Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:351.755.61

Сидоренко
Андрей Эдуардович

# Программный комплекс контроля доступа пользователя к информации, хранимой на смарт-карте

**АВТОРЕФЕРАТ**
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____
___

Научный руководитель

Чернякова Екатерина Викторовна

к.ф.-м.н., доцент

_____

Минск 2018

# ВВЕДЕНИЕ

Национальные идентификационные смарт-карты выдаются гражданам в более чем 100 странах во всем мире. Эти карты могут использоваться в качестве проездных документов — эквивалент паспортам — (так долго, как они принимаются в стране назначения), а также в качестве подтверждения личности в их родной стране [4]. Только несколько стран в наше время не требуют, чтобы их граждане владели и использовали идентификационные карты, например, Австралия, Япония и Соединенные Штаты. Обычно, идентификационные карты более компактны в своей физической форме, чем паспорта и их удобный размер делает их более удобными в использовании в повседневной жизни. Кроме того, в идентификационных картах содержится больше информации о владельце карты, чем в паспортах, такой как домашний адрес, высота человека и цвет глаз.

Введение в Беларуси биометрических документов, в частности идентификационной карты, планируется с января 2019 года. ID-карта заменит некоторые функции нынешнего паспорта и будет единственным документом, удостоверяющим личность. В электронном чипе будут присутствовать персональные данные гражданина, в частности, фотография, электронная подпись и отпечатки пальцев. Карта будет с двумя чипами — контактным и бесконтактным, в них будут содержаться три приложения. Одно из них — идентификационное, а другое криптографическое — электронная цифровая подпись. Она позволит идентифицировать себя на информационных ресурсах, которые будут разрабатываться под карточку. Третье приложение соответствует требованиям ICAO (Международная организация гражданской авиации). Оно предназначено для того, чтобы впоследствии по этой карточке можно было бы пересекать государственную границу в случае заключения соответствующих международных соглашений.

Так как на ID-карте будет содержаться критическая информация о гражданине, очень важно реализовать соответствующие механизмы безопасности. Тема контроля доступа к информации, хранимой на смарт-карте, гарантирование её целостности, является крайне актуальной в настоящей момент, так как сейчас активно ведутся работы в данном направлении.

В данной работе не рассматривается физическая защита идентификационных карт, только лишь программная.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Связь работы с приоритетными направлениями научных исследований**

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлекроники».

**Цель и задачи исследования**

Цель диссертационной работы заключается в разработке программного комплекса для защиты и контроля доступа информации, хранимой на идентификационной смарт-карте.

Для достижения указанной цели в диссертации необходимо было выполнить следующие задачи:

1. Проанализировать проблемы безопасности данных на смарт-картах.
2. Проанализировать и систематизировать информацию по методам защиты информации на смарт-карте.
3. Исследовать и реализовать в виде программного комплекса методы аутентификации и контроля доступа, опираясь на международные рекомендации, касающиеся элементов криптографической защиты для обеспечения доступа к бесконтактной интегральной схеме смарт-карты.

**Апробация результатов диссертации**

Основные положения и результаты диссертации обсуждались на 53 научной конференции аспирантов, магистрантов и студентов БГУИР.

**Опубликованность результатов диссертации**

По результатам исследований, предоставленных в диссертации, опубликовано 2 работы, в том числе 1 статья в сборниках материалов конференций.

**Личный вклад соискателя**

В диссертации представлены результаты исследований, выполненных автором. Личный вклад автора состоит в постановке задач исследования, разработке экспериментальных и теоретических методов их решения, в разработке программного комплекса с методами защиты информации, хранимой на смарт-карте и формулировке выводов.

# КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

## Используемая методология

Сделанные из бумаги идентификационные карты в настоящее время постепенно заменяется электронными удостоверениями личности. На eID карте содержится вся информация, включенная в более старые бумажные карты, но кроме того очень часто на ней хранится биометрические данные (т.е., отпечатки пальцев) владельца карты и цифровая копия фотография в чипе RFID на карте. Для идентификационных карт требуется защита от копирования, клонирования и подделки, чтобы не допустить, чтобы один человек злоупотреблял удостоверением личности или выдавал себя за другого человека - возможно, несуществующего человека. По этой причине при изготовлении этих карточек эмитенты используют контрмеры, которые позволяют физически проверять правильность и достоверность удостоверения личности. Существует две основные организации, которые публикуют международные рекомендации для машиносчитываемых проездных документов и идентификационных карт и по их методам защиты информации на смарт-картах: ICAO (Международная организация гражданской авиации), BSI (Федеральное ведомство по информационной безопасности Германии).

