ПРОГРАММНО-АПАРАТНЫЙ АСПЕКТ ПРИ ЧИПИРОВАНИИ ЧЕЛОВЕКА

А.С. Бондаренко, *магистрант*
П.К. Ярыгин, *магистрант*
М.А. Турилов, *магистрант*
Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ) (Россия, г. Москва)

DOI: 10.24411/2500-1000-2019-11338

Аннотация. *В данной статье приводится описание существующей на данный момент ситуации с ростом уровня технологий чипирования человека, в том числе в разрезе нормативно-правового аспекта. Описывается принцип действия и особенности внедрения микрочипа под кожу человека. Также в статье проводится обзор, оценка и анализ аппаратной организации и программного обеспечения биочипа, используемых на данный момент.*

Ключевые слова: *чипирование, биочип, технология RFID, программная память, файловая система.*

На данный момент изучение средств и методов идентификации человека при помощи биочипа – это относительно новая сфера жизни человека, которая недостаточно хорошо исследована, как многие другие области нашей жизни, которые уже стали ее неотъемлемой частью. Процесс чипирования человека только набирает свою популярность среди специалистов разного рода (в том числе специалистов по информационной безопасности) и пока что не исследуется повсеместно, поэтому рассматриваемая тема имеет научную новизну.

Главы государств и правительств «Большой восьмерки» 22 июля 2000 года приняли «Окинавскую хартию глобального информационного общества» [1], в которой отмечено, что информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества в XXI веке. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Реализация информационного общества невозможна без внедрения электронного правительства.

В 2005 году «Тунисской программой для информационного общества» провозглашались цели электронного правительства в доступе к государственной информации и службам для получения государственных услуг с помощью информационно-коммуникативных технологий [2].

Основной целью формирования и развития информационного общества в Российской Федерации является повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие социально-политической, экономической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий.

27 июля 2010 года был принят Федеральный закон №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [3], который определил основы внедрения универсальной электронной карты (УЭК) – одновременно удостоверения личности, полиса обязательного медицинского страхования, страхового свидетельства пенсионного фонда, банковской карты, проездного билета. Так как УЭК не является обязательным документом, её идентификационные возможности в масштабах всей Российской Федерации весьма ограничены [4].

Данные обстоятельства, вероятно, предопределили следующий шаг – утверждение Распоряжением Правительства РФ от 19 сентября 2013 года №1699 Концепции введения в Российской Федерации удосто-

верения личности гражданина Российской Федерации, оформляемого в виде пластиковой карты с электронным носителем информации, в качестве основного документа, удостоверяющего личность гражданина Российской Федерации на территории Российской Федерации [5].

Заданное направление свидетельствует о возможной интеграции электронного документа, удостоверяющего личность, с телом человека, наиболее вероятной реализацией которой являются устройства радиочастотной идентификации.

Описание технологии RFID

В основу RFID-технологий закладывается способ записи информации о товаре на специальных транспондерах или RFID-метках, а также считывания этой информации на определенном расстоянии с помощью радиосигнала.

Метки с технологией RFID постоянно используются в повседневной жизни – они спрятаны в проездных билетах, банковских картах, наклейках на товарах в магазине, пропусках безопасности, биометрических паспортах [6] и в том числе в смартфонах с использованием платежных систем финансовых технологий (Fintech), таких как Apple и Google Pay. Их используют как замену ключам и паролям, чтобы входить в дома, открывать и заводить машины, входить в операционную систему ноутбука. NFC-метки можно использовать, помимо прочего, для хранения, например, адресов биткоин-кошельков. В Швеции компания Biohax стала партнёром железнодорожных компаний и её чипы можно использовать для хранения информации о билетах.

Также RFID-метки находят применение в розничной торговле как инструмент оптимизации технологических решений и затрат. Позже эти технологии стали использовать в микрочипах, вживляемых ныне под кожу человека. Эти микрочипы-импланты представляют собой маленькие цилиндры габаритами 2x12 мм из несодержащего свинца боросиликатного стекла, либо биологически нейтрального стекла Schott 8625 на основе натриевой извести, внутри которого расположена пассивная радиочастотная метка, которая может читаться/записываться большинством существующих систем, работающих на частоте 13,56МГц по стандарту ISO14443.

