ЕВГЕНИЙ ГЕНГРИНОВИЧ
советник генерального директора
АО «ИнфоТеКС»

КИБЕРУСТОЙЧИВОСТЬ ЭНЕРГЕТИКИ: СТРАТЕГИЯ И КАДРЫ

В контексте цифровой трансформации автоматизированных систем управления технологическими процессами (АСУ ТП) все чаще наряду с информационной безопасностью (ИБ) обсуждается тема киберустойчивости[1]. Этот аспект актуален для всех отраслей, которые отнесены к критической инфраструктуре. Многие предприятия в значительной степени зависят от цифровых систем управления, что приводит к слиянию ИТ-инфраструктуры с АСУ и АСУ ТП. Это способствует росту производительности и снижению влияния человеческого фактора, что, в свою очередь, повышает эффективность бизнеса. Но одновременно появляются новые угрозы – кибератаки и инциденты, которых ранее не существовало.

ПОИСК БАЛАНСА: ГДЕ ПРОХОДИТ ГРАНИЦА МЕЖДУ БЕЗОПАСНОСТЬЮ И ЭФФЕКТИВНОСТЬЮ

В современных условиях компаниям приходится балансировать между двумя важными группами требований. Первые касаются аспектов, от которых напрямую зависит безопасность людей, окружающей среды и, в отдельных случаях, даже национальной инфраструктуры. Это зона, где компромиссы недопустимы: соблюдение всех предписаний строго контролируется надзорными органами.

Вторая категория требований отражает интересы самой компании. Речь идет про эффективность бизнес-процессов, прибыльность и устойчивость к внутренним и внешним рискам. Здесь важна точность оценки: если затраты на безопасность начинают превышать реальные угрозы, бизнес может столкнуться с падением рентабельности.

Эти два подхода не противоречат друг другу – напротив, они дополняют систему управления. Формальное соответствие нормативам позволяет пройти проверки и избежать санкций, но этого недостаточно. Без перехода к риск-ориентированному управлению компания может потерять контроль над критическими процессами. Один из тревожных сигналов – когда ИТ-инфраструктура становится непрозрачной для управленцев, а влияние киберугроз на производственные и финансовые показатели перестает быть очевидным. На практике речь идет не о бесконечных инвестициях в обеспечение ИБ, а о взвешенном анализе рисков и поиске оптимального решения.

Нередко можно услышать: «Сначала запустим систему, а потом пригласим специалистов по ИБ – пусть обеспечивают защиту». Такой подход оборачивается высокой стоимостью и низкой эффективностью. Внешний эксперт не сможет в большинстве случаев адаптировать технологический процесс к устойчивости – кибербезопасность должна быть учтена еще на этапе проектирования.

Цифровая трансформация порождает любопытный парадокс: с одной стороны, цифровизация действительно усиливает безопасность производства – операторы могут управлять процессами дистанционно, не подвергаясь риску в опасных зонах, а с другой – она открывает принципиально новые уязвимости. Преодолеть это противоречие можно только с помощью системного подхода. Устойчивость достигается путем проектирования системы таким образом, чтобы отказы были разделены. Если одна функция выходит из строя, это не должно приводить к отказу других функций, и в проекте должны быть альтернативные способы выполнения отказавшей функции, которые можно вызвать автоматически, немедленно и надежно. Добавляется физическая или логическая избыточность для элементов и взаимосвязей, что обеспечивает переходы к альтернативным элементам и соединениям при необходимости. Тестирование должно проводиться для нормальных и ненормальных сценариев и изучаться на предмет того, может ли злоумышленник намеренно нарушить комбинацию компонентов. Программное обеспечение также должно иметь возможность перехода на альтернативные функции, реализации, конфигурации, местоположения или сегменты сети, которые могут иметь другие слабые стороны, чтобы те же угрозы и опасности не были столь разрушительными для возможностей замены. Тогда меры защиты органично интегрируются в производственный процесс, а не накладываются позже, как дорогостоящая надстройка.

КАК ОБЕСПЕЧИТЬ КИБЕРУСТОЙЧИВОСТЬ В АСУ ТП

В отечественной практике пока нет единства в терминологии: «кибериммунные системы», «конструктивная безопасность», «киберустойчивые решения» – эти понятия используются параллельно, но общепринятого стандарта не существует. Это порождает неоднозначности и затрудняет формирование четких и универсальных требований.