## Уязвимости смарт-карт и рекомендации по методам защиты от международных организаций

Основные уязвимости смарт-карт:

1) Скимминг данных с бесконтактной ИС;
2) Несанкционированный доступ к информации, хранимой на смарт-карте;
3) Перехват обмена информацией между ИС и считывающим устройством;
4) Подмена или изменение данных, хранящихся на ИС;
5) Использование поддельных чипов.
6) Использование поддельных считывателей.

Все сообщения, отправленные и полученные с помощью карты eID, должны быть защищены от подслушивающих устройств и злонамеренных сторон, которые пытаются незаконно получить доступ к конфиденциальной информации о владельце карты и / или его или ее транзакциях. Кроме того,

владелец карты должен выбрать персональный идентификационный номер (PIN), который необходимо ввести в устройство чтения карт, чтобы выполнить аутентификацию. Чтобы обеспечить аутентификацию карты через Интернет, на ID-карте должно быть реализовано несколько криптографических протоколов. Эти протоколы направлены на обеспечение подлинности, целостности и конфиденциальности пользовательских данных. Если объединить международные рекомендации, можно выделить несколько основных протоколов, которые желательно использовать для защиты информации: BAC, PACE, PA, AT, AM, PIN/PUK, проверка сертификата.

1) BAC (Базовый контроль доступа)

Базовый контроль доступа проверяет, что терминал имеет физический доступ к странице данных документа. Протокол устанавливает защищенное соединение на основе машиночитаемой строки документа.

2) Установление соединения с аутентификацией паролем (PACE).

PACE является механизмом взаимной аутентификации между терминалом и чипом, который основан на совместном пароле, например. секретный PIN-код (персональный идентификационный номер), который известен только владельцу или CAN (номер доступа к карте), который напечатан на документе. Этот механизм является заменой BAC и используется для настройки первоначальной связи.

3) Пассивная аутентификация.

Пассивная аутентификация необходима для того, чтобы доказать подлинность данных, хранящихся на микросхеме.

4) Расширенный контроль доступа (EAC).

Контроль расширенного доступа - это механизм взаимной аутентификации между терминалом и чипом на базе инфраструктур открытых ключей (PKI). Терминальная аутентификация ограничивает доступ к данным, хранящимся на чипе, авторизованным терминалам. Чип-аутентификация не только аутентифицирует чип как подлинный, но также обеспечивает надежную защиту шифрования и целостности передаваемых данных.

В соответствии с рекомендациями BSI для осуществления расширенного контроля доступа к данным на бесконтактных микросхемах должны применяться механизмы взаимной аутентификации микросхемы и терминала, входящие в General Authentication Procedure

Таблица 1– Упрощённая схема General Authentication Procedure

| **Микросхема** | **Терминал** |
|---|---|
| Чтение файла EF.CardAccess | |
| | Ввод/Чтение пароля PACE (eID PIN/CAN/MRZ) |
| **PACE** | |
| Передача цепочки сертификатов<br>**Аутентификация терминала** | |
| Чтение файла EF.CardSecurity | |
| | **Пассивная аутентификация** EF.CardSecurity |
| **Аутентификация микросхемы** | |
| *Система проверки*: чтение EF.SOD | |
| | *Система проверки*: проверка подписи EF.SOD (**Пассивная аутентификация**) |
| Считывание разрешённой информации | |
| | *Система проверки*: Расчёт хэш-функций прочитанных групп данных и сравнение с хэшем групп данных, которые хранятся в EF.SOD |

## Инструменты и выбор аппаратной базы для разработки программного комплекса

Для разработки были выбраны следующие инструменты:

1) Смарт-карты на платформе Java Card по следующим причинам:

− необходим комплексный подход к безопасности − с точки зрения системы в целом. Платформа Java Card реализует верхний уровень платформы смарт-карт, которая включает аппаратные средства, «родную» операционную систему и хост-систему, с которой взаимодействует смарт-карта;

− есть информация в открытом доступе по разработке на данной платформе;

− разрабатываемую систему возможно расширять по функционалу без особых трудностей из-за особенностей платформы;

2) Среда для разработки апплетов смарт-карт JavaCard Development Kit. Причины выбора:

− предоставляет как возможность разработки на виртуальной карте, так и использование виртуального терминала;

− включает в себя программу JCIDE, интегрированную среду разработки (IDE), разработанную специально для платформы Java Card;

− включает в себя программу pyApdutool, необходимую для взаимодействия с картой через считыватель.

