Система информационной безопасности

для технологического суверенитета энергетики

Алексей ПЕТУХОВ,
эксперт центра компетенций «Кибербезопасность» НТИ Энерджинет и сообщества RuSCADASec

Максим НИКАНДРОВ,
эксперт центра компетенций «Кибербезопасность» НТИ Энерджинет и сообщества RuSCADASec

Дмитрий ПРАВИКОВ,
эксперт центра компетенций «Кибербезопасность» НТИ Энерджинет и сообщества RuSCADASec

Энергетический сектор России – критически важная отрасль, требующая надежной защиты от киберугроз. Технологический суверенитет в этой сфере подразумевает независимость от иностранных ИТ-решений, безопасность критической инфраструктуры и устойчивость к кибератакам. Для модели технологического суверенитета энергетики сформулированы два ключевых вызова: уязвимость инфраструктуры и контроль над ключевыми энергетическими и цифровыми технологиями. Как обеспечить готовность энергетических компаний к решению возникающих в этой сфере задач?

Составляющие стратегии развития отрасли представил на «ИНЖИР 2025» (Летняя школа инженеров энергетики будущего) министр энергетики Российской Федерации Сергей Евгеньевич Цивилев. В своей лекции он отметил, что главная цель внутреннего рынка – полное и доступное (технически и экономически) обеспечение потребностей промышленности и населения энергией. В приоритете – технологический суверенитет – способность государства владеть всеми доступными технологиями, ключами управления критическими технологиями, чтобы обеспечить независимость нашей экономики.

Технологический суверенитет, формируемый при соблюдении баланса – доступности, надежности и стоимости поставляемых услуг – возможен только в рамках сотрудничества с дружественными странами (Китаем, Вьетнамом, Индией, государствами арабского мира и др.). При этом значимая роль отводится информационной безопасности (ИБ).

Модель технологического Суверенитета

Ключевой показатель эффективности реализации стратегии – доступная стоимость киловатт-часа на весь период жизненного цикла проекта. Для реализации столь амбициозной задачи разработан международный универсальный язык, понятный в любой точке мира, – язык потребностей. При этом за основу

взята пирамида Маслоу, адаптированная для энергетики (рис. 1).

Для каждой отрасли энергетики (нефть и газ, угольная, электроэнергетика) составлена своя пирамида, но уже с основными технологиями и ответственными за них, оценена их зрелость. Инфографика отражает сведения по каждому блоку (то, что есть, и над чем нужно работать). На рис. 2 представлен пример для отрасли «нефть и газ».

Информационная и кибербезопасность представлены для каждой пирамиды, везде отмечены как технологии, уже созданные и готовые к масштабированию или находящиеся в процессе разработки. По информационной безопасности, как и по ряду других компонентов технологического суверенитета еще предстоит определить лидеров (ответственных), поэтому не будем вдаваться в детали появления терминов и их роли, а постараемся предложить свое видение системы информационной безопасности для технологического суверенитета энергетики.

