УДК 004.056.53

А.А. Конев

Модель угроз безопасности защищенного микроконтроллера и обрабатываемой им информации

Рассмотрены и разбиты на категории угрозы, позволяющие получить доступ к хранящимся и обрабатываемым на защищенном микроконтроллере данным с целью скомпрометировать конечное устройство. Категории включают угрозы, направленные на саму информацию, обрабатываемую на микроконтроллере, и угрозы, направленные непосредственно на сам микроконтроллер и его компоненты. Полученная модель угроз позволяет формализовать построение перечня угроз для дальнейшего формирования требований безопасности, предъявляемых к микроконтроллеру во время его разработки, и критериев оценки его защищённости на этапе тестирования.
Ключевые слова: модель угроз, доверие, микросхема, конфиденциальность.
DOI: 10.21293/1818-0442-2022-25-4-80-87

В настоящее время «умные» устройства получили широкое распространение в различных сферах, таких как интернет вещей, автомобильная промышленность, «умные» сети, индустрия пластиковых карт и многие другие. В связи с этим необходимо обеспечивать определенный уровень защищенности, чтобы избежать потенциального нарушения функционирования автоматизированных систем из-за вмешательства злоумышленника.

Для решения проблем безопасности все чаще применяются аппаратные методы обеспечения защищенности устройств. Устройства, реализующие аппаратные механизмы защищенности, известны как защищенные микроконтроллеры [1]. Аппаратная реализация механизмов безопасности показывает высокую эффективность при низком потреблении ресурсов приложений интернета вещей [2]. Также в защищенных микроконтроллерах применяются меры для защиты от внешнего воздействия на микросхему с целью получения доступа к хранящимся или обрабатываемым данным.

Построение модели угроз безопасности защищенного микроконтроллера и обрабатываемой им информации позволяет обнаружить и устранить потенциальные уязвимости на этапе разработки микросхемы и ПО к ней. Построение модели угроз выполняется в несколько шагов – сначала описывается система, выявляются компоненты системы и связи между ними, а потом для каждого элемента составляется перечень угроз.

Под угрозами безопасности понимаются угрозы несанкционированного изменения состояния автоматизированной системы или ее структуры [3], а также несанкционированного доступа к системе (например, угроза несанкционированной замены компонентов и др. [4]). Также угрозы можно разделить на две категории: угрозы безопасности непосредственно системы и угрозы безопасности средствам защиты информации системы.

Проблема построения модели угроз состоит в сложности составления наиболее полного перечня потенциальных угроз для защищаемого объекта. Существующие модели угроз не описывают в полной мере всевозможные угрозы безопасности. Так, в статьях [5–7] представлены списки угроз для устройств интернета вещей, однако они не охватывают все возможные угрозы, потому что при составлении списка угроз не применяется системный подход к построению модели угроз.

Целью данной статьи является демонстрация системного подхода к описанию угроз на примере защищенного микроконтроллера.

Описание типовой защищенной микросхемы

Защищенная микросхема представляет собой программно-аппаратный модуль, предназначенный для обеспечения безопасного хранения и передачи информационных ресурсов (представляющих собой определенную ценность), реализующих выполнение базовых криптографических функций, а также возможность обеспечения доверенного привилегированного управления.

Типовая защищенная микросхема представляет собой [8, 9] интегрированные между собой компоненты: 32-битный (либо 64) RISC-процессор, а также криптографический сопроцессор с возможностью выполнения различных алгоритмов шифрования, например, RSA, ECC, AES, DES, ГОСТ Р 34.12–2015 и др. Как правило, микросхема имеет до 30 КБ статической оперативной памяти (SRAM) и до 1 МБ энергонезависимой памяти, а также защищенный блок управления памятью (MMU). Структура защищенной микросхемы включает в себя различные периферийные интерфейсы для обеспечения взаимодействия с внешней средой, блок управления питанием и генераторы тактовой частоты для обеспечения работы процессора.

Упрощенная блок-схема защищенной микросхемы представлена на рис. 1.

Построение модели угроз

В литературе [10–14], посвященной описанию угроз микросхемы, обычно рассматривают существующие способы проведения атак и механизмы обеспечения защиты. В работе [15] дополнительно рассматриваются источники появления угроз, такие как персонал, несанкционированные компоненты, вредоносное ПО и направления проведения атак на микросхему.

