электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056

Обзор элементов защиты идентификационных карт

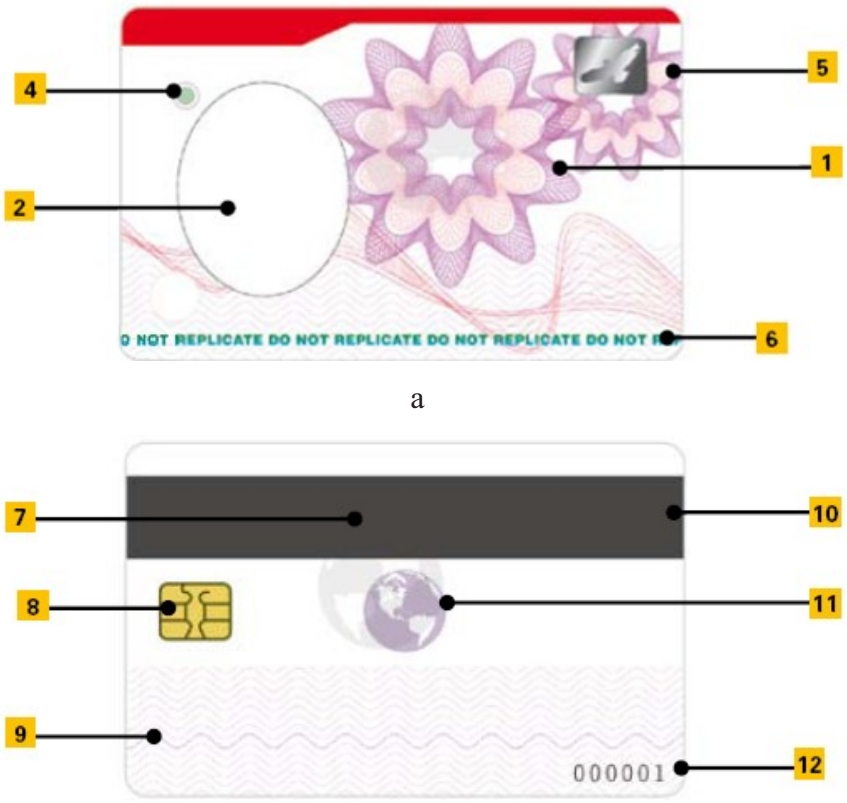
Бессонова Н.А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедры «Биомедицинские технические системы»

Научный руководитель: Спиридонов И.Н., д.т.н., профессор
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана МГТУ им. Н.Э. Баумана
bmt-1@bmstu.ru

В настоящее время идентификационные карты находят всё большее применение в самых различных сферах деятельности человека [2]. Всё чаще их можно увидеть выполненными в виде студенческого билета, удостоверения личности, прав на управление транспортным средством, пропуска на охраняемые объекты. Они успешно заменили устаревшие системы контроля, с их помощью стало возможным полностью автоматизировать систему учёта, допуска и проверки среди организаций разных сфер деятельности и величины, а время на идентификацию сотрудников сокращается до минимума. Идентификационная карта обладает рядом преимуществ перед обычным удостоверением, но их главным и бесспорным преимуществом являются значительные уровни защиты не только от подделки, но и от несанкционированного доступа к личной информации о владельце. Однако лица, заинтересованные в создании фальшивых идентификационных документов, стремятся не отстать от развития отрасли. Данная статья преследует цель объяснить, как сократить риски подделки, используя надежные системы печати защищенных идентификационных карт и новые технологии, способные обеспечить надлежащую защиту от подделок.

Учитывая рекомендации Американской ассоциации владельцев транспортных средств (AABTC), выделяют 3 уровня защиты карт. Первый – это открытые элементы защиты, видимые невооруженным глазом, их легко определить, но при этом очень сложно подделать.

Среди них выделяют технологию Гильоша (рис.1(1), рис.3(4)) – это сложный многоцветный рисунок из множества многократно пересекающихся тончайших кружевных линий, создаваемый благодаря применению математического алгоритма.



