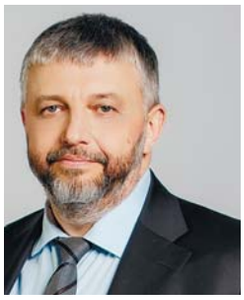

Евгений Генгринович

ИнфоТеКС: «Киберустойчивость необходимо закладывать на этапе проектирования системы»

Цифровизация охватывает множество важных функций, находясь в основе критической инфраструктуры крупных производственных предприятий. В этих условиях отсутствие доверенного фундамента делает систему защиты уязвимой. Как обеспечить надежность и киберустойчивость цифровых решений, рассказал Евгений ГЕНГРИНОВИЧ, советник генерального директора ИнфоТеКС.

Эксперты все чаще говорят, что цифровизация приносит компаниям не только пользу, но и новые риски. Какие угрозы обычно недооцениваются?

– Цифровая трансформация действительно повышает эффективность бизнеса, но недооценка новых рисков может крайне негативно сказаться на результатах этого процесса. Технологическое развитие идет такими темпами, что можно принять за аксиому утверждение: «Любая цифровая система в течение жизненного цикла однажды подвергнется направленному несанкционированному информационному воздействию». Бурное развитие промышленного интернета вещей привело к формированию экосистем управления на основе ИИ-агентов. Роль человека в оперативных решениях постепенно сводится к нулю, поэтому на всем жизненном цикле таких систем нужны инструменты контроля доверия к ним.

Как в таком случае максимально обезопасить ИТ-инфраструктуру предприятий?

– Мы привыкли к термину «безопасность», однако важную роль играет и целостность данных, особенно в системах, управляющих физическими объектами. От целостности зависят качество и логика принимаемых решений, безопасность взаимодействия между программными модулями разных производителей и контроль соблюдения легитимности работы экосистемы. Для обеспечения доверия к информационной экосистеме должны присутствовать четыре элемента целостности: корректность входных данных, предсказуемость алгоритмов их обработки, сохранность истории изменений и соответствие контексту предметной области. Поэтому уже на этапе проектирования системы и ее компонент нужно предусматривать встроенные механизмы адаптации к ИБ-угрозам и кибератакам.

Какие инструменты обеспечения доверия к информационной системе уже появились в России?

– Введен в действие национальный стандарт ГОСТ Р 71252–2024 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем». Одним из решений, соответствующих данному стандарту, является ViPNet SIES, позволяющий реализовать набор криптографических сервисов для устройств автоматизации. Встраиваемые криптомодули и ПО обеспечивают высокую гибкость применения независимо от отрасли. Сертификация ViPNet SIES по уровню КС-3 позволяет производителям индустриальных систем пройти только одну процедуру «Контроль встраивания» с минимальными требованиями к лицензированию. Решение снимает нагрузку криптографических вычислений с центрального процессора функционального устройства. Для заказчиков это значит, что они устанавливают на своих объектах защищенные устройства. Это снижает затраты на наложенные средства защиты и повышает надежность эксплуатации цифровых решений, обеспечивая более высокий уровень киберустойчивости.

На какие еще аспекты нужно обращать внимание для поддержания доверия к цифровым решениям?

– Важно выстраивать процессы подготовки персонала. Разработчики индустриальных систем, инженеры-технологи, отвечающие за эксплуатацию, ранее не сталкивались с вопросами ИБ и устойчивости, поэтому необходимо обеспечить процесс развития новых компетенций специалистов. В этом направлении организована работа с вузами. Для тренировки специалистов создан киберполигон Ampire, моделирующий цифровую инфраструктуру и сценарии кибератак. А на базе НИУ МЭИ открыта первая в России лаборатория по встраиваемым СКЗИ для инженеров и студентов-энергетиков.