RFID-метка состоит из двух частей: первая – интегральная микросхема для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала и некоторых других функций, вторая – антенна для приёма и передачи сигнала [7]. В микрочип встроить элемент питания на данный момент невозможно. Поэтому применяются технологии беспроводной связи RFID и NFC (как в модуле для бесконтактной оплаты в банковской карте). По этой же причине в них нельзя встроить GPS. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования кремниевого КМОП-чипа, размещённого в метке, и передачи ответного сигнала. Они считаются «пассивными», потому что они сами не могут прочитать информацию, а могут только передавать ее в считыватель. И это тоже плюс – RFID-метки не смогут прийти в негодность от разряда батареи.

В импланте содержится уникальный идентификационный код и при необходимости он может быть связан с внешней базой данных, в которой содержится информация о личных данных человека. Несмотря на то, что чипы стеклянные, вероятность их разрушения внутри тела маловероятна. Внедрение чипа-импланта занимает всего несколько секунд (микрочип вводится с помощью специального шприца между большим и указательным пальцами) и не влечет за собой какого-либо дискомфорта.

Все импланты часто относят к RFID, но под этим термином скрывается широкий спектр частот, устройств, протоколов и интерфейсов. Их разделяются на три частотных группы: низкочастотную (125 и 134 кГц), высокочастотную (13,56 МГц) и сверхвысокочастотную (UHF) (800-915 МГц). Чипы RFID и NFC близкие друг к другу технически, обычно они относятся к первой или второй группе. NFC является более сложной формой технологии по сравнению с RFID – NFC-чипы относятся

к чипам высокочастотного RFID-стандарта и имеют ряд особенностей:

– работает на фиксированной частоте: 13,56 МГц;

– способна на двустороннюю связь, поэтому возможности шире;

– дальность считывания не превышает 5 см (у RFID – до 300 м);

– только одна NFC метка может быть просканирована в одно время.

При использовании в чипах-имплантах у каждой технологии есть свои плюсы и минусы. Так, в устройство с NFC можно «поместить» больше функций, в том числе бесконтактную оплату, передачу медицинских или личных данных. Поэтому большинство производителей предлагают право выбора между обоими видами чипов, а покупатель может выбрать, исходя из своих нужд.

Чтобы внести информацию на чип, программируются сами RFID-считывали, чтобы они могли давать доступ на доступ конкретным чипам, а не наоборот, когда ключи записываются на RFID-метки. Если нужно запретить вход определенному микрочипу, то просто из базы данных разрешенного доступа удаляется серийный номер его метки. Так, например, медицинские чипы не содержат медицинских карт, а только коды, которые содержат данные о медицинской информации человека, в том числе информацию об аллергии и предшествующем лечении. Технологии стандартов и приложений в этой области развиваются стремительно, поэтому имплантированный микрочип не может «устареть». Для чипов xNT период сохранения данных составляет 10 лет, а количество циклов записи – 100000.

Аппаратная организация биочипа

В основе аппаратной организации биочипа лежит шинная архитектура вычислительной системы, широко распространённая в вычислительной технике. Основные компоненты интегральной микросхемы – это микропроцессор, схемы памяти, схемы ввода-вывода, схемы синхронизации, схемы защиты, схемы инициализации (стартовые цепи) и внутренняя шина (электрическая магистраль) (рисунок 1).