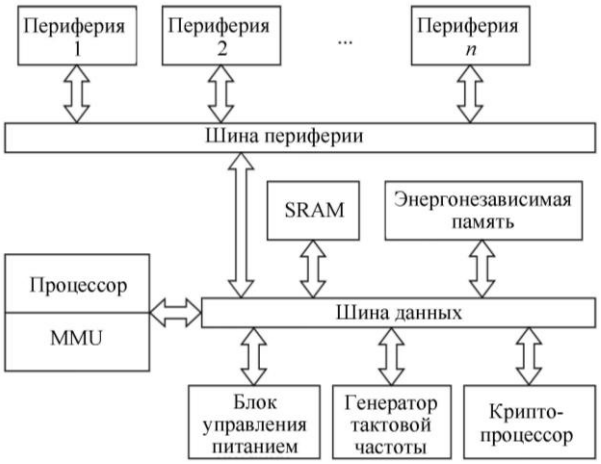

Рис. 1. Структурная схема типовой защищенной микросхемы

Основываясь на моделях, представленных в статьях [3, 4], была представлена модель угроз, которая описывает все потенциально возможные угрозы для защищенных микроконтроллеров за счет выделения отдельных компонентов (и разделения их на те, которые работают или не работают с информацией) и за счет разделения угроз по целям безопасности – конфиденциальности, целостности и защищенности (рис. 2).

Вкратце эту модель угроз можно выразить формулой

$$G = (C_i, CT_i, SG_i),$$

где C_i – наименование компонента, CT_i – тип компонента (взаимодействует с информацией, не взаимодействует с информацией), SG_i – цели безопасности (конфиденциальность, целостность, доступность).

