DOI 10.37882/2223-2966.2024.06.34

РАЗРАБОТКА УНИВЕРСАЛЬНОГО ИДЕНТИФИКАТОРА TOUCH MEMORY ЭЛЕМЕНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ ПРОГРАММНОЙ РЕАЛИЗАЦИИ ВЕДОМОГО УСТРОЙСТВА ПРОТОКОЛА IBUTTON

DEVELOPMENT OF THE UNIVERSAL IDENTIFIER OF THE TOUCH MEMORY ELEMENT OF THE INFORMATION SECURITY SYSTEM USING THE LIBRARY OF THE SOFTWARE IMPLEMENTATION OF THE IBUTTON PROTOCOL SLAVE DEVICE

M. Romanov
E. Petrova
V. Butov
A. Apalkov
S. Parshin

Summary. The paper examines and analyzes contact identification systems based on the OneWire single-wire protocol (iButton) for possible vulnerabilities, the implementation of iButton key-identifier forgeries, as well as the prospects of using the OneWire interface in modern communication systems and information security systems. The developed experimental sample of the universal identifier device «Touch Memory», made on a programmable chip, makes it possible to fine-tune methods and algorithms for protection against unauthorized access by intruders. Despite all the advantages of systems built on iButton technology, they cannot provide absolute information protection. The proposed software implementation solutions developed in the course of this work can serve as material for improving the keys and algorithms of iButton devices. The solutions proposed in the work allow for two-stage identification with a given branching.

Keywords: information protection, access ID, data transfer.

Романов Михаил Сергеевич
кандидат технических наук, старший преподаватель, Воронежский институт МВД России
m.romanov90@mail.ru
Петрова Елена Владиленовна
кандидат технических наук, старший преподаватель, Краснодарский университет МВД России
petrovsemen1@mail.ru
Бутов Владимир Викторович
старший преподаватель, Ростовский юридический институт МВД России
vladimir_butov7@mail.ru
Апальков Александр Владимирович
старший преподаватель, Белгородский юридический институт МВД России имени И.Д. Путилина
aleksandr.apalkov@yandex.ru
Паршин Сергей Владимирович
старший преподаватель, Сибирский юридический институт МВД России
vechnosts@mail.ru

Аннотация. В работе рассматриваются и анализируются системы контактной идентификации, в основе которой лежит однопроводной протокол OneWire (iButton) на предмет возможных уязвимостей, реализации подделок iButton ключей-идентификаторов, а также перспективность использования интерфейса OneWire в современных системах связи и системах защиты информации. Разработанный экспериментальный образец устройства универсального идентификатора «Touch Memory», выполненный на программируемой микросхеме, дает возможность более тонкой настройки методов и алгоритмов защиты от несанкционированного доступа злоумышленников. Несмотря на все преимущества систем, построенных на технологии iButton, они не могут обеспечить абсолютную защиту информации. Предложенные решения программной реализации, разработанные в ходе данной работы, могут послужить материалом для усовершенствования ключей и алгоритмов работы iButton устройств. Предложенные в работе решения позволяют реализовать двухэтапную идентификацию с заданным ветвящимся алгоритмом, что снижает попытки злоумышленника на успех к минимуму. Разработанный макет образца (прототипа) устройства универсального идентификатора «Touch Memory» может иметь применение в служебной деятельности оперативных служб правоохранительных органов в роли универсального ключа для всех iButton устройств на территории проведения оперативных работ. Использование данного решения позволит избавится от многочисленного количества ключей и сложностей при их эксплуатации, достаточно будет иметь при себе один универсальный ключ.

Ключевые слова: защита информации, идентификатор доступа, передача данных.

Обеспечение защиты информации объектов включает в себя целый комплекс организационно-технических мероприятий, среди которых можно выделить контроль и управление доступом в помещения. Для решения этой задачи на объектах вводятся определенные правила функционирования объекта, пропускной режим, а также технические средства контроля и управления доступом: контроллеры, считыватели, устройства, преграждающие управляемые, устройства исполнительные, а также идентификаторы [3, 4]. Система контроля и управления доступом играет немаловажную роль среди систем безопасности и, как правило, устанавливается после охранно-пожарной сигнализации и системы видеонаблюдения [5].

