DOI: 10.58168/PBHT2026_104-113
УДК 004.777

АНАЛИЗ ФИЗИЧЕСКИХ МЕХАНИЗМОВ ФОРМИРОВАНИЯ ПОБОЧНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В СОВРЕМЕННЫХ МИКРОПРОЦЕССОРНЫХ СХЕМАХ

ANALYSIS OF THE PHYSICAL MECHANISMS OF SIDE-CHANNEL INFORMATION LEAKAGE FORMATION IN MODERN MICROPROCESSOR SYSTEMS

Абрасимовская А.Г., преподаватель СПО кафедры общей и прикладной физики, ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова», Воронеж, Россия

Abrasimovskaya A.G., College Teacher of the General and Applied Physics Department, Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia

Аннотация. В статье выполнен аналитический обзор физических механизмов, лежащих в основе формирования побочных каналов утечки информации в современных микропроцессорных системах. Показано, что утечка не сводится к отдельному физическому эффекту, а возникает как кросс-уровневое явление. Предложена обобщенная модель формирования побочного канала, на основе которой раскрыты особенности механизмов утечки. Обосновано, что усложнение архитектуры не устраняет утечки, а изменяет их форму, повышая значение гибридных атак, в которых один физический эффект преобразуется в другую наблюдаемую метрику, включая удаленно измеряемое время. Систематизированы современные меры противодействия и показаны их ограничения. Сделан вывод о необходимости многоуровневой защиты.

Ключевые слова: побочные каналы утечки информации, микроархитектурные атаки, временные атаки, анализ энергопотребления, электромагнитные излучения, тепловые каналы, спекулятивное исполнение, информационная безопасность, защита микропроцессорных систем.

Abstract. The article provides an analytical review of the physical mechanisms underlying the formation of side-channel information leakage in modern microprocessor systems. It is shown that leakage is not limited to a single physical effect, but emerges as a cross-layer phenomenon. A generalized model of side-channel formation is proposed, on the basis of which the specific features of leakage mechanisms are revealed. It is substantiated that increasing architectural complexity does not eliminate leakage, but changes its form, increasing the importance of hybrid attacks in which one physical effect is transformed into another observable metric, including remotely measurable time. Modern countermeasures are systematized and their limitations are shown. The conclusion is made that multi-level protection is necessary.

Keywords: side-channel information leakage, microarchitectural attacks, timing attacks, power analysis, electromagnetic emissions, thermal channels, speculative execution, information security, protection of microprocessor systems.

© Абрасимовская А. Г., 2026

Введение

Современные микропроцессорные системы являются базовой вычислительной платформой для большинства устройств и комплектов. При этом защита обрабатываемой информации больше не может рассматриваться исключительно как задача криптографического алгоритма или программной логики. Реальное выполнение вычислений сопровождается изменением времени доступа к ресурсам, переключением транзисторов, колебаниями тока, электромагнитным излучением, тепловыделением и остаточным сохранением зарядов в памяти. Эти физические проявления формируют класс побочных каналов, позволяющих восстанавливать секретные данные без прямого нарушения математической стойкости алгоритма [1-3].

Актуальность рассматриваемой темы определяется тремя обстоятельствами. Во-первых, современные процессоры становятся все более сложными, что повышает плотность состояний и число оптимизаций, потенциально зависящих от секретных данных. Во-вторых, растет доля мультиарендных и виртуализированных сред, где атакующий и жертва могут разделять аппаратные ресурсы без физического доступа друг к другу. В-третьих, последние исследования показывают тенденцию к гибридизации атак [9, 13-16].

Цель данной работы состоит в том, чтобы системно проанализировать физические механизмы формирования побочных каналов утечки информации в современных микропроцессорных системах и показать, каким образом эти механизмы проявляются на различных уровнях вычислительного стека.

Современное состояние исследований

В научной литературе по побочным каналам можно выделить несколько этапов развития. На первом этапе были сформированы базовые представления о том, что время исполнения и энергопотребление могут зависеть от секретных промежуточных состояний алгоритма. Работа П. Кохера по временным атакам стала поворотной точкой, показав возможность восстановления секретной информации на основе микроскопических различий во времени вычисления [2]. Вскоре была предложена методология дифференциального анализа мощности [3].

