Киберустойчивость в энергетике: как избежать иллюзий?

Евгений Генгринович, *советник генерального директора компании "ИнфоТеКС"*


Фото: ИнфоТеКС

Когда речь заходит о цифровой трансформации в АСУ ТП, наравне с вопросами информационной безопасности все чаще поднимается тема киберустойчивости. Устойчивость важна для любой технологической системы – будь то электроэнергетика, нефтегазовая отрасль или нефтехимия. Основная задача любого технологического процесса – достижение запланированных бизнес-результатов, и службы эксплуатации традиционно отвечают за его надежность.

Но цифровизация управления технологическими процессами приводит к кардинальному изменению методов обеспечения их безопасности, устойчивости и надежности. Задача в том, чтобы бизнес, технологи и отраслевые регуляторы как можно быстрее осознали эти изменения.

Многие компании практически полностью полагаются на цифровые системы управления, что приводит к конвергенции ИТ и инфраструктуры АСУ/АСУ ТП. Это дает бизнесу рост эффективности за счет повышения производительности труда и снижения влияния "человеческого фактора". Но при этом появляются риски новых векторов кибератак и киберинцидентов, которых раньше просто не существовало.

Регуляторная база, касающаяся надежности и безопасности эксплуатации, развивается. Однако в ней пока не хватает четких требований, связанных именно с цифровой составляющей. Кроме того, на местах не всегда хватает компетенций: технологические специалисты зачастую не имеют достаточного опыта работы с современными ИТ-системами.

В качестве иллюстрации рассмотрим абстрактное, но типичное устройство в АСУ ТП. При его проектировании инженеры могут выбрать минимально подходящую слабую микросхему и пластиковый корпус. Но вместо этого они устанавливают защищенный корпус, устойчивый к электромагнитным помехам, и более мощную микросхему, способную выдерживать перегрузки, – например, при скачках напряжения или ударе молнии. То есть изначально закладываются механизмы, повышающие отказоустойчивость.

Аналогичный подход должен применяться и к информационной составляющей: производители и заказчики должны понимать, что без защиты от киберугроз обеспечить требуемый уровень надежности и защищенности будет крайне сложно.

Найти золотую середину

Есть два типа ключевых требований:

1. Mission Critical – требования, критичные для безопасности людей, экологии или вообще государства. Здесь соответствие является обязательным: надзорные органы следят, что все нормы соблюдены.

2. Business Critical – то, что важно для самого бизнеса, его прибыльности и эффективности. Если затраты на безопасность превышают возможные риски, компания рискует стать убыточной.

Эти два аспекта не противоречат друг другу. Формальная безопасность необходима – без нее не пройти проверки. Но если бизнес не перешел на риск-ориентированное управление, рано или поздно он столкнется с проблемами. Например, когда ИТ-инфраструктура превращается в "черный ящик", а руководство не понимает, как киберриски влияют на производство и финансы.

Непростительная ошибка – воспринимать безопасность как лишние расходы. На деле речь не о бесконечных вложениях, а о разумной оценке угроз и поиске баланса.

Нередко можно услышать: "Мы сдадим систему, а потом позовем специалистов по ИБ – пусть обеспечат безопасность". Такой подход неэффективен и дорог. Внешний эксперт не сможет "научить" технологический процесс быть устойчивым – защита должна закладываться на этапе проектирования.

Для цифровой трансформации характерен интересный парадокс: с одной стороны, цифровизация действительно повышает безопасность производства, позволяя операторам управлять процессами дистанционно, минимизируя их присутствие в опасных зонах. Но с другой – она же создает принципиально новые уязвимости в информационной сфере.

Решение этой проблемы лежит в системном подходе. Когда отраслевые стандарты начинают учитывать не только традиционные требования к надежности оборудования, но и современные киберриски, безопасность перестает быть навязанным сверху требованием. Она становится естественным следствием грамотно спроектированного технологического процесса. В таком случае защитные меры органично встраиваются в производственный цикл, а не накладываются постфактум как дорогостоящее дополнение.

