№5/2026

ADPI
Ilmiy xabarnomasi

ISSN 2181-4309

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ АППАРАТНЫХ СРЕДСТВ КЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Ортиков Муроджон
Андижанской государственный технический институт

Annotatsiya.
Ushbu maqolada axborotni kriptografik himoya qilish apparat vositalarini ruxsatsiz kirishdan himoya qilishning asosiy tahdidlari va usullari ko'rib chiqilgan. Himoyaning fizik, sxemotexnik va mantiqiy usullari tahlil qilingan. Korpusni ochishga javob berish mexanizmlari va yon kanallar (side-channel) orqali ma'lumotlarning sizib chiqishidan himoyalanishga alohida e'tibor qaratilgan.
Kalit so'zlar:
axborotni kriptografik muhofaza qilish, AKHV, ruxsatsiz kirish, apparat xavfsizligi, ochish datchiklari, yon kanallar.

Аннотация.
В данной статье всесторонне рассматривается роль логопедической среды в обеспечении всестороннего развития учащихся, обучающихся в инклюзивной системе образования на основе психологического подхода, и совершенствовании процесса предоставления им качественного образования, а также организация логопедической помощи в школах для детей с особыми образовательными потребностями и степень ее влияния на перспективы развития детей. Также описываются эффективные формы и методы организации логопедической помощи в инклюзивной среде с учетом индивидуальных особенностей каждого ребенка.
Ключевые слова:
криптографическая защита информации, КЗИ, несанкционированный доступ, НСД, аппаратная безопасность, датчики вскрытия, побочные каналы.

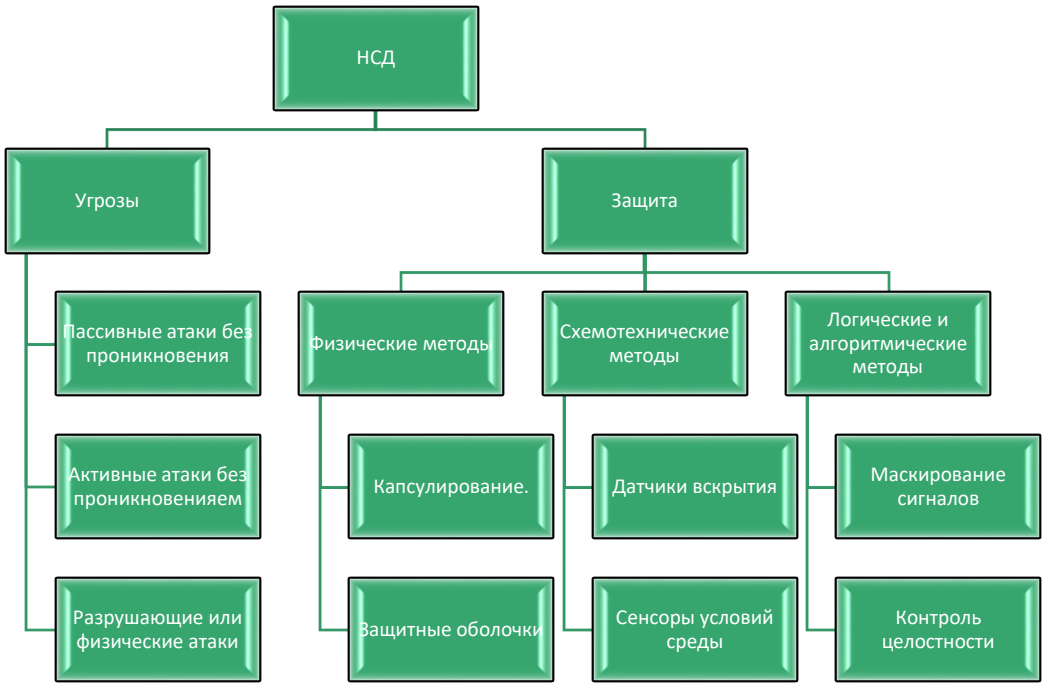
Abstract.
This article examines the key threats and methods for securing hardware cryptographic information protection (CIP) devices against unauthorized access (UA). Physical, circuit-level, and logical protection methods are analyzed. Special attention is paid to tamper-response mechanisms and protection against side-channel attacks.
Keywords:
cryptographic information protection, CIP, unauthorized access, UA, hardware security, tamper sensors, side channels.

Введение. Эффективность современных систем защиты информации во многом зависит от надежности криптографических ключей. Если злоумышленник получает физический доступ к аппаратному модулю безопасности (HSM, токенам, смарт-картам), возникает риск клонирования ключей или модификации логики устройства. В связи с этим разработка и применение методов защиты аппаратных средств КЗИ от НСД является критически важной задачей.