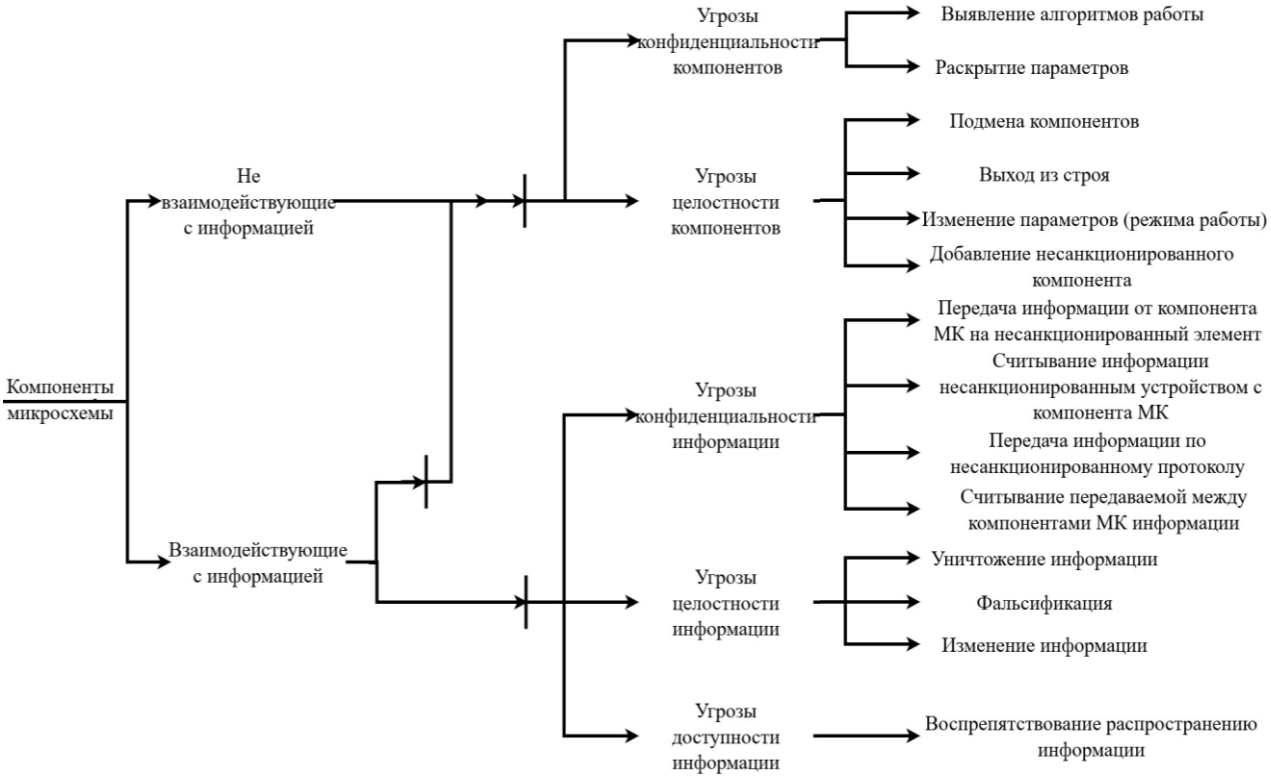

Рис. 2. Категории угроз

В связи с тем, что разработка аппаратной архитектуры микросхемы происходит до либо во время разработки программного обеспечения, невозможно обеспечить исправление аппаратных уязвимостей путем обновления по аналогии с обновлением программного обеспечения. Разработка аппаратного и программного обеспечения должна вестись с учётом всех рисков реализации угроз безопасности в аппаратной архитектуре защищенных микросхем, обеспечивая превентивное решение для достижения высокого уровня доверия.

Для определения характера и направленности потенциальной угрозы введены следующие категории: угрозы конфиденциальности компонентов (УКК) микросхемы, угрозы целостности компонентов (УЦК) микросхемы, угрозы конфиденциальности информации (УКИ), угрозы целостности информации (УЦИ) и угрозы доступности информации (УДИ).

Разделение на данные категории обусловлено возможностью нарушения одного из свойств обеспечения информационной безопасности. Например, для категории УКК актуальны угрозы, связанные с нарушением конфиденциальности архитектурных особенностей непосредственно самих компонентов защищенной микросхемы. Зная структурные особенности реализации компонентов микросхемы, злоумышленник может попытаться изменить режим функционирования микросхемы и впоследствии несанкционированно овладеть конфиденциальной информацией. Также непосредственно сами компоненты могут стать целью злоумышленников, так как

они представляют собой интеллектуальную собственность.

Для компонентов микросхемы, взаимодействующих с информацией, помимо угроз конфиденциальности и целостности компонентов существуют угрозы, связанные с конфиденциальностью, целостностью и доступностью информации.

Для компонентов микросхемы, не взаимодействующих с информацией, существуют только угрозы, связанные с конфиденциальностью и целостностью компонентов микросхемы.

К категории угроз конфиденциальности компонентов (УКК) относятся угрозы, связанные с несанкционированным и вредоносным воздействием на элементы МК с целью нарушения их конфиденциальности (табл. 1).

Таблица 1

Угрозы конфиденциальности компонентов

Наименование	Описание
Выявление алгоритмов работы	К данной подкатегории относятся угрозы, связанные с выявлением информации об алгоритмах работы компонентов МК и использованием ее для реализации атаки на устройство
Раскрытие параметров	К данной подкатегории относятся угрозы, связанные с раскрытием информации о параметрах компонентов МК и использованием ее для осуществления успешной атаки на устройство

К категории угроз целостности компонентов (УЦК) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения их целостности (табл. 2).

Таблица 2

Угрозы целостности компонентов

Наименование	Описание
Подмена компонентов	К данной подкатегории относятся угрозы, связанные с подменой компонентов МК на компоненты, содержащие определенные уязвимости, на этапе проектирования либо на этапе производства микросхемы
Выход из строя	К данной подкатегории относятся угрозы, связанные с уничтожением или отключением компонентов МК
Изменение параметров (режима работы)	К данной подкатегории относятся угрозы, связанные с изменением параметров (режима работы) компонентов МК
Добавление несанкционированного компонента	К данной подкатегории относятся угрозы, связанные с добавлением новых компонентов, содержащих определенные уязвимости, на этапе проектирования либо на этапе производства микросхемы

К категории угроз конфиденциальности информации (УКИ) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения конфиденциальности информации, хранящейся на данном компоненте (табл. 3).

К категории угрозы целостности информации (УЦИ) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения целостности информации, хранящейся на данном компоненте (табл. 4).

