Published in the Slovak Republic
Vestnik policii
Has been issued since 2014.
E-ISSN: 2414-0880
2020, 7(1): 3-9

DOI: 10.13187/vesp.2020.1.3
www.ejournal21.com

Technical Means

Biometric Credit Card

Maria A. Belova [a, *], Vasilisa I. Ryskina [a]

[a] State university of the sea and river fleet of the name of the Admiral S.O. Makarov, Russian Federation

Abstract

This article discusses a new technology for creating bank cards, such as biometric bank cards, which use a combination of a fingerprint scanner and EMV technology. With this method of protecting the card, it is necessary to register the fingerprint. This can be easily done at home using your phone and scanner, or the credit card provider can do it himself. The fingerprint is then encrypted and stored on your card. At the same time, it was noted that the majority of consumers are ready to make changes to the solution for biometric payments, despite some reservations regarding security. The article presents and analyzes the pros and cons of this card system, and also explains how biometric bank cards differ from conventional credit bank cards with contactless payment. It is concluded that the use of biometrics for bank cards will significantly increase the level of its security. The main obstacle to their implementation is that it costs 20 times more to create a biometric credit card than a conventional one, but the cost of new technology always decreases over time.

Keywords: biometric bank card, contactless payment, bank, bank cards, biometrics, technology, PIN, PayPal, recognition, face biometrics, credit cards.

1. Введение

Биометрия все чаще становится частью повседневной жизни. Если посмотреть на смартфоны, то телефоны в последние несколько лет, скорее всего, используют биометрические технологии в виде отпечатков пальцев, радужной оболочки глаза или распознавания лиц. Помимо смартфонов, можно увидите, как биометрическое распознавание используется на пограничном контроле в аэропортах. Биометрия также используется на рабочем месте, где вводятся биометрические данные, чтобы контролировать сотрудников, когда они приходят и уходят в течение дня. И, конечно же, правоохранительные органы давно используют биометрию для поиска и идентификации преступников (Алексанов и др., 2012: 135).

Когда дело доходит до индустрии платежей, биометрия уже начинает работать. Биометрия используется для доступа к цифровым кошелькам, но как насчет кредитных карт? Если вы не знали, существует такое понятие, как биометрическая кредитная карта.

* Corresponding author
E-mail addresses: m-belova123@mail.ru (M.A. Belova)

Хотя биометрическая кредитная карта все еще находится на стадии тестирования, она прилагает все усилия, чтобы идти в ногу с развитием цифровых кошельков.

2. Материалы и методы

Материалами для исследования послужила российская и зарубежная специализированная техническая и справочная литератур, материалы журнальных публикаций, последние достижения в сфере создания технических средств обеспечения безопасности банковской деятельности, а также официальные государственные, ведомственные, нормативные правовые акты России.

Основными методами, используемыми в исследовании, являются методы научного познания: сравнительный и логический анализ, наблюдение, методы экспертных оценок, логические приемы, определения, описания, анализа и синтеза.

3. Обсуждение

Термин «биометрия» может показаться немного пугающим, но на самом деле он довольно прост. Биометрия – это применение статистического анализа к биологическим данным, поэтому, когда говорится о биометрии, на самом деле имеются в виду только расчеты и измерения человеческого тела.

Измеряя уникальные физические и поведенческие характеристики человека, можно использовать их для идентификации. Вот что такое биометрическая аутентификация. Обычно используются маркеры для идентификации, которые можно легко отсканировать, записать и сравнить, например отпечатки пальцев, голоса или радужной оболочки глаза. Однако по мере развития технологий биометрия также может использоваться для идентификации человека по сердцебиению, походке или способу печати (Голдовский, 2010: 426).

Смартфоны – отличный пример того, как биометрия внедрена в повседневную жизнь. Уже никого не удивляет использование своего отпечатка пальца, чтобы разблокировать телефон, войти в свое банковское приложение или совершить платеж через PayPal. Смартфон iPhone, использует в качестве аутентификации распознавание лиц, а Samsung, распознавание радужной оболочки глаза.