Сегодня вопросы безопасности и систем контроля и управления доступом имеют особое значение при проектировании различных систем охраны и оповещения. От них в первую очередь зависит защищённость объектов и систем, имеющих важность для государства и общества от преступных и иных посягательств злоумышленников. Здесь стоит уделить особое внимание вопросам идентификации, от которых напрямую зависит безопасность систем и объектов [1, 2].

В настоящее время системы идентификации окружают нас всюду: пароли, системы считывания отпечатков пальцев, идентификация лица и сетчатки глаза, беспроводная и контактная идентификация. Сегодня они внедрены почти во все системы безопасности. К сожалению, развитие техники и электроники привели не только к созданию таких технически продуманных методов идентификации, но и их обходу и взлому. В связи с этим вопросы устранения уязвимостей систем идентификации имеют решающее значение в сфере безопасности.

Чаще всего реализацией устройств на основе интерфейса передачи данных iButton в системах безопасности является создание ключей идентификаторов так же известных под названием «Touch Memory» или «iButton». Они представляют из себя маленькие цилиндрические корпуса из нержавеющей стали внутрь которых помещен микрочип с набором предустановленных команд. Внешне такие устройства похожи на маленькие литиевые батарейки для часов или небольшие конденсаторы [6].

Рассмотрим структуру и последовательность отправки команд к устройствам (ключам) iButton. Обмен данными начинается с импульса reset от мастера, в свою очередь ведомое устройство отвечает ему импульсом присутствия. Далее мастер отправляет ведомому команду, прочитав которую ведомый отвечает мастеру теми или иными данными [7].

В настоящее время существует стандартный список команд для slave-устройств протокола iButton:

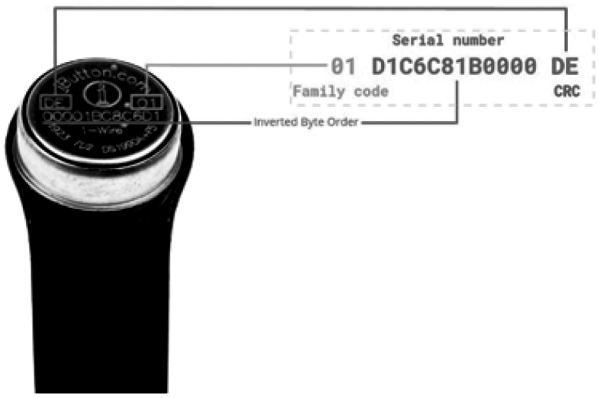

Рис. 1. Данные памяти ключа iButton

1. Команда 0x33 READ ROM (Чтение ПЗУ). Данная команда означает что master хочет получить от slave данные, записанные в его памяти (рис. 1). Применительно для ключей идентификаторов чаще всего это запрос на 64 байта памяти в которые входит код устройства, уникальный номер и байт контрольной суммы. Как альтернатива команде 0x33 может также использоваться команда 0x0F.
2. Команда 0xCC SKIP ROM (игнорирование адресации). Следующая команда говорит о том, что мы опускаем процедуру адресации к slave устройству.

Дело в том, что как говорилось ранее к интерфейсу iButton может быть подключено более чем одно ведомое устройство, таким образом необходимо осуществлять адресацию к тому устройству, от которого хотим получить данные. В случаях, когда мы знаем, что на линии лишь одно ведомое устройство мы можем пропустить этот этап.

3. Команда 0x55 MATCH ROM (Совпадение ПЗУ). Эта команда нужна для выбора конкретного устройства, чей код достоверно известен. После передачи байта 0x55 мастер передаёт полный 8-байтный код (включая код семейства, серийный номер и контрольную сумму) адресуемого устройства, младшими разрядами вперёд. Устройство, у которого зашитый в ПЗУ код соответствует переданному, переходит в активный режим, ожидая дальнейших команд.