К категории угроз доступности информации (УДИ) относятся угрозы, связанные с вредоносным воздействием на компоненты МК с целью нарушения доступности передаваемой информации (табл. 5).

Таблица 3

Угрозы конфиденциальности информации

Наименование	Описание
Передача информации от компонента МК на несанкционированный элемент	К данной подкатегории относятся угрозы, связанные с передачей информации от компонента МК на несанкционированный элемент, внедренный злоумышленником
Считывание информации несанкционированным устройством с компонента МК	К данной подкатегории относятся угрозы, связанные со считыванием информации несанкционированным устройством с компонента МК
Передача информации по несанкционированному протоколу	К данной подкатегории относятся угрозы, связанные с передачей информации по каналу, который не обеспечивает должный уровень защиты передаваемой информации
Считывание передаваемой между компонентами МК информации	К данной подкатегории относятся угрозы, связанные с воздействием на каналы передачи данных между компонентами МК, например, с помощью электромагнитного излучения

Таблица 4

Угрозы целостности информации

Наименование	Описание
Уничтожение информации	К данной подкатегории относятся угрозы, связанные с уничтожением хранимой на компонентах МК информации
Фальсификация	К данной подкатегории относятся угрозы, связанные с подменой информации, хранящейся на компонентах МК
Изменение информации	К данной подкатегории относятся угрозы, связанные с изменением информации вследствие помех или намеренной модификации

Таблица 5

Угрозы доступности информации

Наименование	Описание
Воспрепятствование распространению информации	К данной подкатегории относятся угрозы, связанные с доступностью информации

На рис. 2 представлена блок-схема категорий угроз. Таблицы 6–10 содержат примеры угроз с описанием для каждой категории угроз.

Таблица 6

Угроза конфиденциальности компонентов

Ид.	Наименование угрозы	Описание
УКК1.1	Угроза предсказания результатов генератора случайных чисел	Угроза заключается в возможности обнаружения уязвимостей в алгоритмах генерации псевдослучайных либо случайных чисел, а также непосредственно в реализациях данных компонентов микросхемы. Данная угроза обусловлена недостаточным уровнем надежности алгоритмов генерации псевдослучайных либо случайных чисел, а также наличием уязвимостей непосредственно в самих реализуемых компонентах микросхемы. Реализация угрозы возможна при наличии у злоумышленника сведений о применяемых в микросхеме механизмах генерации псевдослучайных либо случайных чисел, а также сведений о реализованных в них алгоритмах, конфигурационных параметрах, на основании которых злоумышленник может делать предсказания
УКК1.2	Угроза выявления слабостей реализации криптографических алгоритмов	Угроза заключается в возможности определения уязвимостей криптографических алгоритмов, а также уязвимостей непосредственно самих компонентов, реализующих данные алгоритмы. Данная угроза обусловлена недостаточным уровнем надежности криптографического алгоритма, а также ошибками проектирования криптографических компонентов, уязвимостями в линиях взаимодействий с внешними компонентами, неправильными параметрами конфигурации. Реализация угрозы возможна при наличии у злоумышленника сведений о применяемых в микросхеме механизмах шифрования, а также их алгоритмах и конфигурационных параметрах
УКК1.3	Угроза выявления уязвимостей в реализации ядра	Угроза заключается в возможности определения уязвимостей в архитектуре ядра микросхемы, а также уязвимостей в реализующих данную архитектуру компонентах микросхемы. Данная угроза обусловлена недостаточным уровнем надежности реализации архитектурных возможностей ядра микросхемы. Реализация угрозы возможна при наличии у злоумышленника сведений об архитектуре ядра либо сведений о реализации данной архитектуры на компоненте микросхемы
УКК1.4	Угроза выявления уязвимостей в реализации запоминающих компонентов	Угроза заключается в возможности определения уязвимостей запоминающих устройств микросхемы. Данная угроза обусловлена наличием уязвимостей реализации механизмов запоминающих устройств либо наличием неправильных конфигурационных параметров. Реализация угрозы возможна при наличии у злоумышленника сведений об архитектуре запоминающих устройств, при существовании уязвимостей в линиях взаимодействия с внешними компонентами, а также при неправильных параметрах конфигурации
УКК1.5	Угроза обнаружения недекларированных возможностей	Угроза заключается в возможности определения незаявленных либо не соответствующих описанию в документации функциональных возможностей. Данная угроза обусловлена неправильным подходом к разработке защищенных микросхем, устаревшей документации либо несанкционированным внедрением аппаратных закладок в архитектуру компонента микросхемы. Реализация угрозы возможна при наличии у злоумышленника сведений о недекларированных возможностях, либо функциях, не соответствующих заявленной документации
УКК2.1	Угроза определения параметров объектов защиты	Угроза заключается в возможности определения конфигурационных параметров защищенных компонентов, механизмов обеспечения шифрования и других компонентов, связанных с криптографией. Данная угроза обусловлена неправильной установкой конфигурационных параметров либо использованием слабых значений защитных механизмов. Реализация угрозы возможна при наличии у злоумышленника сведений об уязвимостях механизмов защиты
УКК2.2	Угроза определения режима работы ядра	Угроза заключается в возможности определения режима работы устройства для последующего анализа функционирования встроенной программы. Данная угроза обусловлена использованием слабых или неправильных значений параметров конфигурации работы ядра. Реализация угрозы возможна в случае наличия у злоумышленника физического доступа к устройству для выполнения инвазивного либо неинвазивного анализа целевого устройства