Исходя из этого, Mastercard представила свою функцию «Selfie Pay» или Mastercard Identity Check, которая в основном позволяет авторизовать покупки, которые сделаны в Интернете, с помощью программного обеспечения для распознавания лиц на телефоне. (Черкасова, Кийкова, 2011: 201)

Взглянув шире на биометрию, и где она используется в настоящее время, давайте сосредоточимся на кредитных картах. Биометрическая кредитная карта не новость. За последние несколько лет по всему миру было проведено несколько испытаний этой технологии на предмет ее жизнеспособности.

В 2017 году Mastercard опробовала биометрическую кредитную карту в Южной Африке совместно с крупным ритейлером Pick n Pay и Absa Bank, принадлежащим Barclay. Аналогичное испытание прошло в том же году с итальянским банком Intesa Sanpaolo. В 2018 году Bank of Cyprus выпустил собственную биометрическую кредитную карту, а затем в марте этого года Visa объединившись с британским банком NatWest, так же, как Mastercard, подписала сделку с Royal Bank of Scotland, о создании первой биометрической карты в Великобритании (Mastercard biometric card, 2019).

Рис. 1. Разные виды аутентификации на смартфоне

Биометрическая кредитная карта использует комбинацию сканера отпечатков пальцев и технологии EMV. При первом карты, необходимо зарегистрировать отпечаток пальца. Это возможно сделать дома, используя свой телефон и сканер, также это может осуществить сам поставщик кредитной карты. Затем отпечаток пальца зашифровывается и сохраняется на вашей карте (Павлов 2010: 76).

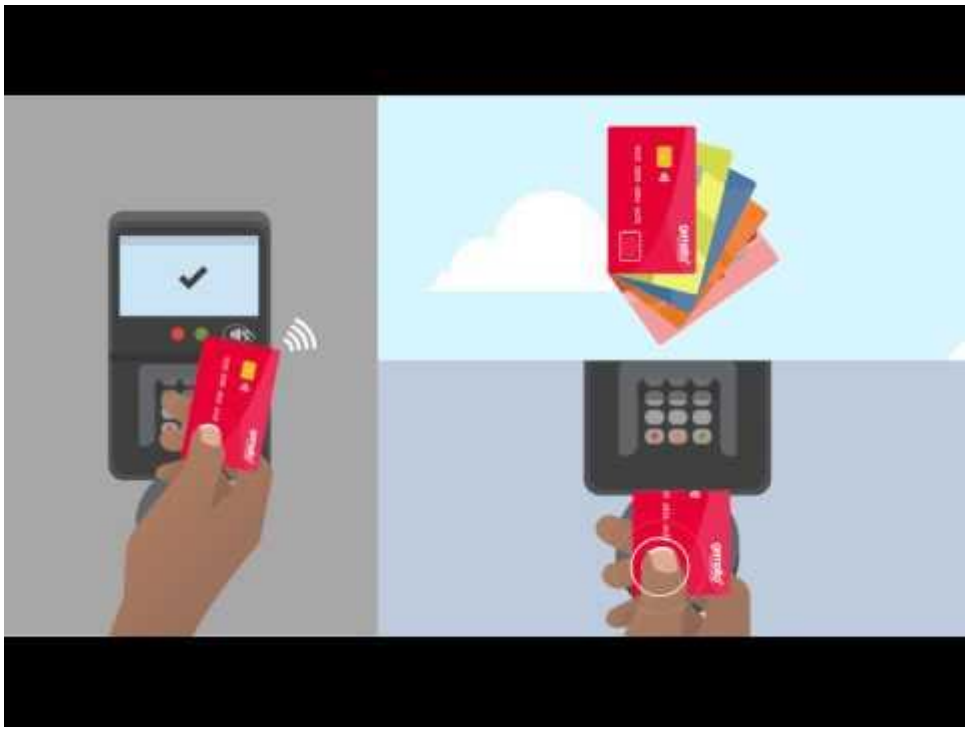

Рис. 2. Пример использования биометрических банковских карт

При использовании карты просто положите палец на небольшой сканер, встроенный в карту, и коснитесь карты или вставьте ее в устройство для чтения карт, чтобы произвести платеж (см. Рисунок 2). Карта получает питание от устройства чтения карт, чтобы активировать устройство считывания отпечатков пальцев, и если показания совпадают с данными отпечатков пальцев, хранящимися на карте, платеж будет авторизован. В отличие от бесконтактных платежей, здесь не будет ограничений на сумму покупки, и он должен работать с любым карточным терминалом по всему миру (Лаврушин, 2016: 149).

