УДК 004.056.5

ОБЛАЧНЫЕ ТЕХНОЛОГИИ И АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ: ВОПРОСЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

П.Ф. Романко, С.А. Фурсанов, Е.И. Баяк
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В данном докладе рассматриваются современные облачные технологии и аппаратные средства защиты информации, используемые для обеспечения безопасности и конфиденциальности данных в условиях массового перехода вычислений в облачные среды. Анализируются угрозы безопасности облачных систем, возможности аппаратных решений (TPM, HSM, TEE) для защиты данных, практические случаи применения технологий (например, Intel SGX и AMD SEV), а также перспективы развития технологий конфиденциальных вычислений. Результаты обзора подтверждают, что интеграция аппаратных методов защиты является ключевым направлением для повышения уровня безопасности облачных инфраструктур.
Ключевые слова: облачные технологии, аппаратные средства защиты, конфиденциальные вычисления, TEE, HSM, TPM, безопасность данных.

CLOUD TECHNOLOGIES AND HARDWARE SECURITY MEASURES: ISSUES OF DATA SECURITY AND CONFIDENTIALITY

P.F. Romanko, S.A. Fursanau, E.I. Bayak
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This report examines modern cloud technologies and hardware-based information security measures used to ensure the security and confidentiality of data in the context of a widespread shift to cloud computing. It analyzes security threats in cloud systems, the potential of hardware solutions (such as TPM, HSM, and TEE) for data protection, practical case studies of technology applications (e.g., Intel SGX and AMD SEV), and the prospects for the development of confidential computing technologies. The review confirms that the integration of hardware security methods is a key approach to enhancing the security level of cloud infrastructures.
Keywords: cloud technologies, hardware security measures, confidential computing, TEE, HSM, TPM, data security.

Введение

Развитие облачных технологий сопровождается увеличением объема передаваемых и обрабатываемых данных, что делает вопросы безопасности и конфиденциальности информации особенно актуальными. Традиционные программные методы защиты уже не всегда способны эффективно противостоять современным угрозам информационной безопасности. В этом контексте аппаратные средства защиты (например, модули безопасного шифрования, доверенные вычислительные среды) играют решающую роль. Настоящий доклад посвящен анализу современных аппаратных технологий, применяемых для защиты облачных систем, и оценке их эффективности с точки зрения безопасности и производительности [1].

Обзор облачных технологий и угроз безопасности

Облачные сервисы делятся на модели IaaS, PaaS и SaaS, каждая из которых предъявляет свои требования к безопасности. Основные угрозы включают атаки на виртуальные машины, утечку данных и компрометацию управляющих систем. Для наглядности приведена таблица, в которой сопоставлены типичные угрозы и возможные меры защиты (табл. 1).

Таблица 1. Основные угрозы и меры защиты в облачных системах
Table 1. Key threats and protection measures in cloud systems

Угроза	Описание	Возможные меры защиты
Атаки на виртуальные машины	Использование уязвимостей гипервизора	Изоляция. обновление ПО, мониторинг
Утечка данных	Несанкционированный доступ к конфиденциальной информации	Шифрование данных, контроль доступа
Атаки на инфраструктуру управления	Попытки компрометации систем администрирования	Аудит, аппаратное разделение функций

Аппаратные средства защиты в облачных системах

Аппаратные технологии, такие как TPM, HSM и доверенные вычислительные среды (TEE), обеспечивают защиту ключей, изоляцию вычислительных процессов и безопасную загрузку системы. Примеры реализованных решений включают Intel SGX, AMD SEV и ARM TrustZone. В качестве упрощенной модели эффективности аппаратной защиты можно записать следующую формулу:

$$E = \frac{C}{T} \times 100\% \quad (1)$$

где E – эффективность в процентах, C – количество защищенных операций, а T – общее количество операций. Такая оценка помогает сравнивать производительность различных аппаратных решений [2, 3].

Аппаратные методы шифрования и управления ключами

Аппаратные средства позволяют реализовать шифрование данных «на лету» и обеспечивают защищенное хранение криптографических ключей. Модули HSM (Hardware Security Module) и TPM (Trusted Platform Module) предоставляют возможности генерации, хранения и управления ключами на физическом уровне, что значительно снижает риск их компрометации. Практическое применение таких методов наблюдается в крупных облачных провайдерах, где аппаратное шифрование помогает снизить задержки и увеличить надежность системы [4]. Кроме того, использование специализированного аппаратного обеспечения повышает общую производительность системы за счет разгрузки программных компонентов.

