УДК 004.087.5 **Технические науки**

Митрошина Екатерина Валерьевна, *студентка,*
5 курс электротехнического факультета
Пермский национальный исследовательский политехнический университет
e-mail: mitroshina.katya@inbox.ru

РАЗРАБОТКА МЕТОДИКИ ОРГАНИЗАЦИИ КОНТРОЛЯ ДОСТУПА С ПОМОЩЬЮ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ

Аннотация: В статье рассматриваются основные функции и возможности интеллектуальных карт, с целью разработки методики организации доступа.

Ключевые слова: Интеллектуальная карта, аутентификация, шифрование.

Abstract: This article describes main features/functions and possibilities of intellectual cards, with the aim of development the methodic of organization access.

Keywords: Smart card, authentication, encryption.

Актуальность изучения вопросов защиты информации с использованием интеллектуальных карт определяется повсеместным распространением компьютерных информационных, банковских, и других видов систем, а также отдельных прикладных программ, применяющих интеллектуальные карты в качестве средства хранения и обработки персональных данных пользователей и персонала компьютерных систем.

Смарт - карта была изобретена французским ученым, Роланом Морено в середине 70 - х годов двадцатого столетия, но только в 80 - е, благодаря развитию технологий, ее практическое использование стало удобным и недорогим. Смарт-карты представляют собой пластиковые карты со встроенной микросхемой. В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, управляющую устройством и контролирующую доступ к объектам в его

памяти. Кроме того, смарт - карты, как правило, обладают возможностью проводить криптографические вычисления. Назначением смарт-карт является одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде [1].

Методика организации контроля доступа с помощью смарт-карт

Организация контроля доступа с помощью смарт-карт на предприятия проводится на основе алгоритма, представленного на рисунке 1.

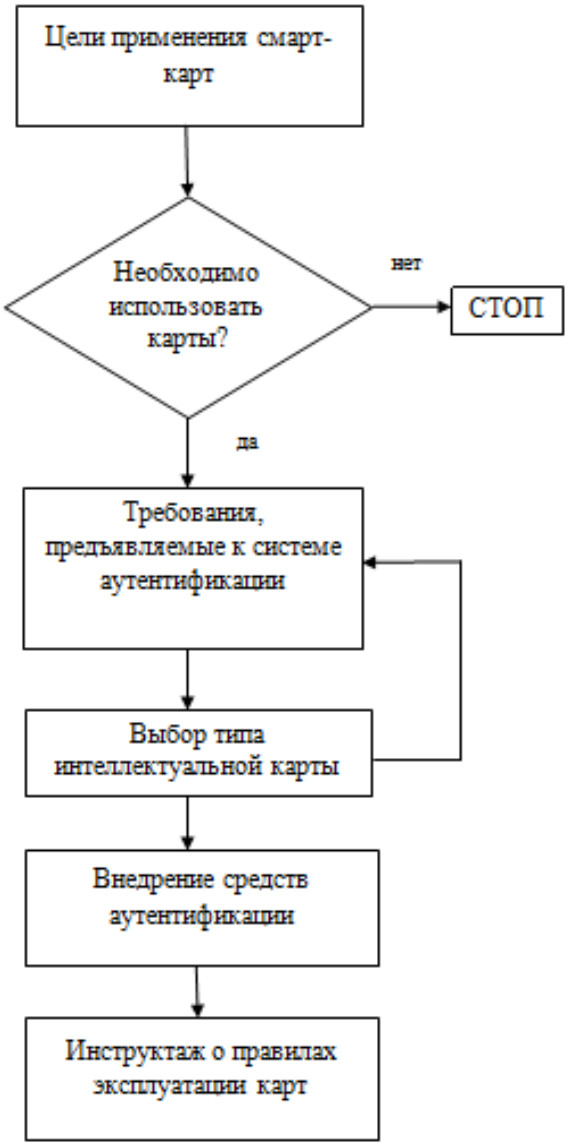

Рисунок 1 - Алгоритм организации контроля доступа с помощью смарт-карт

1. Цели применения интеллектуальных карт

Необходимость использования смарт - карт определяется такими целями предприятия, как:

а) Обеспечение физического контроля доступа:

– обеспечение контроля доступа персонала в различные помещения, а также ограничение доступа персонала на территорию в конкретных ситуациях;

– осуществление дистанционного контроля и фиксации движения транспорта, контейнеров и т.п. на территории предприятия.

