УДК 004.056

Т.А. НИКИТИН[1], Т.И. КОМАРОВ[1], И.Ю. ЖУКОВ[2]

[1]Национальный исследовательский ядерный университет «МИФИ», Москва
[2]ООО «Группа компаний «Инфотактика», Москва

ВОПРОСЫ БЕЗОПАСНОСТИ CXL

CXL (Compute Express Link) – это эволюционное продолжение стандарта PCIe (Peripheral Component Interconnect Express). На физическом уровне он использует тот же интерфейс, что и PCIe, но благодаря более совершенным протоколам на верхнем уровне, CXL способен устранить некоторые существенные недостатки, присущие PCIe. Однако с новыми возможностями появляются и новые вызовы в области обеспечения безопасности и конфиденциальности данных.

Стандарт CXL был разработан для расширения возможностей PCIe. Его основная особенность заключается в том, что эта технология обеспечивает когерентность основной памяти, которая подключается непосредственно к процессору, и памяти CXL-устройств [1].

CXL состоит из трёх высокоуровневых протоколов: CXL.io (инициализация, управление и обмен данными между хостом и устройством); CXL.cache (кэширование устройством информации из памяти хоста); CXL.mem (возможность для хоста обращаться к памяти устройства как к кэшируемой).

Первые версии CXL (CXL 1.0 и CXL 1.1) предназначались для подключения устройств только к одному хосту. Более поздние версии (CXL 2.0 и CXL 3.0) позволяют создавать сложные сети из множества хостов и устройств, объединять их ресурсы, предоставлять совместный доступ и многое другое. Указанные возможности позволяют использовать технологию CXL в дата-центрах для организации внутренних сетей высокопроизводительных вычислительных систем самого различного назначения (машинное обучение и нейронные сети, в частности; моделирование; потоковая обработка данных и т.д.).

Однако возможности, добавленные в новые стандарты технологии CXL, помимо существенного расширения её функциональных возможностей, делают её подверженной тем атакам, которые хорошо известны в контексте сетевых технологий и могут быть высокоуровнево разделены на три категории: неавторизованный доступ к ресурсам и информации; неавторизованное изменение доступной в сети информации; атаки типа «отказ в обслуживании» [2].

Стандарт предлагает несколько механизмов защиты от указанных выше угроз, одним из которых является возможность сквозного шифрования трафика. Однако данные механизмы являются рекомендованными, а не обязательными, и есть риск, что производители оборудования и разработчики программного обеспечения не будут их использовать по умолчанию. Кроме того, нельзя исключать возможность появления новых аппаратных и программных ошибок, которые могут привести к появлению дополнительных уязвимостей.

Уже сейчас существует ряд исследований [3, 4, 5], направленных на создание дополнительных средств защиты сетей на основе технологии CXL, что свидетельствует о недостаточности мер по обеспечению безопасности сетевого взаимодействия, предусмотренных стандартом.

Таким образом, технология CXL является весьма востребованной для построения высокопроизводительных вычислительных систем, но на текущий момент её стандарт не требует применения изложенных в нём механизмов обеспечения безопасности. Более того, их применение не может обеспечить достаточный уровень безопасности для многих применений, т.к. исследований безопасности применения технологии CXL существует не так много, а в имеющихся отмечается недостаточность мер, предусмотренных стандартом, и предлагаются новые.

Переход на технологию CXL необходим для повышения эффективности организации вычислений, в т.ч. на объектах КИИ, но требует более внимательного анализа сопряженных с этим проблем, в т.ч. из области информационной безопасности.

Список литературы

1. Das Sharma D., Blankenship R., Berger D. An Introduction to the Compute Express Link (CXL) Interconnect // ACM Comput. Surv. 2024. т. 56. № 11. С. 1–37. DOI: http://dx.doi.org/10.1145/3669900.

2. Dastres R., Soori M. A Review in Recent Development of Network Threats and Security Measures // International Journal of Computer and Information Sciences. 2021. HAL Id: hal-03128076.

3. Stark S. W., Markettos A. T., Moore S. W. How Flexible Is CXL's Memory Protection? // Commun. ACM. 2023. т. 66. № 12. С. 46–51. DOI: http://dx.doi.org/10.1145/3617580.

4. Choi K. и др. ShieldCXL: A Practical Obliviousness Support with Sealed CXL Memory // ACM Trans. Archit. Code Optim. 2025. т. 22. № 1. с. 1–25. DOI: http://dx.doi.org/10.1145/3703354

5. Li C., Zhao J., Xu Y. Efficient Security Support for CXL Memory through Adaptive Incremental Offloaded (Re-)Encryption. // Proceedings of the 58th IEEE/ACM International Symposium on Microarchitecture (MICRO '25). ACM. 2025. с. 1102–1116. DOI: https://doi.org/10.1145/3725843.3756119.