Эпоха "воздушного зазора"

Концепция полной изоляции критически важных систем, известная как "воздушный зазор", кажется пережитком прошлого. Однако так ли это на самом деле? Рассмотрим этот вопрос на актуальном примере антропоморфных роботов – одной из самых обсуждаемых тем современного технологического ландшафта.

На первый взгляд, такие автономные системы, оснащенные нейронными сетями и сложными алгоритмами, представляются полностью независимыми. Но при ближайшем рассмотрении выясняется, что даже самый совершенный робот неизбежно имеет точки контакта с внешним миром: порты для настройки, модули Wi-Fi, системы обновления прошивок, зарядные устройства. Эти, казалось бы, незначительные элементы инфраструктуры создают потенциальные векторы атаки.

Представим гипотетического робота с "вечной" батареей, не требующий обслуживания в течение ста лет. Казалось бы, идеальная изолированная система. Но он существует не в вакууме – вокруг люди, изменяющаяся среда, непредсказуемые обстоятельства. Получается парадоксальная ситуация: на столетие мы теряем контроль над интеллектуальным устройством, в то время как его программная начинка продолжает эволюционировать и взаимодействовать с окружением через имеющиеся интерфейсы.

Этот пример наглядно демонстрирует: в современном мире абсолютная изоляция цифровых систем – иллюзия. Даже физически отключенное от сети устройство остается уязвимым через человеческий фактор, условия эксплуатации или скрытые функциональные возможности. Более того, стремление к полной изоляции может принести больше вреда, чем пользы, поскольку лишает нас возможности контролировать и своевременно обновлять системы.

Концепция "воздушного зазора" требует радикального переосмысления. Вместо искусственной изоляции нужны продуманные системы контроля и управления, учитывающие реальные условия эксплуатации.

Security by Design в АСУ ТП

В российской практике существует разрозненный понятийный аппарат: "кибериммунные системы", "конструктивная безопасность", "киберустойчивые решения" – все эти термины используются параллельно, но единого стандарта пока нет. Это создает почву для разночтений и затрудняет выработку четких требований.

Примечательно, что в аппаратной части прогресс более очевиден. Разработчики АСУ ТП уже привыкли учитывать физические факторы защиты: помехоустойчивые корпуса, температурные режимы, ограничение доступа к компонентам. Однако, когда речь заходит о микропроцессорной технике и программной составляющей, сохраняется значительный пробел – как в экспертизе самих создателей оборудования, так и в постановке задач со стороны заказчиков.

Ключевая проблема кроется в разрыве цепочки "регулятор – заказчик – производитель". Пока отраслевые стандарты не будут явно требовать встраивания киберустойчивости на этапе проектирования, ситуация будет меняться медленно. Показателен пример электроэнергетики: даже в 2025 г., по действующему Постановлению Правительства № 846 от 28 октября 2009 г., в состав комиссий по расследованию системных аварий не включают в обязательном порядке ИТ- и ИБ-специалистов, а при расследовании причин аварии не предъявляют требования по фиксации прошивок, конфигураций, логов и сетевых настроек информационной инфраструктуры. В результате причины инцидентов сводятся к "браку производства" или "ошибкам персонала", тогда как потенциальные кибератаки остаются за рамками рассмотрения.

Тем не менее позитивные сдвиги есть. Передовые производители, заинтересованные в долгосрочном присутствии на рынке, уже добровольно внедряют принципы безопасной разработки и встраивают в свои устройства сертифицированную криптографию. Постепенно меняется и восприятие заказчиков: все чаще повышение киберустойчивости воспринимается не как избыточные затраты, а как инструмент обеспечения надежности и снижения эксплуатационных расходов.

Этот процесс напоминает сборку сложного механизма: сначала нужно осознать назначение каждой детали, затем – правильно ее установить. Сейчас отрасль проходит этап осознания. И хотя темпы изменений пока отстают от технологических вызовов, вектор движения очевиден: будущее – за системным подходом, где безопасность проектируется, а не дополняется.