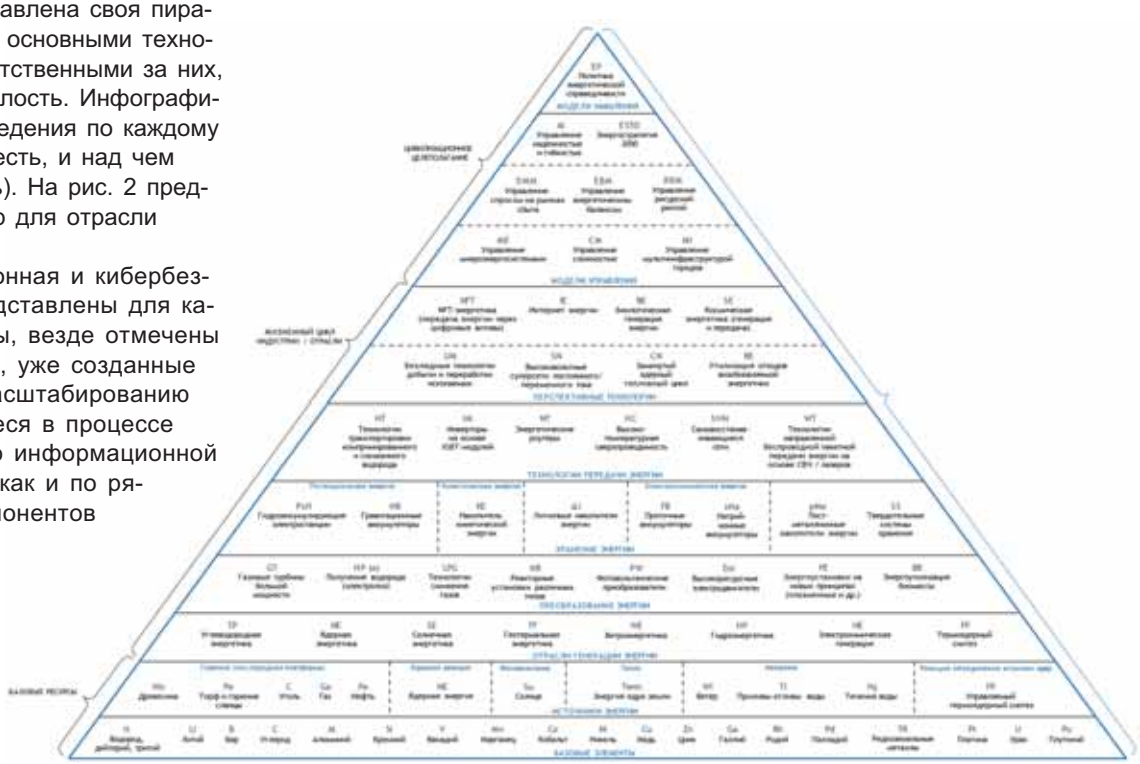

Рис. 1. *Сферы применения промышленного Интернета вещей (IIoT)*

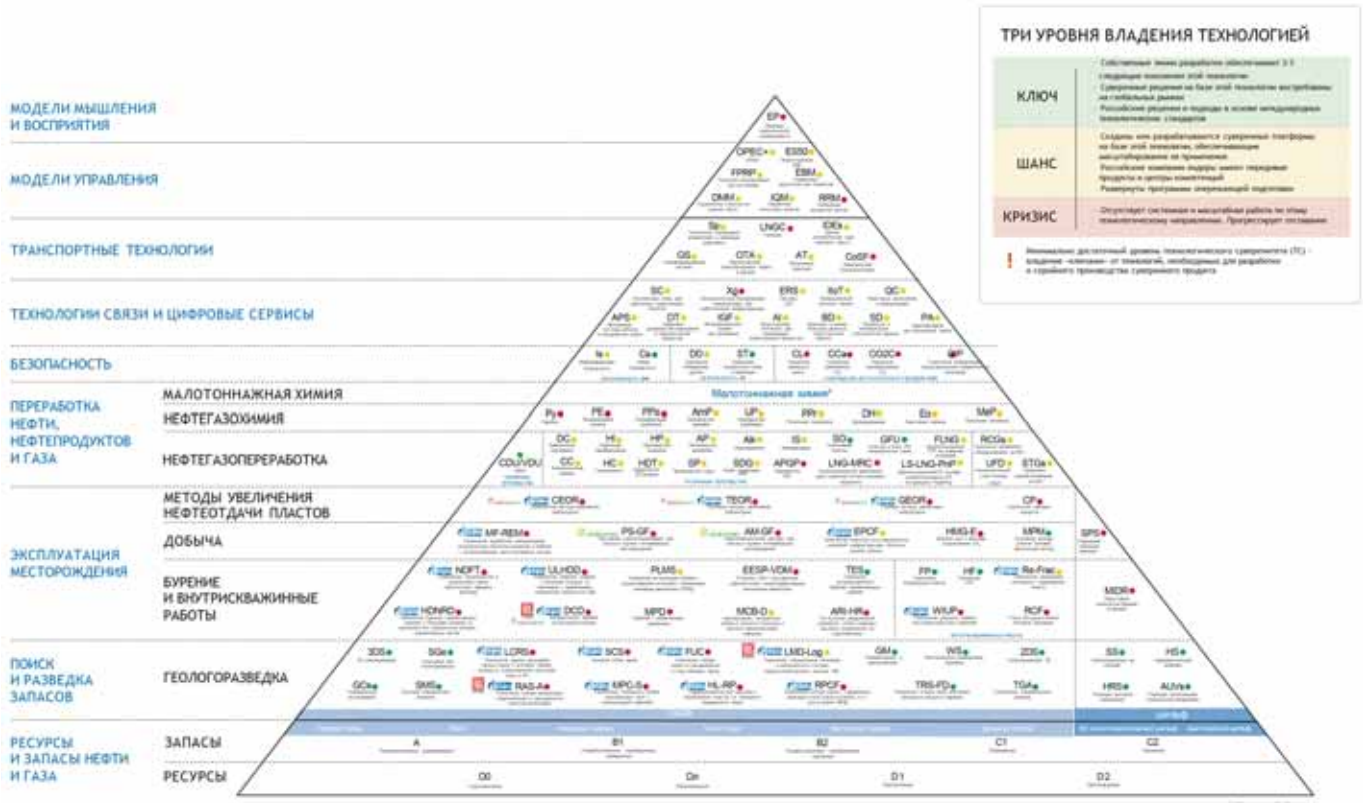

Рис. 2. *Модель технологического суверенитета: энергетика. Нефть и газ*

ИБ как элемент системы управления

В эталонной модели инструменты информационной защиты должны быть частью системы управления компанией: информационная безопасность отвечает за устойчивость и прозрачность процессов деятельности, а также обеспечивает доступность, целостность, конфиденциальность информации и данных, что позволяет оперативно реагировать на изменения.

В условиях расширения ИТ-ландшафтов компаний, а также сложности, масштабов и количества кибератак решение задач ИБ требует значительных инвестиций, если заниматься ими после внедрения или модернизации систем «лоскутным» методом. Важно работать над корпоративной культурой и мышлением сотрудников, корректировать производственные и бизнес-процессы, повышать их формализацию и прозрачность, что является зоной ответственности первых лиц компаний.

Возможно, в типовой модели пирамиды технологического суверенитета на уровне модели управления должен появиться пункт про управление устойчивостью и суверенностью компании, в который войдет управление информационной безопасностью как бизнес-функцией компании.

Например, в организационном управлении есть такое понятие, как «психологическая безопасность» – состояние отношений в команде, составляющих корпоративную культуру, которая создает чувство защищенности каждого сотрудника, при этом он ощущает себя уверенным, свободно выражает мысли, выдвигает гипотезы.

