УДК 004.056

И.Ю. ЖУКОВ[1, 2], Т.И. КОМАРОВ[2], А.В. ЗУЙКОВ[3]

[1]*ООО «Группа компаний «Инфотактика», Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[3]*ООО «Гексагон», Москва*

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Реализация импортозамещения в области построения программно-аппаратных комплексов (ПАК) для критической информационной инфраструктуры (КИИ) требует комплексных решений, которые обеспечат существенное повышение их защищённости. Предлагается разработка отечественных программных и программно-аппаратных решений, которые будут формировать иерархию доверия и соответствующую экосистему, применимую на устройствах практически любых классов.

В настоящее время информационные технологии обеспечивают контроль геолокации промышленного оборудования и транспортных средств, область применения, состояние и выполняемые функции, позволяют удаленно обновлять перечень сервисов, а в случае нарушения лицензионных соглашений, имеют возможность анализировать все события и информационные потоки контролируемого оборудования, а также принимать решения на блокирование как части функций, так и оборудования в целом.

Производители оборудования обладают инструментами [1], позволяющими ему «следить» за проданными ИТ-изделиями, за их пользователями, за технологическим оборудованием, а также вмешиваться в функционирование систем с враждебными целями.

В связи с ужесточением санкционной политики со стороны недружественных стран, резко возросла угроза блокирования или перехвата управления технологическим оборудованием особо важных объектов критической информационной инфраструктуры государства. Следовательно, необходимо интенсифицировать процессы перехода на отечественные решения.

Предлагается построение комплексного решения – выстраивание иерархии доверия (цепочек доверия), которое сможет существенным образом повысить защищённость ПАК, применяемых в КИИ:

- встроенное ПО, выполняющее требования спецификации UEFI (Unified Extensible Firmware Interface) [2] и реализующее безопасные механизмы загрузки с использованием концепций, применяемых как в отечественных аппаратно-программных модулях доверенной загрузки (АПМДЗ), так и в зарубежных решениях, соответствующих спецификации TPM (Trusted Platform Module) [3, 4]);
- хостовая ОС на базе ядра Linux со средствами виртуализации и контейнеризации, которые в полной мере удовлетворяют актуальным требованиям ФСТЭК по защите информации;
- пакетный менеджер и соответствующая инфраструктура (система сборки пакетов, репозитории пакетов), которые смогут обеспечить безопасную доставку пакетов, надёжные обновления и конфигурирование ОС;
- корневой и промежуточные удостоверяющие центры для работы сертификатами и электронными цифровыми подписями, которые должны использоваться во всех компонентах предлагаемого решения;
- специализированные ОС на основе конечных автоматов [5] для особо ответственных применений, где ОС на базе ядра Linux могут являться избыточными, неэффективными или недостаточно защищёнными.

Практическая реализация предложений, представленных выше, является одним из необходимых шагов по переходу на отечественные решения и позволяет существенно повысить безопасность, надёжность и доверие компонентов КИИ.

Список литературы

1. Зегжда Д.П., Жуков И.Ю. Особенности обеспечения информационной безопасности вычислительных систем. Безопасность информационных технологий. Т. 28, № 1, 2021. С. 42–61.

2. UEFI Specification 2.10. URL: https://uefi.org/specs/UEFI/2.10 (дата обращения: 20.09.2023).

3. Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits. San Francisco: No Starch Press Inc., 2019. – 413 с.

4. TPM 2.0 Library Specification. URL: https://trustedcomputinggroup.org/resource/tpm-library-specification (дата обращения: 20.09.2023).

5. Astier J.Y., Zhukov I.Y., Murashov O.N., Bardin A.P. A new OS architecture for IoT. Безопасность информационных технологий. Т. 25б, №1, 2018. С. 19–33.