IV. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях

DOI: 10.25728/iccss.2023.69.73.038

Белов С.И., Пушкарева М.Б.

Задачи обеспечения кибербезопасности интеллектуальных систем энергоснабжения на розничном рынке электроэнергии

Аннотация: В работе рассматриваются вопросы кибербезопасности интеллектуальных систем управления конечного потребителя на этапе разработки цифровых платформ управления энергоресурсами в промышленных системах на розничном рынке электроэнергии. Проводится анализ процесса развития энергоснабжения потребителей и перехода к платформам распределенной электроэнергетики, в которых информационно-управляющая подсистема сопоставима по сложности и ответственности с физической, что соответственно требует обеспечения безопасной эксплуатации и бесперебойного снабжения потребителей, особенно, в условиях импортозамещения. В настоящий момент времени проблема кибербезопасности цифровой энергетики является ключевой и в дальнейшем эта роль будет только возрастать.

Ключевые слова: кибербезопасность, цифровая энергетика, интернет энергии, распределенная энергетика, управление нагрузкой, микроэнергосистема

Основополагающим документом развития отечественной энергетики является Энергетическая стратегия Российской Федерации на период до 2035 года, в результате которой должно быть обеспечено устойчивое, надежное и эффективное удовлетворение внутреннего спроса на энергетические ресурсы и услуги в сфере энергетики, а также энергетическая безопасность страны и обеспечение антитеррористической защищенности

оборудования и информационной инфраструктуры объектов топливно-энергетического комплекса [1].

При этом в Энергетической стратегии РФ особенно отмечено, что в настоящее время в мировой энергетике, включая российскую, происходят процессы, которые на рубеже 30-40-х годов XXI века приведут к смене сложившегося уклада, особенно, в традиционно сложившейся централизованной системе электроснабжения: углеродная энергетика дополнится возобновляемыми источниками энергии, централизованное энергоснабжение – децентрализованным, существенно расширится спектр применения электрической энергии, активно будут внедряться отечественные технологии, оборудование и услуги в сфере энергетики, последовательно развиваться процессы цифровой трансформации и интеллектуализации учета, анализа и управления процессами генерации, передачи и потребления электроэнергии, новые права и возможности получат конечные потребители энергетических ресурсов для внедрения новых цифровых технологий для анализа режимов работы в процессе реального времени и управления собственной нагрузкой.

Процессы возрастающей активности потребителей в управлении своим энергопотреблением, связанные с повышением энергоэффективности, снижении парниковых выбросов и использовании возобновляемых источников энергии, обеспечении энергетической независимости конечного потребителя, развития малой распределенной генерации и децентрализации энергоснабжения, переходом к информационно-телекоммуникационным технологиям и интеллектуальному управлению являются серьезным вызовом в энергетике. Распределенные (малые) источники генерации энергии принципиально изменяют архитектуру и принципы построения энергосистем, применение интеллектуального прогнозирования для автоматизированного управления режимами позволяет повысить точность их планирования, уменьшить дефицит мощности, снизить финансовую нагрузку на потребителей, минимизировать участие человека в этом процессе. Первичным источником информации в подавляющем большинстве случаев являются современные интеллектуальные системы учета электрической и тепловой энергии, которые позволяют не только собирать информацию

в темпе процесса, но и формировать определенный набор управляющих воздействий. Этот фактор становится значимым не только для электросетевого комплекса, он затрагивает газо-, нефте- и теплоснабжающие системы [2].

Современные генерирующие станции малой и средней мощности стали достаточно дешевыми, надежными, технологичными и эффективными, чтобы собственная генерация на их основе успешно конкурировала с покупкой электроэнергии из сети. Возникает новый формат отношений между розничным производителем и промышленными потребителями электрической энергии требующий структурных преобразований энергетических систем и изменений основных положений функционирования розничных рынков электроэнергии, позволяющий извлечь дополнительные экономические выгоды за счет эффективного управления нагрузкой с помощью цифровых интеллектуальных систем.

Постановление Правительства РФ от 21.03.2020 № 320 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам функционирования активных энергетических комплексов» предоставило возможность запуска пилотных проектов по организации промышленными и коммерческими потребителями микрогридов (используемый официальный термин активный энергетический комплекс – АЭК), где энергопринимающие устройства промышленных предприятий, административно-деловых, спортивно-развлекательных и культурных центров с применением инновационных технологий и управляемых интеллектуальных соединений могут объединяться в целях повышения энергосбережения и снижения финансовой нагрузки за энергоресурсы, ведут к снижению затрат у всех потребителей.