Тем самым формируются предпосылки для роста производительности и бизнес-показателей, потому что проблемные вопросы не замалчиваются, а вскрываются и решаются. Это позволяет каждому сотруднику компании ориентироваться не на себя и внутреннюю политику, а на результат – продукты и сервисы, которые компания предоставляет клиентам, партнерам, государству, обществу.

Исследования показали, что если 60% сотрудников находятся в психологической безопасности, компания получает:

- уменьшение текучести кадров на 27%;
- повышение эффективности труда на 20%;
- снижение количества негативных инцидентов на 40%.

При этом в большинстве компаний лишь 30% сотрудников чувствуют себя в психологической безопасности.

Аналогично и с информационной безопасностью, которая формализует деятельность каждого человека, процесса и его результатов. Если результаты работы использовать только для расчетов риска, наказаний, формального выполнения требований регуляторов, то эффективность компании в целом будет низкая, так как многие данные будут скрываться от руководства или упускаться из виду, оставаться без должного внимания.

Если данные, «вскрываемые» при внедрении и развитии ИБ, использовать как вызовы, которые нужно решать для повышения операционной эффективности и предоставления качественных сервисов (услуг, продуктов) клиентам, то картина меняется в лучшую сторону. Пример упрощенного процесса управления устойчивостью и суверенностью компании в части блока информационной безопасности отражен на рис. 3.

Иными словами, изменение мышления руководителей и сотрудников компании, повышение уровня зрелости психологической и информационной безопасности – первый шаг к надежной и эффективной системе информационной безопасности.

