

**БИОМЕТРИЧЕСКИЕ КАРТЫ: ОСНОВНЫЕ ПОНЯТИЯ,
ВОЗМОЖНОСТИ И ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ
BIOMETRIC CARDS: BASIC CONCEPTS, CAPABILITIES
AND FEATURES OF USING**

Стариков А.В., д.т.н., доц.

ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»
г. Воронеж, Россия
star123@yandex.ru

Starikov A.V., DSc (Engineering), Associate Professor
FSBEI HE "Voronezh State University of Forestry and Technologies
named after G.F. Morozov"
Voronezh, Russian Federation

Аннотация: В статье рассмотрены основные понятия, возможности и особенности использования биометрических карт, представляющих собой новый подход в технологии биометрической аутентификации личности.

Abstract: The article considers the basic concepts, possibilities and features of using biometric cards, which represent a new approach in biometric personal authentication technology.

Ключевые слова: биометрическая аутентификация, биометрическая карта, система контроля и управления доступом (СКУД), автоматизация.

Keywords: biometric authentication, biometric card, access control and management system (ACMS), automation.

Биометрические карты представляют собой сравнительно новый подход в технологии биометрической аутентификации. Развитие этого подхода началось еще в 2009 году, когда старт-ап команда Zwiре при финансовой поддержке венчурных инвестиционных фондов из Норвегии приступила к созданию принципиально новых устройств для идентификации физических лиц. Энтузиасты-исследователи из Zwiре попытались совместить преимущества биометрической аутентификации личности с простотой и

доступностью применения электронных карт. После нескольких лет разработок и экспериментов компания Zwiре предложила рынку так называемые биометрические карты, которые могут быть использованы для выполнения платежей, физического и логического контроля доступа и других решений, связанных с биометрической идентификацией личности [1].

По размерам и форме биометрическая карта похожа на обычную пластиковую карту. Однако у нее имеется существенное отличие в виде встроенного в карту дактилоскопического сканера (датчика). Пользователь прикладывает палец к сканеру, считывающему отпечаток пальца, на основе которого формируется его электронный образ. Сформированный образ сравнивается с шаблоном отпечатка, который предварительно записывается в память карты. Если отпечаток пальца пользователя совпадает с шаблоном, то осуществляется обмен данными между картой и считывателем (рис. 1).

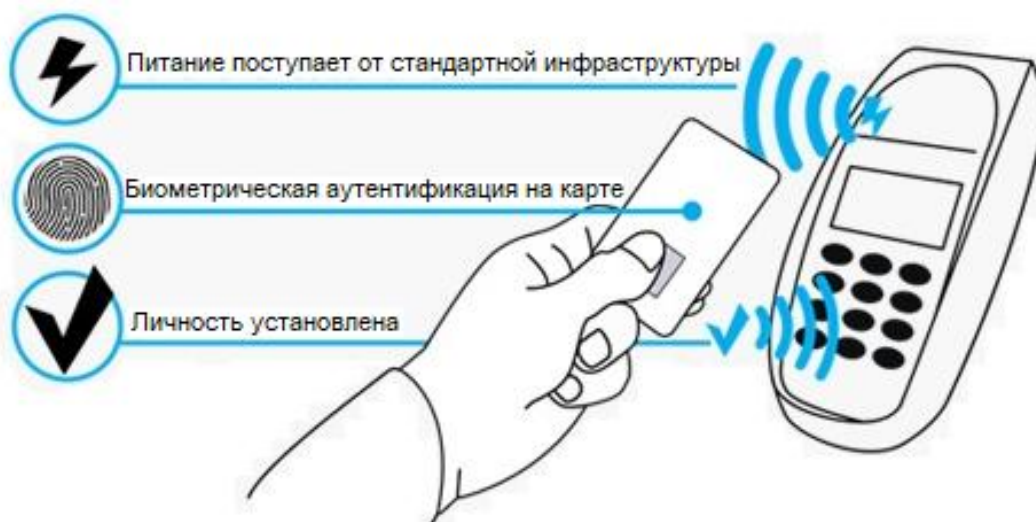


Рисунок 1 – Установление личности пользователя биометрической карты

Особенностью биометрической карты Zwiре является то, что в режиме ожидания (т.е. при отсутствии пальца на сканере) нельзя извне инициировать работу транспондера на карте; это обстоятельство делает невозможным считывание информации и последующее клонирование карты.

Необходимо также отметить, что запись шаблона отпечатка в память может быть выполнена только один раз, т.е. память невозможно перезаписать или каким-либо образом модифицировать. Таким образом, владельцу биометрической карты гарантируется, что в случае ее потери невозможно использование карты сторонними лицами (рис. 2).



Рисунок 2 – Этапы алгоритма для формирования шаблона отпечатка

Кроме того, процесс записи шаблона отпечатка пальца выполняется самим пользователем, а не администратором системы, поэтому проблемы с защитой персональных биометрических данных не возникает, поскольку даже теоретически дактилоскопические данные в этом случае не могут быть переданы сторонним лицам.