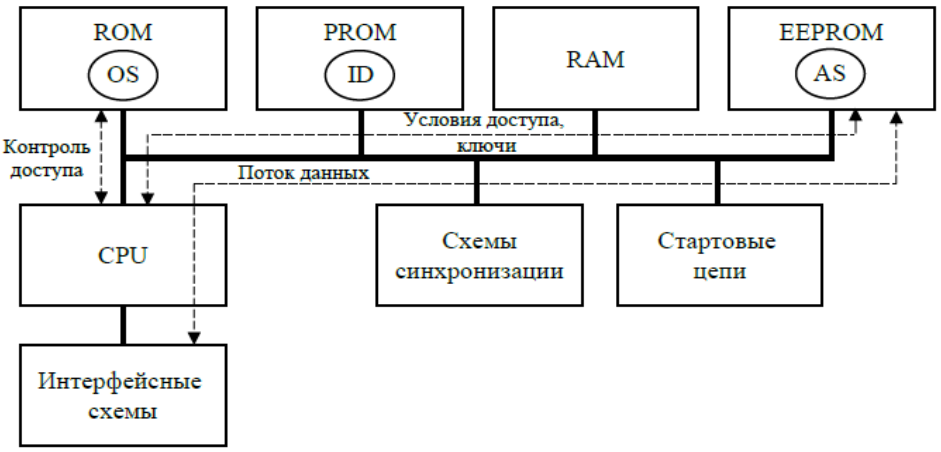

Рис 1. Аппаратная организация и программное обеспечение биочипа

Микропроцессор способен исполнять набор команд, записанных производителем в постоянную память (ROM) и набор команд операционной системы. Предопределённый набор команд выполняется всегда и обеспечивает вступление чипа в контакт с внешним устройством и подготовку его электрических цепей к передаче данных. Более высокоуровневые команды операционной системы, как правило, также реализованы аппаратно в ROM чипа, чтобы достичь более высокого быстродействия при ограниченных аппаратных возможностях чипа.

Биочипы, вживляемые под кожу человеку, имеют следующие виды памяти:

а) Постоянная память (ROM – Read-Only Memory). В ней хранится операционная система (ядро ОС и команды ОС), последовательность операций инициализа-

ции чипа, выполняемых в начале каждого сеанса связи с внешним устройством. Запись этих данных выполняется предприятием-изготовителем.

б) Программируемая постоянная память (PROM реализованный – Programming radio Read-Only Memory). Информация в эту память может быть записана в любой момент времени, но только однажды. В последующем информация может только считываться. Физически PROM представляет собой матричный набор логических вентилей (так называемое масочное ПЗУ). В PROM записываются идентификационные данные о владельце чипа, прикладных программах, эмитенте (в случае использования чипа в качестве персонализированного платёжного инструмента в автоматизированных банковских системах, которые в ряде случаев называют электронными платёжными системами), ставится подпись центра авторизации и т.п. Запись производится центром авторизации на специальном оборудовании, как правило, встроенном в ридер.

в) Программируемая постоянная память со стиранием (EPROM – Erasable Programming Read-Only Memory) отличается от предыдущего типа памяти тем, что позволяет стирать ранее записанную информацию. Однако процесс стирания является очень сложным и дорогостоящим. Поэтому данный тип памяти в настоящее время используется очень редко.

г) Электрически перепрограммируемая постоянная память (EEPROM – Electrically Erasable Programming Read-Only Memory) – обязательно присутствует в любой модели чипов. Преимущество состоит в том, что стирание и запись информации в логические ячейки выполняются электрическими импульсами, кроме того, такие микросхемы памяти достаточно дёшевы. Наличие микропроцессора позволяет организовать не только управление памятью, но и защиту некоторых областей памяти. EEPROM делится на системную область и область прикладных программ. Системная область доступна для чтения/записи только операционной системе чипа. В ней хранятся ключи доступа к файлам, отметки времени, вырабатываемые при совершении транзакций, счётчик транзакций, некоторая другая информация, доступ к которой прикладным программам должен быть закрыт. Область прикладных программ содержит файловую систему чипа: таблицу определения файлов и файлы, хранящие коды и данные прикладных программ. Доступ к этой области возможен не только операционной системе, но и прикладным программам. Поскольку эта область не имеет аппаратной защиты от чтения/записи, информация в ней должна обязательно храниться в зашифрованном виде, во избежание несанкционированного считывания злоумышленником.