Таблица 7

Угрозы целостности компонентов

Ид.	Наименование угрозы	Описание
УЦК1.1	Угроза подделки компонента	Угроза заключается в возможности подмены легитимного компонента на сторонний компонент. Данная угроза обусловлена недостаточным контролем на этапе разработки и производства компонентов микросхемы. Реализация угрозы возможна в случае использования сторонних либо недоверенных компонентов (например, лицензируемых компонентов с неизвестной реализацией архитектуры, а также при использовании зарубежных IP-блоков, произведенных на зарубежных мощностях)
УЦК1.2	Угроза подмены компонента разработки	Угроза заключается в возможности подмены легитимных компонентов отладки и разработки (JTAG, SWD), имеющих привилегированный доступ к различным ресурсам микросхемы, на сторонний компонент. Данная угроза обусловлена недостаточным контролем на этапе разработки и производства компонентов микросхемы. Реализация угрозы возможна в случае использования сторонних либо недоверенных компонентов (например, лицензируемых компонентов с неизвестной реализацией архитектуры)
УЦК2.1	Угроза намеренного вывода из строя компонента	Угроза заключается в возможности вывода из строя компонента, путем вредоносного воздействия на физическую структуру данного компонента. Данная угроза обусловлена недостаточным контролем на этапе разработки и производства компонентов микросхемы. Реализация угрозы возможна в случае использования сторонних либо недоверенных компонентов (например, лицензируемых компонентов с неизвестной реализацией архитектуры)
УЦК2.2	Угроза случайного вывода из строя компонента	Угроза заключается в возможности непреднамеренного вывода из строя компонента путем повреждения физической структуры компонента из-за поражения статическим зарядом либо ввиду неправильной конфигурации. Данная угроза обусловлена недостаточным уровнем обеспечения защиты компонента либо отсутствующим механизмом защиты компонента микросхемы. Реализация угрозы возможна в случае отсутствия требуемой компетенции проектировщиков либо разработчиков компонентов микросхемы
УЦК2.3	Угроза намеренного отключения компонента	Угроза заключается в возможности отключения компонента путем вредоносного воздействия на структуру данного компонента. Данная угроза обусловлена недостаточным уровнем обеспечения защиты от несанкционированного вторжения. Реализация угрозы возможна в случае наличия физического доступа злоумышленника к компонентам системы
УЦК2.4	Угроза случайного отключения компонента	Угроза заключается в возможности непреднамеренного отключения компонента путем повреждения физической структуры компонента из-за поражения статическим зарядом. Данная угроза обусловлена непродуманной системой конфигурации микросхемы. Реализация угрозы возможна в случае отсутствия должных компетенций у проектировщиков либо разработчиков компонентов микросхемы
УЦК3.1	Угроза несанкционированного изменения режима работы компонента	Угроза заключается в возможности несанкционированной модификации режима функционирования компонентов микросхемы. Изменение режима функционирования может быть достигнуто за счёт изменения параметров функционирования микросхемы, таких как частота и входное напряжение. Данная угроза обусловлена недостаточным уровнем обеспечения защиты от вредоносного инвазивного и неинвазивного воздействия. Реализация угрозы возможна в случае, когда злоумышленнику известно расположение компонентов и их назначение
УЦК4.1	Угроза добавления несанкционированного/вредоносного компонента	Угроза заключается в возможности занесения уязвимостей и слабостей вместе с добавлением несанкционированного компонента. Данная угроза обусловлена отсутствием контроля на этапе проектирования и производства МК. Реализация угрозы возможна в случае использования зарубежных IP-блоков, проектирования МК иностранными специалистами и производстве МК на чужих мощностях