а

б

Рис. 1. Элементы защиты пластиковых карт (а – лицевая сторона; б – оборотная сторона)

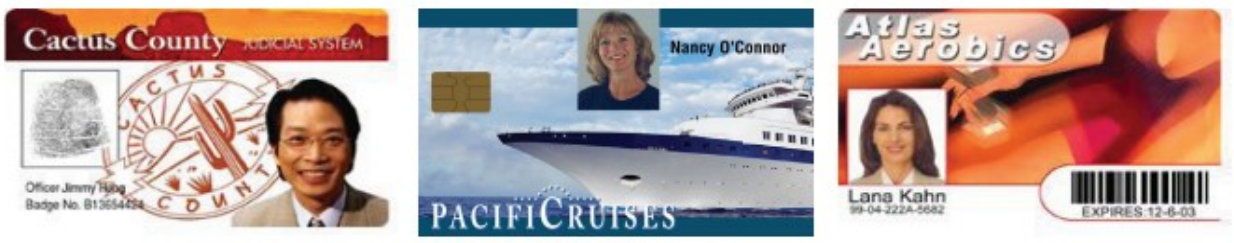
Гильош невозможно в точности воспроизвести при помощи сканера: микроскопическая толщина (от 40 до 70 мкм) и постоянно меняющаяся кривизна каждой линии создают непреодолимые препятствия перед рисующим блоком с недостаточной для выполнения подобных операций разрешающей способностью. Для сканирования сложны даже монохромные гильоши, так как они содержат повторяющиеся периодические элементы, требующие огромной памяти ПК. Повторить гильош, полученный методом орловской печати, когда добавляется еще плавно и произвольно меняющийся цвет каждой линии, невозможно другими способами. Поддельная линия получится либо непрерывной, но монохромной, либо меняющей цвет, но прерывистой, состоящей из растровых точек [4].

В качестве основы для гильоша выступает любая геометрическая фигура, образующая систему координат. Затем задаются две огибающие кривые и после этого задаются функции на заполнение пространства между огибающими. При добавлении сверхтонких линий гильош усложняется (рис.3(4)).

Сейчас гильоширные элементы моделируются специальными компьютерными программами. К ним относятся: Cerber, Гравер, SecuriDesign. Однако программу для

рисования гильошей может приобрести как оригинальный производитель, так и пират, а некоторые ПО находятся в свободном доступе в интернете. Поэтому используют и иные средства защиты.

Одно из них – это фотография держателя карты, которая является обязательным элементом для идентификационных карт (рис.2). Это один из самых простых, но при этом самых эффективных способов защиты документа. Очевидно, что воспользоваться чужой картой может только человек очень похожий на владельца карты. В паспорте, где фотография вклеивается поверх страницы, есть возможность замены фото. Применяемый метод цифровой печати изображений на карте исключают возможность замены изображения, так как вся информация передается с компьютера и печать текста, графики и фотографий осуществляется непосредственно на карте, изображение не выступает над ее поверхностью и защищается лакирующим или ламинирующим покрытием. Современные способы печати дают изображения высокого качества, а требования к фотографиям схожи с теми, что применяются при оформлении паспорта или визы. Как уже говорилось, карты имеют достаточно продолжительный срок службы, но в силу использования фотографии владельца встает вопрос о пересмотре периода, в течение которого по карте можно точно идентифицировать человека. Внешность человека может меняться ввиду различных причин: травм, процессов старения, пластических операций и смены имиджа (цвета волос, прически). Все это может затруднить процесс идентификации. В случае с шенгенской визой, фотография должна быть сделана не ранее 6 месяцев до подачи документов. [1, 2].



Цифровая карта-пропуск с фотографией, голограммой и отпечатком пальца

Цифровая карта-пропуск и дебетовая карта с фотографией и микросхемой

Цифровая клубная карта с фотографией, номером члена клуба и штрих кодом

Рис. 2. Примеры пластиковых карт с фото владельца

Существует целый класс элементов защиты, которые хранят в себе закодированную информацию о владельце. К примеру, магнитная полоска (рис.1(10)) – является самым распространенным способом кодирования информации на пластиковых картах. При помощи специальных устройств, таких как кодировщик магнитной полосы и ридер магнитной полосы, на магнитную полосу записывают информацию и затем

считывают ее. Магнитная полоса содержит три дорожки. На первой записывают ФИО и другие личные данные владельца карты, на второй ее номер и срок действия, а третья используется для записи дополнительной информации. В большинстве случаев для записи используется вторая дорожка. Стоит отметить, что сейчас производят карты с магнитными полосками HiCo (высокий уровень коэрцитивности) и LoCo (низкий уровень коэрцитивности). Коэрцетивность – это уровень магнитного поля, при котором может быть оказано воздействие на данные, закодированные на магнитной полоске. Она показывает, насколько сложно закодировать информацию на магнитной полоске. Магнитные полоски HiCo обеспечивают самый высокий уровень защиты данных на магнитной полоске от внешних магнитных полей и используются для идентификационных карт.