Стоит отметить, что в приказах ФСТЭК № 235 и № 117, Постановлении Правительства № 1272 и Указе Президента № 250 обозначены организационная необходимость и нормативные требования к включению функции информационной безопасности

Рис. 3. *Упрощенный процесс управления устойчивостью и суверенностью компании в области информационной безопасности*

в управление компанией. Руководителям компаний и непосредственно служб ИБ важно приобрести компетенции эффективного управления функцией ИБ как бизнес-инструментом.

Принятие Приказа ФСТЭК от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» означает изменение подходов регулятора к обеспечению информационной безопасности. Данный документ определяет требования к безопасности конкретного класса информационных систем. И как показывает развитие нормативной базы, указанные подходы будут распространяться все шире. Изменение связано, на наш взгляд, с двумя аспектами:

а) закрепление на уровне регулятора в качестве цели обеспечения безопасности информации не только нарушения конфиденциальности, целостности и доступности, но и недопущения негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации (п. 10 требований). Указанная цель является основной с точки зрения организации устойчивого энергообеспечения;

б) оценкой уровня не только защищенности, который определяется через показатель Кзи, но и зрелости процессов обеспечения безопасности информации Пзи (п. 31 требований). Представляется, что текущее развитие нормативной базы подошло к тому уровню, когда требования по обеспечению безопасности информации, общие для всех отраслей, прописаны регулятором максимально детально. Более того, в соответствии с нормативной базой созданы соответствующие подразделения. Задача настоящего этапа – обеспечить эффективность их функционирования, для чего и предназначена оценка уровня зрелости.

Показатели зрелости информационной безопасности

Как следует из нормативных документов, показатель защищенности Кзи может рассчитываться в соответствии с Методикой оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденной ФСТЭК России 2 мая 2024 г. Методика оценки уровня зрелости Пзи пока не представлена, поэтому целесообразно обсудить подходы к ее формированию с точки зрения технологического суверенитета в электроэнергетике.

Предлагается оценивать уровень зрелости обеспечения процессов ИБ по пяти направлениям:

организационно-штатное обеспечение, подразумевающее наличие:
- должности ЗГД по ИБ;
- должности начальника подразделения по ИБ;
- сотрудников подразделения по ИБ;
- контрактов с сервисными организациями;

организационно-плановое обеспечение, предусматривающее наличие:
- политики информационной безопасности;
- годового плана обеспечения информационной безопасности;
- критериев выполнения плана;
- ресурсного обеспечение плана;

процедуры определения формальной и практической защищенности, предусматривающие организацию процессов:
- аттестации защищенных систем по требованиям ИБ;
- анализа угроз;
- управления уязвимостями;
- практической оценки защищенности;

процедуры защиты по цепочкам поставок, подразумевающие:
- применение доверенных ПАК;
- использование сертифицированных средств защиты информации;
- наличие процессов РБПО для собственной разработки;
- наличие процессов проверки поставляемого ПО (методика самотестирования);

мониторинг, предусматривающий:
- взаимодействие с центром мониторинга;
- соблюдение определенных правил;
- передачу сведений об инцидентах;
- получение данных, характерных для предмета мониторинга.

Архитектура информационной безопасности

С организационно-технической точки зрения применяемые меры информационной безопасности должны выбираться, внедряться, настраиваться и эксплуатироваться по принципу нулевого доверия. Дифференцированно следует подходить к каждой локальной системе и компании в целом.

Принцип нулевого доверия означает отсутствие заранее предоставленного доверия к пользователям, устройствам и системам.

Ключевые составляющие нулевого доверия:
- постоянная верификация – каждый запрос на доступ проверяется и анализируется в реальном времени, даже если запрос исходит от внутреннего пользователя;
- минимальные привилегии – каждый пользователь или устройство имеет только тот доступ, который необходим для выполнения конкретных задач. Это ограничивает ущерб в случае компрометации;
- многофакторная аутентификация (MFA) – для доступа используются несколько факторов подтверждения, что усложняет задачу злоумышленникам, даже если они украли пароль или другие данные;

- сегментация сети – сеть делится на изолированные сегменты, для каждого предусматривается своя политика безопасности. Это позволяет ограничить движение данных внутри сети и предотвратить распространение угроз;
- мониторинг и анализ в реальном времени – постоянный сбор и анализ данных о поведении пользователей и устройств помогает выявлять аномалии и возможные угрозы.