Таблица 8

Угрозы конфиденциальности информации

Ид.	Наименование угрозы	Описание
УКИ1.1	Угроза НСД к информации	Угроза заключается в возможности получения несанкционированного доступа к информации путем подмены принимающего компонента МК. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, а также возможностью злоумышленника подключиться к внешним выводам интерфейсов связи. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для НСД к информации, передаваемой между компонентами МК или МК и внешним устройством
УКИ2.1	Угроза считывания содержимого ОЗУ несанкционированным устройством	Угроза заключается в возможности получения несанкционированного доступа к информации путем подключения ОЗУ МК к внешнему элементу, выдающему себя за компонент МК. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для считывания содержимого ОЗУ
УКИ3.1	Угроза передачи данных по незащищенному каналу (интерфейсу)	Угроза заключается в возможности получения несанкционированного доступа к информации, передаваемой по интерфейсу, не обеспечивающему соответствующий уровень защищенности. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, а также возможностью злоумышленника подключиться к внешним выводам интерфейсов связи. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для НСД к информации, передаваемой по незащищенному каналу между компонентами МК или МК и внешним устройством
УКИ3.2	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности отключения мер защиты канала связи для дальнейшего считывания передаваемой по нему информации. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, а также возможностью злоумышленника подключиться к внешним выводам интерфейсов связи. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для отключения мер защиты канала связи и НСД к информации, передаваемой между компонентами МК или МК и внешним устройством
УКИ4.1	Угроза перехвата данных	Угроза заключается в возможности получения несанкционированного доступа к информации путем утечки информации по электромагнитным и электрическим каналам, возникающим за счет побочных электромагнитных излучений передачи информации. Данная угроза обусловлена незащищенной от внешнего воздействия реализацией компонентов МК, отсутствием экранирования. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для считывания передаваемой между компонентами МК информации

Таблица 9

Угрозы целостности информации

Ид.	Наименование угрозы	Описание
1	2	3
УЦИ1.1	Угроза несанкционированного удаления информации	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы хранимая на нем информация была удалена. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для удаления информации

Окончание табл. 9

1	2	3
УЦИ2.1	Угроза подмены данных	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы на него была добавлена фальшивая информация. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для подмены информации
УЦИ3.1	Угроза несанкционированной модификации данных	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы хранимая на нем информация была изменена. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме и наличии физического доступа к МК, позволяющего применить инвазивный метод для изменения информации
УЦИ3.2	Угроза нарушения целостности данных в связи с помехами	Угроза заключается в возможности злоумышленника воздействовать на компонент МК таким образом, чтобы передаваемая по нему информация была изменена случайным образом вследствие помех. Данная угроза обусловлена не защищенной от внешнего воздействия реализацией компонентов МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, наличии физического доступа к МК и специальной аппаратуры генерации помех

Таблица 10

Угрозы доступности информации

Ид.	Наименование угрозы	Описание
УДИ1.1	Угроза блокирования доступа к информации	Угроза заключается в возможности блокирования процесса обмена информацией между компонентами МК. Данная угроза обусловлена использованием не защищенного от блокирования канала, возможностью злоумышленника подключиться к внешним выводам интерфейсов связи, а также отсутствием резервного канала связи между компонентами МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для блокирования доступа к информации
УДИ1.2	Угроза отказа в обслуживании	Угроза заключается во вмешательстве в процесс обмена информацией между компонентами МК с целью подмены передаваемой информации. Данная угроза обусловлена использованием канала, к которому может подключиться злоумышленник и передавать данные для отказа в обслуживании, а также отсутствием резервного канала связи между компонентами МК. Реализация данной угрозы возможна при наличии у злоумышленника сведений о размещении компонентов МК на микросхеме, а также о размещении внешних выводов интерфейсов связи и наличии физического доступа к МК, позволяющего применить инвазивный и/или неинвазивный метод для организации отказа в обслуживании