Биометрические карты Zwiре существенно сокращают объем работ, связанных как с администрированием биометрических терминалов, так и одновременным ведением баз данных СКУД и биометрией, и требующих работы с несколькими программами. Так называемый мэтчинг, т.е. операция сопоставления отпечатка с шаблоном, хранящимся в памяти карты, выполняется по методу 1:1 и происходит достаточно быстро (не более 1,5 секунд). Поэтому не требуется никакой дополнительной базы данных связанной с ней процедурой администрирования и защиты. Биометрические карты доступа Zwiре могут работать на любой установленной СКУД, причем для совместимости необходимо лишь выбрать модель карты с транспондером, который аналогичен применяемому на охраняемом объекте. При этом установка и настройка карты в системе представлена стандартной процедурой добавления карты доступа в СКУД.

В настоящее время компания Zwiре (www.zwiре.com), имеющая штаб-квартиру в столице Норвегии г. Осло, а также свои представительства в 12 странах, продолжает совершенствовать свои инновационные биометрические продукты и услуги. Кроме Zwiре еще ряд компаний, включая и всемирно известные (например, корпорация Samsung), также стали предлагать аналогичные решения, использующие сканер отпечатка пальца на карте [2]. Корпорация Samsung разработала чип биометрической защиты для смарт-карт, особенностью которого является интеграция всех элементов защиты, которые ранее были разнесены по площади карты [3].

Чип защиты, получивший обозначение S3B512C, объединяет в себе элемент безопасности (Secure Element), хранящий конфиденциальные и

криптографические данные, процессор безопасности (Secure Processor), обрабатывающий данные, и сканер отпечатка пальцев (Fingerprint Sensor). На используемых до сих пор моделях биометрических карт все эти элементы находятся в разных местах карты, что усложняет их производство. Samsung заявляет, что их разработка является первым решением на рынке, которое объединяет все части воедино. Схематичный переход к новому решению средств защиты в виде одного чипа на карте показан на рис. 3.

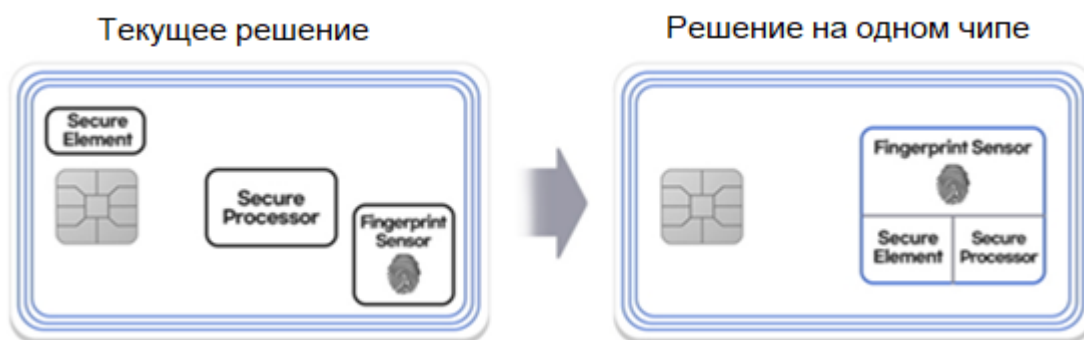


Рис. 3. Переход к интегрированному решению средств защиты на одном чипе

При регистрации карты в ее память могут быть записаны до трех разных шаблонов отпечатков пальцев. Эти шаблоны отпечатков надежно зашифрованы и защищены от несанкционированного доступа.

Подобные биометрические карты могут не только использоваться в качестве надежного средства оплаты, они вполне подходят для использования их в качестве карт доступа в современных биометрических СКУД. В настоящее время ряд производителей СКУД в России обеспечивают такие технические решения [4].

Список литературы

1. Бойко Г. ZWIPE: знакомство с биометрическими картами – Режим доступа: http://secuteck.ru/articles2/sys_ogr_dost/zwipe-znakomstvo-s-biometricheskimi-kartami, загл. с экрана (дата обращения: 23.03.2024).
2. Новые возможности оплаты – биометрические карты со сканером отпечатков пальцев Samsung Biometric Card IC – Режим доступа: <https://news.samsung.com/ru/new-payment-options-biometric-cards-with-samsung-biometric-card-ic-fingerprint-scanner>, загл. с экрана (дата обращения: 23.03.2024).

3. Samsung представила свой чип биометрической аутентификации для смарт-карт – Режим доступа: <https://habr.com/ru/news/647849>, загл. с экрана (дата обращения: 23.03.2024).

4. Применение биометрических карт в СКУД – Режим доступа: <https://www.rgsec.ru/stati/primenenie-biometricheskih-kart-dostupa-v-skud>, загл. с экрана (дата обращения: 23.03.2024).

References

1. Boyko G. ZWIPE: introduction to biometric cards – Access mode: http://secuteck.ru/articles2/sys_ogr_dost/zwipe-znakomstvo-s-biometricheskimi-kartami, cap. from the screen (access date: 03/23/2024).

2. New payment options - biometric cards with a fingerprint scanner Samsung Biometric Card IC – Access mode: <https://news.samsung.com/ru/new-payment-options-biometric-cards-with-samsung-biometric-card-ic-fingerprint-scanner>, cap. from the screen (access date: 03/23/2024).

3. Samsung presented its biometric authentication chip for smart cards – Access mode: <https://habr.com/ru/news/647849>, cap. from the screen (access date: 03/23/2024).

4. Application of biometric cards in access control systems – Access mode: <https://www.rgsec.ru/stati/primenenie-biometricheskih-kart-dostupa-v-skud>, cap. from the screen (access date: 03/23/2024).