УДК 004.056.5

ПОСТРОЕНИЕ ДОВЕРЕННОЙ СРЕДЫ ИСПОЛНЕНИЯ НА БЕЛОРУССКИХ ПРЕДПРИЯТИЯХ

А.А. Ярмольчик, П.Б. Гусаков
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается концепция построения доверенной среды исполнения (Trusted Execution Environment) как современного подхода к обеспечению технической защиты информации на белорусских предприятиях. Проведен анализ международных практик организации безопасных сред, включая Trusted Research Environments и концепцию «Пяти гарантий безопасности». Обоснована необходимость перехода от традиционной модели защиты периметра к созданию контролируемых доверенных сред для обеспечения устойчивости организаций, работающих с конфиденциальной информацией.
Ключевые слова: Доверенная среда исполнения, Trusted Execution Environment, техническая защита информации, изоляция, проектирование, аудит, безопасность, белорусские предприятия, конфиденциальность, интеграция.

BUILDING A TRUSTED EXECUTION ENVIRONMENT AT BELARUSIAN ENTERPRISES

A.A. Yarmolchik, P.B. Gusakov
Educational institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republick of Belarus

Abstract. This article examines the concept of building a Trusted Execution Environment as a modern approach to ensuring technical information security at Belarusian enterprises. It analyzes international practices for creating secure environments, including Trusted Research Environments and the "Five Security Guarantees" conceptThe need to transition from the traditional perimeter security model to the creation of controlled trusted environments to ensure the resilience of organizations handling confidential information is substantiated.
Keywords. Trusted Execution Environment, technical information security, isolation, design, audit, security, Belarusian enterprises, confidentiality, integration.

Введение

В современном мире, характеризующемся стремительной цифровой трансформацией всех сфер деятельности, вопросы обеспечения технической защиты информации выходят на передний план для организаций любого масштаба. Белорусские предприятия, функционирующие в условиях необходимости адаптации к новым геополитическим и технологическим вызовам, сталкиваются с потребностью пересмотра подходов к построению своих информационных систем. Традиционная модель защиты, основанная на создании жесткого периметра вокруг корпоративной сети, постепенно уступает место более гибким и надежным

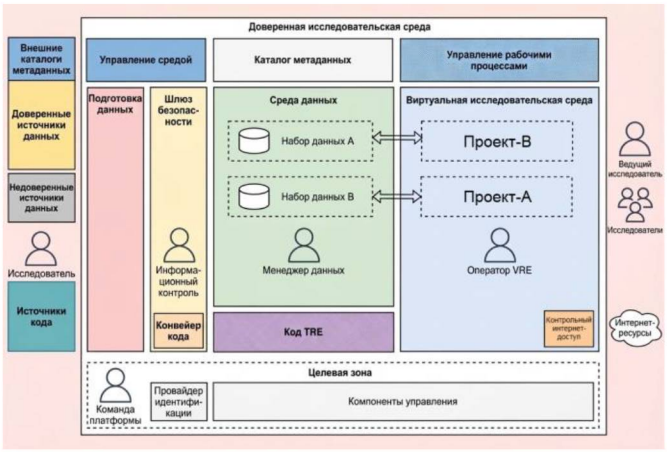
архитектурам. Одной из таких перспективных концепций является построение Trusted Execution Environment (доверенной среды исполнения) – контролируемого пространства, предназначенного для безопасной обработки, хранения и анализа конфиденциальных данных и работы критически важных приложений. В условиях роста числа киберугроз, внедрение принципов доверенных сред становится необходимостью для обеспечения устойчивости и информационной безопасности белорусского бизнеса и государственных учреждений.

