УДК *004.056.5*

# АППАРАТНЫЕ ФУНКЦИИ БЕЗОПАСНОСТИ В ФОРМИРОВАНИИ РЫНОЧНОЙ СТОИМОСТИ IT-ПЛАТФОРМ

А.К. Крамаренко, Н.Д. Егоренков

*Учреждение образования «Брестский государственный технический университет», г. Брест, Республика Беларусь*

**Аннотация.** Актуальность работы – повышение числа атак в контексте физического доступа к устройствам и необходимость изучения значимости аппаратных функций безопасности для степени защищенности и рыночной стоимости IT-платформ. В статье приводятся результаты исследования некоторых аппаратных механизмов безопасности в экосистеме Apple (iOS, iPadOS, macOS). Приведено их сравнение с Android и Windows. Внимание уделено механизмам доверенной нагрузки, апаратного шифрования, защиты памяти устройств. Выделены преимущества глубокой интеграции Apple над TPM 2.0, Titan M/C и TrustZone.

**Ключевые слова:** аппаратная безопасность; Secure Enclave; Apple Silicon; физические атаки; trusted execution environment; биометрическая аутентификация; шифрование данных.

# HARDWARE SECURITY FUNCTIONS IN DETERMINING THE MARKET VALUE OF IT PLATFORMS

A.K. Kramarenko, M.D. Yahorenkau
*Educational Institution "Brest State Technical University", Brest, Republic of Belarus*

**Abstract.** The relevance of this article lies in the increasing number of attacks involving physical access to devices, and the consequent necessity to examine the significance of hardware security features regarding both the level of protection and the market value of IT platforms. This article presents the results of a study examining specific hardware security mechanisms within the Apple ecosystem (iOS, iPadOS, and macOS), comparing them with those found in Android and Windows. Particular attention is devoted to mechanisms for trusted boot, hardware encryption, and device memory protection. The advantages of Apple's deep integration approach relative to TPM 2.0, Titan M/C, and TrustZone are highlighted.
**Keywords:** hardware security; Secure Enclave; Apple Silicon; physical attacks; trusted execution environment; biometric authentication; data encryption.

## Введение

В современных условиях защита от несанкционированного доступа приобретает все большее значение. Угрозы зачастую связаны с физическим доступом к устройству: evil maid, cold boot, прямое извлечение содержимого памяти. Традиционные программные механизмы становятся уязвимыми. В связи с этим, переход к аппаратным функциям безопасности, встроенным в процессор, является необходимым для развития IT-платформ [1]. Экосистема Apple на базе чипов Apple Silicon и модуле Secure Enclave Processor является наиболее эффективной благодаря глубокой аппаратно-программной интеграции. Актуальность работы определяется повышением числа атак в контексте физического доступа к устройствам и необходимостью изучения значимости аппаратных функций безопасности для степени защищенности и рыночной стоимости IT-платформ. Цель – исследовать некоторые аппаратные механизмы безопасности в современных IT-платформах (на примере экосистемы Apple).

## Основная часть

В условиях цифровизации информационная безопасность – это важный фактор, влияющий на доверие пользователей, и, следовательно, на рыночную стоимость IT-платформ [1]. В качестве примера рассмотрим экосистему Apple.

Экосистема Apple (iOS, iPadOS, macOS) работает на принципе аппаратно-программной интеграции. Центральный элемент – Secure Enclave Processor (SEP). Он работает независимо от основного CPU. Также

в нем хранятся криптографические ключи, биометрические шаблоны Face ID / Touch ID и выполняются операции шифрования. Такие ключи остаются в SEP, даже при полном компрометировании операционной системы. Apple Secure Boot позволяет проверить цифровую подпись – от Boot ROM до ядра ОС. Аппаратное шифрование данных (AES-256) включается автоматически [2]. В чипах Apple Silicon (M-серия) и T2 (в старых Intel-маках) также есть Pointer Authentication (PAC), который защищает указатели от атак. Биометрические ключи Face ID / Touch ID создаются и хранятся в SEP, их извлечение практически невозможно даже при физическом доступе к устройству.

