инфотекс

Евгений Генгринович

Советник генерального директора

Цифровой мир: почему киберустойчивость становится главным приоритетом

Мы живём в океане информации, и на сегодняшний день технологии проникли во все сферы: от заводских цехов до городской инфраструктуры. Интеллектуальные системы (ИС) составляют невидимую основу современного промышленного ландшафта.

К ним относятся:

- датчики и контроллеры промышленного интернета вещей
- медицинские приборы и имплантаты
- блоки управления автомобилями
- инфраструктура «умного города»
- потребительские устройства интернета вещей
- беспилотные летательные аппараты (БПЛА)

Они управляют оборудованием в режиме реального времени, обеспечивают работу автономных устройств, отслеживают физические параметры, события и изменения в окружающей среде, формируя единую картину состояния объектов. Именно поэтому в случае сбоя последствия могут носить не только информационный, но и физический характер, и такие системы называют киберфизическими.

ОТ СБОЕВ — К РЕАЛЬНЫМ УГРОЗАМ

Причины нарушений в работе информационной инфраструктуры разнообразны: ошибки разработчиков или пользователей, хакерские атаки или электромагнитные воздействия. Во многих случаях система формально продолжает функционировать, устройства отвечают на запросы, но логика поведения информационной инфраструктуры изменяется.

Последствия подобных сбоев могут быть самые разные, например:

- потеря физического контроля над оборудованием и системами управления
- угроза безопасности и риски для здоровья людей
- промышленный саботаж
- скрытое наблюдение и шпионаж
- регуляторные и правовые риски

В отличие от традиционных инцидентов с информационными системами, восстановление киберфизических систем может потребовать физического ремонта оборудования, замены датчиков или повторной сертификации устройств. В ряде реальных инцидентов скомпрометированные устройства промышленного интернета вещей использовались не в качестве целей, а в качестве инструментария: для создания ботнетов, организации скрытой слежки или точек входа в защищенные информационные среды.

КИБЕРУСТОЙЧИВОСТЬ — ВАЖНЫЙ ФАКТОР В ОЦЕНКЕ НАДЕЖНОСТИ ЦИФРОВЫХ СИСТЕМ

В вопросе оценки надежности функционирования цифровых решений в промышленности на первый план выходит понятие «киберустойчивость» – способность киберфизических систем обеспечивать выполнение бизнес-целей в условиях несанкционированных информационных воздействий. Киберустойчивость прежде всего обеспечивается контролем контекстной целостности данных киберфизических систем.

Целостность гарантирует, что информация не будет изменена без разрешения, а все преобразования поддаются контекстной проверке на протяжении жизненного цикла системы. В то время как доступность обеспечивает бесперебойную работу, конфиденциальность – защиту от несанкционированного доступа, целостность позволяет убедиться, что данные точны, неизменны и соответствуют контексту в разных подсистемах и во времени.

Здесь важно отметить, что киберустойчивость нельзя «добавить» позже – она должна закладываться на архитектурном уровне при проектировании киберфизических систем через реализацию трёх ключевых принципов:

01. Безопасную загрузку, гарантирующую, что устройство запускается только с доверенным программным обеспечением
02. Использование аппаратных корней доверия для криптографических операций и защищённого хранения ключей
03. Непрерывный контроль целостности и поведения системы, который не может быть отключён или изменён в процессе эксплуатации

Если устройство не может в любой момент времени подтвердить собственную целостность, ему нельзя доверять. Встроенная память должна быть криптографически подписана, проверена при загрузке и защищена от несанкционированных изменений путём непрерывного мониторинга. Механизмы обновления – защищены и изолированы от путей управления процессом, поскольку каждое обновление может стать вектором атаки.

Ни одному устройству, команде или сигналу нельзя доверять безоговорочно. Аутентификация, авторизация и проверка поведения должны быть непрерывными, а не осуществляться только в момент запуска. Если команда меняет поведение системы, она должна иметь возможность подтвердить свою легитимность.

Традиционных журналов событий недостаточно – необходим мониторинг результатов: сопоставления паттернов поведения, изменений показаний датчиков, временных аномалий. Когда физический мир становится программируемым, любые отклонения превращаются в сигналы, требующие внимания.