Основная часть

Само понятие Trusted Execution Environment (TEE) не является абсолютно новым и имеет различные интерпретации в мировой практике. В международном контексте широкое распространение получили Trusted Research Environments (TRE) или безопасные среды для работы с данными, которые активно применяются в Великобритании и других странах для организации доступа исследователей к чувствительным медицинским и статистическим данным без риска их утечки. Ключевым принципом организации таких сред является концепция «Пяти гарантий безопасности» (Five Safes), разработанная Службой национальной статистики Великобритании. Эта концепция подразумевает обеспечение безопасности на пяти уровнях: безопасные люди (Safe people), безопасные проекты (Safe projects), безопасные данные (Safe data), безопасные настройки среды (Safe settings) и безопасные выходные результаты (Safe outputs) [1]. Данный подход позволяет реализовать среду, в которой исследователь получает доступ к вычислительным мощностям и данным в защищенном периметре, но не может несанкционированно скопировать информацию вовне. Применение подобных архитектурных решений, например, на базе облачных платформ, позволяет использовать передовые сервисы безопасности для соответствия строгим требованиям управления данными.

На рисунке показаны типичные элементы, обычно встречающиеся в TRE. Однако для белорусских предприятий особый интерес представляет иная грань понятия доверенной среды, а именно техническая реализация Trusted Execution Environments – доверенных сред исполнения на аппаратном и системном уровне. TEE представляют собой изолированные области на процессоре или в системе, гарантирующие защиту кода и данных даже в случае компрометации основной операционной системы [2]. Эти технологии, включающие аппаратные решения от различных производителей, направлены на обеспечение доверенной загрузки, изоляцию критически важных вычислений и защиту памяти от несанкционированного доступа. Методы построения таких сред основываются на расширении классической цепочки доверия от аппаратного обеспечения до прикладного программного обеспечения,

что позволяет гарантировать целостность исполняемого кода и конфиденциальность обрабатываемых данных даже на потенциально скомпрометированной платформе. Применение таких технологий критически важно для защиты ключевых систем белорусских предприятий, обрабатывающих персональные данные, коммерческую тайну или иную чувствительную информацию.



Функциональная архитектура TRE
Functional architecture of TRE

Процесс проектирования и аудита TEE для предприятия должен учитывать всю совокупность этих факторов – от глобальных концепций безопасности до локальных нормативных требований и интеграционных задач. Доверенная среда – это не единичное устройство или программа, а комплексное организационно-техническое решение. Как следует из спецификации SATRE (Standardised Architectures for Trusted Research Environments), разработанной при участии многих организаций, успешная реализация TRE требует рассмотрения не только технологических компонентов, но и управленческих процессов, ролей пользователей, процедур контроля доступа и управления. Применительно к белорусским реалиям, построение такой среды должно начинаться с детального аудита существующих информационных активов и бизнес-процессов, определения категорий данных, требующих максимальной защиты, и моделирования угроз. На этапе проектирования необходимо выбрать архитектурный шаблон – будет ли это изолированная среда исполнения для конкретного критического приложения, виртуальная исследовательская среда для работы с базами данных, либо же комплексная система защиты всего предприятия, основанная на принципах нулевого доверия. Ключевым элементом здесь является интеграция с существующей инфраструктурой и используемыми средствами защиты информации, включая сертифицированные в Беларуси средства криптографической защиты и межсетевые экраны.

Заключение

Построение TEE на белорусских предприятиях представляет собой многогранную задачу, лежащую на стыке передовых мировых практик организации безопасных сред, региональных интеграционных инициатив в рамках ЕАЭС и жестких требований национального законодательства в области технической защиты информации. Переход от концепции защиты периметра к созданию контролируемых, изолированных и верифицируемых сред исполнения является закономерным ответом на усложнение ландшафта угроз и повышение требований к сохранности конфиденциальных данных. Дальнейшее развитие данного направления будет неразрывно связано как с совершенствованием аппаратных платформ и методов изоляции, так и с гармонизацией нормативной базы на национальном и наднациональном уровне, что позволит создавать по-настоящему надежные и функциональные доверенные цифровые пространства.

Список использованных источников / References

1. Amazon Web Services [Electronic resource]. URL: https://aws.amazon.com.
2. Shepherd C., Markantonakis K. (2024) *Trusted Execution Environment.*

Сведения об авторах

Ярмольчик А.А., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alexey24yarmolchik02@gmail.com.

Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».

Information about the authors

Yarmolchik A.A., Cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alexey24yarmolchik02@gmail.com.

Gusakov P.B., Master's Degree, Head of Cycle, Educational Institution "Belarusian State University of Informatics and Radioelectronics".