Все перечисленные выше виды памяти могут хранить информацию не только в период активной работы чипа, но и при отключённом питании.

Сейчас EEPROM-память в интегральных микросхемах чипов всё чаще заменяется на FRAM-память (Ferrit Random Access Memory) - разновидность оперативной памяти на ферритовых логических элементах, которая позволяет хранить данные при отключённом источнике питания, а благодаря прогрессу технологии легко размещается в интегральной микросхеме [8].

д) Оперативная память (RAM – Random Access Memory) предназначена для временного хранения данных при выполнении микропроцессором чипа операций в ходе осуществления транзакции. При отключении питания вся хранящаяся в ней информация стирается.

Так как биочип имеет радиоинтерфейс, схемы ввода-вывода (интерфейсные схемы, I/O System) включают в себя антенну, выполняемую чаще всего в виде маленькой металлической катушки, и обеспечивают преобразование электрических импульсов в радиочастотный сигнал и обратно.

Схемы синхронизации используются для синхронизации внутренних цепей чипа и включают генератор тактовых импульсов, делители частоты, счётчик-таймер и др.

Начало сеанса связи между чипом и устройством доступа (ридером) инициру-

ется их стартовыми цепями. Когда чип попадает в поле действия ридера, схема инициализации ридера посылает сигнал по контакту RST аналогичной цепи чипа. Ответный сигнал чипа вырабатывает специальное сообщение для ридера о начале коммуникационного протокола. После этого все дальнейшие сообщения между чипом и ридером передаются в режиме шифрования. Эта процедура является обязательным начальным шагом процесса взаимной аутентификации чипа и ридера.

Необязательным, но часто используемым на практике элементом аппаратной части чипа является криптопроцессор, обладающий следующими возможностями и функциями:

– контроль доступа к данным прикладных программ через функции ОС;

– аппаратно реализованные алгоритмы шифрования и цифровой подписи;

– аппаратно реализованные функции для работы с идентификационной информацией.

Программное и информационное обеспечение чипа включает операционную систему чипа, прикладные программы (приложения) и идентификационную информацию.

Операционная система чипа (OS import – Operating операции System) – упрощённый аналог «настоящих» операционных систем. Представляет собой набор микрокодов, записанных в ROM, которые принято разделять на ядро OS и команды OS. Ядро OS – это набор микрокоманд, выполняемых при установлении сеанса связи с ридером, обеспечивающих работу с аппаратурой чипа и интерфейс с внешним устройством. Ядро OS является аналогом загрузочных программ обычной ОС. Команды OS – это специфицированный набор процедур, также, как правило, для повышения быстродействия реализованных аппаратно, предназначенный для работы с прикладными программами и данными, обеспечения механизма безопасности чипа. Выделяют следующие группы команд OS:

– команды работы с данными прикладных программ: создание и удаление файлов, чтение данных из файлов различных форматов: структурированных и бесструктурных, выбор директории (для иерархической файловой системы), позиционирование указателя, обновление записей в файлах различных типов, добавление записи к файлу;

– команды обеспечения безопасности – их часто выделяют в отдельную группу, называемую «системой безопасности» чипа (SF – Security Features). Это довольно большая группа команд, предназначенных для обеспечения безопасности данных, хранящихся и обрабатываемых чипом, защиты файлов, операций с ключевой и идентификационной информацией. В SF входят следующие команды: выработка случайного числа, аутентификация внешнего устройства, аутентификация чипа для внешнего устройства, загрузка файла ключей, закрытие файла, объявление файла недействительным и снятие этой блокировки, аутентификация пользователя, блокировка аутентификации пользователя, изменение условий доступа к файлам и др. Если чип поддерживает работу с асимметричными криптографическими алгоритмами, то к перечисленным

– командам добавляется группа команд для работы с открытыми ключами: внутренняя и внешняя аутентификация с открытым ключом, загрузка ключа, чтение ключа, вычисление хэш-функции, проверка ключа, проверка цифровой подписи;

– команды обслуживания чипа предназначены для выполнения вспомогательных операций, таких как форматирование файловой системы и др.;

– некоторые другие команды: чтение файла статистики транзакций, выбор коммуникационного протокола, изменение скорости обмена с внешним устройством и т.п.

