УДК 004.413
doi: 10.26583/bit.2024.4.04

Олег Н. Дьяков
АО «Аладдин Р.Д.»,
ул. Докукина, 16, стр. 1, Москва, 129226, Россия,
e-mail: O.Dyakov@aladdin.ru, https://orcid.org/0009-0004-5696-8595

СПЕЦИАЛЬНОЕ ВСТРОЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДОВЕРЕННОЙ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ

Аннотация. Разработка и производство доверенной электронной компонентной базы (ЭКБ) связаны с решением комплексных задач, по выполнению требований технологической, функциональной и информационной безопасности изделия. В статье рассматриваются аспекты обеспечения доверия к ЭКБ через организацию цепочек доверия, основанных на применении технических подходов, реализованных в интегральных микросхемах с программно-аппаратной архитектурой. Особое внимание уделяется специальному встроенному программному обеспечению, которое устанавливается на этапе производства интегральной микросхемы. Правильно спроектированное специальное встраиваемое программное обеспечение интегральной микросхемы может существенно повысить уровень безопасности устройства, помочь в организации доверенной цепочки поставки и эксплуатации прибора, обеспечить защиту от фальсификации (идентификация, строгая аутентификация микросхемы), поддержать процедуры безопасной загрузки и запуска системного и прикладного программного обеспечения. Данная статья будет интересна специалистам по разработке доверенной ЭКБ, доверенных программно-аппаратных комплексов (ПАК), системным интеграторам КИИ, разработчикам сквозных технологических процессов по разработке и производству доверенных устройств и информационных систем.

Ключевые слова: доверенная ЭКБ, доверенный ПАК, технологическая безопасность, функциональная безопасность, информационная безопасность, производство микросхем, защита памяти, встроенное программное обеспечение, доверенная цепочка поставки, инсталляция встроенного ПО.

Для цитирования: ДЬЯКОВ, Олег Н. СПЕЦИАЛЬНОЕ ВСТРОЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДОВЕРЕННОЙ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ. Безопасность информационных технологий, [S.l.], т. 31, № 4, с. 67–86, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1716. DOI: http://dx.doi.org/10.26583/bit.2024.4.04.

Oleg N. Dyakov
JSC "Aladdin R.D.",
Dokukina str., 16, building 1, Moscow, 129226, Russia,
e-mail: O.Dyakov@aladdin.ru, https://orcid.org/0009-0004-5696-8595

Special embedded software of trusted electronic component

Abstract. Development and production of trusted electronic components is associated with solving complex problems of fulfilling the requirements of technological, functional and information security of the product. The proposed publication considers aspects of ensuring trust in the hardware and software systems through the organization of trust chains based on the use of technical approaches implemented in integrated circuits with hardware and software architecture. Attention is paid to special embedded software, which is installed at the stage of production of the integrated circuit. Correctly designed special embedded software of an integrated circuit can significantly increase the level of device security, help in organizing a trusted supply chain and operation of the device, provide protection against counterfeiting (identification, strict authentication of the chip), support procedures for safe loading and launch of system and application software. This publication will be of interest to specialists in the development of trusted electronic

components, trusted devices, system integrators of critical information infrastructure, developers of end-to-end technological processes for the development and production of trusted devices and information systems.

Keywords: trusted electronic component, trusted devices, technological security, functional safety, information security, chip production, memory protection, embedded software, trusted supply chain, installation of embedded software.

For citation: DYAKOV, Oleg N. Special embedded software of trusted electronic component. IT Security (Russia), [S.l.], v. 31, no. 4, p. 67–87, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1716. DOI: http://dx.doi.org/10.26583/bit.2024.4.04.

Введение

Основным признаком доверенной радиоэлектронной продукции является соответствие требованиям обеспечения технологической независимости, функциональности, надёжности и защищённости[1]. Доверенная радиоэлектронная продукция должна преимущественно состоять из доверенных компонентов (ИС, программное обеспечение) и производиться в рамках доверенной цепочки разработки и поставки.

Ключевыми элементами современного электронного устройства являются цифровые интегральные микросхемы с программно-аппаратной архитектурой (микроконтроллеры, процессоры, системы на кристалле) [1, 2], содержащие одно или несколько процессорных ядер, память для кода и данных программ, внутренние шины обмена информацией, периферийные устройства и т.д.

В вычислительной технике встроенное программное обеспечение (прошивка) [3, 4] – это программное обеспечение, которое выполняет низкоуровневый контроль аппаратных компонент вычислительного устройства. Для относительно простого устройства, разработанного на базе системы на кристалле, встроенное программное обеспечение может выполнять все функции управления, мониторинга и манипулирования данными. Для более сложных устройств встроенное программное обеспечение может обеспечивать относительно низкоуровневое управление [5], а также услуги аппаратной абстракции для программного обеспечения более высокого уровня, такого как операционная система.

Для поддержки работы интегральных микросхем с программно-аппаратной архитектурой используется специальное встроенное программное обеспечение, которое заносится в энергонезависимую память микросхемы (ПЗУ, ЭППЗУ, флэш-память) на этапе производства и используется на протяжении всего жизненного цикла радиоэлектронного устройства.

При разработке современных микросхем встроенному программному обеспечению уделяется большое внимание, так как оно может существенно повысить уровень безопасности устройства, выявить нарушение целостности и правильности функционирования, обеспечить защиту от контрафакта и потенциальных аппаратных и программных закладок, поддержать безопасную загрузку и запуск системного и прикладного программного обеспечения.

Специальное встроенное программное обеспечение используется для целей тестирования во время производства микросхемы, а также предоставляет дополнительные функции, облегчающие использование аппаратных компонент при производстве и эксплуатации радиоэлектронного устройства.

В общем случае интегральная микросхема с программно-аппаратной архитектурой включает:

[1]ПНСТ 911-2024. Критическая информационная инфраструктура. Доверенные интегральные микросхемы и электронные модули. Общие положения.

– аппаратные компоненты ИС (аппаратные средства, включая физическую память);
– данные конфигурации и данные инициализации, относящиеся к поведению функций безопасности;
– встроенное программное обеспечение тестирования ИС;
– встроенное программное обеспечение поддержки ИС.

Далее в данной статье под термином интегральная микросхема (ИС) будем подразумевать цифровую интегральную микросхему с программно-аппаратной архитектурой.

1. Специальное встроенное программное обеспечение доверенной ИС

Процессы разработки и производства ИС можно разделить на три отдельных этапа (рис. 1)[2].