Аппаратные средства криптографической защиты информации (аппаратные СКЗИ) - это специализированные физические устройства и микросхемы, предназначенные для выполнения криптографических операций (шифрования, дешифрования, хеширования, генерации ключей и проверки электронных подписей) на аппаратном уровне. В отличие от чисто программных решений, они изолируют критически важные процессы и ключи внутри защищенной физической среды. Это делает невозможным перехват ключей через вредоносное ПО или оперативную память компьютера [1]. Не смотря на это, абсолютной защиты не существует: если программные угрозы здесь нивелируются, то на первый план выходит уязвимость

ISSN 2181-4309

самого оборудования перед несанкционированным доступом (НСД). Наличие физического контакта с устройством открывает злоумышленникам возможности для кражи, модификации или аппаратного анализа компонентов. Несанкционированный доступ (НСД) к средствам криптографической защиты информации (СКЗИ) - это доступ к самому криптографическому устройству, его ключевой информации или защищаемым данным, осуществляемый с нарушением установленных правил разграничения доступа, политик безопасности или действующего законодательства. Простыми словами: это ситуация, когда к СКЗИ или его ключам прикасается, подключается или управляет тот, кто не имеет на это законного права. Применительно к аппаратным средствам КЗИ, НСД имеет свою специфику, так как злоумышленник пытается обойти не только логические (пароли, права в ОС), но и физические барьеры. Визуализация всех значимых аспектов НСД представлена на следующей схеме, которая не только структурирует базовые элементы концепции, но и служит наглядным инструментом для их дальнейшего детального анализа.



Классификация угроз аппаратным средствам КЗИ

Пассивные атаки без проникновения - это скрытый класс угроз, при котором злоумышленник перехватывает конфиденциальные данные и секретные ключи путем измерения естественных физических параметров работающего устройства, полностью сохраняя его целостность и не оставляя никаких следов воздействия. В основе таких атак лежит высокоточный сбор информации по сторонним каналам, таким как колебания потребления электроэнергии процессором при обработке нулей и единиц, утечки электромагнитного излучения от внутренних компонентов, микроскопические изменения времени выполнения математических операций, а также акустические шумы от работы элементов питания на плате. Главная опасность данного подхода заключается в его абсолютной незаметности для встроенных датчиков вскрытия и систем логирования, что позволяет злоумышленнику с помощью доступного

коммерческого оборудования (осциллографов, зондов и направленных микрофонов) скомпрометировать СКЗИ, пока владелец уверен в его штатной и безопасной работе [2].

Активные атаки без проникновенияем называется класс угроз, при котором злоумышленник умышленно создает экстремальные внешние условия для нарушения штатной логики работы крипточипа, не разрушая при этом физическую целостность самого устройства. В основе таких методов лежит искусственное провоцирование кратковременных вычислительных ошибок (Fault Injection), которые заставляют процессор СКЗИ пропускать шаги проверки PIN-кодов, выдавать незашифрованные данные вместо криптограмм или использовать поврежденные ключи, что позволяет математически вычислить их оригинал. Для реализации атаки используются резкие скачки и просадки напряжения в линиях питания, манипуляции с тактовой частотой генератора, мощные электромагнитные импульсы, направленное радиочастотное излучение или экстремальный нагрев и охлаждение платы. Опасность данного подхода заключается в том, что устройство не получает необратимых физических повреждений и после перезагрузки продолжает функционировать нормально, однако криптографическая стойкость системы полностью компрометируется без видимых следов взлома.

Разрушающие или физические атаки - это наиболее радикальный класс угроз, при котором злоумышленник осуществляет прямое физическое проникновение во внутреннюю структуру крипточипа, полностью или частично разрушая защитную оболочку устройства для получения прямого доступа к его полупроводниковым компонентам. Реализация таких атак требует наличия дорогостоящего лабораторного оборудования (например, сфокусированных ионных пучков FIB, электронных микроскопов и химических кислот для декапсуляции кремниевого кристалла), с помощью которого удаляется защитный компаунд, нейтрализуются физические датчики вскрытия и огоняются внутренние шины данных. После проникновения атакующий может использовать микрозонды для прямого считывания битов секретного ключа из ячеек памяти в момент их передачи, физически модифицировать топологию микросхемы, пережигать лазером встроенные предохранители безопасности или подключаться к технологическим линиям отладки [3].