Потенциал российского рынка коммерческих и промышленных микрогридов к 2028 году достигнет 1,2 ГВт в год установленной мощности. Реализация этого потенциала позволит российской экономике, по приблизительной оценке, за 2020-2028 годы получить экономический эффект до 150 млрд рублей за вычетом инвестиций в микрогриды [3].

Новая бизнес-практика создания и обеспечения функционирования микрогридов промышленных и коммерческих

потребителей создает новые возможности не только для организаторов и пользователей этой практики, но и для разработчиков новых технологий и поставщиков технологических решений для микрогридов.

Быстрыми темпами разрабатываются и внедряются цифровые технологии, в состав которых включают интернет вещей, 3D-моделирование, моделирование и прогнозирование на основе анализа «больших данных» (Big Data), интеллектуальные электрические сети (Smart Greed), интеллектуальные датчики и счетчики, нейросети, облачные и туманные вычисления, создающие виртуальную и дополненную реальность, компьютерную имитацию на основе цифровых двойников, роботизацию производства и аддитивные технологии. Все эти технологии начинают активно внедряться на уровне конечного потребителя энергоресурсов для оптимизации управления энергопотреблением для улучшения показателей энергоэффективности и сбережения энергоресурсов.

В энергетической политике России происходит поступательное движение по развитию розничного сегмента электроэнергетики на принципах интернета энергии (Internet of Energy) как «экосистемы» производителей и потребителей энергии, где вместо традиционной системы «производство-распределение-сбыт-потребление» появляется принципиально новая модель свободного обмена энергоресурсами и услугами участниками рынка.

Цифровое преобразование энергетики позволяет на базе интегрированных отраслевых цифровых платформ нового поколения обеспечить равный доступ массовых рядовых участников розничного энергетического рынка к полному спектру возможностей и функций субъектов энергетики. Каждый владелец даже небольшой мощности генерирующего оборудования имеет возможность не только потреблять энергетические ресурсы, поставляемые уполномоченными операторами централизованных энергосистем, но и самостоятельно генерировать, хранить и передавать в общую сеть часть собственных энергоресурсов [4].

Современные цифровые технологии благодаря своему быстродействию позволяют практически в режиме реального времени отслеживать меняющиеся процессы в работе различного оборудования и технологических процессов, представлять эту работу в удобном для быстрого анализа форме, прогнозировать

нагрузку, своевременно реагировать на критические отклонения от нормального режима работы и автоматически управлять режимами работы различного оборудования.

С развитием распределенной генерации, с появлением все большого количества потребителей в промышленности и вплоть до уровня домохозяйств, позволяющих активно изменять привычные профили нагрузок, усложняются цифровые модели для прогнозирования и управления энергопотребления.

Совершенствование энергоэффективных и цифровых технологий приводит к масштабной смене технологического уклада в энергетике, неизбежно меняет облик всех существующих в мире энергосистем и формирует новые принципы управления ими. Идет постепенная интеграция систем электро-, тепло-, газо-, хладоснабжения в единую энергетическую экосистему, базирующуюся на инновационных технологиях и интеллектуализации энергопотребления. Возрастающая роль потребителей в управлении энергопотреблением, использование собственных источников генерации и альтернативных источников энергии, применение умных сетей, совместное производство электроэнергии, тепла и холода на уровне генерации и объединение потребителей в микросистему с интеграцией систем энергоснабжения конечного потребителя в единую энергетическую энергосистему требует пересмотра принципов построения, функционирования и развития энергосистем. Цифровизация интегрированных энергетических систем и их интеллектуализация охватывают широкий комплекс вопросов, включая технические, организационные, регуляторные, экономические и другие.

Развитие энергетики и, особенно, электроэнергетики в XXI веке идет настолько бурными и революционными темпами, что, соответственно, требует совершенно новых подходов и знаний в управлении этими процессами, включая управление потреблением энергетических ресурсов в целях повышения энергетической эффективности всех конечных пользователей: от крупных предприятий до небольших организаций, населения и домохозяйств.

