосу и изображению лица позволит всем желающим пользоваться банковскими продуктами и услугами безопасно [2]. Альфа банк запустил идентификацию клиентов по "отпечатку ладони" (по рисунку вен ладони) [3]. Тинькофф Банк использует систему распознавания лица на встрече с клиентом, а также тестирует распознавание личности в банкоматах. Использование аутентификации по голосу при общении со службами банка снизило время обслуживания и уменьшило в четыре раза нагрузку на колл-центр, также уменьшилось влияние "человеческого фактора" и повысилась безопасность [4].

Приведем анализ существующих систем аутентификации для правильного выбора дополнительной системы аутентификации для банковских систем самообслуживания с целью создания полноценной, надежной системы идентификации и аутентификации пользователей банковских карт.

Пин-код. Сегодня для аутентификации пользователей в АТМ преимущественно используется четырехзначный пароль, который знает только владелец карты. Свое широкое распространение он получил благодаря простой и дешевой технической реализации и тем, что число цифр является легко запоминаемым.

Но использование ПИН-кода, как одного фактора для аутентификации - небезопасно, так как уберечь его в тайне это непростая задача, потому что существуют легко используемые способы утечки информации. Перечислим некоторые из них:

1) ПИН-код можно подсмотреть с применением и без применения технических средств;

2) ПИН-код может быть разглашен самим держателем карты;

3) ПИН-код может быть записан на носителе, хранимом рядом с картой;

3) ПИН-код можно получить специальными техническими средствами. Как пример, использование ложной клавиатуры-накладки, которая накладывается на основную клавиатуру.

Как видно, ПИН-код может быть легко скомпрометирован и использован в любое время и в любом месте, что говорит о необходимости использования дополнительных факторов аутентификации. В рассмотрение взяты биометрические системы аутентификации, так как важной особенностью является то, что ключом является сам человек, и ничего дополнительного запоминать или носить не надо [5].

Система распознавания лица при помощи стандартной видеокамеры (2D). Данная система работает по следующему принципу: с видеокамеры в модуль распознавания поступают кадры, сделанные видеокамерой. Модуль распознавания обрабатывает эти кадры выделяя лицо и его характеристики. Затем эти данные поступают в модуль анализа идентификационных данных, где происходит: сравнение лица, полученного от 2D видеокамеры, с лицами из БД и оповещение о результате данного сравнения.

Преимуществом данной системы является ее простота внедрения, так как сегодня в современных банкоматах уже установлены видеокамеры. Современные алгоритмы распознавания могут распознавать человека вне зависимости от несильных внешних изменений, старения, косметики. Но их можно попытаться обмануть при помощи фотографии или изображения. Для предотвращения возможности такого обмана рекомендуется использовать стереоскопические камеры для получения 3D изображений лиц [5].

Система распознавания лица при помощи стереоскопической видеокамеры (3D). Данная система позволяет уже считывать объемное изображение лица, тем самым обмануть ее при помощи фотографий и изображений не получится.

Рисунок 1 – Камера LucidCam

Система состоит из нескольких камер (обычно две), расположенных определенным образом (рис.1), которые синхронно делают фотографии человека. Далее из полученных фотографий строиться 3D модель лица. После производится анализ полученной модели и моделей из БД - сравниваются их антропометрические особенности. В конце выдается результат данного сравнения.

Преимуществами данной системы являются: высокий уровень надежности распознавания, устойчивость к поворотам головы и влиянию артефактов в виде бороды, усов, очков и т. д. на лице [5].

Система распознавания отпечатка пальца. Основной задачей данной системы является считывание отпечатка пальца. Датчики считывания можно разделить на три класса:

1. Оптические;
2. Полупроводниковые;
3. Ультразвуковые.

Оптические датчики основываются на использовании оптических методов получения изображения. Их преимуществом является высокая четкость сканирования. Из недостатков можно перечислить: необходимость периодической очистки датчика, так как загрязнения, негативно влияют на его работу, и более высокая цена по сравнению с датчиками на полупроводниках.

Датчики на полупроводниках используют свойства полупроводников для получения изображения поверхности пальца. Преимуществами данной системы являются низкая цена и наличие решений малых габаритов. Недостатком же является низкая четкость сканирования по сравнению с остальными классами датчиков.

Ультразвуковые датчики сканируют палец ультразвуком и определяют отпечаток по расстояниям от датчика до гребня или до впадины кожного рельефа пальца. Главным преимуществом данного класса является самая высокая точность сканирования по сравнению с остальными классами. Недостатками можно назвать самую высокую цену и немалые размеры самого устройства.