Практические случаи использования и анализ эффективности

Анализ практических кейсов показывает, что применение аппаратных средств защиты существенно повышает уровень безопасности облачных платформ. Так, сравнительный анализ технологий Intel SGX и AMD SEV демонстрирует, что обе технологии имеют свои преимущества и ограничения по производительности и уровню защиты. Пример сравнительной таблицы приведен ниже.

Таблица 2. Сравнение производительности и уровня защиты аппаратных решений
Table 2. Comparison of performance and security levels of hardware solutions

Технология	Среднее время обработки (мс)	Уровень защиты (условный балл)
Intel SGX	12.5	8
AMD SEV	14.0	7
TPM	10.0	6

Исследования [4, 5] показывают, что интеграция аппаратных методов позволяет не только повысить безопасность, но и обеспечить необходимый уровень производительности для обработки критически важных данных.

Перспективы развития и новые тренды

Будущие направления развития включают интеграцию машинного обучения для мониторинга состояния аппаратных компонентов, развитие мультиоблачных и гибридных архитектур с усиленной аппаратной защитой, а также совершенствование технологий конфиденциальных вычислений. Ожидается, что дальнейшее развитие аппаратных средств позволит снизить накладные расходы на безопасность и повысить устойчивость систем к новым видам кибератак [2, 5].

Заключение

В докладе был проведен обзор современных облачных технологий и аппаратных средств защиты, таких как TPM, HSM и TEE, с анализом их роли в обеспечении безопасности и конфиденциальности данных. Рассмотренные практические кейсы и сравнительный анализ демонстрируют, что аппаратные методы являются важным элементом комплексной системы защиты облачных сервисов. Перспективы развития в направлении интеграции интеллектуальных методов мониторинга и создания гибридных архитектур открывают новые возможности для повышения надежности информационных систем.

Список использованных источников

1. Субашини, С. и Кавита, В. (2011). Обзор проблем безопасности в моделях предоставления облачных вычислений. Journal of Network and Computer Applications. 34(1), 1–11.

2. Костан, В. и Девадас, С. (2016). Объяснение Intel SGX. Cryptology ePrint Archive. Отчет 2016/086.

3. Артур, У., Челленер, Д. и Гольдман, К. (2014). Практическое руководство по TPM 2.0: Использование TPM в новой эре безопасности. Syngress.

4. Мазер, Т., Кумарасвам, С. и Латиф, С. (2009). Безопасность и конфиденциальность в облачных вычислениях: Корпоративный взгляд на риски и соответствие. O'Reilly Media.

5. Чжан, Ц., Чен, Л. и Бутаба, Р. (2010). Облачные вычисления: современное состояние и исследовательские вызовы. Journal of Internet Services and Applications, 1(1), 7–18.

References

1. Subashini, S. & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. Journal of Network and Computer Applications, 34(1), 1–11.

2. Costan, V. & Devadas, S. (2016). Intel SGX Explained. Cryptology ePrint Archive, Report 2016/086.

3. Arthur, W., Challener, D. & Goldman, K. (2014). A Practical Guide to TPM 2.0: Using the TPM in the New Age of Security. Syngress.

4. Mather, T., Kumaraswamy, S. & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media.

5. Zhang, Q., Cheng, L. & Boutaba, R. (2010). Cloud Computing: State-of-the-Art and Research Challenges. Journal of Internet Services and Applications, 1(1), 7–18.

Сведения об авторах

Романко П.Ф., студент. учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pavelromanko7710@gmail.com.
Баяк Е.И., инженер-программист ОИАСУ. учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», e.baiak@bsuir.by.

Information about the authors

Romanko P.F., student. Educational Institution "Belarusian State University of Informatics and Radioelectronics". pavelromanko7710@gmail.com
Bayak E.I., software engineer. Automated Control Systems Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics". e.baiak@bsuir.by.

Фурсанов С.А., инженер-программист ОИТ, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», s.fursanov@bsuir.by.

Fursanau S.A., software engineer, Information Technology Department. Educational Institution "Belarusian State University of Informatics and Radioelectronics". s.fursanov@bsuir.by.