В условиях децентрализации архитектуры энергосистем появляется возможность совместной работы огромного множества распределенных потребителей, при этом с числом участников

взаимодействия растет сложность управления цифровой и технологической базой большого количества участников. Пользователи такой системы могут быть владельцы любого генерирующего, накапливающего и потребляющего энергетического оборудования (промышленного, коммерческого, бытового), имеющего общую точку присоединения к энергетическим сетям и информационным каналам, интегрироваться в систему через интерфейсы и стать полноценными участниками новых сервисов и бизнес-моделей интернета энергии, оказывая друг другу услуги, например, такие как поставка электрической энергии.

Малая генерация, системы накопления энергии, регулируемая нагрузка конечных потребителей, интегрированные между собой и с централизованной энергосистемой, представляют собой неиспользованный до сих пор ресурс для повышения эффективности энергосистем. Распределенная энергетика повышает эффективность энергосистемы за счет снижения потребности в присоединенной мощности, появления локальных самобалансирующихся объединений генераторов и потребителей малой мощности, масштабного вовлечения массы небольших, но многочисленных энергетических активов конечных пользователей в процессы управления энергосистемой. Энергосистема, обладающая способностью к интеграции новых пользователей и децентрализованному управлению большим множеством распределенных энергетических объектов, будет играть решающую роль развития электроэнергетики в ближайшее время [5].

В будущих распределенных энергосистемах информационно-коммуникационная составляющая процессов управления силовым оборудованием становится все более сложной и ответственной с точки зрения обеспечения нормального функционирования и возрастающих требований потребителей к надежности их электроснабжения и качеству поставляемой им электроэнергии. В условиях цифровизации такую энергосистему во все большей мере требуется рассматривать как сложный кибер-физический комплекс, имеющие новые свойства и обостряющиеся проблемы надежности и кибербезопасности.

В этом направлении необходимо проведение разносторонних исследований, рекомендации которых позволят обеспечить

необходимый уровень кибербезопасности цифровых интеллектуальных энергосистем. Множественные примеры реальных ситуаций кибератак на электроэнергетические объекты промышленных предприятий, подстанций, электростанций и анализ результатов в части формирования сценариев потенциально возможных кибератак для выявления уязвимых мест и разработки кибер-физических моделей энергосистемы для исследования последствий кибератак для обоснования мероприятий по противодействию киберугрозам и снижению негативных последствий в результате их возможной реализации приведены в [6].

Постоянно растет и развивается множество потребителей нового поколения с применением современных технологий и электрооборудования с интеллектуальными свойствами, использованием собственных объектов генерации, ВИЭ и систем накопления энергии. Это – высокотехнологичные и роботизированные предприятия, системы жизнеобеспечения, энергоэффективные здания, центры обработки данных (ЦОД) и другие потребители, требующие особых условий надежности и качества электроснабжения.

В связи с интенсивным развитием распределенной генерации и автоматически управляемого электрооборудования на стороне потребителя объемы вовлекаемых в управление объектов генерации могут быть очень серьезными, а количеством самих активных потребителей и управляемого оборудования на их стороне с многообразием типов потребителей, их свойств и запросов могут на порядки превышать масштабы управления в традиционной электроэнергетике.

Электроснабжение активных потребителей должно быть обеспечено инфраструктурой интеллектуальных измерений с интеллектуальными датчиками и счетчиками контроля коммерческого и технологического расхода электроэнергии для энергоэффективного управления собственным энергопотреблением и взаиморасчетов в режиме реального времени за полученную или отданную электроэнергию между другими участниками локального розничного рынка энергоресурсов.

Эти приборы, помимо выстраивания системы интеллектуального управления спросом, могут обеспечить контроль

надежности электроснабжения, качества электрической энергии и являются интерфейсом для связи с агрегатором и существующим оператором рынка на верхнем уровне для интеграции распределенной генерации разного типа в сеть общего пользования.

В соответствии с бизнес-моделью агрегатор АЭК должен собрать мощность всех потребителей и осуществлять с помощью весьма продвинутых и новых технологий биллинговых расчетов, смарт-контрактов и технологий распределенных реестров рассчитываться с клиентом. Такое участие происходит в реальном времени, требует автоматической регистрации сделки и развития универсальной системы связи от бытовых сетей до центров диспетчерского управления верхнего уровня, основанной на единых моделях данных.