3) Intelij Idea − интегрированая среда разработки для языка программирования Java. Необходима для разработки хост-программы.

**Разработка программного комплекса**

Первым этапом разработки стало создание системы взаимодействия смарт-карты и терминала без дополнительной реализации контроля доступа. Программный комплекс позволяет персонализировать карту и считывать с неё информацию.

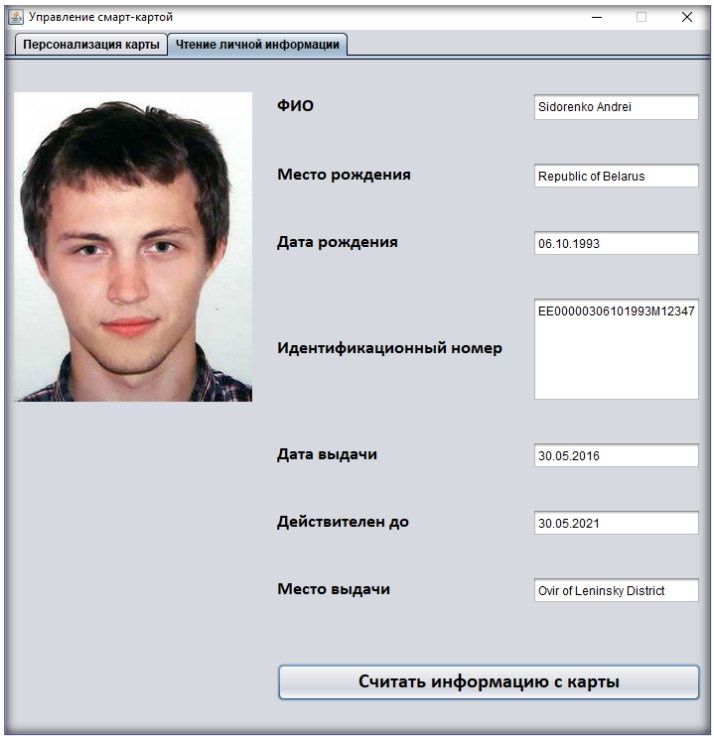


**Рисунок 1 – Внешний вид программы**

Данная система из защиты включала в себя только лишь блокировку от повторной персонализации карты, но не имело никакой другой защиты, кроме встроенных алгоритмов самой платформы Java Card. Зная идентификатор апплета карты, нужные коды инструкции, которые можно

получить различными способами (сниффинг, анализ кода хост прогрммы и т.д.) можно считать незашифрованные данные с карты в hex формате.

После добавления методов защиты, которые описаны в работе, процесс аутентификации принял следующий вид:

Таблица 2 – Схема аутентификации разработанного программного комплекса

| **Микросхема** | **Терминал** |
|---|---|
| | Ввод/Чтение пароля PIN |
| Проверка пароля PIN | |
| Запрос сертификата | |
| Передача сертификата | |
| | *Система проверки*: Проверка сертификата и извлечение открытого ключа карты |
| *Система проверки*: чтение EF.SOD | |
| | *Система проверки*: проверка подписи EF.SOD (**Пассивная аутентификация**) |
| Считывание разрешённой информации | |
| | *Система проверки*: Расчёт хэш-функций прочитанных групп данных и сравнение с хэшем групп данных, которые хранятся в EF.SOD |

Добавление PIN кода вносит в программу пользовательский секрет. Он используется как один из паролей доступа к информации, которая хранится на смарт-карте.