Пока существуют кредитные карты, будет осуществляться мошенничество с ними. И хотя провайдеры карт усердно работают над внедрением новых способов борьбы с мошенничеством, преступники всегда находят новые способы их обойти. Биометрическая аутентификация – это просто следующий шаг в борьбе с мошенничеством в сфере кредитными картами.

Но, конечно, это не все, что биометрия может предложить миру кредитных карт. Использование биометрии может помочь как индустрии кредитных карт, так и пользователям кредитных карт (Скиннер, 2009: 216).

Биометрическая кредитная карта может лучше защитить данные держателя карты. С биометрической кредитной картой биометрические данные никогда не покидают карту. Контрольные данные отпечатков пальцев надежно хранятся на микросхеме карты и никогда не должны храниться на серверах провайдера карты или где-либо еще. Это похоже на уже существующую систему с биометрической аутентификацией смартфона.

Использование биометрии безопаснее, чем использование PIN-кода. Так же, как использование PIN-кода было безопаснее, чем использование подписи.

Биометрия может помочь избавить мир от небезопасных PIN-кодов и паролей. Одна из основных проблем с PIN-кодами и паролями заключается в том, что вам нужен уникальный для всего. К сожалению, средний человеческий мозг не приспособлен для запоминания такого количества PIN-кодов или паролей, что означает, что пользователи могут использовать одни и те же или те, которые легко угадать. Если в качестве пароля используется биометрию, запоминать последовательность PIN-кодов или паролей больше не нужно (Thales, 2019).

Биометрическая кредитная карта упрощает платежи. Любой, кто пользовался бесконтактными платежами, знает, насколько они удобны. Чтобы совершить покупку необходимо приложить карту, и покупка совершена. Но сумма платежа все равно ограничена. Превысив суммы больше 1000 рублей необходимо ввести свой PIN-код, что несколько замедляет работу. С биометрической кредитной картой процесс такой же быстрый и простой, как и платежи в кассу, но при этом нет ограничений на сумму покупки.

Там, где есть положительная сторона, обычно есть и обратная сторона. Вот некоторые из факторов, которые могут умалить преимущества биометрических кредитных карт (Гамза и др., 2015: 388).

Пользователи беспокоятся о безопасности своих биометрических данных. Хотя существующая в настоящее время система должна означать, что все биометрические данные хранятся на самой карте, существует вероятность того, что эти данные будут неправильно сохранены, проданы или украдены. Кража ваших биометрических данных может стать огромной проблемой. В конце концов, вы можете изменить свой PIN-код, но вы не можете точно изменить свои отпечатки пальцев.

Сбор биометрических данных заставляет людей нервничать из-за того, что они могут попасть в чужие руки. Под этим подразумевается не только преступники. Некоторые организации выступают против биометрии, поскольку они позволяют правительствам хранить так много наших данных, которые затем можно использовать для отслеживания и, теоретически, ограничения нашей деятельности (Павлов 2010: 42).

Создания стандартной EMV-карты имеет небольшую стоимость, а создание биометрической кредитной карты стоит в 20 раз дороже. Хотя стоимость новой технологии со временем всегда снижается, эта первоначальная стоимость может оказаться препятствием.

4. Результаты

Биометрические технологии развиваются каждый день. Будь то крошечные батарейки, используемые в биометрических кредитных картах, чтобы они оставались заряженными в течение многих лет между использованиями, или внедрение технологии блокчейн в безбумажные путешествия, чтобы позволить путешественникам выбирать, когда и где хранить свои биометрические данные – все определенно становится напряженно в мире биометрии. Это просто вопрос того, как далеко можно продвинуть технологию и какие препятствия могут встать на ее пути (Ярочкин, 2004: 231).

Когда дело доходит до технологий в целом, каждая инновация – это шаг к чему-то лучшему. Биометрические данные войдут в индустрию платежей независимо от того, как они в конечном итоге будут использоваться: по оценкам Visa, биометрия будет использоваться для более 18 миллиардов транзакций к 2021 году, что на 83,7 % больше, чем в 2016 году.