На втором этапе акцент сместился к общесистемным вычислительным платформам, где значимым источником утечки стала иерархия памяти. Атака FLUSH+RELOAD продемонстрировала высокоразрешающий и малошумный способ наблюдения за активностью жертвы через разделяемую кэш-память последнего уровня [4]. Далее микроархитектурные исследования расширились на предсказатели переходов, буферы трансляции адресов, структуры внеочередного исполнения и другие внутренние ресурсы процессора. Этот этап фактически доказал, что побочный канал может быть встроен в саму логику оптимизации производительности.

Третий этап был связан с транзиентным исполнением. Работы Meltdown и Spectre показали, что спекулятивно выполняемые операции, хотя и откатываются с архитектурной точки зрения, способны изменять микроархитектурное состояние процессора и, следовательно, оставлять наблюдаемые следы, пригодные для восстановления данных [5, 6].

Современные обзоры рассматривают побочные каналы как семейство тесно связанных механизмов, объединенных общим принципом секретозависимой модуляции наблюдаемого

сигнала. Так, исследования 2021-2025 гг. подробно анализируют угрозы для криптографических реализаций, разнородных вычислительных платформ, процессорных микроархитектур и блоков предсказания переходов [8, 10-12]. Эти работы показывают, что при классификации утечки необходимо учитывать уровень абстракции, доступную атакующему инфраструктуру, степень совместного использования аппаратных ресурсов и возможность удаленного измерения.

Несмотря на значительный прогресс, в литературе сохраняются три методологических разрыва. Во-первых, многие работы фокусируются на конкретной технике извлечения, но не раскрывают единый физический механизм возникновения утечки. Во-вторых, часто смешиваются побочные каналы и скрытые каналы, хотя последние предполагают непреднамеренную утечку [1]. В-третьих, недостаточно проработан вопрос о том, как один физический эффект преобразуется в другую наблюдаемую метрику, что особенно важно для современных гибридных атак.

Физические механизмы формирования побочных каналов

1. Обобщенная модель формирования утечки

Анализ литературы позволяет сформулировать обобщенную модель побочного канала. На входе имеется секрет S и вычислительная процедура F, внутри которой хотя бы часть операций выполняется по траектории, зависящей от S или от связанных с ним промежуточных величин. Эта зависимость изменяет внутреннее состояние аппаратной платформы H. Далее состояние H модулирует некоторый физический носитель P – время отклика, потребляемую мощность, электромагнитное поле, акустические колебания, температуру или сохранность битов в памяти. Наконец, атакующий измеряет наблюдаемую метрику O и строит процедуру вывода I(S|O), позволяющую восстановить секрет полностью или частично.

Таким образом, причина утечки – существование секретозависимой вариативности вычисления. Поэтому одинаково неверно сводить проблему только к алгоритму или только к аппаратуре.

С учетом сказанного, побочный канал целесообразно определять как непреднамеренный кросс-уровневый канал переноса информации, в котором секретозависимая вариативность вычисления преобразуется в измеряемый физический сигнал. Такое определение позволяет ясно отделить побочные каналы от скрытых каналов, где отправитель и получатель сознательно используют нештатный механизм передачи данных [1].

2. Временной и микроархитектурный механизм

Временной канал является наиболее универсальной формой внешнего наблюдения. Он возникает тогда, когда секретные данные влияют на длительность выполнения команды, последовательности команд или запроса к ресурсу. На уровне программной логики это может быть ветвление по условию, различная длина цикла, обращение к таблице по секретозависимому индексу либо обработка исключения. На уровне микроархитектуры временная вариативность создается конкуренцией за кэш-линии, буферы, конвейерные порты, блоки предсказания переходов и другие ресурсы [2, 10, 12].

Особую роль играет иерархия памяти. Разница между попаданием в кэш и обращением к более медленному уровню памяти хорошо измерима и потому давно используется как носитель утечки. В атаках типа FLUSH+RELOAD или PRIME+PROBE наблюдается не сам

секрет, а его влияние на состояние разделяемого ресурса, которое затем преобразуется во временную разницу [4, 11]. Иначе говоря, кэш здесь выступает промежуточным физико-логическим буфером, связывающим приватное вычисление жертвы и измерение атакующего.