Среди наиболее дешевых способов персонализации выделяют нумерацию идентификационных карт (рис.1(12)). Различают систематический и серийный номер карты. Систематический номер карточки вносится и в память карточки (если это карточка с микросхемой), и печатается или эмбоссируется при персонализации карточки. Систематический номер служит для внешнего отличия одной карточки от другой. Он вводится для удобства держателей карточек и с целью документального учета карточек у эмитента. Использование базы данных для идентификации и учета карт значительно повышает надежность данной системы. Сотрудник службы охраны сравнивает данные, имеющиеся на карте, с теми, что хранятся в базе данных.

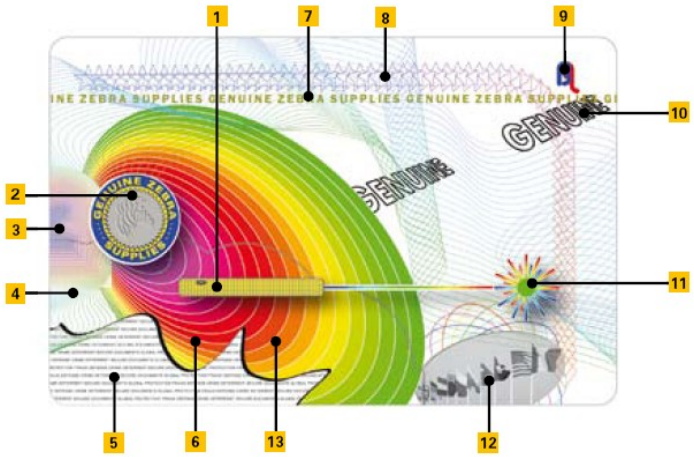


Рис. 3. Элементы защиты пластиковых карт

Защитные ламинирующие пленки с использованием голограмм являются очень распространенным способом защиты карт от подделки. Здесь выделяют множество различных техник. К примеру, изображения, созданные с помощью технологии Pixel-

Grafix, представлены набором пикселей или точек, которые подвергаются воздействию луча лазера под различными углами, что позволяет добиться максимальной яркости изображения даже при обычном освещении.

Существуют двухмерные голограммы (рис. 1(5)), которые созданы путем записи на фотографической пластине или пленке образца наложения, созданного с применением разделенного лазерного луча. Такие голограммы выполнены в нескольких цветах и накладываются в один слой без визуального ощущения глубины изображения. Также применяются двух/трехмерные голограммы (рис. 3(2)), которые представлены несколькими слоями двухмерных изображений, при этом изображения голограммы визуально располагаются одно за другим – в результате создается визуальное ощущение глубины или трехмерной голографической структуры.

Также используют технологию смещения изображения (рис. 3(8)). Она предусматривает смещение вида двух разных изображений по мере вращения объекта слева направо. Смещение вида изображения происходит равномерно с первого изображения на второе. Аналогичны смещению изображений двухканальные изображения (рис. 3(9)) и вертикальный или горизонтальный наклон голограммы (рис. 3(10), рис. 3(6)). Первая технология подразумевает быстрый переход от одного изображения к другому в результате вращения голограммы слева направо, а вторая – появление на изображении цветных полос по вертикали или горизонтали. Наряду с вышеупомянутыми способами существует линейный кинетический эффект (рис. 3(13)), когда голографическое изображение может быть видно только под определенным углом. Также внутри микроструктуры голограммы может быть скрыто изображение (рис. 3(1)), видимое только при попадании на него лазерного луча, что позволяет установить подлинность голографического изображения.

Две аналогичные технологии – это псевдоцвет и изображение в серых тонах. Псевдоцвет (рис. 3(11)) позволяет видеть само изображение в любом положении, но естественный цвет достигается только при наклоне голограммы под определенным углом. Техника создания голограммы с помощью изображений в серых тонах (рис. 3(12)) позволяет представить изображение в серых тонах в отличие от традиционных естественных цветов.

Рис. 4. Элементы защиты

Сейчас очень распространены контактные карты (рис. 1(8)), которые взаимодействуют с ридером при непосредственном прикосновении металлической контактной площадки карты и считывающей головки устройства. Этот метод является самым простым, поэтому контактные карты и ридеры имеют небольшую цену. Но за это приходится платить потертостью контактов и, как следствие, постепенным износом карты или ридера при частом использовании. Как правило, износостойкость карты и ридера исчисляется несколькими сотнями тысяч срабатываний.