Методы защиты от НСД

Физические методы (Пассивная защита) - комплекс конструктивно-технологических решений, направленных на создание непреодолимых физических барьеров вокруг критических компонентов СКЗИ для предотвращения их визуального осмотра, инструментального зондирования и несанкционированной модификации. В отличие от механизмов активного реагирования, пассивная защита не требует электропитания и функционирует непрерывно с момента производства устройства. Ее главная задача — сделать стоимость и техническую сложность физического проникновения к крипточипу экономически невыгодными для злоумышленника, гарантируя разрушение структуры хранения данных при любых попытках преодоления защитных барьеров.

Капсулирование. Это метод защиты, заключающийся в заливке электронных компонентов и печатной платы СКЗИ специальными химическими составами (компаундами, эпоксидными смолами или керамическими материалами) для создания монолитного защитного слоя вокруг крипточипа. Плотная структура полимера делает

невозможным визуальный осмотр топологии платы, затрудняет доступ к контактам и препятствует бесконтактному съему информации. При попытке злоумышленника растворить или сколоть этот слой химическим или механическим путем происходит неизбежное физическое разрушение полупроводниковых кристаллов, печатных проводников и ячеек памяти, что приводит к полной потере работоспособности устройства и гарантирует уничтожение секретных ключей шифрования.

Защитные оболочки - это многослойные внешние барьеры, экраны и кожухи, окружающие критически важные узлы аппаратного модуля для предотвращения несанкционированного визуального, электромагнитного и механического доступа. Они изготавливаются из специализированных сплавов с высокой магнитной проницаемостью (например, пермаллоя), которые эффективно поглощают и рассеивают побочные электромагнитные излучения, полностью блокируя пассивные атаки методом ЕМ-анализа. Кроме того, внутренние поверхности таких оболочек часто покрываются токопроводящим рисунком-сеткой (матрицей из хрупких микропроводников), малейшее повреждение или изменение сопротивления которой при попытке сверления или вскрытия мгновенно регистрируется датчиками безопасности аппаратного модуля.

Схемотехнические методы (Активная защита) - это комплекс аппаратных и логических решений, обеспечивающих непрерывный автоматический мониторинг физического состояния СКЗИ и динамическое реагирование на любые попытки несанкционированного доступа. В отличие от пассивных барьеров, active-защита функционирует в режиме реального времени (в том числе при выключенном основном питании устройства за счет автономных батарей) и предназначена для оперативного обнаружения атак на ранней стадии. Главной целью схемотехнических методов является мгновенное уничтожение (затирание) критически важных данных и секретных ключей в энергозависимой памяти до того, как злоумышленник успеет извлечь их или завершить сессию взлома [4].

Датчики вскрытия (Тамперные цепи) - это специализированные электронные контуры и микропереключатели, которые контролируют геометрическую и механическую целостность корпуса СКЗИ. Они могут быть реализованы в виде подпружиненных кнопок, размыкающихся при снятии крышки, оптических элементов, фиксирующих появление света внутри закрытого корпуса, или непрерывных проводящих дорожек, нанесенных на внутренние стенки устройства. При любом нарушении непрерывности тамперной цепи — будь то сверление, сдвиг кожуха или обрыв защитной сетки — датчик мгновенно генерирует аппаратное прерывание, которое запускает процедуру экстренной очистки ключевой памяти (Zeroization) и блокирует работу устройства.

Сенсоры условий среды - это интегрированные в архитектуру крипточипа аппаратные датчики, предназначенные для обнаружения активных атак без проникновения (внесения сбоев) путем контроля физических параметров окружения. Они непрерывно измеряют внутреннюю температуру кристалла, стабильность тактовой частоты процессора, а также уровень и форму напряжения на линиях питания. Если злоумышленник пытается спровоцировать сбой в вычислениях с помощью экстремального замораживания платы, резкого скачка напряжения или радиочастотного импульса, сенсоры мгновенно фиксируют выход параметров за

ISSN 2181-4309

допустимые технологические границы и переводят СКЗИ в режим безопасной аппаратной блокировки, предотвращая компрометацию алгоритмов.

Логические и алгоритмические методы - это программно-математические способы защиты, реализуемые на уровне архитектуры криптографических алгоритмов и микрокода устройства для нейтрализации скрытых атак без проникновения. В отличие от физических барьеров, данные методы не пытаются остановить внешнее воздействие, а модифицируют сам процесс вычислений так, чтобы перехваченные физические сигналы или спровоцированные ошибки стали абсолютно бесполезны для злоумышленника. Главной целью логических методов является математическое скрытие корреляции между обрабатываемыми данными (секретными ключами) и физическими проявлениями работающего чипа, а также оперативное обнаружение любых искажений в структуре СКЗИ.