Информационная безопасность должна быть реализована на всех этапах жизненного цикла, поэтому речь идет не только о минимизации функциональности создаваемых систем, но и о контроле/ограничении возможностей нерегламентных действий в процессах внедрения, восстановления, обновления, эксплуатации и вывода систем из эксплуатации.

Принцип нулевого доверия трансформирует информационную безопасность в бизнес-функцию, отвечающую за предоставление ясности в ИТ- и ОТ-ландшафтах, что улучшает управление. В частности, формируется среда, в которой все компоненты определены и прослеживается их использование. Кроме того, это позволяет:

а) сэкономить средства на обработке информации благодаря снижению потребности в количестве обрабатываемых данных и информационных потоков, количестве необходимых сотрудников и уменьшению числа возможных сценариев атак;

б) сделать систему более сложной для атакующих, поскольку даже с предоставленным доступом их возможности изменять данные и функции значительно ограничены.

Вместе с тем нельзя не отметить сложность и продолжительность выстраивания системы ИБ с нулевым доверием для крупных компаний, а также ее избыточность для некоторых систем. Поэтому предлагаемая дифференцированная модель доверия подразумевает гибкость набора используемых мер для каждой системы индивидуально, но с учетом специфики деятельности организации, например в отношении:

- критических систем (влияющих на услуги, продукты и сервисы, оказываемые компанией третьим лицам и государству, для электроэнергетики это может быть противоаварийная автоматика и дистанционное управление) – полное нулевое доверие;
- второстепенных процессов (сопутствующих или помогающих, например систем видеонаблюдения, публичных информационных ресурсов) – упрощенные меры.

Не менее важно обеспечить приоритезацию рисков – защищать в первую очередь то, что в случае компрометации остановит основной процесс или вызовет аварию.

Таблица. Пример состава основных блоков системы ИБ для технологического суверенитета

Управление	Стратегия и руководство	Руководство программой безопасности
		Обеспечение соответствия внешним требованиям
	Угрозы и риски	Моделирование угроз
		Подход к управлению рисками
	Поставки и внешние зависимости	Управление безопасностью поставок ИТ-компонентов
		Управление зависимостями от внешних ИТ-сервисов
Меры	Управление доступом	Управление учетными записями
		Контроль доступа
	Защита активов	Управление активами, изменениями и конфигурацией
		Физическая защита активов
	Защита данных	Модель и политика защиты данных
		Реализация механизмов защиты данных
Процессы укрепления безопасности	Уязвимости и обновления безопасности	Поиск и оценка уязвимостей
		Управление обновлениями безопасности
	Ситуационная осведомленность	Мониторинг и отслеживание событий ИБ
		Поддержание осведомленности о состоянии ИБ
	Реагирование и восстановление	План реагирования на инциденты безопасности
		Поддержание непрерывной работы и восстановление

Инструмент устойчивого развития

Для компаний со зрелой системой ИБ указанные принципы, возможно, покажутся банальными. Однако согласно данным ФСТЭК лишь 11% компаний защищены от минимальных кибератак. Исследования центра компетенций «Кибербезопасность» «Энерджинет» показывают, что у более 70% компаний третий или ниже уровень зрелости в сфере ИБ из пяти. Улучшение ситуации зависит от изменения соответствующих взглядов и понимания того, как ИБ, будучи инструментом устойчивого развития и прозрачности процессов, эффективного управления, помогает компании достигать стратегических результатов.

Пример основных блоков системы ИБ представлен в таблице, разработанной Industrial Internet Consortium как «Модель зрелости безопасности Интернета вещей: описание и целевое использование». Стоит отметить, что модель – часть мер информационной безопасности, которые необходимо реализовывать при выполнении требований Закона № 187-ФЗ, приказов ФСТЭК №№ 239, 117, 31, 21 и 17.

Верхушкой модели технологического суверенитета энергетики является способ восприятия. Похоже, пришло время ИБ-сообществу создать свою пирамиду с архитектурой модели системы информационной безопасности (от уровня мышления до уровня базовых ресурсов). В рамках центра компетенций «Кибербезопасность» национальной технологической инициативы «Энерджинет» эксперты приступают к такой работе и будут рады взаимодействию. ■