Отечественное оборудование для электроэнергетики

Есть ли альтернатива импорту?

Уже много лет органами исполнительной и законодательной власти Российской Федерации осуществляются последовательные шаги по развитию импортозамещения в различных областях экономики. Не является исключением и электроэнергетика, вопросы расширения применения отечественного оборудования в которой поднимаются во многих государственных документах, начиная с Энергетической стратегии Российской Федерации.

Андрей ФУРАШОВ[1], Александр КОЗЛОВСКИЙ[2], Владимир МАТИСОН[3]

Исторически сложилось так, что многие объекты, в том числе системообразующие, были модернизированы на базе импортного оборудования ещё до появления полноценных отечественных аналогов, необходимых для модернизации. Сегодня ситуация существенно изменилась — в целом ряде сегментов рынка оборудования для электроэнергетики присутствует российское оборудование, не уступающее по своему техническому уровню продукции ведущих мировых компаний. Это поставило перед российской электроэнергетикой вопрос не только применения такого отечественного оборудования на новых объектах, но и проведения плановой замены импортного оборудования на действующих объектах, в первую очередь по причинам обеспечения энергетической безопасности. Именно в области безопасности, а уже затем в поддержке развития российских производителей лежат основные причины импортозамещения в критической инфраструктуре страны, одной из основных отраслей которой является электроэнергетика.

Средой производства и передачи электроэнергии является первичное оборудование — генераторы, воздушные и кабельные линии электропередачи, выключатели, трансформаторы и другое оборудование, по которому непосредственно течёт электрический ток. Технический уровень этого оборудования определяется его конструкцией и технологиями производства, а также используемыми материалами и комплектующими изделиями. Уникальные технологии предприятий ОПК, научные школы ведущих отраслевых центров позволяют создавать современное оборудование, а там, где имеющихся компетенций не хватает — развивать эти компетенции, привлекая в обоснованных случаях для запуска процесса развития зарубежные.

Само первичное оборудование работает только так, как заложено в его конструкции — исполняя поступающие на него команды. Поэтому надлежащим образом изготовленное и протестированное первичное оборудование само по себе не несёт скрытых угроз.

Формирование управляющих команд, определяющих работу первичного оборудования и в конечном итоге — всей энергосистемы, в автоматическом, полуавтоматическом (автоматизированном) или ручном (по командам оператора) режимах осуществляют контроллеры первичного оборудования, вторичное оборудование и управляющие системы верхнего уровня (специальное программное обеспечение и информационно-коммуникационное оборудование). Ещё до начала широкой цифровизации в электроэнергетике практически всё это оборудование и системы уже строились на базе цифровых

1 Председатель правления Национального совета по энергетической безопасности и защите критической инфраструктуры.

2 Депутат Государственной Думы, председатель Экспертного совета по энергетическому машиностроению, электротехнической и кабельной промышленности.

3 Член экспертного совета Национального совета по энергетической безопасности и защите критической инфраструктуры.

устройств. В эпоху же цифровизации функционал и роль такого оборудования и систем, которые стали фактически IT-инфраструктурой отрасли, многократно возросли. Вместе с этим возросли и угрозы — характерные для IT-сферы и специфические для электроэнергетики. Широко известным стало отключение компрессорных станций «Газпрома», которое произошло в 2012 году по сигналу со спутника именно через цифровое управляющее оборудование.

Федеральный закон № 223 от 18.07.2011 «О закупках товаров, работ, услуг отдельными видами юридических лиц» был принят именно в целях расширения применения отечественного оборудования в целом ряде базовых отраслей экономики, в том числе в энергетических. Этого, по мнению целого ряда экспертов, требуют нарастающие санкции, обострение международной обстановки и конкурентной борьбы в мире. Однако, как отмечали многие спикеры на форуме «Госзаказ-2021», недостаточная система ответственности за выполнение положений этого закона как заказчиками, так и поставщиками не позволила в полной мере достичь поставленных целей, несмотря на то, что российские производители вторичного оборудования имеют производственные мощности, позволяющие полностью обеспечить потребности российской энергетики. Сомневаться же в качестве отечественного цифрового вторичного оборудования для энергетики не приходится, практически все отечественные продукты для этого рынка прошли не только процедуру добровольной сертификации, но и строжайшую отраслевую аттестацию, а целый ряд производителей имеют и сертификаты зарубежных испытательных центров, таких, как, например, DNV GL — одного из мировых лидеров в области консалтинга, испытаний и сертификации для мировой энергетической отрасли.