Прикладное ПО (AS – Application Software) частично может быть записано в PROM-память, частично – в EEPROM. ПО чипа должно разрабатываться в связи с ПО устройств, осуществляющих работу с ним, работа всех компонентов ПО должна быть согласована между собой и с форматами файлов, хранящихся на чипе. Отдельное ПО необходимо записи на чип информа-

ции о владельце, эмитенте, порядкового номера, ключей, идентификаторов и т.п.

Программирование памяти чипов осуществляется с помощью специальных инструментальных пакетов, включающих транслятор текстов программ с языков высокого уровня и ассемблера в коды микропроцессора чипа, а также программный эмулятор микропроцессорной системы чипа для отладки и тестирования ПО.

Так же, как и понятие «операционная система», термин «файловая система» перенесён на чипы из области «полноценных» компьютерных систем. Для идентификационных микрочипов он обозначает способ логической организации хранения данных в перезаписываемой памяти (EEPROM) чипа и также является упрощённым, адаптированным аналогом «настоящих» файловых систем. В современных чипах применяются два основных способа организации файловой системы: зонная и иерархическая. Оба типа файловых систем изображены на рисунке 2.

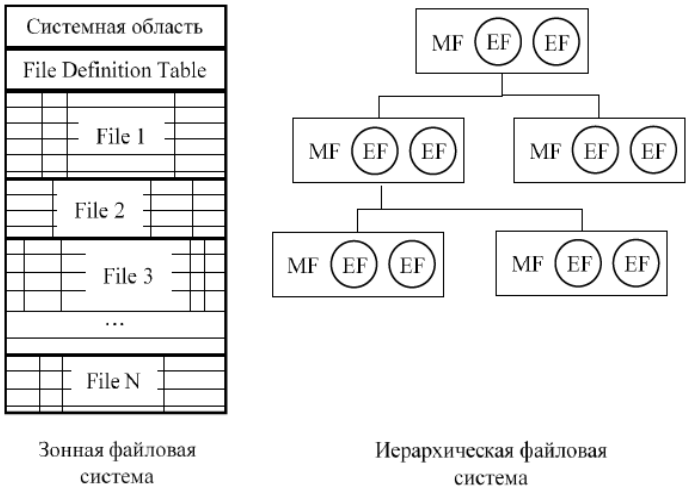

Рис. 2. Типы файловых систем чипов

Более простым является зонный способ организации файловой системы (или зонирование). В этом случае область прикладных программ EEPROM логически разбивается на зоны. В каждой зоне организуется структура данных в виде таблицы записей, называемой файлом. Для каждого из них определяется его формат (структура записей), зависящий от конкретного приложения. Каждый файл при зонной организации памяти представляет собой форматированную таблицу, состоящую из одинаковых записей. По младшим адресам области прикладных программ EEPROM формируется таблица определения файлов (FDT– File Definition Table) – аналог FAT (File Allocation Table) (рисунок 2). FDT – это также таблица, конкретный формат которой оговаривается стандартами ISO и спецификациями производителей, в которую записываются для каждого файла: адрес начала файла в памяти, метки защиты файла по чтению/записи, расширение метки защиты, длина записей файла, число записей, тип файла, имя файла, указатель текущей записи, указатель конца файла.

Более сложной и совершенной является иерархическая файловая система, имеющая древовидную логическую структуру (рисунок 2). Так же, как и зонная, иерархическая файловая система (ФС) состоит из FDT и файлов. Файлы иерархической ФС подразделяют на три типа:

– мастер-файл (MF – Master File) – помещается в корне ФС (аналог корневой директории жёсткого диска);

– файлы-ветви (DF – Dedicated Files) – содержат данные, атрибуты, и в ряде случаев, выполняемые программы (возможно, относящиеся к различным приложениям);

– элементарные файлы (EF – Elementary Files) – содержат текущие данные выполняемых программ и результаты транзак-

ций (также, возможно, относящиеся к различным приложениям).