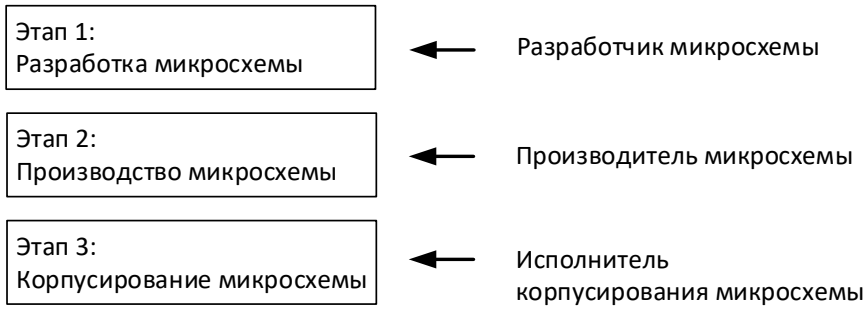

Рис. 1. Общая схема жизненного цикла изготовления ИС

Специальное встроенное программное обеспечение представлено на данных этапах следующим образом:

– Разработка ИС (этап 1):
  – дизайн ИС;
  – разработка специализированного встроенного программного обеспечения ИС.
– Производство ИС (этап 2):
  – интеграция и изготовление фотошаблонов;
  – производство ИС;
  – инициализация (загрузка и активация специализированного встроенного программного обеспечения);
  – тестирование ИС;
  – предварительная параметризация (запись индивидуальных данных, параметризация функций безопасности, запись информации о прохождении этапов жизненного цикла ИС).
– Корпусирование ИС (Этап 3):
  – корпусирование ИС;
  – тестирование ИС;
  – при необходимости параметризация (нанесение идентификаторов на корпус ИС, запись информации о прохождении этапов жизненного цикла ИС).

[2]Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.

Функциональность специализированного встроенного программного обеспечения должна быть подробно описана в технической документации на ИС.

1.1 Встроенное программное обеспечение тестирования ИС

Специальное встроенное программное обеспечение тестирования ИС предназначено для:

- поддержки тестирования при производстве микросхемы;
- поддержки тестирования при эксплуатации микросхемы;
- поддержки встроенного аппаратного и программно-аппаратного самотестирования микросхемы.

Термин «встроенное самотестирование» (BIST)[3] используется для описания аппаратных и программно-аппаратных механизмов микросхемы, которые могут использоваться для обнаружения скрытых неисправностей [6]. BIST позволяет микросхеме проводить периодические самопроверки для выявления неисправностей [7]. Результаты этих самопроверок затем могут использоваться микросхемой для обработки неисправностей и обеспечения того, чтобы устройство оставалось в безопасном состоянии.

Встроенное самотестирование может использоваться для калибровки аналоговых и цифровых компонентов ИС, для обнаружения дефектов ИС, для выполнения аутентификации аппаратных компонентов ИС (например, на основе использования физически не клонируемых функций).

Результаты самотестирования должны записываться в память микросхемы и быть доступны при выполнении процедуры аудита состояния изделия со стороны специального программного обеспечения поддержки ИС.

1.2 Встроенное программное обеспечение поддержки ИС

Встроенное программное обеспечение поддержки ИС предназначено для:

- параметризации и инициализации системы безопасности микросхемы;
- определения целостности компонентов микросхемы (аппаратные модули, программный код, данные);
- предоставления интерфейсов и механизмов безопасной загрузки исполняемого кода и данных в перепрограммируемую память микросхемы;
- обеспечения интерфейса для выполнения внешнего технического аудита микросхемы;
- предоставления сервисов аппаратной абстракции для программного обеспечения более высокого уровня (запись в EEPROM, управление сопроцессорами, доступ к защищённой памяти, управление режимами работы процессора и т.д.);
- предоставления сервисов поддержки корня доверия для операций идентификации и аутентификации устройства, безопасной инсталляции и обновления встроенного программного обеспечения, безопасного старта системы.

Для доверенных ИС [8, 9] с высоким уровнем безопасности для запуска системы используется технология цепочки доверия, которая предполагает проверку целостности и аутентичности последовательно запускаемых компонент программного обеспечения системы [10]. Каждый предыдущий элемент цепочки доверия проверяет (измеряет) следующий элемент, при успешном выполнении процедуры проверки выполняется передача управления следующему элементу цепочки. В начале цепочки доверия находится корень доверия (Root-of-Trust, RoT) – код и данные, использующие некоторый

[3]NXP Semiconductors. Using the Built-in Self-Test (BIST) on the MPC5744P. Document Number: AN0. 2017.

вычислительный механизм, который стартует первым и гарантирует, что устройство запускается правильно, а его компоненты и операционная система защищены от фальсификации[4].

Основные свойства корня доверия (RoT):

- RoT должен включать код, который выполняется первым при инициализации вычислительного ядра во время холодного старта платформы.
- Код RoT должен быть неизменяемым или изменения должны контролироваться только уникальным идентифицируемым владельцем.
- RoT должен быть проверен независимой стороной (лабораторией тестирования), способной оценить вычислительный механизм, код и данные.
- Производитель аппаратной платформы должен создать и инициализировать RoT в процессе производства.

Корень доверия может быть составной частью встроенного программного обеспечения поддержки ИС.

Основное назначение корня доверия – это обеспечение процедуры безопасного старта системы и поддержка операций безопасной инсталляции/обновления программного обеспечения системы. Дополнительно корень доверия может предоставлять для программного обеспечения вышележащих уровней следующие сервисы безопасности:

- аутентификация программных и аппаратных компонент и данных,
- обеспечение конфиденциальности программных компонент и данных,
- контроль целостности программных компонент и данных,
- измерение (поддержка цепочки доверия),
- отчётность (поддержка удалённого аудита),
- инсталляция и обновление программного обеспечения.

Для эффективной реализации функций поддержки цепочки доверия и операций строгой аутентификации компонентов системы используется технология Инфраструктуры Открытых Ключей (Public Key Infrastructure, PKI), лежащая в основе цифровых сертификатов, которая включает в себя всё, что используется для обеспечения криптографии с открытым ключом [11].

Основная цель любой PKI – создание защищённой среды, используемой участниками, приложениями и оборудованием, через управление ключами и сертификатами. Сертификаты и ассиметричные ключи составляют краеугольный камень PKI, выступая в качестве основы, с помощью которой может быть поддержано доверие к конечной точке [5].

Для поддержки PKI специализированное встроенное программное обеспечение должно реализовать: алгоритмы ассиметричной криптографии, вычисление хэш функций, процедуры безопасного хранения ключей [12, 13].

2. Встроенные механизмы поддержки доверия к ИС

Для эффективного и безопасного функционирования специального встроенного программного обеспечения в микросхеме должны быть реализованы внутренние механизмы поддержки доверия к ИС и устройству в целом [14]. В табл. 1 приведён краткий перечень широко применяемых на практике технических механизмов обеспечения доверия к ИС.