ФУНДАМЕНТ ИНФРАСТРУКТУРЫ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Гарантией приемлемого уровня киберустойчивости служит применение сертифицированных средств криптографической защиты информации (СКЗИ). Особенности применения криптографических механизмов в киберфизических системах отражены в действующем ГОСТ Р 71252–2024 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем». Стандарт адаптирует криптографические механизмы для индустриальных и встраиваемых решений, позволяя работать даже в сетях без IP. Стандартизация криптографических протоколов и подходов создаёт основу для интероперабильных мультивендорных решений.

АО «ИнфоТеКС» – одна из ведущих российских компаний в области информационной безопасности. В продуктовой линейке вендора более 50 наименований для надежной и комплексной защиты инфраструктуры предприятий. Обладая глубокой экспертизой, мы понимаем, что проектированием киберфизических систем должны заниматься отраслевые специалисты, наша задача – предоставить необходимый инструментарий и квалифицированную экспертизу. Для этих целей было разработано решение ViPNet SIES, позволяющее реализовать как сценарии аппаратного корня доверия, так и целого ряда функций киберфизических систем для повышения их киберустойчивости.

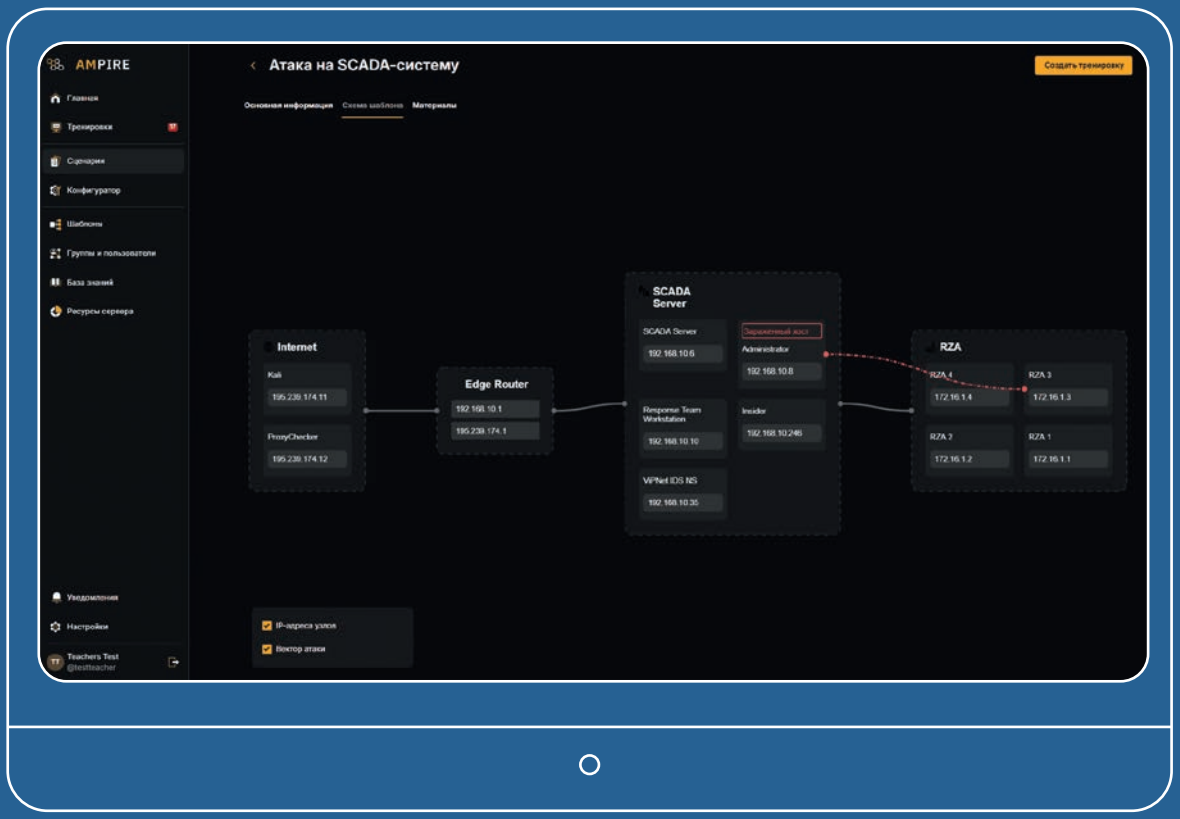
Решение прошло сертификацию регуляторов и полностью соответствует ГОСТ Р 71252. Компонентами решения ViPNet SIES являются встраиваемые криптомодули и ПО, что обеспечивает гибкость применения в различных отраслях: топливно-энергетическом комплексе, нефтехимической промышленности, электроэнергетике и не только. Благодаря сертификации компонент ViPNet SIES по классу СКЗИ КС 3 производителям киберфизических систем для получения высокого уровня безопасности и устойчивости своих продуктов требуется пройти только одну процедуру – «Контроль встраивания» – с минимальными требованиями к лицензированию. При этом криптографические вычисления выполняются на отдельном устройстве, не загружая центральный процессор, что особенно важно для энергоэффективных и автономных систем.