Заключение

В статье были представлены 26 угроз получения доступа к хранящимся и обрабатываемым на защищенном микроконтроллере данным, из которых 12 угроз нарушения конфиденциальности, 12 угроз нарушения целостности и 2 угрозы нарушения доступности. Данные угрозы были разделены на категории в соответствии с особенностями компонентов, на которые они воздействуют, а именно на компоненты, которые обрабатывают или не обрабатывают информацию, а также на подкатегории согласно основным целям безопасности.

Статья подготовлена в рамках реализации программы ЛИЦ «Доверенные сенсорные системы» (договор № 009/20 от 10.04.2020) при финансовой поддержке Минкомсвязи России и АО «РВК». Идентификатор соглашения о предоставлении субсидии – 0000000007119P190002.

Литература

1. Lee B. Design and Implementation of Secure Cryptographic System on Chip for Internet of Things / B. Lee, I.-G. Lee, M. Kim // IEEE Access. – 2022. – Vol. 10. – P. 18730–18742.

2. Ramalingam S. A Holistic Systems Security Approach Featuring Thin Secure Elements for Resilient IoT Deployments / S. Ramalingam, H. Gan, G. Epiphaniou, E. Mistretta // Sensors. – 2020. – Vol. 20, No. 18. – P. 5252.

3. Новохрестов А.К. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин // Вестник Иркутского государственного технического университета. – 2017. – Т. 21, № 12. – С. 93–104.

4. Новохрестов А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады ТУСУР. – 2016. – Т. 19, № 3. – С. 111–114.

5. A survey on internet of things security: Requirements, challenges, and solutions / H. HaddadPajouh, A. Dehghantanha, R.M. Parizi, M. Aledhari, H. Karimipour // Internet of Things. – 2021. – Vol. 14. – P. 100129.

6. Security Considerations for Internet of Things: A Survey / A. Jurcut, T. Niculcea, P. Ranaweera, N.-A. Le-Khac // SN Computer Science. – 2020. – Vol. 1, No. 4. – P. 1–19.

7. Jurcut A.D. Introduction to IoT Security / A.D. Jurcut, P. Ranaweera, L. Xu // Wiley 5G Ref. – 2019. – P. 27–64.

8. Performance Analysis of Secure Elements for IoT / M. Noseda, L. Zimmerli, T. Schläpfer, A. Rüst // IoT. – 2021. – Vol. 3, No. 1. – P. 1–28.

9. Deshpande V. PulSec: Secure Element based framework for sensors anomaly detection in Industry 4.0 / V. Deshpande, L. George, H. Badis // IFAC-PapersOnLine. – 2019. – Vol. 52, No. 13. – P. 1204–1209.

10. Yu Q. Proactive Defense Against Security Threats on IoT Hardware / Q. Yu, Z. Zhang, J. Dofe // Modeling and Design of Secure Internet of Things. – 2020. – P. 407–433.

11. He Y. The Study on Hardware Security and Its Defense Measures // SHS Web Conf. – 2022. – Vol. 144. – P. 1–5.

12. Using Honeypots for ICS Threats Evaluation / N. Dutta N. Jadav N. Dutiya D. Joshi // Recent Developments on Industrial Control Systems Resilience – 2019 – P. 175–196.

13. Nagata M. Physical Attack Protection Techniques for IC Chip Level Hardware Security / M. Nagata, T. Miki, N. Miura // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. – 2022. – Vol. 30, No. 1. – P. 5–14.

14. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools / W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, H. Li // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2021. – Vol. 40, No. 6. – P. 1010–1038.

15. Flaus J.-M. Threats and Attacks to ICS // Cybersecurity of Industrial Systems. – 2019. – P. 91–120.

Конев Антон Александрович
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)
Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-3222-9956
Тел.: +7 (382-2) 70-15-29
Эл. почта: kaa@fb.tusur.ru

Konev A.A.