РИСКИ И УГРОЗЫ – ВЫМЫСЕЛ ИЛИ РЕАЛЬНОСТЬ?

Насколько же велики риски и угрозы от применения импортного оборудования в отечественной электроэнергетике? Стоит ли уделять им столько внимания?

Давая ответ на эти вопросы, оставим в стороне классическую информационную безопасность, о которой сейчас не говорит только ленивый. Её главная рекомендация для технологических систем — создание «воздушного зазора». Это означает исключение какой-либо физической связи технологических систем с корпоративными информационно-коммуникационными системами, особенно имеющими связь с сетью Интернет. Однако, как показывает мировой опыт, такой «воздушный зазор» не является панацеей.

В 2010 году, с использованием человеческого фактора для преодоления такого «зазора», была успешно реализована целевая атака на оборудование объекта по обогащению урана в Иране. Однако одного эффективного использования человеческого фактора для успеха этой атаки было бы недостаточно.

Одним из первых анализ этой атаки выполнил немецкий IT-специалист Ральф Лангер. Он отметил[4], что сложность вредоносного кода, занесённого в «изолированную» (!) технологическую систему, говорит о возможности его создания только большим коллективом разработчиков, содержать который под силу ограниченному числу развитых стран. При этом анализ, выполненный специалистами компании Symantec[5], показал, что этот код был разработан именно под оборудование конкретных производителей (программируемые контроллеры и системы управления частотно-регулируемыми приводами электродвигателей центрифуг), которое было установлено на объекте. Без знаний о том, какое оборудование предполагалось атаковать, успешность атаки была бы маловероятной.

Возникает вопрос — какая связь между этим уже довольно далёким событием в Иране и современными угрозами российской энергетике? Ответ до удивления прост.

Жизненный цикл применения оборудования на объекте электроэнергетики, как и многих других отраслей, состоит из этапов проектирования, строительно-монтажных, пусконаладочных работ и ввода оборудования в эксплуатацию, сопровождения эксплуатации, вывода из эксплуатации и утилизации.

Практически на всех этапах работ, за исключением вывода из эксплуатации и в большинстве случаев утилизации, участвуют специалисты компании, производящей оборудование. Начиная с этапа проектирования компании-производители требуют указания объекта внедрения и полной характеристики условий применения поставляемого оборудования.

4 «Column one: The lessons of Stuxnet», The Jerusalem Post (https://www.jpost.com/opinion/columnists/column-one-the-lessons-of-stuxnet дата доступа 16.06.2021).

5 «Компания Symantec выпустила комплексный бюллетень с описанием вируса W32.Stuxnet, атаковавшего АЭС в Бушере», ИКС медиа (https://www.iksmedia.ru/news/3464312-Kompaniya-Symantec-vypustila-komple.html дата доступа 16.06.2021), Nicolas Falliere, Liam O Murchu and Eric Chien «W32.Stuxnet Dossier Version 1.4 (February 2011)», Symantec (https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf дата доступа 16.06.2021).

В нашем случае это означает в том числе и предоставление полной информации о той части отечественной энергосистемы, в которой находится строящийся или модернизируемый объект, т.е. характеристик этой части энергосистемы и её режимных параметров.

В строительно-монтажных, пусконаладочных работах и вводе оборудования в эксплуатацию специалисты компании, поставившей оборудование, принимают участие как минимум в качестве шеф-инженеров, а часто выступают непосредственными исполнителями работ. Таким образом, информация об энергосистеме становится доступной достаточно широкому кругу лиц, среди которых при использовании импортного оборудования оказываются и иностранные или подконтрольные иностранным юридические и физические лица.