б) Обеспечение логического контроля доступа:

– ограничение доступа к ресурсам информационной системы предприятия, тем самым организовать доступ к защищаемым данным, программам и т.п., только уполномоченных пользователей [3].

2. Требования, предъявляемые к системе аутентификации информации

– физические свойства и характеристики карты должны соответствовать стандартам ISO-7810 «Идентификационные карты — физические характеристики», ISO-7816 «Идентификационные карты — карты с микросхемой с контактами»;

– смарт - карты и считыватели должны использовать специальный алгоритм взаимной аутентификации, который гарантирует, что обмен информацией происходит между действительно настоящей, оригинальной картой и считывателем, обмен защищен и невозможна подмена данных [4];

– необходимо применение криптостойких алгоритмов шифрования, что позволяет сохранить конфиденциальность данных;

– использование операция диверсификации ключей, заключающаяся в генерации ключей для обмена информации с использованием секретного ключа и уникального серийного номера карты, которая гарантирует уникальность ключа обмена для каждой карты, что исключает возможность клонирования карт [2];

– считыватели должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков;

– конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов;

– производитель идентификаторов должен гарантировать, что код данного идентификатора не повторится, или указать условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами;

– считыватели при взломе и вскрытии, а также в случае обрыва или короткого замыкания подходящих к ним цепей не должны вызывать открывание преграждающего устройства.

Исходя из поставленных требований, переходим к выбору смарт - карты для организации контроля доступа.

3. Выбор типа интеллектуальной карты

Разновидности интеллектуальных карт и их основные характеристики приведены в таблице 1.

Таблица 1 - Характеристики интеллектуальных карт

	Контактные смарт-карты	Бесконтактные смарт-карты	
		Низкочастотные	Высокочастотные
Стандартизация	ISO-7810, ISO-7816	ISO-7810, ISO-7816	ISO-7810, ISO-7816, ISO-14443, ISO-156993
Радиочастотный диапазон	-	50-500 кГц	10MHz-15МГц
Проверка целостности данных	Да	Да	CRC 16 бит, бит четности, побитное кодирование, контроль разрядов
Взаимная аутентификация	Да	Нет	Да
Диверсификация ключей	Да	Нет	Да
Шифрование	Аппаратно реализованы DES/3DES/MAC.	Нет	Да
Дальность считывания	-	От 0,1 м. до 0,2 м.	От 0,1 м. до 0,9 м.
Скорость передачи данных	До 223 кбит/сек	100 кбит/сек	106 кбит/сек
Пользовательская память	256 КБайт	32 байта	32 байта
Срок хранения данных	10 лет	10 лет	10 лет
Стоимость (* по отношению к сравниваемым вариантам)	***	*	**

В соответствии с выбранным типом интеллектуальной карты подбирается подходящее оборудование для считывания.

Выводы:

– По сравнению с контактными, бесконтактные системы обеспечивают наибольшую пропускную способность за счет точности, надежности и удобства считывания кода, т.к не тратится время на точное ориентирование, вставку карты и ее транспортирование через считыватель.

– Высокая долговечность карт и считывателей бесконтактной технологии, поскольку практически отсутствует их износ, т.к нет взаимно движущихся частей и связанного с этим механического износа, не надо обслуживать и производить замену считывающих головок.

– Для применения в экстремальных условиях считыватели бесконтактной технологии значительно надежнее любых контактных, поскольку дистанционный метод считывания позволяет их сделать герметичными и конструктивно защищенными от механических и климатических воздействий.

