УДК 004.056.53

АРХИТЕКТУРА ТЕХНИЧЕСКОЙ ЗАЩИТЫ И ВЫБОР ДОВЕРЕННОЙ ЭЛЕМЕНТНОЙ БАЗЫ ДЛЯ ИЗМЕРИТЕЛЬНЫХ IoT-СИСТЕМ

П.К. Маевский

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается актуальная проблема технической защиты измерительных устройств Интернета вещей (IoT) на аппаратном уровне. Обосновывается необходимость внедрения концепции доверенной среды на этапе проектирования, что особенно критично при выводе новых продуктов на рынок. Предложен подход к выбору микроконтроллеров с аппаратной поддержкой криптографических стандартов Республики Беларусь (СТБ 34.101.31) для обеспечения целостности и конфиденциальности передаваемых данных.

Ключевые слова: техническая защита информации; измерительные системы; доверенная среда; аппаратное шифрование; микроконтроллеры; интернет вещей; криптографические алгоритмы; СТБ 34.101.31; сертификация; кибербезопасность.

ARCHITECTURE OF TECHNICAL PROTECTION AND SELECTION OF TRUSTED ELEMENT BASE FOR MEASURING IoT-SYSTEMS

P.K. Mayeuski

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article deals with the urgent problem of technical protection of Internet of Things (IoT) measuring devices at the hardware level. The necessity of implementing the trusted environment concept at the design stage is justified, which is especially critical

when launching new products. An approach to selecting microcontrollers with hardware support for cryptographic standards of the Republic of Belarus (STB 34.101.31) to ensure the integrity and confidentiality of transmitted data is proposed.
Keywords: technical information protection; measuring systems; trusted environment; hardware encryption; microcontrollers; internet of things; cryptographic algorithms; STB 34.101.31; certification; cybersecurity.

Введение

Стремительный рост количества подключенных устройств Интернета вещей (IoT), включая промышленные и бытовые измерительные приборы, формирует новые вызовы в области технической защиты информации. Датчики телеметрии, умные счетчики и различные трекеры все чаще становятся объектами кибератак, направленных на подмену данных или перехват управления. Разработка аппаратных измерительных устройств, в том числе в рамках подготовки бизнес-плана для вывода на рынок новых технологических стартапов, требует закладки архитектуры безопасности еще на этапе базового проектирования. Отсутствие такого подхода делает невозможным прохождение экспертизы в соответствии с требованиями Оперативно-аналитического центра при Президенте Республики Беларусь и внедрение приборов на критически важных объектах. Целью данной работы является формирование концепции выбора доверенной элементной базы для измерительных систем.

Основная часть

Современные портативные измерительные приборы обладают ограниченными вычислительными ресурсами и жесткими рамками энергопотребления. При этом передаваемые телеметрические данные должны защищаться с использованием сертифицированных криптографических алгоритмов, в частности, в соответствии с СТБ 34.101.31. Программная реализация ресурсоемких алгоритмов на слабых микроконтроллерах (MCU) приводит к быстрому разряду батареи устройства и недопустимым задержкам в передаче данных.

Эффективным решением данной проблемы является концепция «доверенной среды» (Trusted Execution Environment) на аппаратном уровне. В архитектуру измерительного прибора необходимо закладывать SoC (System-on-a-Chip) или микроконтроллеры, имеющие встроенные аппаратные криптографические сопроцессоры, физически изолированную память для хранения ключей и защиту портов отладки (JTAG). В общем виде процесс формирования криптограммы для защиты конфиденциальности данных измерительного прибора в режиме сцепления блоков можно выразить формулой:

$$C_i = E_K(P_i \oplus C_{i-1}), \quad (1)$$

где C_i – текущий блок шифротекста; E_k – функция аппаратного шифрования на ключе K (например, по стандарту BelT); P_i – блок открытых телеметрических данных; $\oplus$ – операция побитового сложения по модулю 2; C_{i-1} – предыдущий блок шифротекста.

Аппаратная реализация функции E_k позволяет существенно снизить нагрузку на центральный процессор прибора по сравнению с программной реализацией [1]. Кроме того, физическое разделение зон памяти предотвращает несанкционированное считывание прошивки или модификацию калибровочных коэффициентов измерительного датчика даже при наличии физического доступа к устройству. Выбор компонентной базы должен осуществляться с учетом необходимости минимизации рисков наличия недекларированных возможностей в зарубежных микросхемах [2].

Заключение

Интеграция аппаратных модулей безопасности в архитектуру измерительных приборов является обязательным условием для создания конкурентоспособного и защищенного продукта. Для инженерных команд, разрабатывающих новые приборы учета или контроля параметров среды, применение микроконтроллеров с аппаратной поддержкой отечественных криптографических стандартов значительно упрощает процедуру сертификации и допуска к эксплуатации на объектах информационной инфраструктуры Республики Беларусь.

Список использованных источников

1. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. (2003) Математические и компьютерные основы криптологии. Минск, Издательство «Новое знание».

2. Малюк А. А. (2020) Теория защиты информации. Москва, Издательство «Горячая линия-Телеком».

References

1. Kharin Yu. S., Bernik V. I., Matveev G. V., Agievich S. V. (2003) Mathematical and Computer Foundations of Cryptology. Minsk, Novoe Znanie Publishing House (in Russian).

2. Malyuk A. A. (2020) Information Security Theory. Moscow, Goryachaya Liniya-Telecom Publishing House (in Russian).

Сведения об авторе

Маевский П. К., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mmauglik1113@gmail.com.

Information about the author

Maevsky P. K., Cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mmauglik1113@gmail.com.