Недостатками системы распознавания отпечатка пальца являются: необходимость оборудовать банкоматы датчиком сканирования, а также отсутствие решений, которые с высокой вероятностью не могли бы быть скомпрометированы, так как уже сейчас искусственный интеллект может создавать «мастер отпечаток» для обхода системы аутентификации по отпечатку пальца [6].

Система распознавания карты вен руки. Принцип работы данной системы следующий: инфракрасная камера делает снимок руки. Карта вен формируется благодаря свойству гемоглобина, который поглощает ИК-излучение, в результате вены отображаются в виде четких линий.

Рисунок 2 – Турникетный считыватель вен ладони PV-TS

Особенностью данной системы является то, что она считывает то, что находится в теле, внутри руки, поэтому получить эти данные от самого человека сложно. А оставшийся след руки после применения не влияет на работу системы.

Преимуществами данной системы являются: бесконтактное взаимодействие с устройством, возможность сканирования в перчатках, отсутствие влияния факторов мелких повреждений кожного покрова, невосприимчивость к обману при помощи муляжа руки.

Недостатками являются: чувствительность сканера к солнечным лучам и лучам галогенных ламп, заболевания вен, оказывающих влияние на работу системы, и необходимость оборудовать банкоматы датчиком сканирования [5].

Система распознавания сетчатки глаза. Основным элементом данной системы является специальная камера, которая делает серию снимков глаза. После выбираются наиболее четкие фотографии, и они начинают анализироваться для распознавания. Данный метод признан самым надежным из всех методов биометрической аутентификации.

Преимуществами данной системы являются: высокая надежность распознавания, сетчатка глаза человека не меняется с возрастом, и система работает бесконтактным способом.

Недостатками можно назвать: некоторые глазные болезни влияют на сетчатку глаза, человек, проходящий процесс аутентификации, должен не двигаться некоторое время [5], датчики для данной системы необходимо монтировать в банкоматы, а также немногие клиенты захотят подвергать свои глаза излучению, которое может быть не безопасным и создающим дискомфорт при некоторых настройках системы и многократном применении.

Система распознавания голоса. Преимуществами данной системы являются простота внедрения и использования, также сама система работает бесконтактным способом [7].

Из недостатков можно назвать: влияние болезней горла, произношения, посторонних шумов, полосу пропускания голосового сигнала устройств связи на точность распознавания.

Сводная таблица параметров. Обобщим параметры, приведенных выше систем, в таблицу (табл.1) для их анализа и вычисления целевой функции по методу экспертных оценок. Для оценок параметров был использован метод простого ранжирования. Метод заключается в том, что в оценке параметров системы участвует группа экспертов. Каждый эксперт, участвовавший в оценке, оценивает цифровым эквивалентом параметры объекта. Затем, с помощью методов математической статистики получают обобщенное мнение экспертов в виде количественной оценки [8].

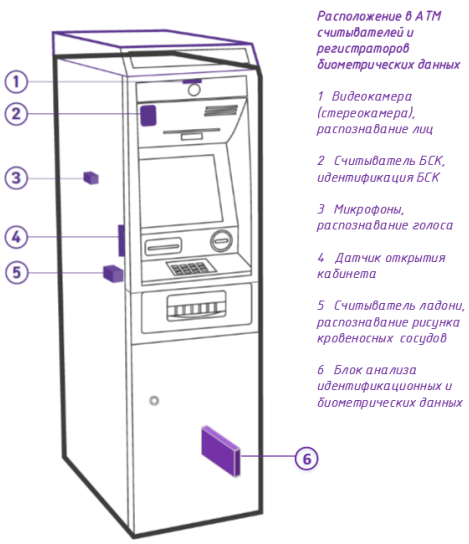

Рисунок 3 – Расположение в АТМ считывателей и регистраторов биометрических данных

Таблица 1 – Параметры рассмотренных систем аутентификации

Системы аутентификации и их параметры	1. Система распознавания лица (2Д)		2. Система распознавания лица (3Д)		3. Система распознавания отпечатка пальца		4. Система распознавания карты вен руки		5. Система распознавания сетчатки глаза		6. Система распознавания голоса	
Общий уровень безопасности (P1)	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
	0.1%	2.5%	0.0005%	0.1%	0.001%	0.6%	0.0008%	0.01%	0.0001%	0.4%	0.003%	0.15%
	Низкий (2)		Высокий (3)		Очень низкий (1)		Высокий (3)		Очень высокий (4)		Низкий (2)	
Потребность в ресурсах для осуществления фальсификации (P2)	Низкая (2)		Высокая (3)		Низкая (2)		Очень высокая (4)		Очень высокая (4)		Низкая (2)	
Чувствительность к влиянию внешних факторов (P3)	Высокая (2)		Низкая (3)		Высокая (2)		Низкая (3)		Низкая (3)		Высокая (2)	
Легкость внедрения (P4)	Очень высокая (4)		Высокая (3)		Низкая (2)		Высокая (3)		Низкая (2)		Высокая (3)	
Уровень комфорта применения клиентами (P5)	Очень высокий (4)		Очень высокий (4)		Низкий (2)		Высокий (3)		Очень низкий (1)		Очень высокий (4)	
Цена (P6)	Низкая (3)		Высокая (2)		Очень низкая (4)		Высокая (2)		Очень высокая (1)		Низкая (3)	