Маскирование сигналов называется метод защиты от атак по сторонним каналам (потребления энергии, радиоизлучения и времени), основанный на смешивании реального секретного ключа со случайными математическими величинами (масками) непосредственно в процессе выполнения криптооперации. Перед началом вычислений алгоритм случайным образом разделяет оригинальные данные на несколько независимых частей, которые обрабатываются процессором по отдельности, а финальный результат собирается обратно в исходный вид на самом последнем шаге. В результате такой случайной трансформации физический профиль устройства (например, осциллограмма тока или спектр излучения) каждый раз выглядит уникально, что полностью разрушает статистическую связь между потреблением энергии и битами секретного ключа, делая дифференциальный анализ (DPA) математически невозможным [5].

Контроль целостности - это комплекс алгоритмических процедур, направленных на непрерывную проверку подлинности и неизменности исполняемого микрокода, структуры памяти и логики работы аппаратного модуля СКЗИ. Он реализуется через регулярное вычисление и проверку криптографических контрольных сумм (хеш-функций или кодов аутентификации сообщений) для прошивки устройства как на этапе загрузки, так и в процессе выполнения циклов шифрования. Если злоумышленник пытается внедрить вредоносный код через атаку на цепочку поставок или спровоцировать кратковременный вычислительный сбой методом лазерного облучения (Fault Injection), система контроля мгновенно фиксирует несовпадение эталонной и текущей контрольных сумм, блокирует выполнение криптографической операции и переводит устройство в режим аварийной остановки.

Заключение

Аппаратные средства криптографической защиты информации (СКЗИ) представляют собой фундамент современной информационной безопасности, обеспечивая надежную изоляцию криптографических ключей от программных угроз и вредоносного ПО. Однако, как показал проведенный анализ, перенос критических вычислений в физическую среду порождает специфический класс угроз, связанных с несанкционированным доступом (НСД) непосредственно к оборудованию.

Современная классификация угроз включает в себя пассивные атаки по сторонним каналам, активные методы внедрения вычислительных сбоев, а также радикальные разрушающие (физические) атаки на полупроводниковые кристаллы. Столь широкий

спектр векторов взлома делает неэффективной защиту, основанную только на каком-то одном подходе.

Для обеспечения гарантированной безопасности аппаратных СКЗИ сегодня применяется исключительно эшелонированная (многоуровневая) система защиты, сочетающая в себе три ключевые группы методов:

- Физические (пассивные) методы (капсулирование и защитные оболочки) - создают долговременные барьеры, стремясь сделать взлом экономически нецелесообразным и технически трудновыполнимым.

- Схемотехнические (активные) методы (тамперные цепи и сенсоры среды) - непрерывно мониторят состояние устройства и мгновенно уничтожают секретные ключи при любой попытке физического вскрытия или искусственного изменения условий работы.

- Логические и алгоритмические методы (маскирование сигналов и контроль целостности) - математически скрывают связь между процессами в чипе и его физическими проявлениями, защищая СКЗИ от скрытого съема информации.

Таким образом, только системная интеграция физической стойкости, аппаратного самоконтроля и математического маскирования алгоритмов позволяет создавать современные криптографические модули, способные противостоять как рядовым нарушителям, так и высокотехнологичным атакам в условиях специализированных лабораторий.

Список литературы:

1. Что такое аппаратное СКЗИ и какие они бывают - Портал документации Рутокен - Сервер документации Рутокен
2. Kocher P., Jaffe J., Jun B. Differential Power Analysis // Advances in Cryptology — CRYPTO '99. — Springer, Berlin, Heidelberg, 1999. — Vol. 1666. — P. 388–397. *(Классический англоязычный источник по пассивным атакам).*
3. Горбачев А. А. Физико-химические методы анализа и деструктивного взлома интегральных схем аппаратных СКЗИ // Защита информации. Инсайд. — 2022. — № 4. — С. 18–25.
4. ГОСТ Р 58410-2019. Информационная технология. Криптографическая защита информации. Требования к средствам криптографической защиты информации, реализующим функции шифрования и имитозащиты. — М.: Стандартинформ, 2019.
5. Кузнецов А. В., Смирнов Д. М. Логические и алгоритмические методы противодействия дифференциальному анализу энергопотребления в крипточипах // Вопросы кибербезопасности. — 2023. — № 1 (49). — С. 52–60.