[1] Киберустойчивость – это способность системы поддерживать приемлемый уровень обслуживания в условиях информационных воздействий.

Примечательно, что в аппаратной части прогресс заметен гораздо сильнее. Разработчики АСУ ТП давно учитывают физические аспекты защиты: от использования экранированных корпусов до соблюдения температурных норм и ограничений физического доступа к узлам. Однако в области обеспечения киберустойчивости микропроцессоров и программного обеспечения, по-прежнему сохраняется серьезный пробел – как в технической компетенции разработчиков, так и в формулировке задач со стороны заказчиков.

Основная трудность заключается в разрыве взаимодействия между регулятором, заказчиком и производителем. Пока нормативные документы прямо не предписывают включать киберустойчивость в проектные фазы, изменения будут идти медленно. Тем не менее, позитивные сдвиги уже происходят. Производители, ориентированные на долгосрочную работу в отрасли, начинают добровольно внедрять принципы безопасной разработки, включая сертифицированные средства криптографической защиты в архитектуру устройств. Постепенно меняется и подход заказчиков: все чаще инвестиции в киберустойчивость воспринимаются не как излишние расходы, а как необходимый инструмент повышения надежности и снижения эксплуатационных издержек.

Этот процесс можно сравнить со сборкой сложного механизма: сначала необходимо понять функции каждой детали, затем установить каждую из них на свое место. Сегодня отрасль как раз проходит стадию осмысления. Пусть темпы пока отстают от вызовов времени, но направление очевидно: будущее за системным подходом, в котором устойчивость, защищенность и безопасность закладывается в проект, а не добавляется в последнюю очередь.

ФОРМИРОВАНИЕ НОВОЙ КОРПОРАТИВНОЙ КУЛЬТУРЫ КАК СПОСОБ НАУЧИТЬ ЭНЕРГЕТИКОВ ОСНОВАМ ИБ

Регуляторные нормы, касающиеся безопасности и надежности эксплуатации, продолжают развиваться. Однако им пока недостает четких положений, отражающих цифровую специфику. Кроме того, непосредственно на объектах эксплуатации часто наблюдается нехватка экспертизы: специалисты-технологи не всегда обладают достаточными знаниями в области современных ИТ-систем.

Для преодоления данной проблемы необходимо начать формирование новой корпоративной культуры, в которой станет аксиомой: инженер-технолог, не обладающий базовыми знаниями в сфере ИТ и ИБ, оказывается неэффективным звеном, неспособным обеспечить надежную эксплуатацию современных цифровых решений. На этапе перехода, пока вузы еще не выпускают специалистов с такими компетенциями в должном объеме, оптимальным решением должно стать – создание эксплуатационных подразделений нового формата. В них будут работать ИТ и ИБ-специалисты совместно с технологами, которые понимают тонкости производственных процессов.

Стоит также развеять распространенное заблуждение, будто современный инженер-технолог не в состоянии дополнительно осваивать вопросы ИТ и ИБ из-за высокой нагрузки. В действительности, в цифровой инфраструктуре таких специалистов потребуется немного – на уровне крупной корпорации достаточно команды из 4-5 человек. Основную работу в процессе эксплуатации смогут выполнять технологи со среднеспециальным образованием, используя готовые решения, без необходимости глубокого технического понимания, подобно тому, как мы ежедневно пользуемся смартфонами, не вникая в их внутреннее устройство.

С развитием централизованных платформ для управления и обеспечения безопасности, появлением цифровых двойников и киберполигонов, станет возможным оперативно анализировать причины сбоев и устранять их с помощью удаленных подключений или действий специалистов на местах. А в перспективе следующего технологического этапа таких исполнителей все чаще будут заменять автоматизированные системы и роботы.

Для наглядности представим типовое устройство в составе АСУ ТП. При его разработке инженеры могли бы использовать минимально соответствующую слабую микросхему и простой пластиковый корпус. Но они выбирают защищенную оболочку, устойчивую к электромагнитным помехам, и мощный чип, способный выдерживать перегрузки, например, при скачке напряжения или ударе молнии. То есть закладываются элементы, повышающие надежность. Такой же принцип должен применяться и к информационным системам: как производители, так и заказчики должны осознавать, что без защиты от киберугроз достичь требуемого уровня устойчивости и безопасности практически невозможно.