Элементарные файлы, в общем случае, могут быть нескольких типов (рис. 3):

– линейный файл с фиксированной длиной записей;

– линейный файл с переменной длиной записей;

– линейный циклический файл с фиксированной длиной записей;

– «прозрачный» файл – бесструктурный файл, допускающий чтение/запись по указателю в произвольный адрес в пределах области, отведённой под файл;

– файлы команд приложений (ASC – Application Specific Command Files) – файлы, содержащие исполняемые коды прикладных программ, записанные в виде последовательности команд операционной системы. Смысл ASC-файлов в том, что они позволяют приложению создавать свои макрокоманды операционной системы, необходимые данному конкретному приложению, состоящие из последовательности команд OS, уже реализованных аппаратно, что позволяет достичь высокого быстродействия.

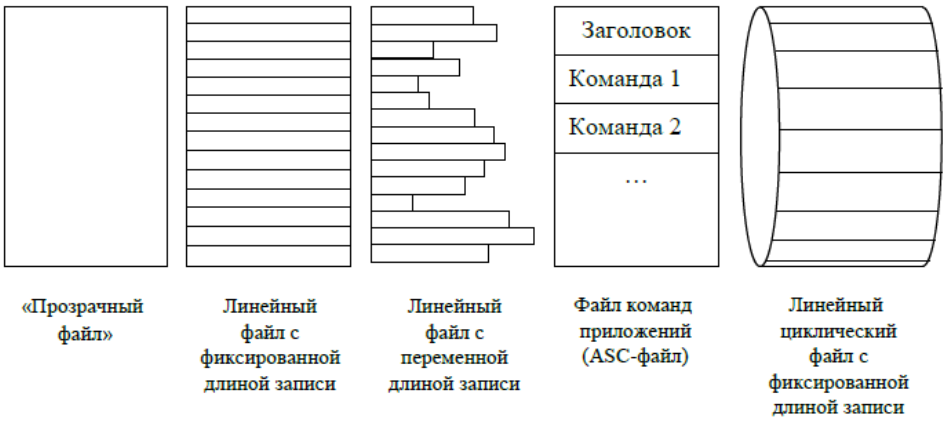

Рис. 3. Форматы файлов, используемые в чипах

Каждый файл иерархической ФС может иметь предопределённые условия доступа, оговаривающие перечень допустимых операций с ним, которые уже нельзя будет изменить в процессе эксплуатации чипа.

Таким образом, можно сказать, что биочип это во многом очень удобная технология, которая активно исследуется в последние несколько 20 лет и индустрия производства которой тоже шагнула сильно. На данный момент потенциал использования имплантируемых чипов ограничен и нынешние функции чипов (открытие дверей без ключей и пропусков, хранение паролей и т.д.) – это только первый шаг развития, в перспективе ожидается, что он может избавить от необходимости носить с собой различные документы, такие как паспорта, удостоверения личности, водительские права и т.д., о чем можно судить по направлениям, заданным в законодательных актах Российской Федерации.

Однако массовое внедрение микрочипов может привести к противоречиям с нравственными и религиозными ценностями людей и размыванию общепризнанных гражданских прав и свобод человека, а значит, чипизация потребует, как минимум, пересмотра широкого перечня национальных и международных правовых норм и актов [9]. Ключом к обеспечению того, чтобы разработки RFID использовались назначению, будет значимое и активное законодательство, разработанное для предотвращения возможных злоупотреблений на проходе.

Также, стоит сказать, что проведение массового чипирования людей хотя бы на государственном уровне довольно затратно (стоимости продажи и вживления чипов представлены ранее). Для массового внедрения микрочипов их цена, как считают эксперты, должна упасть в 10 раз, поэтому на сегодняшний день и используются более дешевые и простые аналоги идентифи-

кации личности (например, магнитные пропуска). Со временем, по мере развития технологии, цена на их производство должна упасть и тогда чипизация населения сможет принести экономическую выгоду для общества.

