Максим ХАРАСК:

«Важен баланс между качеством, скоростью и доступностью импортозамещения АСУ ТП»

До 2025 года российские компании обязаны полностью перейти на российское ПО. Это требование касается и систем промышленной автоматизации. О комплексной стратегии обеспечения безопасности АСУ ТП и других систем КИИ при переходе на российские решения рассказывает директор департамента развития технических продаж Innostage Максим Хараск.

– Как обеспечить безопасный переход на отечественное ПО с учетом возрастающей хакерской активности?

– В условиях повышенных рисков наиболее выигрышной стратегией является комплексный подход, который позволяет оценить достаточность уже примененных решений и необходимость их импортозамещения для максимально эффективного результата. Таким образом достигается баланс между качеством, скоростью и доступностью перехода на российское ПО.

И именно этот принцип компания Innostage, имеющая большой опыт достаточно бесшовного импортозамещения, взяла за основу своего подхода к киберустойчивости. Для нас важно одновременно с миграцией ПО и данных обеспечить защиту и бесперебойность ключевых сервисов и технологических процессов. Причем так, чтобы та титаническая работа, которая в это же самое время производится «под капотом», не отразилась на технологических и бизнес-процессах компании.

– Какие этапы включает предложенная вами стратегия?

– На начальном этапе проводится оценка уровня кибербезопасности с анализом текущего состояния ИТ-инфраструктуры и выявление потенциальных точек проникновения.

Далее актуализируется дизайн целевой архитектуры и определяется взаимосвязь артефактов. Принципы проектирования безопасной инфраструктуры сформулированы Innostage как признанным экспертом-киберархитектором.

Третий этап – трансформация инфраструктуры и определение важности каждого объекта защиты с учетом количества процессов, необходимых для обеспечения его кибербезопасности, а также внедрение защитных мер.

Четвертый этап – подготовка и обучение персонала. Все сотрудники регулярно проходят обучение по повышению осведомленности, а эксплуатационный персонал участвует в киберучениях и совершенствует навыки работы с СЗИ.

Заключительный этап – независимая оценка устойчивости отдельных систем и организации в целом. Она проводится с использованием внешних пентестов и запуска программы bug bounty.

– Как в вашем подходе учтены особенности защиты АСУ ТП?

– Системы промышленной автоматизации существенно отличаются от корпоративных, но их специфика также укладывается в рамки нашего подхода к киберустойчивости. Основные угрозы информационной безопасности в АСУ ТП включают заражение вредоносным кодом, атаки из внешних сетей, несанкционированный доступ к данным и компонентам системы, а также приведение системы в состояние «отказ в обслуживании». Алгоритмы устранения этих потенциальных проблем включены в 1–4 уровни методологии, разработанной Innostage.

– Заказчики при этом должны выбирать решения и оборудование определенных производителей?

– В этом вопросе у компаний почти нет ограничений. В наш пул вендоров входит более сотни отечественных производителей, исходя из пожеланий заказчика и тех ИТ-активов, которые у него уже есть в наличии, мы можем порекомендовать комбинации, оптимальные с точки зрения бюджета, функционала и уровня защищенности.

Innostage также разрабатывает и внедряет собственные решения для защиты от кибератак, проведения киберразведки, мониторинга и реагирования на инциденты, их расследования и устранения последствий. В продуктовом портфеле как универсальные решения, так и разработки, созданные специально для АСУ ТП и других объектов критической информационной инфраструктуры. Все они могут быть интегрированы с продуктами других производителей и внедрены в строящуюся инфраструктуру. ■