Для заказчиков это означает, что они устанавливают на своих объектах защищенные самим производителем устройства, с более высоким уровнем киберустойчивости, что снижает затраты на наложенные средства защиты и повышает надежность эксплуатации киберфизических систем. Системный подход позволяет сформировать единый мультивендорный ландшафт доверия и поддерживать его на всём жизненном цикле.

Состав решения ViPNet SIES

ЦИФРОВЫЕ ДВОЙНИКИ И ПОДГОТОВКА КАДРОВ

Эксплуатация киберфизической инфраструктуры обязательно должна опираться на цифровые двойники, так как они дают возможность тестировать любые изменения на виртуальной модели до их внедрения в реальные производственные системы. Цифровой двойник может быть интегрирован с киберполигоном для анализа киберустойчивости инфраструктуры и подготовки/тестирования персонала профильных подразделений. Например, совместно с Центром НТИ МЭИ реализована интеграция киберполигона «Ampire» с цифровым двойником электроэнергетической инфраструктуры.



Шаблон, моделирующий энергетическую подстанцию и кибератаки, направленные на вызов короткого замыкания

Важным аспектом для процессов цифровизации и обеспечения киберустойчивости внедряемых решений является выстраивание новых процессов подготовки персонала. Разработчики индустриальных систем, инженеры-технологи зачастую не сталкивались с вопросами информационной безопасности и киберустойчивости. По этой причине необходимо обеспечить процесс развития новых компетенций у профильных специалистов. В этом направлении организована работа с вузами и корпоративными университетами по всей территории Российской Федерации.

Более 40 российских университетов создали учебные лаборатории на базе киберполигона «Ampire». Ampire создаёт тренировочное виртуальное пространство, моделирующее цифровую инфраструктуру, и позволяет отрабатывать сценарии кибератак для развития компетенций в области защиты критической инфраструктуры. В 2024 году на базе кафедры релейной защиты и автоматики НИУ МЭИ была открыта первая в России лаборатория по встраиваемым СКЗИ. Лаборатория предназначена для подготовки инженеров-разработчиков индустриальных решений, студентов-энергетиков и преподавателей.

Демонстрация А.В. Новаку лаборатории по встраиваемым СКЗИ на кафедре РЗА НИУ «МЭИ»

ЗАКЛЮЧЕНИЕ

Промышленный интернет вещей, БПЛА и роботизированные системы меняют не только устройство мира, но и способы воздействия на него. Киберпространство больше не ограничивается данными и коммуникационными сетями – оно охватывает воздушное пространство, инфраструктуру и автономное принятие решений. Повторюсь: самые опасные воздействия не объявляют о себе, устройство продолжает работать. Но где-то между замыслом и исполнением контроль над инфраструктурой незаметно переходит из рук в руки.

Лаборатория по встраиваемым СКЗИ на кафедре РЗА НИУ «МЭИ»

Киберполигон «Ampire»

Продукты ИнфоТеКС для защиты систем промышленной автоматизации