Выводы

В настоящее время нет точных данных о том, сколько людей имеют RFID-метки в организме, но согласно оценкам биохакинговой компании Dangerous Things, это число составляет от 60 тыс. до 90 тыс. людей по всему миру. Как видно, за 20 последних лет число людей с биочипом составляет всего лишь одну тысячную процента от населения планеты, но потенциал у этой технологии по-настоящему велик.

Эксперты считают, что биочип – это инструмент ближайшего будущего, в котором появятся функции, расширяющие возможности человека – функции, увеличивающие силу мышц, стабилизирующие артериальное давление, а, возможно, улучшающие и мыслительные способности человека. Со временем гражданское общество, скорее всего, трансформируется в электронное общество, в силу чего глобальная чипизация населения – лишь вопрос времени.

Но в то же время существует проблема в обеспечении защиты данных, хранящихся на микрочипе, так как многие современные технологии разрабатываются с весьма посредственной проработкой вопросов безопасности. А это является важнейшим пунктом при внедрении таких технологий в тело человека.

Библиографический список

1. *Президент России*. – Окинавская хартия Глобального информационного общества [Электронный ресурс]. – URL: http://www.kremlin.ru/supplement/3170/ (дата обращения 19.05.2019).

2. *Тунисская программа* для информационного общества [Электронный ресурс]. – URL: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1-ru.pdf (дата обращения 12.05.2019).

3. *Консультант Плюс*. – Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 г. №210-ФЗ [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_103023/ (дата обращения: 18.05.2019 г.).

4. *Консультант Плюс.* – Указ Президента Российской Федерации от 13.03.1997 г. №232 «Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации» [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_13631/ (дата обращения: 01.05.2019 г.).

5. *Консультант Плюс*. – Распоряжение Правительства Российской Федерации от 19.09.2013 г. №1699-р «Об утверждении Концепции введения в Российской Федерации удостоверения личности гражданина Российской Федерации, оформляемого в виде пластиковой карты с электронным носителем информации, и плана мероприятий по реализации Концепции» [Электронный ресурс]. – URL: http://www.consultant.ru/document/cons_doc_LAW_152151/ (дата обращения: 18.05.2019 г.).

6. *Виляева Е.Н.* Перспективные направления развития защитных признаков в паспортно-визовых документах и методы их проверки как способ обеспечения национальной безопасности / Е.Н. Виляева, Д.Н. Копылов, Ю.Н. Максимычев, В.В. Алтынников // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. – 2011. – С. 93–103.

7. *ГОСТ Р ИСО/МЭК 14443*-1-2013. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 1. Физические характеристики [Электронный ресурс]. – Введ. 2013-22-11. – М.: Стандартинформ. – 2013 – 73с. – URL: http://docs.cntd.ru/document/1200108020 (дата обращения: 15.05.2019 г.).

8. *Хабр. – Технология* FRAM [Электронный ресурс]. – URL: https://habr.com/post/390389/ (дата обращения 15.05.2019)

9. *Доклад Специального* докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом г-на Мартина Шейнина [Электронный

ресурс]. – URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/A.HRC.16.51_ru.pdf (дата обращения 03.05.2019).

HARDWARE AND SOFTFARE ASPECT WHEN CHIPPING A PERSON

A.S. Bondarenko, *graduate student*
P.K. Yarygin, *graduate student*
M.A. Turilov, *graduate student*
National research nuclear university "MEPhI" (NRNU MEPI)
(Russia, Moscow)

Abstract. *This article describes the current situation with the increasing level of human chipping technology, including in the context of the regulatory aspect. The principle of action and features of the introduction of a microchip under the human skin are described. The article also provides a review, assessment and analysis of the hardware organization and biochip software used at the moment.*

Keywords: *chipping, biochip, RFID technology, program memory, file system.*