Известны последствия аварии на ПС «Чагино» в мае 2005 года[6], когда дефицит реактивной мощности в энергосистеме, вызванный аварией в одном из её узлов, привёл к крупному региональному нарушению электроснабжения, которое восстанавливали более суток. Тогда по счастливому стечению обстоятельств удалось избежать тяжёлых последствий, но жизнедеятельность более 6,5 млн человек, транспортной инфраструктуры и связи, работа промышленных предприятий были существенно нарушены. Это была техногенная катастрофа, однако не вызывает сомнений, что обладание информацией об энергосистеме создаёт возможность антропогенной инициации аналогичных аварий, если атакующая сторона хорошо знает куда нанести короткий и точный удар (как в каратэ), чтобы парализовать работу энергосистемы или её большой части, питающей важнейших потребителей.

Другого рода угрозы возникают при сопровождении эксплуатации цифрового оборудования. Такое сопровождение подразумевает не только поддержание работы электронных блоков, но и обновления программного обеспечения. А такие обновления создают сразу две угрозы. Во-первых, если поставляемое оборудование проверяется на наличие незадекларированных возможностей, то обновления программного обеспечения такую проверку не проходят и с ними можно занести в устройство любой вредоносный код. А во-вторых, обновления часто производятся дистанционно через сеть Интернет, что требует хотя бы временного подключения к этой сети оборудования электроэнергетического объекта. При этом если время сеанса становится известно иностранным партнерам, то появляется возможность в это же время провести целевую атаку на технологическую сеть объекта.

Таким образом, владея указанной выше информацией, имея знания о доступных уязвимостях и используя те же методы, что и в 2010 году в Иране, можно в нужный момент вызвать серьёзные системные аварии в энергосистеме. Более того, такая информация и знания позволяют выделить критические точки в энергосистеме и планировать террористические акции, при которых, воздействуя на одну из таких точек, достаточно легко можно вызывать такие аварии в нужной части энергосистемы. Именно так в 2021 году в том же Иране была выведена из строя система электроснабжения другого объекта по обогащению урана. Как отмечено в Доктрине энергетической безопасности Российской Федерации, такие события в энергосистеме страны могут привести к «причинению вреда жизни и здоровья граждан и нарушению нормального функционирования организаций, в том числе организаций ТЭК, и отраслей экономики Российской Федерации». Поэтому представляется важным отнесение к обеспечивающим безопасность страны объектов электроэнергетики и, в частности, объектов магистральных системообразующих сетей и объектов, осуществляющих электроснабжение потребителей, обеспечивающих обороноспособность и основные жизненные потребности населения, функционирование органов власти и важнейших отраслей экономики.

Это позволит распространить на объекты электроэнергетики требования, действующие в отношении объектов, обеспечивающих безопасность страны, внедрить при необходимости новые специфические для электроэнергетики комплексные меры, исключающие потенциальную возможность попадания информации о российской энергосистеме к источникам угроз, которые в определённых условиях могут быть реализованы для нарушения работы этой энергосистемы и питающихся от неё потребителей, в том числе обеспечивающих обороноспособность страны. Одной из безусловно важнейших мер является ограничение распространения информации путём соответствующего ограничения круга участников перечисленных выше работ на объектах электроэнергетики только российскими юридическими и физическими лицами, что требует и применения на этих объектах только отечественного оборудования.

В настоящее время такие ограничения в явном виде отсутствуют. Так, например, Приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении тре-

6 «Авария в энергосистеме Москвы 25 мая 2005 года. Досье», ТАСС (https://tass.ru/info/1992764 дата доступа 16.06.2021).

бований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» предусматривает лишь недопустимость передачи «информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны субъекта критической информационной инфраструктуры». Также этот приказ «в случае технической невозможности исключения удалённого доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в значимом объекте» допускает такой доступ с принятием «организационных и технических мер по обеспечению безопасности такого доступа».