Далее сравним в данном контексте Android и Windows [2]. В Android основной механизм – ARM TrustZone. Он генерирует доверенную среду выполнения (TEE). В устройствах Google Pixel также используется отдельный чип Titan M2. Он хранит ключи, изучает целостность загрузки. При этом из-за фрагментации платформы (разные производители) уровень интеграции ниже, чем у Apple. Для сравнения, в Windows – TPM 2.0 (дискретный или firmware-вариант). Он контролирует загрузку и хранение ключей для BitLocker. В некоторых устройствах также есть и Microsoft Pluton (аналог Secure Enclave). Исследование позволило выделить некоторые преимущества Apple. Ключевым является такое, как: SEP связан с SoC и ОС (обеспечивается максимальная защита от physical access-атак (evil maid, cold boot, прямое чтение памяти)). В Android и Windows модульный подход влияет на гибкость системы, в тоже время он увеличивает уязвимость при физическом доступе (ключи извлекаются из наименее изолированных компонентов) [3]. Проеденное исследование показало, что аппаратный уровень Apple формирует наибольшую устойчивость у к атакам физического доступа Его конкуренты, предлагают открытые, но менее защищенные решения.

## Заключение

Проведенный анализ позволяет сделать следующие выводы. Технически глубокая интеграция обеспечивает Apple большую защиту от физических атак. Модульные архитектуры Android и Windows схожи по функциям, но уступают Apple в устойчивости из-за фрагментации и меньшей изоляции некоторых компонентов. В бизнес-аспекте позиционирование устройств Apple создает премиальный сегмент бренда. Android и Windows ищут баланс между открытостью системы и защитой. Также, на наш взглаяд, изолированная архитектура Apple упрощает выполнение требований регуляторов. А ключи шифрования Apple физически недоступны для ОС. В Android и Windows в этом контексте требуются дополнительные настроек и сторонние средства. Таким образом, при повышении интенсивности атак с физическим доступом

аппаратная безопасность – это фундамент доверия. В Apple синергия инженерных решений задает планку, к которой вынуждены подстраиваться конкуренты.

## Список использованных источников

1. Крамаренко А. К., Русенко В. Н. (2024) Интеграция программного обеспечения в бизнес: процесс, проблемы и перспективы. Интеллектуальные ресурсы – региональному развитию. (1), 232–237.

2. Костяйнен К., Дхар А., Чапкун С. (2020) Выделенные чипы безопасности в эпоху защищенных анклавов. IEEE Security & Privacy. 18 (5), 38–46. (На англ. яз.).

3. Равичандран Дж. (2023) Обнаружение новых микроархитектурных уязвимостей безопасности в современных процессорах. Магистерская диссертация, Массачусетский технологический институт. (На англ. яз.).

## References

1. Kramarenko A. K., Rusenko V. N. (2024) Integration of Software into Business: Process, Problems and Prospects. Intellectual Resources – Regional Development. (1), 232–237 (in Russian).

2. Kostiainen K., Dhar A., Capkun S. (2020) Trusted Hardware in the Era of Secure Enclaves. IEEE Security & Privacy. 18 (5), 38–46 (in English).

3. Ravichandran J. (2023) Discovering New Microarchitectural Security Vulnerabilities in Modern Processors. Master's Thesis, Massachusetts Institute of Technology (in English).

## Сведения об авторах

**Крамаренко А.К.,** канд. экон. наук, доц., доц. кафедры бухгалтерского учета, анализа и аудита, учреждение образования «Брестский государственный технический университет», annnakramarenko@yandex.by

**Егоренков Н.Д.,** студент факультета электронно-информационных систем, учреждение образования «Брестский государственный технический университет», egorenkovnikita0@gmail.com.

## Information about the authors

**Kramarenko A.K.,** Cand. Sci. (Econ.), Associate Professor, Associate Professor of the Department of Accounting, Analysis, and Audit, Educational Institution "Brest State Technical University", annnakramarenko@yandex.by

**Yahorenkau N.D.,** student, Faculty of Electronic Information Systems, Educational Institution "Brest State Technical University", egorenkovnikita0@gmail.com.