УДК 004.056

Д.А. ДЯТЛОВ, Е.А. НЕЩЕРЕТНЯЯ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРОАКТИВНАЯ БЕЗОПАСНОСТЬ КАК ОСНОВА ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Анализируется задача обеспечения технологической независимости объектов критической информационной инфраструктуры. Рассматривается процесс замены импортных компонентов на отечественные. Предлагается подход, при котором служба безопасности выступает в роли интегратора, формирующего сквозные требования и обеспечивающего целостность всей многоуровневой экосистемы – от производства электронной компонентной базы до эксплуатации сложных программно-аппаратных комплексов.

Введение

Курс на технологическую независимость объектов критической информационной инфраструктуры (КИИ) [1] – это не просто переход на отечественную электронную компонентную базу (ЭКБ) и программно-аппаратные комплексы (ПАК), а возможность построить принципиально новую, целостную и доверенную экосистему. Традиционная модель, где безопасность «добавляется» к готовому изделию, упускает суть проблемы [2]. Безопасность – это системное свойство, зависящее от всех ее уровней и их взаимосвязи. В этой новой парадигме специалист по безопасности должен трансформироваться из контролера в интегратора, обеспечивающего сквозную защищенность на всех этапах жизненного цикла КИИ.

От требований к архитектуре безопасности

Рассматривая КИИ «по вертикали» [3]: объект КИИ – система – ПАК – программное обеспечение – ЭКБ, становится очевидной недостаточность защиты только на одном (как правило, канальном) уровне [4]. Безопасность системы определяется прочностью самого слабого звена. Задача интегратора – выстроить эту цепь таким образом, чтобы не было слабых звеньев.

В рамках предлагаемого подхода роль специалиста по безопасности КИИ становится проактивной. Ключевыми функциями с точки зрения интегратора являются:

- формирование требований – разработка единого свода правил,

обязательных для всех участников экосистемы;

- контроль цепочки поставок – аудит производственных и логистических процессов, внедрение практик, исключающих риски подмены компонентов на этапе сборки и доставки;
- проектирование и внедрение единой системы управления всей экосистемы;
- координация взаимодействия между испытательными лабораториями, разработчиками и заказчиками;
- создание типовых, заранее протестированных и сертифицированных схем построения защищенных систем для объектов КИИ.

Заключение

Технологический суверенитет – это, в первую очередь, суверенитет над архитектурой, стандартами и процессами, обеспечивающими безопасность. Служба безопасности объектов КИИ готова выступить драйвером этих изменений, взяв на себя роль интегратора и архитектора доверия. Построив целостную, прозрачную и управляемую экосистему, можно гарантировать, что каждый отечественный чип, каждая плата и каждая программа будут не просто «аналогами», а элементами новой, действительно защищенной основы для КИИ.

Список литературы

1. Агафонов Н.Ю. Процесс импортозамещения в критической информационной инфраструктуре. Актуальные исследования. 2024, № 30 (212), с. 18–21. URL: https://apni.ru/article/9841-process-importozamesheniya-v-kriticheskoj-informacionnoj-infrastrukture. EDN: PDHUCP.

2. Попов А.В., Сплюхин Д.В., Сысоев В.Н., Хлыстов М.А., Цыгунька А.И. Цифровая устойчивость промышленности: почему встроенные системы информационной безопасности нельзя отодвигать на второй план. Энергоэксперт. 2025, № 2 (94), с. 16–20. URL: https://www.elibrary.ru/download/elibrary_82363953_26457192.pdf. EDN: GWKZIC.

3. Кессаринский Л.Н., Никифоров А.Ю. Подход к заданию общих требований к доверенной электронной компонентной базе для регулируемого рынка критической информационной инфраструктуры в вопросах и ответах. Безопасность информационных технологий. 2025, № 1, т. 32, с. 8-16. URL: https://bit.spels.ru/index.php/bit/article/view/1761/1457. EDN: EENLAL.

4. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам. Вопросы кибербезопасности. 2022, № 2 (48), с. 39-51. DOI: 10.21681/2311-3456-2022-2-39-51.