Совершенно очевидно, что контроль, предусмотренный в вышеназванном приказе, не уничтожит в памяти контролируемого лица полученную им информацию. Это также позволяет этому лицу быть в том числе и работником зарубежных организаций, а также организаций, находящих под прямым или косвенным контролем иностранных физических и (или) юридических лиц. А отсутствие ограничений на круг лиц, которым может быть предоставлен удалённый доступ к программным и программно-аппаратным средствам объекта, и расположение устройств, «которым разрешён удалённый доступ к программным и программно-аппаратным средствам значимого объекта» позволяет предоставлять удалённый доступ вышеуказанным работникам, в том числе с использованием устройств, расположенных за пределами Российской Федерации. Как при этом исключить занос вредоносного кода — совершенно не ясно.

Современные процессы как в киберпространстве, так и в обороте информации вне цифровых информационно-коммуникационных систем требуют более жёстких и ясно сформулированных ограничений на оборот информации, касающейся значимых объектов критической жизнеобеспечивающей инфраструктуры, как в части её построения, так и, что очень важно, систем, обеспечивающих её операционные технологии.

КАКОЕ ОБОРУДОВАНИЕ – ОТЕЧЕСТВЕННОЕ И ПОЧЕМУ?

До недавнего времени критерием отечественного оборудования было его окончательное изготовление на территории Российский Федерации. Это позволяло называть отечественным оборудованием даже такие устройства, которые локализовались путём изготовления по «отвёрточным» технологиям посредством сборки из готовых импортированных блоков. Для цифровых устройств это означало использование импортных электронных блоков с уже установленным программным обеспечением. В лучшем случае в Российской Федерации производились корпусные детали, а в худшем — импортировались и они. Даже финальные операции заводской наладки и внедрения осуществлялись при этом на основе полученных ограниченных знаний о такой квазилокализованной продукции и реализуемом ею функционале. Говорить о развитии знаний, компетенций, применении доступных высокотехнологичных отечественных компонентов и обеспечении безопасности объектов, на которых применялась такая продукция, при таком подходе к локализации невозможно. Это был путь к наращиванию отставания.

Сегодня ситуация радикально изменилась к лучшему. Понятие «российская продукция» формализовано, и чтобы относиться к её разряду, оборудование должно пройти экспертизу и быть включено в Реестр продукции, произведённой на территории Российской Федерации[7]. Для успешного прохождения экспертизы оборудование должно соответствовать требованиям, указанным в Постановлении Правительства РФ от 17 июля 2015 года № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации».

Одновременно предпринимаются серьёзные усилия для того, чтобы стимулировать приоритетное применение в нашей стране продукции, включённой в вышеуказанный реестр. В первую очередь на это направлен уже упоминавшийся Федеральный закон № 223 от 18.07.2011, а также целый ряд постановлений Правительства РФ.

К сожалению, в ряде случаев постановление № 719 не учитывает техническую специфику, особенно в тех случаях, когда речь идет об оборудовании, которое изначально не было цифровым, но стало им по мере развития. Именно таким является практически всё цифровое электроэнергетическое оборудование. Так, например, требование владения правами на конструкторскую и технологическую документацию не ограничивает возможности передачи таких прав российской дочерней структуре иностранной компании, т.к. не требуется, чтобы эта документация была и разработана в Российской Федерации. Это особенно важно для программного обеспечения, которое определяет весь функционал цифрового оборудования. Было бы целесообразно ввести требование выполнения разработки в РФ

7 Реестр промышленной продукции, произведённой на территории Российской Федерации (https://gisp.gov.ru/pp719v2/pub/prod/ дата доступа 16.06.2021).

в рамках предприятий, не контролируемых иностранными юридическими и физическими лицами.