[4]GlobalPlatform Technology. Root of Trust Definitions and Requirements. Version 1.1.1, Public Release, June 2022.
[5]RFC 5280. Internet X.509 PKI Certificate and CRL Profile.

Таблица 1. Встроенные механизмы обеспечения доверия к ИС

#	Встроенный механизм	Уровень ИС			
		1	2	3	4
1	Неизменяемый уникальный номер ИС (формируется на этапе изготовления)	*	*	*	*
2	Одноразовая программируемая память для записи информации о прохождении стадий жизненного цикла ИС (Integrated Circuit Life Cycle, данных конфигурации безопасности, и т.д.)	*	*	*	*
3	Возможность необратимого отключения аппаратных механизмов загрузки и отладки встроенного программного обеспечения	*	*	*	*
4	Защищённая от несанкционированного доступа память для хранения критических данных		*	*	*
5	Уровни привилегий выполнения потока вычислительного ядра		*	*	*
6	Управление доступом к памяти (MMU/MPU)		*	*	*
7	Механизм автоматического обнаружения и коррекции ошибок памяти (Error-Correcting Code)		*	*	*
8	Контроль целостности аппаратной платформы (BIST), встроенного программного обеспечения и данных при запуске		*	*	*
9	Генератор случайных чисел			*	*
10	Криптографические средства для поддержки строгой аутентификации и шифрования			*	*
11	Наличие тщательно верифицированного корня доверия (код и данные) для поддержания процедур доверенной инсталляции/обновления встроенного ПО и доверенного запуска.			*	*
12	Скремблирование данных внутренних и внешних информационных шин				*
13	Инженерные средств защиты от физических атак и атак по побочным каналам				*
14	Входы для экстренной блокировки критической функциональности (Tamper Protection)				*

Механизмы в табл. 1 расположены в порядке возрастания требований к безопасности ИС. Микросхемы разделены на четыре группы по оснащённости механизмами поддержки доверия.

Уровень 1 предлагает минимальный набор, поддерживающий трассируемость цепочки поставки и базовую защиту от клонирования и подмены программного обеспечения.

Уровень 2 предполагает наличие у ИС аппаратных механизмов контроля целостности аппаратных компонент, кода и данных, и контроля потока выполнения программы. Данный уровень позволяет существенно повысить надёжность изделия и безопасность выполнения программного обеспечения.

Уровень 3 предполагает использование криптографических методов обеспечения защиты от фальсификаций и применение цепочек доверия для доверенной инсталляции, обновления и запуска программного обеспечения.

Уровень 4 относится к микросхемам, которые должны эффективно противостоять различным физическим атакам и атакам по побочным каналам.

Необходимый уровень доверия можно достигнуть только за счёт взаимного рационального использования аппаратных и программных методов обеспечения технологической, функциональной и информационной безопасности.

Ниже представлен далеко не полный перечень основных угроз цепочке поставок доверенной радиоэлектронной продукции и некоторые подходы по минимизации данных угроз.

Угрозы процессам стадий жизненного цикла доверенной радиоэлектронной продукции[6]:

- контрафакт (производство неучтённого оборудования, производство на несертифицированных производствах);
- повторное использование (использование списанного оборудования);
- недостаточная верификация (использование оборудования, не прошедшего полный цикл проверок);
- деградация характеристик;
- устаревание функциональности;
- ошибки дизайна;
- злонамеренное изменение функциональности (изменение характеристик);
- атаки на систему через недоверенную ИС (блокировка работы, фальсификация показаний, воровство конфиденциальной информации, и т.д.).

Контрмеры по минимизации угроз цепочке поставок:

- прозрачное управление жизненным циклом;
- обеспечение безопасного режима исполнения кода;
- обеспечение неизвлекаемости чувствительных данных;
- использование самотестирования изделий;
- использование криптографических методов проверки целостности и аутентичности;
- обеспечение безопасного удалённого обновления программного обеспечения и данных;
- обеспечение безопасного удалённого аудита характеристик;
- аудит изделий и процессов производства.

Ниже будет представлено более подробное описание каждого встроенного механизма обеспечения доверия к ИС и его влияние на парирование угроз доверенной цепочке поставки ИС.

Многие перечисленные механизмы могут одновременно поддерживать выполнение требований к микросхеме по работоспособности, надёжности, стойкости, информационной безопасности (ИБ), функциональной безопасности (ФБ) и технологической безопасности (ТБ).

[6]GUIDELINES FOR SECURING THE INTERNET OF THINGS. European Union Agency for Cybersecurity (ENISA), 2020; RFC 9124. A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices. January 2022; Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules until March 31, 2022. On April 1, 2022.

Неизменяемый уникальный номер ИС

Применение:

- сквозная идентификация ИС на протяжении всего жизненного цикла;
- вывод уникальных криптографических ключей;
- использование для индивидуальных настроек ИС и устройства в целом;
- защита от повторного использование ИС (использование списанного оборудования).

Контрмеры по минимизации угроз цепочки поставок:

- прозрачное управление жизненным циклом;
- аудит изделий и процессов.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
			*	*	*

Одноразовая программируемая память для записи информации о прохождении стадий жизненного цикла ИС

Применение:

- запись информации о прохождении определённой фазы жизненного цикла (кто, где, когда);
- перевод ИС и устройства в целом в следующее состояние жизненного цикла;
- возможность необратимой блокировки функциональности ИС;
- защита от повторного использования (использование списанного оборудования);
- защита от недостаточной верификации (использование оборудования, не прошедшего полный цикл проверок).

Контрмеры по минимизации угроз цепочки поставок:

- прозрачное управление жизненным циклом;
- проверка целостности и аутентичности изделия.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
			*	*	*

Возможность необратимого отключения аппаратных механизмов загрузки и отладки встроенного программного обеспечения

Применение:

- защита от контрафакта (воровство прошивки и данных, клонирование);
- защита от несанкционированной подмены встроенного программного обеспечения;
- злонамеренное изменение функциональности (изменение характеристик);
- защита от реверс-инжиниринг.

Контрмеры по минимизации угроз цепочки поставок:

- обеспечение неизвлекаемости чувствительных данных.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*		*	*	*

Защищённая от несанкционированного доступа память для хранения критических данных

Применение:

– безопасное хранение ключей и паролей;
– безопасное хранение профилей безопасности;
– безопасное хранение журналов самотестирования и измерений процесса запуска.

Контрмеры по минимизации угроз цепочки поставок:

– обеспечение неизвлекаемости чувствительных данных (ключей, паролей и т.д.).