Новые вызовы для кадровой политики

Электроэнергетика переживает глубокую трансформацию, которая требует принципиально нового подхода к подготовке кадров. Сегодня уже недостаточно быть просто энергетиком – необходимо разбираться в сетевых технологиях и вопросах кибербезопасности. Шестилетний опыт сотрудничества компании "ИнфоТеКС" с Центром НТИ МЭИ показывает, что современному специалисту по релейной защите уже необходимы знания сетевых протоколов, как части архитектуры цифровых подстанций, базовых механизмов криптографии и информационной безопасности.

Однако подготовка таких специалистов – лишь часть решения. Гораздо сложнее оказалось интегрировать их в существующую систему эксплуатации у заказчиков. Выпускники с современными междисциплинарными знаниями часто сталкиваются с непониманием со стороны работодателей. Традиционные энергокомпании просто не готовы оценивать и достойно оплачивать такие компетенции, что создает парадоксальную ситуацию: с одной стороны – острая нехватка квалифицированных кадров, с другой – невостребованность подготовленных специалистов.

Решение этой проблемы требует системного подхода. Крупным энергокомпаниям необходимо создать центры компетенций в составе 10–15 высококвалифицированных специалистов, способных работать на стыке энергетики, ИТ и ИБ. При этом на местах можно ограничиться инженерно-техническим персоналом с базовой подготовкой. Но главное – нужно менять саму корпоративную культуру, пересматривать подходы к организации эксплуатации и оплате труда. Цифровая трансформация – это не просто новые технологии, но и новые принципы управления кадрами, без которых современные решения останутся нереализованным потенциалом.

Удручающе выглядят случаи, когда специалист по релейной защите, получив знания в области ИТ и информационной безопасности, уходит в банковский сектор. Однако в ходе общения с выпускниками МЭИ, защитившими магистерские диссертации на стыке цифровых технологий и надежности энергосистем, становится очевидным: перед нами уникальные профессионалы. Их ценность – в редком сочетании глубокого понимания эксплуатационных процессов с современными цифровыми компетенциями.

В отличие от обычного программиста, чьи функции постепенно берет на себя искусственный интеллект, такие междисциплинарные эксперты останутся востребованными как минимум ближайшие 10–15 лет.

Ключевая задача – показать молодым специалистам перспективы такого профессионального пути. Ведь именно они будут формировать цифровой ландшафт критически важных отраслей экономики в предстоящие годы.

Суверенитет и прагматизм

Перед субъектами КИИ, особенно в энергетике, стоит сложная дилемма. С одной стороны, существует очевидная необходимость замены иностранных решений, производимых компаниями из недружественных стран. С другой – вопрос о целесообразности полного перехода на суверенные разработки требует взвешенного подхода.

Следует признать, что задача импортозамещения во многом обусловлена объективными обстоятельствами. Однако важно учитывать исторический контекст: многие системы автоматизации в России просто не разрабатывались в необходимых объемах, поскольку существовали доступные и надежные зарубежные аналоги.

В этой ситуации более продуктивным представляется стратегический подход, который можно обозначить как "импортоопережение". Речь идет не о механической замене "коробки на коробку", а о выстраивании комплексного проекта цифровой трансформации. При таком подходе:

- устаревшие устройства могут временно сохраняться как исполнительные механизмы,
- базовые системы управления создаются на новых отечественных платформах,
- критерием выбора становится не географическое происхождение решения, а его прозрачность и контролируемость.

Особое внимание следует уделить Mission Critical-системам, обеспечивающим национальную безопасность. Для них, по аналогии с оборонной промышленностью, может быть оправдан полный переход на суверенные решения – даже в ущерб экономической эффективности. Однако в других случаях необходим баланс между требованиями безопасности и бизнес-реалиями.

Путь к технологическому суверенитету лежит не через тотальное замещение, а через продуманную модернизацию с четким разделением систем по степени их критичности. ●