Одна из причин этого может заключаться в том, что большинство потребителей готовы внести изменения в решение для биометрических платежей, несмотря на некоторые оговорки относительно безопасности. Согласно опросу (см. Рисунок 3), проведенному по заказу Visa, более 85 % опрошенных ими потребителей были заинтересованы в использовании биометрических данных для подтверждения своей личности или осуществления платежей. Мало того, 70 % считали, что биометрия упростит платежи, а 46 % считали, что они более безопасны, чем использование паролей или PIN-кодов (Visa Security, 2017).

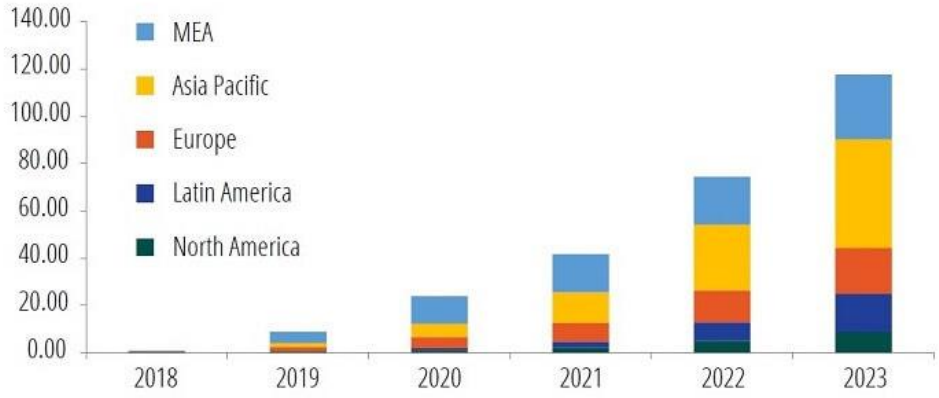

Рис. 3. Результаты опроса, проведенные по заказу Visa

5. Заключение

Использование биометрии для банковских карт значительно повысит уровень ее безопасности. Пройдет некоторое время, прежде чем пользователи начнут получать биометрические кредитные карты. Чтобы повысить безопасность своей кредитной карты необходимо:

- Использовать уникальный PIN-код для каждой карты. Сделайте так, чтобы было трудно угадать, и никому не говорите, что это такое.
- Помнить, куда кладете свою карту. Следите за скиммерами кредитных карт в банкоматах и считывателях карт.
- Регулярно проверять выписки по кредитной карте. Если обнаруживаете какие-либо транзакции, которые не можете распознать, сообщите о них провайдеру карты для расследования.
- Будьте осторожны при использовании карты в Интернете. Используйте только надежные сайты, никогда не используйте общедоступный Wi-Fi при совершении покупок в Интернете или при доступе к онлайн-банкингу и регулярно обновляйте свое программное обеспечение безопасности.
- Никому не сообщайте данные своей кредитной карты. Никакая законная компания не позвонит вам или не отправит электронное письмо с просьбой обновить информацию о кредитной карте.

Литература

Алексанов и др., 2012 – *Алексанов А.К., Демчев И.А., Доронин А.М.* Безопасность карточного бизнеса. Бизнес-энциклопедия. Московская Финансово-Промышленная Академия, ЦИПСиР, 2012.

Гамза и др., 2015 – *Гамза В.А., Ткачук И.Б., Жилкин И.М.* Безопасность банковской деятельности. Москва. Юрайт, 2015.

Голдовский, 2010 – *Голдовский И.М.* Банковские микропроцессорные карты. М.: ЦИПСиР: Альпина Паб лишерз, 2010.

Лаврушин, 2016 – *Лаврушин О.И.* Банковская система в современной экономике. Москва: КноРус Медиа, 2016.

Павлов, 2010 – *Павлов А.В.* Основы организации безопасности банков. Москва: Академия, 2010.

Скиннер, 2009 – *Скиннер К.* Будущее банкинга. Мировые тенденции и новые технологии в отрасли. М.: Гревцов Паблишер, 2009.

Черкасова, Кийкова, 2011 – *Черкасова Е.А., Кийкова Е.В.* Информационные технологии в банковском деле. Москва: Академия, 2011.

Ярочкин, 2004 – *Ярочкин В.И.* Безопасность банковских систем. М.: Ось-89, 2004.

Mastercard biometric card, 2019 – Mastercard biometric card «Driving cardholder security and convenience» [Electronic resource]. URL: https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/biometrics/biometrics-card.html (date of access: 27.09.2020).