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*		*	*	*

Уровни привилегий выполнения потока вычислительного ядра

Применение:

– разделение доступа к командам процессора, периферии и областям памяти в зависимости от режима (привилегий) исполняемого кода;
– позволяет существенно повысить надёжность выполнения исполняемого кода в случае ошибок или сбоев.

Контрмеры по минимизации угроз цепочки поставок:

– обеспечение безопасного режима исполнения кода;
– обеспечение неизвлекаемости чувствительных данных.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*	*	*	*	

Управление доступом к памяти (MMU/MPU)

Применение:

– разделение доступа к периферии и областям памяти в зависимости от профиля безопасности потока/процесса;
– позволяет существенно повысить надёжность выполнения исполняемого кода в случае ошибок или сбоев;
– позволяет на аппаратном уровне разграничить код и данные различных процессов потоков/процессов.

Контрмеры по минимизации угроз цепочки поставок:
- обеспечение безопасного режима исполнения кода;
- обеспечение неизвлекаемости чувствительных данных.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*	*	*	*	

Механизм автоматического обнаружения и коррекции ошибок памяти (Error-Correcting Code)

Применение:
- автоматическое обнаружение искажения данных и кода в процессе выполнения программы;
- автоматическая коррекция ошибок;
- позволяет существенно повысить надёжность выполнения исполняемого кода в случае ошибок или сбоев;
- обнаружение деградации характеристик.

Контрмеры по минимизации угроз цепочки поставок:
- обеспечение безопасного режима исполнения кода;
- использование самотестирования изделий.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*	*	*	*	

Контроль целостности аппаратной платформы (BIST), встроенного программного обеспечения и данных при запуске

Применение:
- автоматическое обнаружение аппаратных сбоев, искажения данных и кода в процессе старта ИС;
- позволяет существенно повысить надёжность выполнения исполняемого кода в случае ошибок или сбоев;
- обнаружение деградации характеристик и внедрения злонамеренного кода.

Контрмеры по минимизации угроз цепочки поставок:
- обеспечение безопасного режима исполнения кода;
- использование самотестирования изделий;
- обеспечение безопасного удалённого аудита характеристик.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*		*	*	*

Генератор случайных чисел

Применение:

– генерация индивидуальных криптографических ключей;
– поддержка протоколов строгой аутентификации;
– поддержка протоколов безопасного доступа.

Контрмеры по минимизации угроз цепочки поставок:

– обеспечение безопасного удалённого обновления программного обеспечения и данных;
– обеспечение безопасного удалённого аудита характеристик;
– аудит изделий и процессов.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
			*		

Криптографические средства для поддержки строгой аутентификации и шифрования

Применение:

– поддержка протоколов строгой аутентификации;
– поддержка протоколов безопасного доступа.

Контрмеры по минимизации угроз цепочки поставок:

– обеспечение безопасного удалённого обновления программного обеспечения и данных;
– обеспечение безопасного удалённого аудита характеристик;
– аудит изделий и процессов.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
			*	*	*

Наличие тщательно верифицированного корня доверия (код и данные) для поддержания процедур доверенной инсталляции/обновления встроенного ПО и доверенного запуска

Применение:

– автоматическое обнаружение искажения данных и кода в процессе запуска программы;
– обнаружение деградации характеристик и внедрения злонамеренного кода;
– безопасное обновление программного обеспечения при обнаружении ошибок дизайна, новых уязвимостей, необходимости расширения функционала.

Контрмеры по минимизации угроз цепочки поставок:

– прозрачное управление жизненным циклом;
– использование криптографических методов проверки целостности и аутентичности;

– использование самотестирования изделий;
– обеспечение безопасного режима исполнения кода;
– обеспечение безопасного удалённого обновления программного обеспечения и данных;
– обеспечение безопасного удалённого аудита характеристик;
– аудит изделий и процессов.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*		*	*	*

Скремблирование данных внутренних и внешних информационных шин
Применение:
– защита от контрафакта (воровство прошивки и данных, клонирование);
– защита от реверс-инжиниринга;
– противодействие атакам по побочным каналам.

Контрмеры по минимизации угроз цепочки поставок:
– обеспечение неизвлекаемости чувствительных данных.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*		*	*	*

Инженерные средств защиты от физических атак и атак по побочным каналам
Применение:
– защита от контрафакта (воровство прошивки и данных, клонирование);
– защита от реверс-инжиниринга;
– противодействие атакам по побочным каналам;
– позволяет существенно повысить надёжность выполнения исполняемого кода в случае ошибок или сбоев.

Контрмеры по минимизации угроз цепочки поставок:
– обеспечение неизвлекаемости чувствительных данных;
– обеспечение безопасного режима исполнения кода.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
*	*		*	*	*

Входы для экстренной блокировки критической функциональности (Tamper Protection)

Применение:

- экстренное уничтожение критических данных при попытке вскрытия устройства;
- защита от контрафакта (воровство прошивки и данных, клонирование).

Контрмеры по минимизации угроз цепочки поставок:

- обеспечение неизвлекаемости чувствительных данных.

Поддержка выполнения требований доверия к ИС:

Требования к доверенной ИС					
Работоспособность	Надёжность	Стойкость	ИБ	ФБ	ТБ
			*	*	*

3. Безопасная инсталляция встроенного программного обеспечения

Для реализации цепочки поставки доверенных радиоэлектронных устройств необходимо поддержать на уровне специализированного программного обеспечения ИС процедуру безопасной инсталляция встроенного программного обеспечения (Secure Firmware Install, SFI)[7].

Процедура SFI предназначена для:

- защиты прошивки встроенного программного обеспечения у Контрактного Производителя доверенной Аппаратной Платформы (АП) при программировании устройств;
- предотвращения неконтролируемого перепроизводства АП.

Цели безопасности SFI достигаются за счёт того, что:

- защищённую прошивку возможно установить только в оригинальную ИС;
- количество успешно проведённых инсталляций подсчитывается в модуле безопасности (SM);
- проверяется подлинность, целостность и конфиденциальность встроенного программного обеспечения и данных конфигурации;
- прошивка и данные конфигурации передаются в ИС в зашифрованном виде.

На рис. 2 показан типичный производственный процесс, когда Разработчик АП создаёт прошивку и требует, чтобы эта прошивка была загружена в ИС во время производства. За производственный процесс отвечает Контрактный Производитель, который закупает основные электронные компоненты через каналы продаж или дистрибуции.

В этом типичном сценарии Разработчик АП отправляет прошивку Контрактному Производителю в открытом виде: код приложения потенциально подвергается атакам или копированию. Разработчик АП должен доверять Контрактному Производителю, надеясь, что код его приложения не будет украден или подделан, и что Контрактный Производитель не будет производить устройства в избыточном количестве.