Транзиентные атаки усилили это представление. В механизмах Meltdown и Spectre секрет извлекается потому, что спекулятивно выполненный фрагмент успевает закодировать информацию в состоянии кэша до архитектурного отката [5, 6]. Следовательно, фундаментальная утечка связана с асимметрией между архитектурной видимостью состояния и физической необратимостью микроархитектурных следов на коротком интервале времени.

Современные процессоры дополняют картину динамическим управлением частотой и напряжением. Работа Hertzbleed показала, что секретозависимая мощность может изменять частоту процессора, а значит, и общее время выполнения, превращая энергетическую зависимость в удаленно наблюдаемый временной канал [9].

Следовательно, временной механизм нельзя сводить лишь к программным ветвлениям. Отсюда следует и ограниченность простого требования постоянства времени: оно необходимо, но само по себе не гарантирует отсутствия утечки, если физическая среда исполнения остается секретозависимой.

3. Энергетический механизм

Энергетический механизм обусловлен тем, что динамическое потребление CMOS-схем зависит от активности переключений, эффективной емкости, напряжения и частоты. Когда различные значения обрабатываемых данных вызывают различающиеся паттерны коммутации транзисторов, формируется измеримая вариация мощности. В специализированных криптографических устройствах и смарт-картах такая зависимость уже давно используется в SPA и DPA-атаках [3].

Для микропроцессорных систем энергетический канал сложнее вследствие суперпозиции множества параллельных процессов. Однако именно эта сложность лишь изменяет модель статистической обработки. Современные исследования подтверждают, что при наличии достаточной выборки и адекватной модели наблюдения энергетическая утечка сохраняется и на высокопроизводительных ядрах [11].

Физически энергетическая утечка формируется в силовой сети кристалла и платы. Переключение внутренних узлов вызывает колебания тока, напряжения и связанного с ними электромагнитного поля. Поэтому мощность и электромагнитное излучение следует рассматривать как тесно сопряженные проекции единого процесса энергопереноса. На практике это означает, что подавление только одного из наблюдаемых признаков не гарантирует устранения канала целиком.

Принципиально важно и то, что энергетический канал способен проявляться опосредованно. Если система управления питанием использует обратную связь по мощности для изменения частоты, вариации потребления могут стать причиной временной утечки, как это показано в Hertzbleed [9]. Следовательно, в архитектурах общего назначения энергетический механизм нередко реализуется через другие параметры, зависимые от энергопотребления.

4. Электромагнитный механизм

Электромагнитный механизм возникает вследствие изменения токов. Любой изменяющийся ток создает электромагнитное поле, а его пространственно-временная структура несет сведения о распределении вычислительной активности. В отличие от интегральной мощности, электромагнитное излучение может обладать лучшей локализацией.

Исторически электромагнитные каналы ассоциируются с TEMPEST-подобными сценариями, то есть с перехватом информационно значимых излучений. Однако современные работы показывают, что область применения значительно шире. Так, в исследовании Screen Gleaning было продемонстрировано считывание изображения с мобильного устройства через электромагнитный побочный канал [13].

Особый интерес представляют гибридные EM-атаки на микроархитектурные события памяти. В работе 2024 г. показано, что обращения к DRAM могут использоваться как электромагнитно наблюдаемый носитель кэш-утечки, то есть измеряемая переменная переносится из тайминга в электромагнитное поле [14].

Практическая значимость электромагнитного механизма определяется возможностью бесконтактного съема и высоким потенциальным пространственным разрешением. В то же время эффективность атаки сильно зависит от расстояния, полосы измерения, конструкции корпуса, трассировки платы и внешнего шума. Поэтому электромагнитный канал часто оказывается более требовательным к измерительной аппаратуре, но и более информативным при корректной настройке эксперимента.