Thales, 2019 – Thales «Biometric payment card (fingerprint authentication)». [Electronic resource]. URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/emv-biometric-card (date of access: 30.09.2020).

Visa Security, 2017 – Visa Security «Consumers ready to switch from passwords to biometrics, study shows». [Electronic resource]. URL: https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html (date of access: 30.09.2020).

References

Aleksanov i dr., 2012 – *Aleksanov, A.K., Demchev, I.A., Doronin, A.M.* (2012). Bezopasnost' kartochnogo biznesa. Biznes-entsiklopediya [Security of the card business. Business encyclopedia]. Moskovskaya Finansovo-Promyshlennaya Akademiya, TsIPSiR. [in Russian]

Cherkasova, Kiikova, 2011 – *Cherkasova, E.A., Kiikova, E.V.* (2011). Informatsionnye tekhnologii v bankovskom dele [Information technologies in banking.]. Moskva: Akademiya. [in Russian]

Gamza i dr., 2015 – *Gamza, V.A., Tkachuk, I.B., Zhilkin, I.M.* (2015). Bezopasnost' bankovskoi deyatel'nosti [Security of banking]. Moskva. Yurait. [in Russian]

Goldovskii, 2010 – *Goldovskii, I.M.* (2010). Bankovskie mikroprotsessornye karty [Banking microprocessor cards]. M.: TsIPSiR: Al'pina Pab lisherz. [in Russian]

Lavrushin, 2016 – *Lavrushin, O.I.* (2016). Bankovskaya sistema v sovremennoi ekonomike [The banking system in the modern economy]. Moskva: KnoRus Media. [in Russian]

Mastercard biometric card, 2019 – Mastercard biometric card «Driving cardholder security and convenience» [Electronic resource]. URL: https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/biometrics/biometrics-card.html (date of access: 27.09.2020).

Pavlov, 2010 – *Pavlov, A.V.* (2010). Osnovy organizatsii bezopasnosti bankov [Fundamentals of bank security organization]. Moskva: Akademiya. [in Russian]

Skinner, 2009 – *Skinner, K.* (2009). Budushchee bankinga. Mirovye tendentsii i novye tekhnologii v otrasli [The Future of banking. Global trends and new technologies in the industry]. M.: Grevtsov Pablisher. [in Russian]

Thales, 2019 – Thales «Biometric payment card (fingerprint authentication)». [Electronic resource]. URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/emv-biometric-card (date of access: 30.09.2020).

Visa Security, 2017 – Visa Security «Consumers ready to switch from passwords to biometrics, study shows». [Electronic resource]. URL: https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html (date of access: 30.09.2020).

Yarochkin, 2004 – *Yarochkin, V.I.* (2004). Bezopasnost' bankovskikh system [Security of banking systems]. M.: Os'-89. [in Russian]

Биометрическая кредитная карта

Мария Александровна Белова [a, *], Василиса Игоревна Рыськина [a]

[a] Государственный университет морского и речного флота имени адмирала С.О. Макарова, Российская Федерация

Аннотация. В данной статье рассмотрена новая технология создания банковских карт, такая как биометрические банковские карты, которые используют комбинацию сканера отпечатков пальцев и технологии EMV. При этом способе защиты карты, необходимо зарегистрировать отпечаток пальца. Это легко сделать дома, используя свой телефон и сканер, или же это может осуществить сам поставщик кредитной карты. Затем отпечаток пальца зашифровывается и сохраняется на вашей карте. При этом отмечено, что большинство потребителей готовы внести изменения в решение для биометрических платежей, несмотря на некоторые оговорки относительно безопасности. В статье приведены и проанализированы плюсы и минусы данной системы карт, а также разъяснено, чем биометрические банковские карты отличаются от обычных кредитных банковских карт с бесконтактной оплатой. Сделан вывод, что использование биометрии для банковских карт значительно повысит уровень ее безопасности. Главным препятствием их внедрения является то, что создание биометрической кредитной карты стоит в 20 раз дороже чем обычной, но стоимость новой технологии со временем всегда снижается.

Ключевые слова: биометрическая банковская карта, бесконтактная оплата, банк, банковские карты, биометрия, технологии, PIN-код, PayPal, распознание, биометрия лица, кредитные карты.

* Корреспондирующий автор
Адреса электронной почты: m-belova123@mail.ru (М.А. Белова)