[7]AN5510 - Rev 1 - September 2020. Overview of the secure secret provisioning (SSP) on STM32MP1 Series;
AN4992 - Rev 13 - June 2022. STM32 MCUs secure firmware install (SFI) overview;
GPC_SPE_134. GlobalPlatform Open Firmware Loader for Tamper Resistant Element Version 1.3, April 2021.

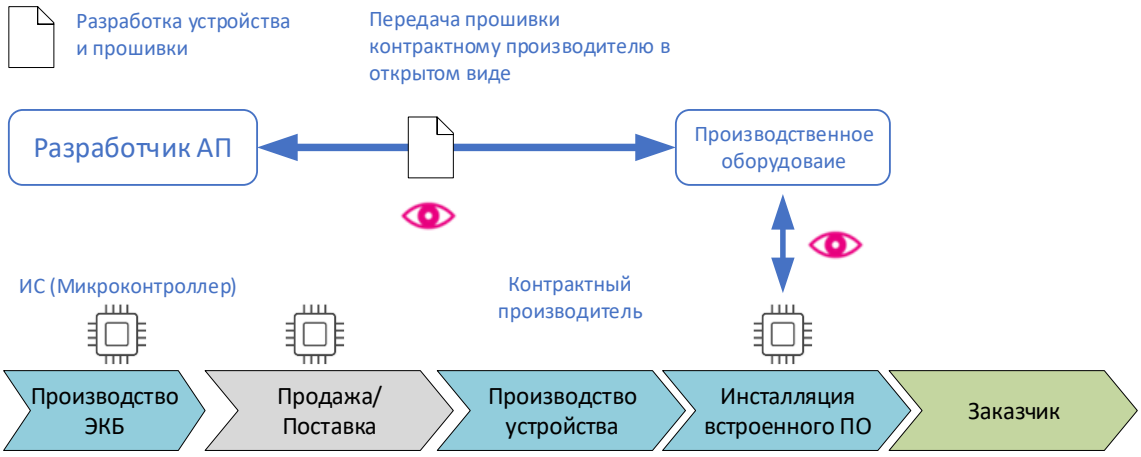

Рис. 2. Недоверенная цепочка поставки ПАК

При производстве с поддержкой технологии безопасной инсталляции Разработчик АП создаёт и управляет своим собственным секретным ключом шифрования (или ключом встроенного ПО, как показано на рис. 3), который используется для шифрования кода приложения и конфигурации. Данный ключ используется ИС для расшифровки пакета SFI. Все ИС снабжены уникальным закрытым ключом и сертификатом. Контрактный Производитель может приобрести ИС с SFI через обычные каналы продаж/поставки. Затем Контрактный Производитель может безопасно установить прошивку с помощью доверенного производственного оборудования, поддерживающего технологию SFI, так что прошивка никогда не будет видна в открытом виде на уровне Контрактного Производителя.

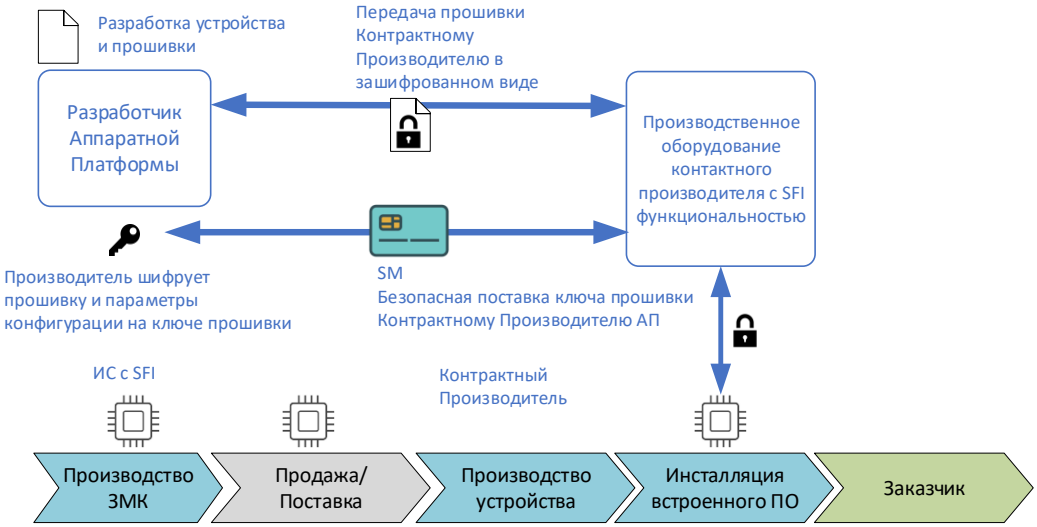

Рис. 3. Доверенная цепочка поставки изделий с использованием доверенной ИС и технологии SFI

SM (Security Module) может быть выполнен в виде отдельного аппаратного модуля, например, смарт-карты, и предназначен для безопасного переноса ключа прошивки в оборудование Контрактного Производителя.

Задачи SFI включают в себя:
- распределение ключей;
- безопасный механизм загрузки во внутреннюю флэш-память;
- безопасный механизм взаимодействия ИС и внешней флэш-памяти;
- функции защиты памяти;
- безопасный загрузчик.

3.1 SFI ключевая схема

Для выполнения операций шифрования и аутентификации SFI процесс использует различные ключи и криптографические механизмы.

В общем случае могут применяться как стандарты NIST, так и ГОСТ, в зависимости от возможностей ИС и выбранной криптографической схемы.

Основные криптографические ключи SFI процесса приведены в табл. 2.

Таблица 2. Ключи SFI

Наименование ключа	Тип ключа	Назначение	Генерация	Хранение	Использование
K_I	AES, ГОСТ 34.12-2018 (Кузнечик)	Ключ шифрования образа прошивки	SM	SM	SM, IC
KP_{IC}	ECC, RSA, ГОСТ 34.10-2018	Публичный ключ IC, используется в операциях аутентификации	IC	IC	SM, IC
KS_{IC}	ECC, RSA, ГОСТ 34.10-2018	Секретный ключ IC, используется в операциях аутентификации	IC	IC	IC
CKP_{IC}	ECC, RSA, ГОСТ 34.10-2018	Сертификат публичного ключа KP_{IC}, на ключе KS_{CA} центра сертификации	CA	IC	SM, IC
KP_{CA}	ECC, RSA, ГОСТ 34.10-2018	Публичный ключ центра сертификации, используется для проверки сертификатов	CA	SM	SM
KS_{CA}	ECC, RSA, ГОСТ 34.10-2018	Секретный ключ центра сертификации, используется для генерации сертификатов	CA	CA	CA

Где CA – Certificate Authority, IC – Integrated Circuit (доверенная ИС), SM – Security Module.