На сегодняшний день в связи с многочисленными удачными попытками имитировать ключ iButton разработчики систем безопасности создали довольно много алгоритмов проверки подлинности. Рассмотрим основные из них:

1. При первом подключении iButton ключа к считывающему устройству master может не генерировать импульс reset, в большинстве современных систем первое подключение ведомого устройства означает, что ведомый должен сразу выдавать импульс присутствия (presanse);

2. Считывающее устройства могут посылать произвольные команды на iButton идентификаторы, при этом все поступающие команды должны игнорироваться ключом;
3. В качестве основных команд могут использоваться альтернативные.

Исходя из описанных методов проверки подлинности стоит отметить, что в системах, работающих на протоколе iButton бывают и заводские уязвимости, которые не сразу удается заметить.

Так, например в памяти нового считывателя как разрешенный идентификатор может быть запрограммирован ключ из одних единиц, или из одних нулей.

Таким образом при выборе систем стоит обращать внимание и на этот фактор, ведь он является в данном случае ключевым слабым местом.

Для более полного анализа и оценки протокола iButton был разработан макет универсального ключа Touch Memory. В ходе разработки ключа были поставлены цели по реализации создания устройства, соответствующего современным требованиям микро и радиоэлектроники, из них можно перечислить следующие:

1. Малый вес и габариты.
2. Автономность и бесперебойность.
3. Отсутствие элементов питания.
4. Возможность использования устройства в широком диапазоне температур.
5. Защита от неблагоприятных сред таких, как сырость, грязь.

За основу построения универсального ключа был взят микроконтроллер attiny 13 компании Microchip. Преимущество данного выбора заключается в возможности использования данного программируемого чипа на достаточно низких напряжениях и малых токах, соответственно тока утечки с iButton интерфейса вполне хватит чтобы микроконтроллер нормально функционировал.

Для обеспечения малого веса и габаритов ключ был изготовлен на smd компонентах. Проектирование универсального ключа происходило среде разработки Microchip Studio и САПР Altium designer. В среде Altium designerразрабатывалосьобщееустройствоплатыключа.

Первым этапом было создание принципиальной схемы устройства. Схема включает в себя минимальный набор радиоэлектронных компонентов необходимых для реализации протокола iButton его работы на паразитном токе, то есть питании от линии передачи данных. В устройстве были использованы следующие компоненты (рис. 2):

— микроконтроллер Attiny 13 (корпус — soic-8);
— диод Шотки 1n5817 (корпус — sma);
— конденсатор на 1мкФ (smd-1206);
— переключатель, осуществляющий переключение между идентификаторами.

Далее с помощью встроенных инструментов программы, по принципиальной схеме была создана печатная плата будущего ключа. В ходе разработки макет печатной платы устройства получился следующих габаритов: 25x20x1.

Инструментарий программы позволяет в ходе разработки печатной платы автоматически создавать 3D модель платы (рис. 3).

После разработки чертежей и моделей платы ключа был подобран исходя из габаритов платы будущий корпус, и воссоздан в среде 3D моделирования 3D Max (рис. 4, рис. 5).