Контактная карта состоит из контактной области (6 или 8 контактов квадратной или овальной формы) (рис. 5(1)), микропроцессора (рис. 5(2)) и пластиковой основы (рис. 5(3)) и не содержит батареек, энергия поддерживается ридером.

Рис. 5. Устройство контактной смарт-карты

Когда карта вставляется в ридер, чип соприкасается с электрическими коннекторами и ридер может считать или записать информацию с чипа. Форма карты, контактов, их расположение и назначение регламентируются в стандартах ISO/IEC 7816 и ISO/IEC 7810. Стандарт ISO/IEC 7816 регламентирует также протоколы обмена и некоторые аспекты работы с данными.

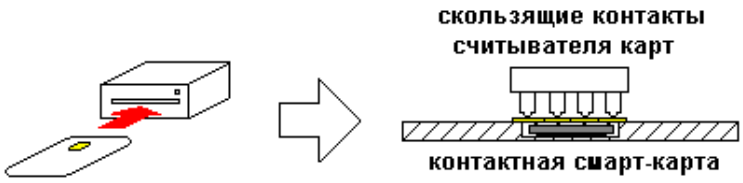


Рис. 6. Принцип действия контактной смарт-карты

Также на идентификационных картах можно выделить элементы безопасности второго уровня, которые поддаются проверке при помощи несложных процедур с использованием таких средств, как увеличительное стекло или источник ультрафиолетового света.

К примеру, при тщательном рассмотрении пластиковых карт можно заметить микротекст, который представляется человеческому глазу в виде тонкой линии (рис. 1(9), рис. 3(3), рис. 7). Этот элемент защиты доступен для прочтения с использованием 8 или 10-кратного увеличения. В качестве дополнительной меры защиты используется печать микротекста с использованием разных шрифтов и даже слов с ошибками. Обычная высота шрифта микротекстом – до 250 мкм.

Рис. 7. Микротекст

Но не так давно эта технология была усовершенствована, и на пластиковых картах все чаще появляется нанотекст, который относится уже к третьему уровню защиты (рис. 3(5)). В отличие от микротекста для прочтения такого текста необходимо использовать микроскоп. Довольно часто данный элемент защиты используется совместно с голографической печатью. С разрешением приблизительно 100 нанометров, стало возможным печатать более 20 голографических символов на пространстве шириной в человеческий волос (около 80 микрон). Очевидно, что повторить текст микро- и наноразмера невозможно на устройстве с недостаточной разрешающей способностью.

Также повышают уровень защиты карты элементы, видимые в определенном источнике света. Часто используются непрозрачные метки (рис. 1(7), рис. 8), которые распечатываются во внутреннем слое карты. Это изображение видно только при применении направленного источника света. Но наиболее распространенными остаются изображения, наносимые инфракрасными чернилами (рис. 1(4), рис. 4(1)) или чернилами, реагирующими на ультрафиолет (рис. 1(11), рис. 4(3)). Используются многоцветные элементы, светящиеся в УФ свете, которые наносятся на внутреннюю поверхность ламинирующей пленки. Принцип действия для инфракрасных чернил очень похож, но в отличие от УФ чернил, инфракрасные бесцветны и реагируют только при воздействии пучка лазерного излучения заданной частоты. Также используют изменяющие цвет чернила (рис. 1(6), рис. 3(7)), что обеспечивает высокую защиту карты, показывая распечатанный текст или изображение в разных цветах в зависимости от угла наклона. Использование изменяющих цвет чернил на темном фоне создает более глубокий цветовой эффект.

Рис. 8. Непрозрачные метки

Но порой и перечисленных элементов защиты бывает не достаточно, тогда используют глубоко скрытые или микроскопические элементы. Элементы третьего уровня включают изображения или объекты, скрытые в структуре самой карты или нанесенные на поверхности карты с применением специальных средств. Как правило, такие элементы можно проверить только в случае использования специальных оптических сканеров или иных средств считывания данных.

Среди них можно отметить одну из новинок в сфере контроля и управления доступом – бесконтактные smart-карты. Внутрь такой карты встраивают микропроцессорную микросхему, данные с которой считываются при помощи радиосигнала без физического контакта карты с ридером. Данная технология пришла на смену Proximity технологии и отличительной чертой smart-карт стала возможность не

только чтения информации с микросхемы карты, но и хранения и перезаписи определенных ее частей.