Для аутентификации ИС используется сертификат публичного ключа ИС (KP_{IC}), который формируется на секретном ключе (KS_{CA}) центра сертификации (CA) и загружается в ИС на этапе изготовления микросхемы.

3.2 SFI описание процесса загрузки во внутреннюю флэш-память

SFI – это механизм, который обеспечивает безопасную и контролируемую со стороны разработчика установку прошивки в ненадёжной производственной среде (например, у Контрактного Производителя). SFI реализован в безопасном загрузчике, который является частью встроенного программного обеспечения поддержки ИС.

Обобщённо SFI процесс записи во внутреннюю флэш память представлен на рис. 4 и заключается в том, что вся прошивка и данные конфигурации шифруются с помощью секретного ключа прошивки K_I с использованием специальной программы SFI упаковщика (1)[8].

Разработчик АП загружает в SM секретный ключ прошивки (K_I), публичный ключ центра сертификации (KP_{CA}) и максимальное значение счётчика инсталляций (2).

Контрактный Производитель должен использовать доверенное оборудование для запуска процесса SFI и отправки зашифрованного образа прошивки в ИС (3).

SM отвечает за:

– надёжное хранение секретного ключа образа прошивки K_I;

– проверку сертификата CKP_{IC} (4), который используется для аутентификации ИС (5);

– создание и предоставление лицензии безопасному загрузчику для защищённой установки зашифрованной прошивки в ИС (6);

– подсчёт количества загруженных ИС.

ИС поставляется с уникальной парой ключей (секретный и открытый ключи), которые формируются в процессе изготовления ИС. Доступ к секретному ключу устройства предоставлен только встроенному безопасному загрузчику, который извлекает секретный ключ K_I (7) путём расшифровки лицензии с использованием закрытого ключа устройства.

Благодаря функциям безопасности и криптографическим алгоритмам SFI поддерживает безопасное программирование прошивки во внутреннюю флэш-память и обеспечивает защиту прошивки (конфиденциальность, подлинность и целостность) на этапе производства устройства у контрактного производителя.

Безопасный загрузчик получает и расшифровывает встроенное ПО и байты параметров и записывает их во внутреннюю флэш-память ИС (8).

Этапы SFI процесса (рис. 4):

1. Получение зашифрованного SFI образа прошивки с использованием ключа K_I.
2. Загрузка в SM секретного ключа прошивки K_I.
3. Передача зашифрованного SFI образа прошивки в ИС (запуск процесса SFI).
4. Считывание сертификата ИС (CKP_{IC}) и загрузка его в SM.
5. Проверка сертификата ИС и извлечение из сертификата публичного ключа ИС (KP_{IC}).
6. Зашифрование K_I на ключе KP_{IC} (получение лицензии). Уменьшение счётчика инсталляций. Передача лицензии в ИС.
7. Извлечение из лицензии секретного ключа прошивки K_I. Для данной операции используется секретный ключ ИС (KS_{IC}).
8. Расшифрование SFI образа прошивки на ключе K_I. Запись кода программы и байтов конфигурации.

Примечание. В случае использования ECC на этапе (6) используется механизм выработки сессионных ключей по схеме ECKA (для российских алгоритмов VKO P 50.1.113-2016).

[8](1) – номер этапа выполнения SFI процесса на рис. 4.

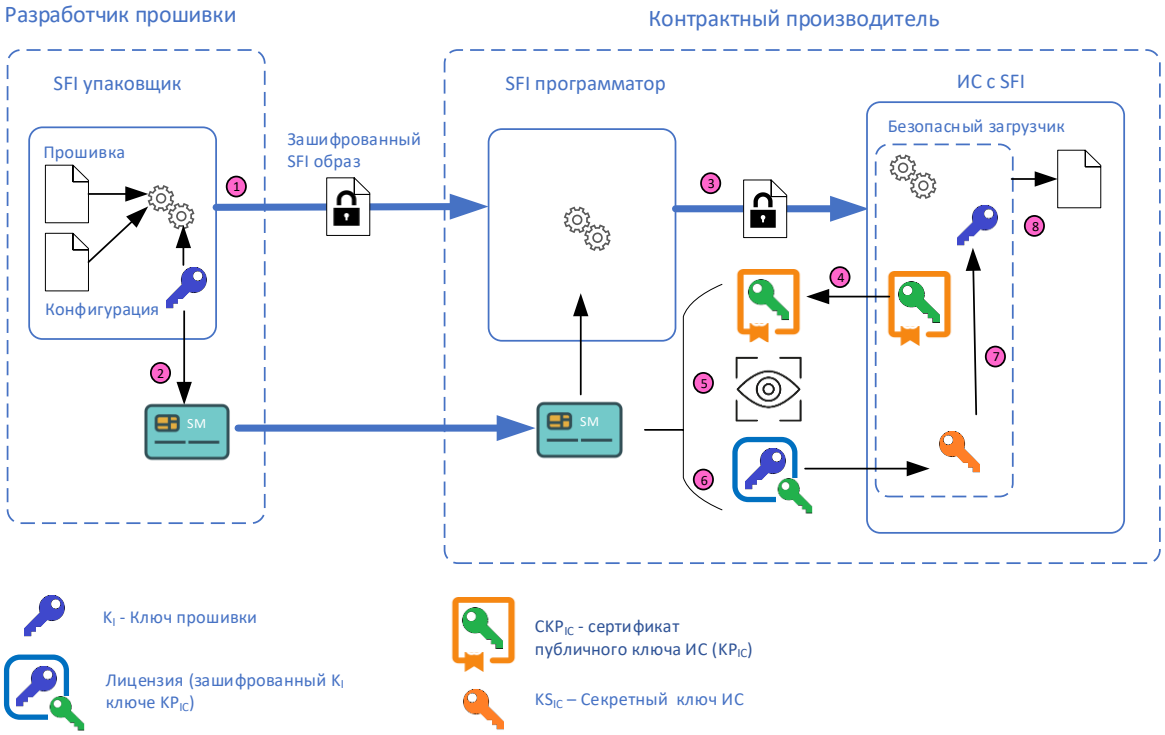

Рис. 4. Общая схема SFI процесса

Безопасный загрузчик представляет из себя часть специального встроенного программного обеспечения ИС.

Если ИС сбрасывается во время получения секретного ключа прошивки K_I (7), все конфиденциальные данные стираются перед перезапуском начальной процедуры SFI.