Параметр «Общий уровень безопасности» определяется по коэффициенту ложного пропуска (показатель FAR) и по коэффициенту ложного отказа в доступе (показатель FRR) (взяты усредненные FAR и FRR по методам аутентификации);

Возможное расположение в АТМ считывателей биометрических данных приведено на Рис.3. Верхний дополнительный отсек с оптически прозрачной передней панелью потребуется для установки системы видеокамер (3D), например, LucidCam (Рис. 1).

Выбор системы аутентификации. Для выбора оптимальной системы аутентификации воспользуемся следующей целевой функцией:

$$\max_i(W_i = \alpha_1 \times P1_i + \alpha_2 \times P2_i + \alpha_3 \times P3_i + \alpha_4 \times P4_i + \alpha_5 \times P5_i + \alpha_6 \times P6_i) \quad (1)$$

Выбор весов следующий (веса определяют степень важности параметра):

$\alpha_1 = 3$;
$\alpha_2 = 3$;
$\alpha_3 = 2$;
$\alpha_4 = 1$;
$\alpha_5 = 2$;
$\alpha_6 = 1$;

Рассчитанные показатели W_i:

$W_1 = 31$;
$W_2 = 37$;
$W_3 = 23$;
$W_4 = 38$;
$W_5 = 35$;
$W_6 = 30$;

Максимальными значениями целевой функции W_i являются W_2 и W_4. Таким образом, лучшими дополнениями к стандартной системе аутентификации являются: 2."Система распознавания лица (3D)" и 4."Система распознавания карты вен руки".

Выводы. Применение дополнительных систем аутентификации не гарантирует на сто процентов защищенность клиента, но значительно усложняет жизнь злоумышленников. Так как им для кражи средств придется собирать больше информации, использовать дополнительные инструменты и им потребуется больше ресурсов, включая временные затраты, для создания фальсификата. Основной проблемой и в тоже время опасностью, которая таится за применением биометрических способов аутентификации, является компрометация биометрических данных клиента на всю жизнь в случае их кражи. Поэтому важно найти золотую середину по организации системы аутентификации, использующую данные клиента, на основе которых в случае кражи нельзя было бы изготовить фальсификаты, или это изготовление являлось бы очень ресурсозатратным.

По расчетам показателей целевой функции рекомендовано использование системы распознавания лица (3D) или системы распознавания карты вен руки, как дополнение к системе аутентификации, использующей ПИН-код. Этот выбор во многом объясняется тем, что эти системы устойчивы к ошибкам I и II рода. Также, для обхода системы стереоскопии, можно воспользоваться маской, но которую изготовить злоумышленнику будет весьма ресурсозатратно, так как она должна в точности соответствовать антропометрическим параметрам лица, а также, ее использование может привлечь к себе внимание работников банка. Для обхода системы распознавания карты вен руки нужна копия руки с кровеносной системой, изготовить которую практически невозможно. Еще одним показателем, по которому данные системы лидируют - это их простое использование и применение, тем самым они не будут создавать дискомфорт клиентам банка.

Литература

1. Кузнецов С. Сбербанк сокращает разрыв между общим технологическим развитием и технологиями безопасности // Журнал ПЛАС. 2018. № 9.

2. Банк Русский Стандарт начал принимать биометрические данные клиентов // Журнал ПЛАС. 2018. URL: https://www.plusworld.ru/daily/banki-i-mfo/bank-russkij-standart-nachal-prinimat-biometricheskie-dannye-klientov/.

3. Альфа-Банк запустил идентификацию клиентов по отпечатку ладони // Журнал ПЛАС. 2018. URL: https://www.plusworld.ru/daily/tehnologii/alfa-bank-zapustil-identifikatsiyu-klientov-po-otpechatku-ladoni/.