Одновременно такое усиление требований по выполнению разработки в Российской Федерации будет способствовать реализации общенациональной задачи подъёма отечественной микроэлектроники. Только за счёт применения в отечественных разработках можно сформировать первоначальный спрос на отечественные микроэлектронные компоненты, обеспечить подтверждение их качества, отработать техническую поддержку разработчиков, создав тем самым фундамент для вывода этих компонентов на внешние рынки.

Требования по применению отечественных микроэлектронных компонентов уже вводятся в постановление № 719. Однако тут существуют подводные камни. На XIX отраслевой научно-технической конференции радиоэлектронной промышленности в Ялте в сентябре 2020 года вице-премьер РФ Дмитрий Чернышенко отметил, что «цифровая трансформация невозможна без развития электронной промышленности, это те направления, которые идут рука об руку. Без доступных, надёжных, современных продуктов отечественной радиоэлектроники это сделать будет невозможно, тем более они должны быть созданы так, как требуют сегодняшнее время, ситуация — с учётом требований национальной и информационной безопасности. К сожалению, последние 15 лет импортная техника доминирует на наших рынках. Наша доля — российских производителей — в районе 10%, в ряде сегментов ещё ниже»[8]. В результате этими десятью процентами, обеспеченными имеющимися мощностями и технологиями, наша микроэлектронная промышленность закрывает в первую очередь потребности критических потребителей — предприятий оборонно-промышленного комплекса и производителей космической техники.

Однако поворот к производителям гражданской продукции уже начался. Как отметил на Международном промышленном форуме «Интеллект машин и механизмов» заместитель министра промышленности и торговли РФ Василий Шпак: «Внедряя меры поддержки, мы будем концентрироваться как на создании новых производственных мощностей, так и на модернизации уже существующих. В первую очередь, будем обращать внимание на те критически важные технологические переделы, которые позволят обеспечивать суверенитет и закрывать вопросы, связанные с обороной, а также поддерживать продукты с высокой инвестиционной привлекательностью, высокой серийностью и маржинальностью»[9].

И здесь ключевым фактором, безусловно, является серийность, поскольку развёртывание новых микроэлектронных производств по технологиям, необходимым в гражданской электронной продукции, требует огромных инвестиций. Директор по стратегическому развитию ПАО «Микрон» Карина Абагян в интервью YouTube-каналу PRO Hi-Tech рассказала[10], что инвесторам из Арабских Эмиратов, несмотря на миллиардные долларовые инвестиции в компанию Global Foundries, не удалось выйти на рынок высокопроизводительных микропроцессоров, на котором около 90% занимает тайваньская компания TSMC. А высокую эффективность бизнесу этой компании обеспечивают мегасерийные заказчики, в первую очередь — Apple, AMD, Nvidia, Qualcomm. При этом, по её словам, «фабрику уровня 7 нм можно построить ориентировочно за 15 млрд долларов». Для оптимального использования доступных инвестиционных ресурсов потребуются выверенные решения по стратегии развития отечественного микроэлектронного производства и формирования спроса на его продукцию.

Генеральный директор ПАО «Микрон» Гульнара Хасьянова отмечает, что её компания конкурирует «и в России, и на зарубежных рынках в тех сегментах, где нужны не традиционные шаблонные продукты, а индивидуальные решения, отвечающие требованиям заказчиков»[11]. По её словам, в области продуктов широкого применения «необходимо сформировать внутренний спрос на готовую продукцию, в которой применяются национальные электронные компоненты. А это не может быть сделано одномоментно, так как связано, в том числе, с изменением цепочек поставок, которые складывались на протяжении последних десятилетий. И рынок, и наши конкуренты уйдут дальше, пока отечественные аналоги зарубежных чипов будут осваиваться и внедряться в уже выпускаемые изделия. Поэтому для российской микроэлектроники важны

8 «Чернышенко сообщил, что в России доля отечественной микроэлектроники не превышает 10%», ТАСС (https://tass.ru/ekonomika/9576695 дата доступа 16.06.2021).