Security threat model for protected microcontroller and the information it processes

The threats that allow access to data stored and processed on a secure microcontroller in order to compromise the end device are considered and divided into categories. The categories include threats that target the proper information processed on the microcontroller and threats that target the microcontroller itself and its components directly. The resulting threat model allows formalizing the construction of a list of threats for further formation of security requirements for the microcontroller during its development, and criteria for assessing its security at the testing stage.

Keywords: threat model, trust, chip, privacy.
DOI: 10.21293/1818-0442-2022-25-4-80-87

References

1. Lee B., Lee I.-G., Kim M., Design and Implementation of Secure Cryptographic System on Chip for Internet of Things, IEEE Access, 2022, vol. 10. pp. 18730–18742.

2. Ramalingam S., Gan H., Epiphaniou G., Mistretta E., A Holistic Systems Security Approach Featuring Thin Secure Elements for Resilient IoT Deployments, Sensors, 2020, vol. 20, no. 18. MDPI AG, p. 5252.

3. Novokhrestov A. K., Konev A.A., Shelupanov A.A., N.S Egoshin. A Model of Threats to the Security of Information and its Carriers. *Vestnik of the Irkutsk State Technical University*, vol. 21, no. 12 (131), 2017, pp. 93–104 (in Russ.).

4. Novokhrestov A.K. et al. Model of threats to automatic system for commercial accounting of power consumption. *Proceedings of TUSUR University*, vol. 19, no. 3. Tomsk State University of Control Systems and Radioelectronics (TUSUR), pp. 111–114, 2016 (in Russ.).

5. HaddadPajouh H., Dehghantanha A., Parizi R. M., Aledhari M., Karimipour H. A survey on internet of things security: Requirements, challenges, and solutions, *Internet of Things*, 2021, vol. 14. Elsevier BV, p. 100129.

6. Jurcut A., Niculcea T., Ranaweera P., Le-Khac N.-A. Security Considerations for Internet of Things: A Survey. *SN Computer Science*, 2020, vol. 1, no. 4. Springer Science and Business Media LLC.

7. Jurcut A.D., Ranaweera P., Xu L. *Introduction to IoT Security*. Wiley 5G Ref. Wiley, 2019, pp. 1–39.

8. Noseda M., Zimmerli L., Schläpfer T., Rüst A. Performance Analysis of Secure Elements for IoT. *IoT*, 2021, vol. 3, no. 1, MDPI AG, pp. 1–28.

9. Deshpande V., George L., Badis H. PulSec: Secure Element based framework for sensors anomaly detection in Industry 4.0. *IFAC-PapersOnLine*, 2019, vol. 52, no. 13, Elsevier BV, pp. 1204–1209.

10. Yu Q., Zhang Z., Dofe J. Proactive Defense Against Security Threats on IoT Hardware, Modeling and Design of Secure Internet of Things, 2020, Wiley, pp. 407–433.

11. He Y. The Study on Hardware Security and Its Defense Measures. *SHS Web of Conferences*, 2022, vol. 144, EDP Sciences, p. 02011.

12. Dutta N., Jadav N., Dutiya N., Joshi D. Using Honeypots for ICS Threats Evaluation, Recent Developments on Industrial Control Systems Resilience. Springer International Publishing, pp. 175–196, 2019.

13. Nagata M., Miki T., Miura N. Physical Attack Protection Techniques for IC Chip Level Hardware Security. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2022, vol. 30, no. 1. Institute of Electrical and Electronics Engineers (IEEE), pp. 5–14.

14. Hu W., Chang C.-H., Sengupta A., Bhunia S., Kastner R., Li H. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2021, vol. 40, no. 6, pp. 1010–1038.

15. Flaus J.- M. Threats and Attacks to ICS, Cybersecurity of Industrial Systems. 2019, Wiley, pp. 91–120.

Anton A. Konev
Candidate of Science in Engineering, Assistant Professor,
Department of Complex Information Security of Electronic Computing Systems (KIBEVS), Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID 0000-0002-3222-9956
Phone: +7 (382-2) 70-15-29
Email: kaa@fb.tusur.ru