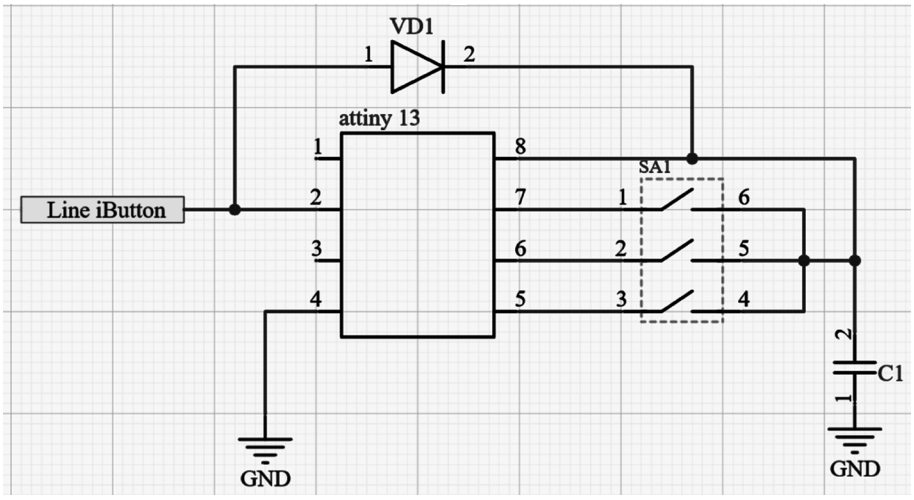

Рис. 2. Схема электрическая принципиальная образца (прототипа) устройства универсального идентификатора «Touch Memory»

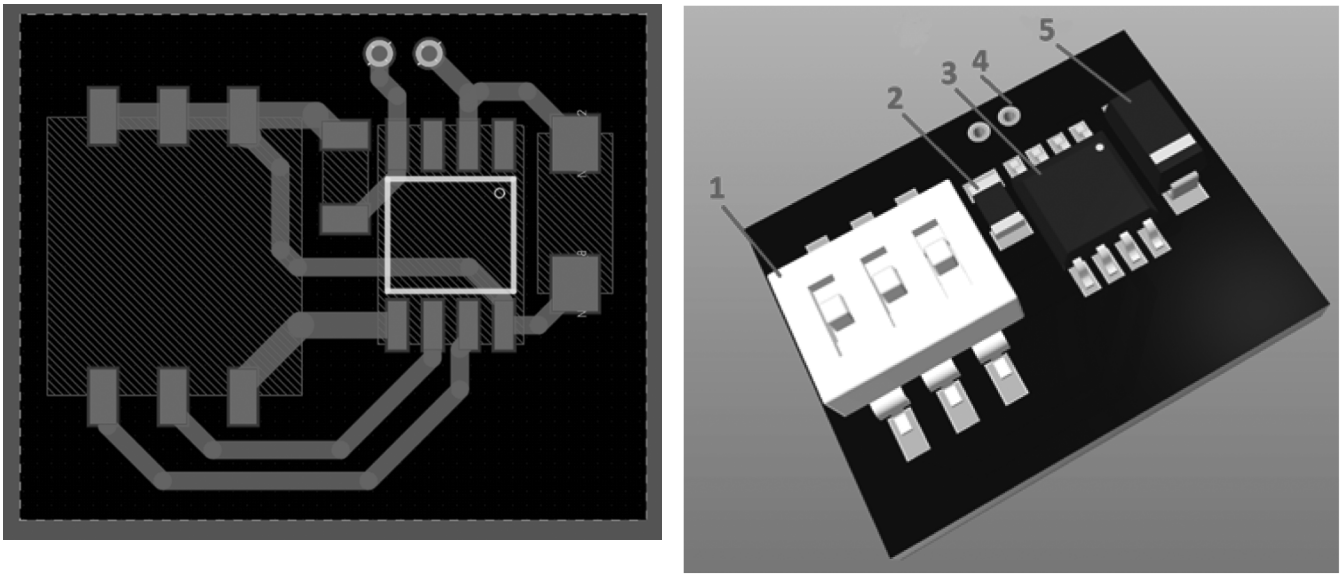

Рис. 3. Печатная плата и 3D модель
(1 — переключатель, 2 — конденсатор, 3 — микроконтроллер Attiny13, 4 — контакты для подключения контактной площадки ключа, 5 — диод 1n5817)

В последующем реальная плата была создана, и помещена в реальный корпус.