Во время выполнения процесса SFI безопасный загрузчик никогда не позволяет никакому другому коду получить доступ к пользовательской флэш-памяти или SRAM.

4. Функции защиты памяти

Доверенная ИС должна иметь набор средств для функциональной защиты внутренней памяти от чтения и модификации при выполнении встроенного программного обеспечения.

Наиболее распространёнными являются следующие механизмы защиты:

– RDP (ReaDout Protection): предотвращает доступ к флэш-памяти через JTAG/SWD интерфейс для всей флэш-памяти и выделенным областям SRAM.
– PCRDP (Proprietary Code ReaDout Protection): предотвращает доступ для чтения к настраиваемым областям флэш-памяти/SRAM, при выполнении стороннего программного обеспечения (защита от вредоносного стороннего кода).
– WRP (WRite Protection): предотвращает случайные или злонамеренные операции записи/стирания.

Управление режимами защиты памяти выполняется с помощью специальных регистров опций.

Функции защиты памяти используются при работе безопасного загрузчика SFI процесса.

4.1 Защита от несанкционированного чтения RDP

Функция защиты чтения RDP обычно предлагает три уровня защиты для всей SRAM и флэш-памяти, а также для резервных регистров:

- Уровень 0 означает «нет защиты». Это заводская установка по умолчанию. Операции чтения, записи и стирания разрешены для SRAM, флэш-памяти, а также резервных регистров. На уровне 0 могут быть изменены биты в регистрах опций.
- Уровень 1 обеспечивает полную защиту от чтения памяти чипа, которая включает флэш-память, резервные регистры, а также содержимое выделенных областей SRAM. Обнаружение попытки доступа к флэш-памяти, регистрам резервного копирования или к SRAM, вызывает серьёзную системную ошибку, которая блокирует выполнение всего кода до следующего сброса питания. Обратите внимание, что биты регистров опций все ещё могут быть изменены на уровне 1.
- Уровень 2 обеспечивает те же функции защиты для SRAM, флэш-памяти и резервных регистров, что и уровень 1. Однако есть три основных отличия. Соединение отладчика JTAG/SWD отключено (доступа нет даже у производителя ИС, чтобы гарантировать отсутствие бэкдоров), режим загрузки принудительно установлен на пользовательскую флэш-память независимо от настроек загрузки. После установки уровня 2 биты регистров опций больше нельзя изменить.

Изменение уровня защиты RDP разрешено только при текущем уровне защиты «1». Изменение уровня защиты с «1» на «0» автоматически сотрёт всю пользовательскую флэш-память, SRAM и резервные регистры.

4.2 Защита от считывания проприетарного кода PCRDP

Защита от считывания проприетарного кода (Proprietary Code Readout Protection, PCRDP) это способ защитить код стороннего программного обеспечения, независимо от настройки уровня RDP. Третьи стороны могут разрабатывать и продавать определённые модули и библиотеки программного обеспечения для ИС, а OEM-разработчики могут использовать их при разработке собственного кода приложения. Защита от считывания проприетарного кода помогает обеспечить конфиденциальность стороннего программного обеспечения. Другими словами, PCRDP заключается в предотвращении чтения конфиденциального кода вредоносным программным обеспечением или отладчиками. Защищённая область предназначена только для выполнения и может быть доступна только центральному процессору ИС в виде кода инструкции, в то время как все другие виды доступа (DMA; отладка; чтение, запись и стирание данных с использованием центрального процессора) строго запрещены.

Защищённые области от считывания кода во флэш-памяти определяются байтами опций.

После определения областей PCRDP единственным способом отключить эту функцию защиты является изменение уровня защиты RDP с «1» на «0», что стирает всю флэш-память.

4.3 Защита от записи WRP

Механизм защиты флэш-памяти от записи предназначен для предотвращения нежелательного доступа для записи к определённым областям флэш-памяти, таким как загрузчик или константы калибровки, которые не изменяются. Области защиты от записи определяются битами регистров опций. Операции стирания обрабатываются как операции записи в защищённых областях, то есть они не разрешены.

Заключение

Специальное встроенное программное обеспечение является важной частью доверенной интегральной микросхемы с программно-аппаратной архитектурой и играет ключевую роль в обеспечении доверенной цепочки поставки, поддержки операций безопасной загрузки и запуска программного обеспечения ПАК.

Специальное встроенное программное обеспечение используется для целей тестирования во время производства микросхемы, а также предоставляет дополнительные функции, облегчающие использование аппаратных компонент при производстве и эксплуатации радиоэлектронного устройства.

Специальное встроенное программное обеспечение является зоной ответственности разработчика интегральной микросхемы и должно быть загружено/активировано в процессе изготовления ИС.

Для эффективной реализации функций поддержки цепочки доверия и операций строгой аутентификации компонентов ПАК необходимо использовать технологии криптографической защиты информации, PKI и корня доверия (RoT). Необходимый уровень доверия можно достичь только за счёт взаимного рационального использования аппаратных и программных методов обеспечения технологической, функциональной и информационной безопасности.

При организации распределённого серийного производства доверенных ПАК задача унификации набора функций и интерфейсов взаимодействия со специальным встроенным программным обеспечением ЭКБ становится актуальной задачей, требующей особого внимания при разработке линейки серийных доверенных микросхем и ПАК на их основе.

СПИСОК ЛИТЕРАТУРЫ

1. Veena S. Chakravarthi, Shivananda R. Koteshwar, System on Chip (SOC) Architecture. A Practical Approach. Springer Cham, ISBN 978-3-031-36241-5, August 2023. – 159 p. DOI: https://doi.org/10.1007/978-3-031-36242-2.
2. Рогожин К.В. Отечественные процессоры и микропроцессоры в цифровых вычислительных устройствах. Системы управления и обработки информации. 2021, № 3(54), с. 76–81. – EDN: HULDLK.
3. Lee E.A. and Seshia S.A. Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, ISBN 978-0-262-53381-2, 2017. URL: https://ptolemy.berkeley.edu/books/leeseshia/releases/LeeSeshia_DigitalV2_2.pdf (дата обращения: 07.10.2024).
4. Бондарев А. Операционные системы. какая она - идеальная ОС для встроенных систем? Системный администратор. 2020, № 12(217), с. 16–21. – EDN: NZHMYI.
5. Югансон А.Н., Заколдаев Д.А. Подход к оценке защищенности встроенного программного обеспечения в условиях нечеткости входной информации. Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2020, № 1, с. 50–56. DOI: 10.24143/2072-9502-2020-1-50-56. – EDN: DWIPLR.
6. Chen Li; Dey S.; Sanchez P.; Sekar K.; Chen Ying. Embedded Hardware and Software Self-Testing Methodologies for Processor Cores. IEEE Xplore: 06 August 2002. DOI: 10.1145/337292.337599.
7. Abdil Rashid Abdil Rashid Mohamed. Built-In Self-Test (BIST) Built-In Self-Test (BIST). Embedded Systems Laboratory (ESLAB) Embedded Systems Laboratory (ESLAB). Linköping Linköping University, Sweden University, Sweden. URI: https://www.ida.liu.se/~zebpe83/teaching/test/lec12.pdf (дата обращения: 10.09.2024).
8. Белоус А., Солодуха В. Доверенная ЭКБ для доверенных аппаратно-программных платформ: проблемы и пути решения. Часть 1. Электроника: наука, технология, бизнес. 2021, № 3(204), с. 98–104. DOI: 10.22184/1992-4178.2021.204.3.98.104. – EDN: LSUULG.
9. Белоус А., Солодуха В. Доверенная ЭКБ для доверенных аппаратно-программных платформ: проблемы и пути решения. Часть 2. Электроника: наука, технология, бизнес. 2021, № 4(205), с. 72–77. DOI: 10.22184/1992-4178.2021.205.4.72.76. – EDN: BKANKK.
10. Марков А.С. Важная веха в безопасности открытого программного обеспечения. Вопросы кибербезопасности. 2023, № 1(53), с. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12. – EDN: OHYLTR.

11. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. Монография ISBN: 978-5-9912-0213-8 Горячая линия – Телеком. 2011. – 248 с. – EDN: KWAAHG.
12. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Новый подход к разработке алгоритмов многомерной криптографии. Вопросы кибербезопасности. 2023, № 2(54), с. 52–64. DOI: 10.21681/2311-3456-2023-2-52-64. – EDN: JXHQMI.
13. Беляев С.С., Будько М.Б., Будько М.Ю., Гирик А.В., Грозов В.А. Построение функции генерации криптографически стойких псевдослучайных последовательностей на базе алгоритма шифрования «Кузнечик». Вопросы кибербезопасности. 2021, № 4(44), с. 25–34. DOI: 10.21681/2311-3456-2021-4-25-34. – EDN: GBNJBU.
14. Малышев В.А., Толстых А.В., Алейников С.А. Унификация автоматизированных систем военного назначения за счёт специального программного обеспечения, реализованного на микросервисной архитектуре. Моделирование, оптимизация и информационные технологии. 2022;10(3). DOI: 10.26102/2310-6018/2022.38.3.010.

REFERENCES:

[1] Veena S. Chakravarthi, Shivananda R. Koteshwar, System on Chip (SOC) Architecture. A Practical Approach. Springer Cham, ISBN 978-3-031-36241-5, August 2023. – 159 p. DOI: https://doi.org/10.1007/978-3-031-36242-2.
[2] Rogozhin K.V. Domestic processors and microprocessors in digital computing devices. Information management and processing systems. 2021, no. 3(54), p. 76–81 (in Russian). – EDN: HULDLK.
[3] Lee E.A. and Seshia S.A. Introduction to Embedded Systems - A Cyber-Physical Systems Approach, Second Edition, MIT Press, ISBN 978-0-262-53381-2, 2017. URL: https://ptolemy.berkeley.edu/books/leeseshia/releases/LeeSeshia_DigitalV2_2.pdf (accessed: 07.10.2024).
[4] Bondarev A. Operating systems. what is the ideal OS for embedded systems? System Administrator. 2020, no. 12(217), p. 16–21 (in Russian). – EDN: NZHMYI.
[5] Yuganson A.N., Zakoldaev D.A. An approach to assessing the security of embedded software in conditions of fuzzy input information. Bulletin of the AGTU. Ser.: Management, computer engineering and computer Science. 2020, no. 1, p. 50–56. DOI: 10.24143/2072-9502-2020-1-50-56 (in Russian). – EDN: DWIPLR.
[6] Chen Li; Dey S.; Sanchez P.; Sekar K.; Chen Ying. Embedded Hardware and Software Self-Testing Methodologies for Processor Cores. IEEE Xplore: 06 August 2002. DOI: 10.1145/337292.337599.
[7] Abdil Rashid Abdil Rashid Mohamed. Built-In Self-Test (BIST) Built-In Self-Test (BIST). Embedded Systems Laboratory (ESLAB) Embedded Systems Laboratory (ESLAB). Linköping Linköping University, Sweden University, Sweden. URI: https://www.ida.liu.se/~zebpe83/teaching/test/lec12.pdf (accessed: 10.09.2024).
[8] Belous A., Solodukha V. Trusted ECB for trusted hardware and software platforms: problems and solutions. Part 1. Electronics: science, technology, business. 2021, no. 3(204), p. 98–104. DOI: 10.22184/1992-4178.2021.204.3.98.104 (in Russian). – EDN: LSUULG.
[9] Belous A., Solodukha V. Trusted ECB for trusted hardware and software platforms: problems and solutions. Part 2. Electronics: science, technology, business. 2021, no. 4(205), p. 72–77. DOI: 10.22184/1992-4178.2021.205.4.72.76 (in Russian). – EDN: BKANKK.
[10] Markov A.S. An important milestone in the security of open source software. Cybersecurity issues. 2023, no. 1(53), p. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12 (in Russian). – EDN: OHYLTR.
[11] Gorbatov V.S., Polyanskaya O.Y. Fundamentals of PKI technology. Monograph ISBN: 978-5-9912-0213-8 Hotline – Telecom. 2011. – 248 p. (in Russian). – EDN: KWAAHG.
[12] Moldovyan A.A., Moldovyan D.N., Moldovyan N.A. A new approach to the development of algorithms for multidimensional cryptography. Cybersecurity issues. 2023, no. 2(54), p. 52–64. DOI: 10.21681/2311-3456-2023-2-52-64 (in Russian). – EDN: JXHQMI.
[13] Belyaev S.S., Budko M.B., Budko M.Yu., Girik A.V., Grozov V.A. Construction of a cryptographically stable pseudorandom sequence generation function based on the "Grasshopper" encryption algorithm. Cybersecurity issues. 2021, no. 4(44), p. 25–34. DOI: 10.21681/2311-3456-2021-4-25-34 (in Russian). – EDN: GBNJBU.
[14] Malyshev V.A., Tolstykh A.V., Aleynikov S.A. Unification of automated systems for military purposes by means of special software implemented using microservice architecture. Modeling, Optimization and Information Technology. 2022;10(3). DOI: 10.26102/2310-6018/2022.38.3.010 (in Russian).

Поступила в редакцию – 08 октября 2024 г. Окончательный вариант – 16 ноября 2024 г.
Received – October 08, 2024. The final version – November 16, 2024.