4. Тинькофф Банк в 6 раз сократил число случаев кредитного мошенничества благодаря биометрии // Журнал ПЛАС. 2018. URL: https://www.plusworld.ru/daily/banki-i-mfo/tinkoff-bank-v-6-raz-sokratil-sluchai-kreditnogo-moshennichestva-blagodarya-biometrii-2/.

5. Якименко А.А., Вихман В.В. Биометрические системы контроля и управления доступом в задачах защиты информации. Новосибирск: Изд. НГТУ, 2016. 54 с.

6. ИИ создал «мастер-отпечаток» для разблокировки смартфонов // SecurityLab. 2018. URL: https://www.securitylab.ru/news/496546.php.

7. Десятчиков А.А., Ковков Д.В., Лобанцов В.В., Маковкин К.А., Матвеев И.А., Мурынин А.Б., Чучупал В.Я. Комплекс алгоритмов для устойчивого распознавания человека // Известия РАН. Теория и системы управления. 2006. № 2. С. 1-12.

8. Громова Н. М., Громова Н. И. Основы экономического прогнозирования. М.: Академия Естествознания, 2007. 112 с.

УДК 621.923.9

РАЗРАБОТКА УСТРОЙСТВА И МЕТОДОВ ПОЛУЧЕНИЯ ШАРОВИДНЫХ ЭЛЕМЕНТОВ ИЗ САМОЦВЕТНЫХ КАМНЕЙ

Ходжаев Т.А., Мирзоалиев И., Мирзоалиев А.И.

Таджикский технический университет имени академика М.С. Осими
Душанбе, Таджикистан

Большинство изделий из самоцветных камней типа бусы, четки, ожерелье и др., состоит из шариков. Изготовление сферических тел из самоцветных камней является одним из трудоёмких задач. Кроме того, существующие способы не обеспечивают правильность формы шариков. В процессе изготовления из-за больших сил давления нередки случаи поломки шариков. В отличие от традиционной обработки рассмотрим другую схему, в которой используется процесс центробежной абразивной обработки.

Рассмотрим схему обработки (рис. 1), при которой обрабатываемое тело установленное в сепараторе, совершает сложное движение, относительное и переносное движения которого являются вращательными. Под действием переносной центробежной силы обрабатываемые шары прижимаются к внутренней стенке барабана. Шары под действием силы тяжести прижимаются к поверхности инструмента, закрепленного к внутренней стенке барабана, и обрабатываются при скольжении по поверхности инструмента. Скорость относительного скольжения и соответственно производительность обработки зависят от установившейся частоты вращения сепаратора. Рассматривая динамику процесса, определяем частоту вращения шаровидных заготовок, от которой зависит производительность и точность обработки.

Рассмотрим вращающий сепаратор и абразивный круг, а также обрабатываемые тела как одну систему и для определения момента сопротивления и зависимости угловых скоростей вращения тела и диска применим теорему об изменении кинетического момента системы, согласно которой: производная по времени от кинематического момента системы относительно оси вращения равна алгебраической сумме моментов всех внешних сил относительно этой оси.

$$\frac{dK_z}{dt} = \sum_{k=1}^{n} m_z\,(\bar{F}k^e) \qquad (1)$$

где,

$$K_z = K_{z_1} + K_{z_2} + K_{z_3}, \qquad (2)$$

K_{z_1}, K_{z_2}, K_{z_3}– собственно кинетические моменты вращающихся дисков и обрабатываемых тел.

$$K_z = J_{zi} \cdot \omega_i; \quad J_{zi} = \frac{m_i R_i^2}{2}; \quad \omega_i = \frac{\pi n_i}{30} \qquad (3)$$

$$K_{z_1} = \frac{m_1 R^2}{2} \cdot \frac{\pi n_1}{30} = \frac{\pi m_1 R^2 \cdot n_1}{60} \qquad (4)$$

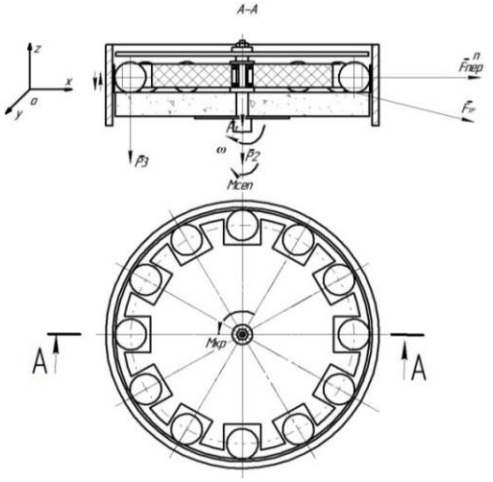

Рисунок 1 – Схема действия сил при обработке шаров из самоцветных камней