Электронная схема бесконтактной карты включает в себя smart-чип и антенну. Антенна карточки представляет собой печатные проводники, а smart-чип объединяет приемник, передатчик и энергонезависимую память, хранящую коды доступа и дополнительную информацию (рис. 9). Идентификация объекта производится по цифровому коду, хранимому в памяти smart-чипа и излучаемому в диапазоне радиоволн. Наибольшее применение получили карты с диапазоном 13,56 МГц с малой дальностью действия 10–20 см, поэтому невозможно считывать информацию дистанционно. Стандарт ISO 14443 определяет антиколлизионный протокол передачи данных.

В карте может храниться биометрическая информация пользователя и информация, записанная в машиносчитываемой зоне (MRZ – Machine Readable Zone). Информация, находящаяся в машинописной зоне документа, после считывания ридером проверяется путем электронного сравнения с данными, хранящимися на бесконтактной интегральной схеме. Обмен данными между картой и ридером происходит по зашифрованному протоколу, а доступ к памяти возможен только при предъявлении секретных ключей. Система открытых ключей, рекомендованная ICAO, применяется повсеместно для сохранения конфиденциальности и целостности информации. Также в качестве меры безопасности может применяться базовый контроль доступа (Basic Access Control, BAC). BAC использует разновидность PIN-кода. Обмен информацией между бесконтактной картой и ридером инициирует ключ, записанный в машиносчитываемой зоне карты. Таким образом, дистанционно получить доступ к информации на бесконтактной карте невозможно.

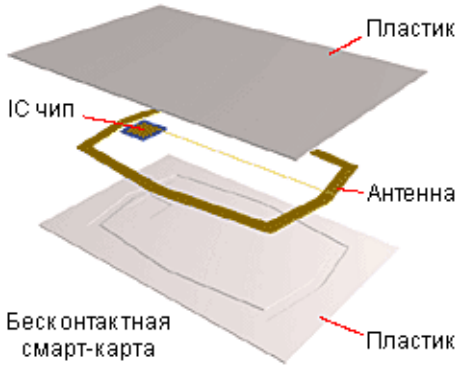


Рис. 9. Устройство smart-карты

Оценка элементов защиты идентификационных карт

	Стоимость	Уникальность	Уровень защиты	Возможность хранения личных данных (+/-)
Гильоширный элемент	+ + +	+	+ + +	-
Фото владельца	+	+ +	+ +	+
Магнитная полоса	+	+ + +	+	+
Нумерация	+	+ + +	+	-
Голограмма	+ +	+	+ +	-
Контактные карты	+ +	+ + +	+ + +	+
Микро- / нанотекст	+ +	+	+ +	-
Непрозрачные метки	+	+	+ +	-
ИК, УФ чернила, чернила, изменяющие цвет	+	+	+ +	-
Бесконтактные карты	+ + +	+ + +	+ + +	+

В сфере технологий обеспечения защиты идентификационных карт отмечается мощный прорыв: сегодня процесс производства идентификационных карт позволяет создавать карты с защитой от подделки, практически исключая возможность дублирования. Основываясь на приведенной выше таблице, а также учитывая технические и экономические факторы, государственные и коммерческие организации могут создавать уникальные уни- или мультимодальные системы защиты и выбирать необходимый уровень защиты. Однако стоит отметить, что даже в организациях с низким уровнем секретности не используются унимодальные системы защиты. Обычно идентификационная карта представляет собой комбинацию элементов всех трех уровней защиты. Это объясняется двумя причинами. Во-первых, чем больше в идентификационной карте реализовано элементов защиты, тем сложнее подделать такую карту. Во-вторых, уникальные элементы защиты, известные только службе безопасности данной организации, облегчают процесс проверки и подтверждения подлинности карт.

Список литературы

1. Идентификационные карты с высоким уровнем защиты, zebra technologies, 2009. 11 с.
2. Обеспечение безопасности процесса печати идентификационных карт, zebra technologies, обзорный доклад, 2010. 4 с.

3. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. - М.: Горячая линия-Телеком, 2010. 272 с.
4. Григорян М. Гильош – защитная сетка //giljosh.cn: сайт Гильош. URL. http://giljosh.cn/articles.php?lng=ru&pg=10 (дата обращения:12.10.2012).