5. Тепловой механизм

Тепловой канал формируется вследствие преобразования потребляемой электрической энергии в тепло. Температура обладает выраженной инерционностью. По этой причине долгое время тепловые побочные каналы считались малопрактичными. Однако современные исследования показали, что при определенных условиях тепловая зависимость может быть измерима и использоваться для восстановления информации либо построения скрытых межъядерных взаимодействий [15].

С физической точки зрения тепловая утечка возникает, когда различные вычислительные режимы создают неодинаковое распределение мощности по функциональным блокам кристалла. Далее это распределение передается, формируя наблюдаемое температурное поле. Информационная емкость такого канала обычно ниже, чем у временных или энергетических каналов, однако он может быть устойчив к отдельным видам маскирования, особенно если атакующий использует встроенные температурные датчики или связанные с ними события прерываний [15].

Работы ThermalBleed и ThermalScope переводят тепловые побочные каналы в область практических сценариев [15]. Они показывают, что тепловая инерция меняет спектральные характеристики утечки: канал становится более медленным, но способен переносить информацию в условиях, где высокочастотные измерения мощности или электромагнитного поля затруднены.

Следовательно, тепловой механизм особенно значим в многопроцессорных и встраиваемых системах с общей тепловой средой, ограниченным охлаждением и длительными

повторяющимися нагрузками. В таких условиях температура становится носителем коррелированной с секретом информации.

6. Акустический механизм

Акустические побочные каналы в контексте микропроцессорных систем возникают чаще как результат электромеханического преобразования сопутствующих процессов. В узком смысле акустический канал становится значимым тогда, когда секретозависимая вычислительная активность вызывает различимый акустический паттерн.

Физически такой канал связан либо с модуляцией нагрузки на элементы питания, вызывающей колебания в слышимом или околозвуковом диапазоне, либо с повторяющимися механическими действиями. Хотя акустические атаки чаще рассматриваются применительно к периферийным устройствам, в микропроцессорных системах они важны как напоминание о том, что любой путь преобразования электрической активности в наблюдаемую физическую величину потенциально может стать носителем утечки.

Практическая опасность акустических каналов обычно ниже, чем у временных и кэш-каналов. Тем не менее для высокозащищенных систем их нельзя полностью игнорировать.

7. Механизм остаточных данных и реманентность памяти

Отдельный класс физических механизмов связан с неполным исчезновением информационного состояния после завершения вычисления. Наиболее известным примером является атака через холодную перезагрузку, основанная на том, что содержимое DRAM не исчезает мгновенно после отключения питания и может сохраняться в течение времени, достаточного для частичного восстановления ключевого материала [5].

Физическая причина такого явления заключается в конечной скорости утечки заряда из ячеек памяти и в температурной зависимости процесса релаксации. В этом смысле механизм реманентности расширяет понятие побочного канала – информационно значимым оказывается не только динамический след вычисления, но и остаточное состояние носителя.

Современные исследования показывают, что даже при частичной деградации содержимого возможно восстановление криптографических ключей на основе структурных ограничений и алгоритмов поиска [5]. Это особенно важно для систем, где предполагается безопасное завершение сеанса путем простого отключения питания. Если очистка памяти не производится надежно, временной разрыв между вычислением и атакой не устраняет риск компрометации.

Сравнение вышеописанных механизмов формирования побочных каналов представлено в таблице 1.

Проведенный анализ позволяет сформулировать несколько обобщающих положений. Во-первых, побочный канал почти никогда не является изолированным физическим эффектом. Он представляет собой композицию причин, распределенных по нескольким уровням: алгоритм задает структуру вычисления, компилятор определяет конкретные инструкции, микроархитектура распределяет их по внутренним ресурсам, схемотехника формирует энергетический и электромагнитный след, а измерительная среда определяет,