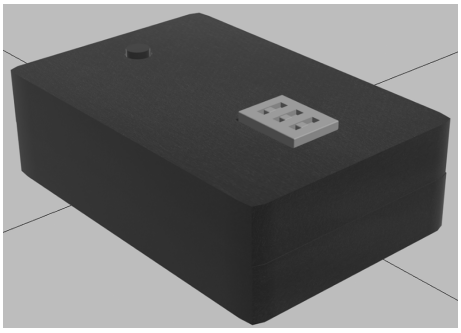

Рис. 4. 3D модель образца (прототипа) устройства универсального идентификатора «Touch Memory» в собранном виде

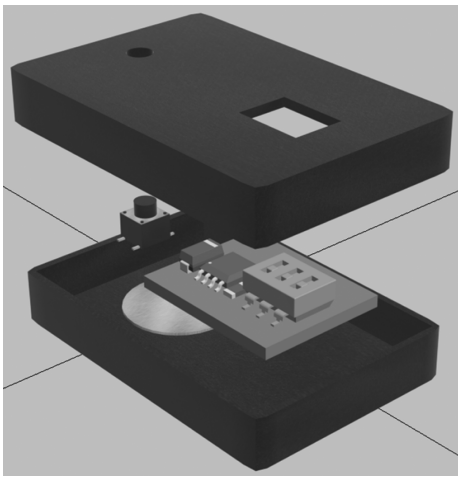

Рис. 5. 3D модель конструкции образца (прототипа) устройства универсального идентификатора «Touch Memory»

Разработанный в ходе работы образец (прототип) устройства универсального идентификатора «Touch Memory», выполненный на программируемой микросхеме, дает возможность более тонкой настройки методов и алгоритмов защиты от несанкционированного доступа злоумышленников. Несмотря на все преимущества систем, построенных на технологии iButton, они не могут обеспечить абсолютную защиту информации.

Разработанный макет образца (прототипа) устройства универсального идентификатора «Touch Memory» может иметь применение в служебной деятельности оперативных служб правоохранительных органов в роли универсального ключа для всех iButton устройств на территории проведения оперативных работ. Использование данного решения позволит избавится от многочисленного количества ключей и сложностей при их эксплуатации, достаточно будет иметь при себе один универсальный ключ.

Следующим этапом работы будет создание программного обеспечения микроконтроллера (среде Microchip studio на языке C). Выбор данного подхода можно объяснить достаточно высокой оптимизацией прошивок, написанных в данной среде, в частности на языке C, который в свою очередь хорошо деассемблируется до двоичного кода. Стоит заметить, что Microchip studio является официальной средой поддержки микроконтроллера, поэтому ошибки при сборке проекта сведены к минимуму.

ЛИТЕРАТУРА

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Постановление Правительства РФ от 10 июля 2019 г. N 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации».
3. ГОСТ 17021-88 Микросхемы интегральные. Термины и определения.
4. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
5. Кубасов И.А., Лекарь Л.А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России. 2023. №3 (67). URL: https://cyberleninka.ru/article/n/vnedrenie-perspektivnyh-sistem-monitoringa-i-analiza-bolshih-dannyh-poluchennyh-v-seti-internet-dlya-obespecheniya-deyatelnosti (дата обращения: 21.04.2024).
6. Романов М.С. Выбор критериев оптимальности принятия решений ОВД // Охрана, безопасность, связь — 2014: материалы международной научно-практической конференции. Воронеж: Воронежский институт МВД России, 2015. С. 153–154.
7. Сагидова М.Л. Современные системы контроля и управления доступом // Международный журнал гуманитарных и естественных наук. 2022. №9-1. URL: https://cyberleninka.ru/article/n/sovremennye-sistemy-kontrolya-i-upravleniya-dostupom (дата обращения: 21.04.2024).
8. Шуругин С.В., Матвеев А.У., Грицкевич Е.В. Разработка и анализ концептуальной модели биометрической информации с точки зрения действующей нормативно-правовой базы // Интерэкспо Гео-Сибирь. 2021. №. URL: https://cyberleninka.ru/article/n/razrabotka-i-analiz-kontseptualnoy-modeli-biometricheskoy-informatsii-s-tochki-zreniya-deystvuyuschey-normativno-pravovoy-bazy (дата обращения: 21.04.2024).

Журнал «Современная наука: актуальные проблемы теории и практики»