ГДЕ ГОТОВЯТ СПЕЦИАЛИСТОВ ПО РАЗРАБОТКЕ ЗАЩИЩЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УЧЕТА ЭЛЕКТРОЭНЕРГИИ

Электроэнергетическая отрасль переживает масштабные изменения, требующие переосмысления подходов к подготовке специалистов. Сегодня одного лишь профильного образования в энергетике уже недостаточно – требуется понимание сетевых технологий и основ кибербезопасности. Компания «ИнфоТеКС»[2] совместно с Центром НТИ МЭИ[3] подготовили специальный учебный курс «Введение в разработку защищенных Интеллектуальных систем учета электроэнергии (ИСУЭ) и АСУ ТП с

[2] [Электронный ресурс]. URL: *https://infotecs.ru/*
[3] [Электронный ресурс]. URL: *http://nti.mpei.ru/*

использованием ViPNet SIES»[4], который объединяет накопленный опыт в области криптографической защиты информации и создания отечественных программно-аппаратных комплексов для обеспечения кибербезопасности объектов электроэнергетики. Курс проходит на базе НИУ МЭИ.

Курс имеет глубокую практическую направленность, при освоении курса слушатели учатся развертывать инфраструктуру решения ViPNet SIES[5], встраивать криптографический модуль ViPNet SIES Core[6] в устройства нижнего уровня ИСУЭ и АСУ ТП, интегрировать программный комплекс ViPNet SIES Unit[7] с системами верхнего уровня ИСУЭ и АСУ ТП, обеспечивать реализацию резервированной защищенной связи между устройствами верхнего и нижнего уровня, а также удаленно управлять и обслуживать встроенные средства криптографической защиты информации.

Действующие разработчики устройств и программного обеспечения компаний-производителей систем промышленной автоматизации, систем коммерческого учета электроэнергии, систем релейной защиты и противоаварийной автоматики – все они реальные и потенциальные слушатели курса.

КАДРОВАЯ ПОЛИТИКА В НОВЫХ УСЛОВИЯХ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Обучение специалистов – лишь часть общей задачи подготовки кадров. Куда сложнее оказывается их включение в действующую эксплуатационную систему у заказчика. Молодые выпускники с современными, комплексными знаниями нередко сталкиваются с недопониманием и недооценкой со стороны работодателей. В результате складывается парадокс: отрасль остро нуждается в компетентных кадрах, но при этом подготовленные профессионалы часто остаются невостребованными.

Чтобы преодолеть этот разрыв, необходим комплексный подход. Крупным энергокомпаниям целесообразно формировать центры компетенций – небольшие, но квалифицированные команды из 10-15 человек, работающие на стыке энергетики, ИТ и ИБ. В то же время на местах достаточно технического персонала с базовой подготовкой. Для достижения требуемого результата ключевым моментом становится необходимость трансформации самой корпоративной культуры – от методов эксплуатации до системы мотивации. Цифровизация требует не только новых технологий, но и новой философии управления кадрами. Без этого даже самые передовые решения останутся нереализованными.

Особенно обидны случаи, когда подготовленный для работы в области электроэнергетики инженер по релейной защите, освоивший ИТ и ИБ, вынужден уходить в банковскую или другую отрасль. Между тем общение с магистрами НИУ «МЭИ», защитившими работы на пересечении цифровизации и надежности энергосистем, показывает: перед нами действительно уникальные кадры. Их ценность в том, что они одинаково хорошо разбираются как в технических процессах, так и в цифровых технологиях.

Самое важное – донести до молодых специалистов, насколько перспективен этот путь. Ведь именно они в будущем будут определять цифровую архитектуру критически важных секторов экономики.

ПРЕДЛАГАЕМЫЕ ПУТИ РЕШЕНИЯ

Зрелая культура обеспечения киберустойчивости энергокомпаний, полагаем, должна включать:

- Принятие решений с учетом рисков на этапе внесения изменений, а не только после их внедрения.
- Обучение инженеров оценке уровня киберустойчивости во время ввода в эксплуатацию, закупок и запросов на изменение.
- Совместную ответственность специалистов ИТ, ИБ, АСУ/АСУТП и технологами, при этом киберустойчивость должна рассматривается как условие утверждения проекта и подтверждения эксплуатационной готовности.