Таблица 1 – Сопоставление основных механизмов формирования побочных каналов

Механизм	Источник зависимости от секрета	Наблюдаемая метрика	Типичный нарушитель	Характерные ограничения
Временной	ветвления, латентность памяти, состояние кэша, DVFS	время ответа, длительность операции	локальный или удаленный	малые различия, влияние ОС и шума сети
Энергетический	переключения транзисторов, распределение нагрузки	мощность, ток, напряжение	физический доступ или близкий зонд	требуется высокая частота измерения и фильтрация шума
Электромагнитный	локальные токи в проводниках и узлах	ЕМ-излучение, спектр, пространственный профиль	бесконтактный наблюдатель вблизи устройства	зависимость от корпуса, расстояния и полосы приемника
Тепловой	пространственное распределение мощности	температура, тепловые прерывания, тепловой след	соседний процесс или датчик	низкая полоса пропускания, тепловая инерция
Акустический	электромехани-ческая реакция питания и периферии	звук, вибрация	наблюдатель в помещении	сильная зависимость от конструкции и внешнего шума
Реманентный	сохранение зарядов в памяти после завершения работы	остаточные данные	физический доступ после отключения	ограниченное временное окно, деградация данных

какая именно метрика станет доступной атакующему. Такая интерпретация объясняет, почему одинаковая программа может иметь различную устойчивость на разных процессорах.

Во-вторых, в современных системах наблюдается выраженная гибридизация каналов, поэтому традиционная классификация по принципу один физический носитель - один тип атаки становится недостаточной. Для практики безопасности важнее понимать путь преобразования секрета в измеряемый сигнал.

В-третьих, результаты подтверждают необходимость строгого различения побочных и скрытых каналов. Смешение этих понятий приводит к ошибкам в выборе защитных мер.

В-четвертых, усложнение процессорной архитектуры не устраняет утечки, а перераспределяет их по новым механизмам. Новые технологии повышают производительность, но одновременно увеличивают число внутренних состояний, зависящих от данных. В результате современная защита должна оценивать корректность вычисления и безопасность аппаратной оптимизации [7, 10, 12].

Полученные выводы показывают ограниченность одноуровневых контрмер, иначе устранение одного наблюдаемого канала может лишь перевести утечку в другой, менее очевидный носитель.

Систематизированные меры многоуровневой защиты представлены в таблице 2.

Таблица 2 – Многоуровневые меры противодействия и их ограничения

Уровень защиты	Основные меры	Какой механизм ослабляется	Ключевые ограничения
Алгоритмический	constant-time, маскирование, отказ от secret-dependent lookup	временные и энергетические зависимости на уровне вычисления	может быть нарушен компилятором или микроархитектурой
Программно-системный	изоляция процессов, настройка ОС, патчи, контроль таймеров	микроархитектурные и транзиентные каналы	снижение производительности и неполное покрытие сценариев
Аппаратный	экранирование, фильтрация, сегментация ресурсов, защищенные ускорители	энергетические, ЕМ и часть кэш-каналов	стоимость, сложность интеграции, остаточная утечка
Эксплуатационный	ограничение физического доступа, мониторинг, процедурная очистка памяти	реманентные, контактные и измерительные атаки	не устраняет логическую причину утечки
Верификационный	лабораторные измерения, TVLA-подобные тесты, профилирование платформы	обнаружение комбинаций нескольких каналов	требует компетенций и специализированной аппаратуры

Заключение

Побочные каналы утечки информации в современных микропроцессорных системах формируются как результат непреднамеренного преобразования секретозависимой вычислительной активности в наблюдаемый физический сигнал. Проведенный анализ показал, что временные, энергетические, электромагнитные, тепловые, акустические и реманентные каналы имеют общую причинную структуру, но различаются по физическому носителю, модели нарушителя, спектральным характеристикам и доступным защитным мерам.

Так, побочный канал является кросс-уровневым явлением. Он возникает не только из-за свойств алгоритма или аппаратуры по отдельности, а из-за их взаимодействия в конкретной реализации. Поэтому эффективная защита должна строиться как многоуровневая система.

Усложнение архитектуры современных процессоров, распространение виртуализированных сред и развитие гибридных методов наблюдения делают проблему

побочных каналов одной из центральных для современной информационной безопасности. Дальнейший прогресс в области защищенных вычислений должен оцениваться не только по метрикам производительности и функциональности, но и по степени физической ненаблюдаемости критических вычислительных процессов.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Piessens, F. Side-Channel Attacks: A Short Tour / F. Piessens, P. C. van Oorschot // IEEE Security & Privacy. – 2024. – Vol. 22, No. 2. – P. 75-80. – DOI: 10.1109/MSEC.2024.3352848.