Пассивная аутентификация решает проблему целостности информации. При выполнении пассивной аутентификации создается переменная, в которой хранятся хэши переменных, которая подписывается закрытым ключом карты (электронная цифровая подпись) для защиты от изменения. Сравнив хэш полученных от карты данных с хэшем из файла безопасности можно утверждать, что данные не были изменены. Электронная цифровая подпись генерируется только лишь один раз, при персонализации, далее лишь производится проверка подписи и формируется хэш. Электронная цифровая подпись данных позволяет подтвердить неизменность данных. Данная реализация является более быстрой по сравнению с вариантом пассивной аутентификации, описанной в международных рекомендациях, так

как хэш высчитывается один раз из конкатенации переменных, хранимых на смарт-карте.

Проблему отсутствия гарантии, что данная цифровая подпись принадлежит определенному физическому или юридическому лицу решает добавление сертификата открытого ключа, выданного удостоверяющим центром. В этом случае появляется 3-я сторона, которой доверяют обе стороны, и которая подтверждает, что данный открытый ключ принадлежит тому или иному человеку

**Практическая значимость программного комплекса**

Разработанный программный комплекс наглядно показывает, как можно уменьшить количество атак на смарт-карту, путем добавления механизмов защиты в алгоритм. Реализованные алгоритмы уменьшают количество возможных атак на смарт-карту, но не ограничивают полностью. К вопросу безопасности соответствующим специалистам всегда нужно подходить самым серьезным образом, так как именно от безопасности чаще всего зависит общее состояние и работоспособность системы. Всегда следует учитывать и анализировать новые угрозы безопасности, которые со временем могут появляться в мире

# ЗАКЛЮЧЕНИЕ

Германия - не единственная страна, которая двигается к идентификационным картам со встроенным электронным чипом. Фактически, многие европейские страны идут или уже начали использовать национальные электронные удостоверения личности. Так обстоит дело, например, в Бельгии, Эстонии, Финляндии, Италии, Нидерландах, Португалии, Испании и Швеции. Также ожидается, что карты eID будут развернуты (или уже используются) за пределами Европы, например, в Бразилии, Индонезии, Малайзии, на Филиппинах, в Афганистане, Бахрейне, Омане, Катаре, Саудовской Аравии, ОАЭ и многих других странах. В Беларуси также ожидается внедрение идентификационной смарт-карты и биометрического паспорта с чипом.

Смарт-карты представляют собой удобный способ аутентификации пользователей к информационным ресурсам. Однако на начальном этапе смарт-карты часто содержит лишь базовые инструменты защиты данных, либо не содержит их вовсе. Даже, если таковые инструменты и имеются, то они зачастую реализованы в самом общем виде и не обеспечивают высокого уровня безопасности, особенно для серьёзных проектов, которые этого требуют. Поэтому требуется заранее определить необходимые методы защиты данных исходя из потенциального использования продукта. Если же проект серьёзный, как, например, машиносчитываемый проездной документ в виде идентификационной карты, то следует также придерживаться международных рекомендаций, которые в полной мере описывают алгоритмы контроля доступа к информации.

В процессе работы были приобретены навыка работы с современной прикладной программой для симуляции и прослушивания команд между смарт картой и хост-программой (JCIDE). Данная программа в полной мере выполняет свои задачи и наглядно показывает процесс коммуникации смарт-карты с терминалом.

Также была разработана демонстрационная программа контроля доступа к информации, хранимой на смарт-карте, с постепенным внедрением выбранных методов безопасности, согласно международным рекомендациям, и их последующим анализом. Конечно, в некоторой степени, в силу использования симулятора, а не реальной смарт-карты, некоторые методы защиты были реализованы в упрощенном виде, но они в полной мере показывают необходимость внедрения того или иного модуля для контроля доступа к информации.

# СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Зенин, К. Н. Система электронного документооборота / К. Н. Зенин, А. Э. Сидоренко, В. Е. Терентьев // Информационные технологии в образовании, науке и производстве : III Международная научно-техническая интернет-конференция, 20-21 ноября 2015 г. Секция 2 [Электронный ресурс]. - [Б. и.], 2015.

2–А. Сидоренко А. Э. Механизм Аутентификации Терминала/ А.Э. Сидоренко // 53-я научная конференция аспирантов, магистрантов и студентов БГУИР – Минск, 2017 – С.60 – 61.