– Высокочастотные технологии рекомендуется использовать там, где должно передаваться большое количество данных и где требуются высокая скорость считывания на большом расстоянии, например, контроль транспортных средств. Большое расстояние считывания в высокочастотных системах позволяют устанавливать считыватели на воротах или шлагбаумах, а бесконтактные карты закреплять на ветровом или боковом стекле автомобиля. Большая дальность действия делает также возможной безопасную маскированную установку считывателей вне пределов досягаемости нарушителей.

– Низкочастотные технологии целесообразно использовать там, где не требуется больших дистанций считывания, например, для организации входа в информационную систему [5].

4. Этапы внедрения средств аутентификации для контроля доступа на предприятии

– Документальное оформление принятых решений о необходимости внедрения системы аутентификации с помощью смарт - карт.

– Выбор подрядчика на выполнение внедрения системы и составление технического задания, в котором прописываются все технические особенности проекта.

– Сопровождение монтажных, а также разработка/корректировка внутренних нормативных документов по пропускному режиму.

– Пусконаладочные работы и ввод системы в эксплуатацию. На этом этапе необходимо плотно подключить к процессу сотрудников, которые будут непосредственно эксплуатировать систему. Сотрудники должны пройти теоретическое обучение, а также, участвуя в процессе пуско-наладки приобрести практические навыки.

5. Информирование пользователей о правилах хранения и эксплуатации карт

Смарт - карты являются чувствительными электронными приборами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанные устройства могут выйти из строя [6].

Следующие правила эксплуатации и хранения обеспечат длительный срок службы смарт-карт и сохранность конфиденциальной информации пользователя:

1. С целью обеспечения сохранности информации, закодированной на смарт-карте, не допускается деформировать или повреждать ее поверхность. Необходимо оберегать смарт-карты от сильных механических воздействий, таких как падение с высоты, сотрясения, вибрации, ударов и т.п.

2. Запрещается стирка смарт-карт в моющих средствах, контакт с органическими растворителями и т.д, а также необходимо избегать загрязнения микросхемы.

3. Запрещается изгиб смарт-карты более чем на 20°, а также перекручивание карты более 30 градусов в обе стороны.

4. Интеллектуальная карта должна храниться при температуре 0 …+50 градусов Цельсия.

5. Необходимо избегать воздействия на смарт-карты сильных электрических или магнитных полей.

Подводя итоги проделанной аналитической работы можно сделать вывод, что смарт-карты являются неотъемлемой частью системы защиты информации на предприятии. Учитывая совокупность таких критериев, как высокая защищенность и безопасность, удобство в использовании, возможность применения одной карты во множестве различных приложений можно сказать, что применение смарт-карт является правильным выбором, когда требуется не только безопасный контроль физического доступа, но и уверенность в расширении решаемых задач в будущем. Но, несмотря на все достоинства, смарт-карты имеют ряд недостатков, связанных с таким человеческим фактором, как кража карт. Однако данную проблему уже решают многие предприятия, разрабатывая карты с уже встроенной системой защиты.

Библиографический список:

1. А. А. Варфоломеев. Защита информации с использованием интеллектуальных карт. Учебное пособие. — М.: Российский университет дружбы народов , 2008 — 87 с.

2. Выбор технологии доступа. [Электронный ресурс] // URL: http://idsec.ru/articles/100916_cardscompare.htm (дата обращения: 10.11.2016).

3. Виды смарт - карт. [Электронный ресурс] // URL: http://dengi.polnaya.info/platezhnye_sistemy/smart_karta/ (дата обращения: 5.11.2016).

4. Smart - карты: актуальность применения и многофункциональность. [Электронный ресурс]. URL: http://www.secuteck.ru/articles2/sys_ogr_dost/smartkarti_aktyalnost_primeneniya_mnogofunkcionalnost_page148/ (дата обращения: 5.11.2016).

5. Смарт - карты. [Электронный ресурс] // URL: http://kunegin.narod.ru/ref6/sc1/index.htm (дата обращения: 10.11.2016).

6. Смарт - технологии. [Электронный ресурс] // URL: http://www.idexpert.ru/technology/122/ (дата обращения: 11.11.2016).