2. Kocher, P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems / P. C. Kocher // Advances in Cryptology – CRYPTO'96 : Lecture Notes in Computer Science. – Vol. 1109. – Berlin ; Heidelberg : Springer, 1996. – P. 104-113. – DOI: 10.1007/3-540-68697-5_9.

3. Kocher, P. Differential Power Analysis / P. Kocher, J. Jaffe, B. Jun // Advances in Cryptology – CRYPTO'99 : Lecture Notes in Computer Science. – Vol. 1666. – Berlin ; Heidelberg: Springer, 1999. – P. 388-397. – DOI: 10.1007/3-540-48405-1_25.

4. Yarom, Y. FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack / Y. Yarom, K. Falkner // 23rd USENIX Security Symposium (USENIX Security 14). – San Diego, 2014. – P. 719-732.

5. Banegas, G. On Recovering Block Cipher Secret Keys in the Cold Boot Attack Setting / G. Banegas, R. Villanueva-Polanco // Cryptography and Communications. – 2025. – Vol. 17, No. 2. – P. 311-335. – DOI: 10.1007/s12095-022-00625-z.

6. Specter Attacks: Exploiting Speculative Execution / P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom // 2019 IEEE Symposium on Security and Privacy (SP). – Los Alamitos : IEEE, 2019. – P. 1-19. – DOI: 10.1109/SP.2019.00002.

7. Xiong, W. Survey of Transient Execution Attacks and Their Mitigations / W. Xiong, J. Szefer // ACM Computing Surveys. – 2021. – Vol. 54, No. 3. – Art. No. 54. – P. 1-36. – DOI: 10.1145/3442479.

8. Naghibijouybari, H. Microarchitectural Attacks in Heterogeneous Systems: A Survey / H. Naghibijouybari, E. Mohammadian Koruyeh, N. Abu-Ghazaleh // ACM Computing Surveys. – 2022. – Vol. 55, No. 7. – Art. No. 142. – P. 1-40. – DOI: 10.1145/3544102.

9. Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86 / Y. Wang, R. Paccagnella, E. T. He, H. Shacham, C. W. Fletcher, D. Kohlbrenner // 31st USENIX Security Symposium (USENIX Security 22). – Boston, 2022. – P. 679–697.

10. Timing Side-Channel Attacks and Countermeasures in CPU Microarchitectures / J. Zhang, C. Chen, J. Cui, K. Li // ACM Computing Surveys. – 2024. – Vol. 56, No. 7. – Art. No. 178. – P. 1-40. – DOI: 10.1145/3645109.

11. A Survey of Microarchitectural Side-Channel Vulnerabilities, Attacks, and Defenses in Cryptography / X. Lou, T. Zhang, J. Jiang, Y. Zhang // ACM Computing Surveys. – 2021. – Vol. 54, No. 6. – P. 1-37. – DOI: 10.1145/3456629.

12. Kim, J. A Survey of Side-Channel Attacks on Branch Prediction Units / J. Kim, H. Jang, Y. Shin // ACM Computing Surveys. – 2025. – Vol. 57, No. 11. – Art. No. 282. – P. 1-36. – DOI: 10.1145/3734218.

13. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel / Z. Liu, N. Samwel, L. Weissbart, Z. Zhao, D. Lauret, L. Batina, M. Larson // Proceedings of the Network and Distributed System Security Symposium (NDSS). – 2021. – DOI: 10.14722/ndss.2021.23021.

14. Cache Side-Channel Attacks Through Electromagnetic Emanations of DRAM Accesses / J. Maillard, T. Hiscock, M. Lecomte, C. Clavier // Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT). – 2024. – P. 262-273. – DOI: 10.5220/0012813200003767.

15. Kim, T. ThermalBleed: A Practical Thermal Side-Channel Attack / T. Kim, Y. Shin // IEEE Access. – 2022. – Vol. 10. – P. 25718-25731. – DOI: 10.1109/ACCESS.2022.3156596.