9 «В Севастополе проходит Международный промышленный форум «Интеллект машин и механизмов», пресс-релиз Минпромторга РФ (https://minpromtorg.gov.ru/press-centre/news/#!v_sevastopole_prohodit_mezhdunarodnyy_promyshlennyy_forum_intellekt_mashin_i_mehanizmov дата доступа 16.06.2021).

10 «Создание CPU по этапам на заводе Mikron и почему без 7нм остались Global Foundries», видеоматериал канала «PRO Hi-Tech» (https://youtu.be/PVczz3uU3j4 дата доступа 16.06.2021).

11 11 «Русские чипы для цифровой экономики», интервью генерального директора ПАО «Микрон» Г.Ш. Хасьяновой изданию Computerworld Россия (https://mikron.ru/company/press-center/about-us/2409/ дата доступа 16.06.2021).

не только импортозамещение, но и «импортоопережение», то есть разработки для тех областей применения, которые будут расти. Очень важно определить такие рынки и предложить востребованную ими продукцию, предоставить отечественным производителям микросхем возможность развития и увеличения доходов, нарастить инвестиции в перспективные исследования и разработки.

Поэтому так важна уже начатая совместная работа предприятий электросетевого комплекса и генерации с отечественными производителями цифрового оборудования для электроэнергетики и микроэлектронных компонентов. Эта работа как раз направлена на формирование отраслевого спроса на оборудование, использующее в максимально возможном объёме отечественную электронную компонентную базу, и определение этапности изменения требований к этому объёму с учётом имеющихся планируемых технологических возможностей и производственных мощностей отечественных производителей электронной компонентной базы.

Такое взаимодействие участников рынка позволит сформировать и обеспечить загрузку этих производителей большими экономически и технологически целесообразными объёмами универсальных компонентов, что является важнейшим условием поступательного развития отечественного микроэлектронного производства. Одновременно появится возможность обеспечить конкурентоспособные цены и для малых партий специализированных изделий без ущерба для экономической эффективности их производителей — путём дозагрузки технологических линий, на которых производятся массовые универсальные компоненты.

Для цифровой электроэнергетики такими универсальными компонентам являются микроэлектронные компоненты, предназначенные для выполнения периферийных задач — реализации информационно-коммуникационных сетей и ввода/вывода информации. Эти задачи являются общепромышленными не только для электроэнергетики и ТЭК в целом, но и для систем автоматизации других отраслей экономики. Поэтому на первом этапе целесообразно в постановлении № 719 сделать упор на применение отечественных микроэлектронных компонентов, предназначенных для выполнения вышеуказанных задач.

Это логично и с точки зрения приоритетного обеспечения безопасности электроэнергетических объектов, поскольку именно через информационно-коммуникационные сети и устройства ввода/вывода информации происходит доступ к центральным процессорным модулям устройств. Поэтому выполнение этих сетей и устройств на доверенной отечественной электронной компонентной базе минимизирует угрозы нарушения функционирования электроэнергетических объектов путём воздействия на центральные процессорные модули цифрового оборудования этих объектов. В результате создаётся временной запас на перевод без ущерба для безопасности этих центральных процессорных модулей на отечественные микроэлектронные компоненты.

Такой подход позволяет сформировать стратегию пошагового внедрения отечественных микроэлектронных компонентов в оборудование для электроэнергетики, начиная с минимального требования «один микропроцессор/микроконтроллер» и обеспечения при этом экономической эффективности и безопасности реализуемых решений и заканчивая расширенным применением всего доступного спектра изделий отечественной микроэлектронной промышленности.

ЕСЛИ ПОТЯНУТЬ ЗА НИТОЧКУ

Как видим, клубок проблем на самом деле не такой уж запутанный. Стоит потянуть за ниточку обеспечения безопасности работы энергосистемы, как сами собой на неё начинают «нанизываться» решения широкого комплекса задач.

Совместные хорошо продуманные и скоординированные действия регуляторов и профессионального сообщества, безусловно, позволят достичь поставленных целей по обеспечению как надёжного и эффективного электроснабжения, так и технологической независимости ключевых отраслей российской экономики, в том числе электроэнергетической.