Например, процессы ввода в эксплуатацию будут включать вопросы киберустойчивости в качестве стандартной практики:

- Как эта новая система подключается к сети?
- Кто управляет логическим доступом после развертывания?
- Какие меры безопасности предусмотрены для доступа поставщика?
- Поддаются ли все точки удаленного доступа аудиту и контролю?

Эти вопросы не теоретические; они отражают реальные точки входа для злоумышленников и должны стать частью повседневных инженерных решений.

В процедурах проектирования и закупок необходимо сформировать практику контроля:

- наличия программы и методики испытаний на киберустойчивость от поставщиков;
- проведения испытаний на виртуальных моделях, симулирующих реальную инфраструктуру;
- представления периодичности и методики проведения плановых проверок, включающих корректировки программного обеспечения, проверку учетных данных и аудит журнала доступа;
- оценки киберустойчивости и её соответствия нормам в качестве предварительного условия для ввода – запуска в эксплуатацию.

[4] [Электронный доступ]. URL: *http://nti.mpei.ru/course-vipnetsies/*
[5] [Электронный доступ]. URL: *https://infotecs.ru/solutions/zashchita-isue/*
[6] [Электронный доступ]. URL: *https://infotecs.ru/products/vipnet-sies-core/*
[7] [Электронный доступ]. URL: *https://infotecs.ru/products/vipnet-sies-unit/*

При практической интеграции в инженерные рабочие процессы организациям следует предусматривать приведение в соответствие существующих эксплуатационных процессов с новым цифровым окружением. Многие инженерные рабочие процессы уже включают в себя этапы обеспечения безопасности, качества и соответствия. Поддержка киберустойчивости может быть внедрена путем целенаправленных, высокоэффективных изменений, включая оценку киберустойчивости существующих процессов.

ФОРМИРОВАНИЕ КОРПОРАТИВНОЙ КУЛЬТУРЫ

Корпоративная культура формируется посредством повторения, прозрачности и закрепления. Руководители по безопасности давно осознали важность регулярных процедур – инструктажей на рабочем месте, производственных обходов и коротких собраний по безопасности, которые внедрили важность управления рисками в повседневную работу.

Эти подходы помогают развить чувство сопричастности и необходимости личного вклада к достижению поставленных задач у сотрудников и укрепить идею о том, что кибербезопасность, как и устойчивость, является ответственностью каждого.

Для поддержания культурных изменений требуются практические инструменты, которые закрепляют желаемое поведение. Вместо строительства новых систем с нуля, организации могут адаптировать существующие ресурсы и процессы, с учетом нового цифрового окружения.

Необходимо добавить тему киберустойчивости в стандартные программы обучения в вузах, колледжах, при переподготовке и повышении квалификации специалистов, а также при инструктажах на предприятиях и в организациях. Следует также разработать и внедрить в энергокомпаниях панели мониторинга для отслеживания ключевых показателей уровня киберустойчивости (например, количество активов с проверенными контролями доступа, процент систем с обновленной прошивкой), создать рабочие инструкции по обеспечению киберустойчивости, которые помогут инженерам выявлять распространённые уязвимости (например, открытые порты, пароли по умолчанию, неуправляемый удалённый доступ).

Простые, последовательные подсказки в нужных местах помогают командам формировать привычки, а привычки стимулируют изменения в корпоративной культуре эксплуатации.

ЗАКЛЮЧЕНИЕ

Цифровая трансформация индустрии, безусловно, значительно повысит ее эффективность и безопасность. Цифровые решения обеспечат сокращения сроков смены технологических циклов. Но необходимо проявлять осторожность, должную предусмотрительность и мудрость, чтобы гарантировать, что технологические достижения в конечном итоге не обойдутся нам слишком дорого. Существует ограниченный период — окно возможностей — когда мы можем разработать целостную концепцию безопасности, которая будет базироваться на киберустойчивых устройствах и решениях, реализует безопасную связь между конечными точками и обеспечит управление киберустойчивостью и ее мониторинг. Этому должны способствовать культурные стимулы, структурные изменения зон ответственности, прозрачность принятия решений руководством и постоянное повышение квалификации специалистов на соответствующих курсах и при работе на местах.

Интеграция цифровых решений в существующие рабочие процессы, электронные реестры, закупки, ввод в эксплуатацию и обслуживание, гарантируют, что киберустойчивость станет частью повседневной деятельности.