Крайне критичным моментом для насыщенной различным электрооборудованием и цифровым продуктом микроэнергосистемы является зависимость надежности работы такой системы от сети общего пользования. Внезапное нарушение внешнего электроснабжения, если распределенные объекты собственной генерации не смогут мгновенно обеспечить достаточную мощность для надежного энергоснабжения потребителей микроэнергосистемы, может привести к коллапсу локального характера: потере не только электроснабжения, но и водоснабжения, теплоснабжения, газоснабжения, а также Интернета.

С другой стороны, внезапные нарушения внутри микроэнергосистемы может повлиять на устойчивость и надежность энергосистемы высшего уровня, к которой присоединен АЭК. Практика технологического/режимного/противоаварийного управления в энергосистеме такова, что конечный потребитель всегда рассматривался как пассивный элемент, подчиненный системным задачам. Система автоматического мониторинга и управления со стороны системного и рыночного операторов энергосистемы не доходит до уровня среднего напряжения конечного потребителя, при этом распределительные сети среднего напряжения проектируются и эксплуатируются для радиального режима работы и не предполагают приема мощности от конечного потребителя. Существующих средств связи системных операторов

совершенно недостаточно для их настройки на новые объекты и задачи технологий активного потребителя.

Таким образом, для существующей системы управления в электроэнергетике в технологическом и рыночном/торговом аспектах решение данных задач начинается с чистого листа.

Эффективное использование ресурсов активного потребителя требует развития моделей рынка, сферы системных услуг, в том числе процесса ценообразования на розничном рынке в режиме реального времени, выстраивания целостной системы управления спросом и кардинального развития цифровых платформ управления технологических и информационных платформ надежного взаимодействия многочисленных участников системы активного потребления энергоресурсов на розничном рынке.

Вопросы кибербезопасности в связи с распространением концепции интеллектуальных систем энергоснабжения на розничном рынке электроэнергии должны рассматриваться во взаимосвязи в энергетической безопасностью России, поскольку энергетика связана со всеми отраслями и во многом обеспечивает их функционирование. Возрастание угроз кибербезопасности с развитием интеллектуальных энергетических систем, а также с повышением уровня компьютеризации и интеллектуализации энергетики необходимо рассматривать как одну из важнейших современных угроз энергетической безопасности России.

Повышенная сложность информационной сети повышает количество уязвимостей для потенциальных атак и непреднамеренных ошибок. Сети, взаимосвязанные с другими сетями, которые также могут занимать несколько «умных» доменов сети, увеличивают вероятность каскадных аварий. Большое количество взаимосвязей программных компонентов увеличивает уязвимость программного кода, что упрощает злоумышленникам внедрение в программный код вредоносного кода и уязвимостей. По мере увеличения узлов сети увеличивается и число точек входа в систему для злоумышленников.

В России до сих пор нет однозначного понимания кибербезопасности. Часто ее считают синонимом информационной безопасности или ее составляющей, в силу чего кибербезопасности не уделяется достаточного внимания. Кибербезопасность целесообразно рассматривать как результат конвергенции пяти

основных составляющих: безопасность приложений, информационная безопасность, сетевая безопасность, безопасность интернет-приложений, защита ключевых информационных систем объектов критических инфраструктур.

Внедрение современных информационных технологий и повышение уровня интеллектуальности энергетических систем усугубляет проблему кибербезопасности, и, соответственно, энергетической безопасности

Среди этих угроз до последнего времени не рассматривались угрозы кибербезопасности, реализация которых может спровоцировать серьезнейшие чрезвычайные ситуации в энергетике, чреватые значительным снижением возможностей обеспечения энергоресурсами потребителей.

Например, в случае успешной атаки киберпреступников на компьютеры, контролирующие работу энергосистемы, локальные аварии могут перейти в общесистемные и последствия могут быть катастрофическими для целого города, региона или даже страны.

В последние годы в России активно ведутся исследования в области кибербезопасности электроэнергетических систем (ЭЭС). Это обусловлено участившимися кибератаками на ЭЭС, уязвимость которых возросла в связи с их интеллектуализацией и цифровизацией, в результате чего ЭЭС превратились в кибер-физические системы, в которых информационно-управляющая подсистема сопоставима по сложности и ответственности с физической.

Киберугрозы, возникающие как результат применения современных ИТ, можно рассматривать на примере мультиагентного подхода к системам, которые открыты к большим потокам разнородных данных от разнородных источников и возможности подключения новых типов агентов, поэтому являются принципиально уязвимыми с точки зрения кибербезопасности, и необходимы новые способы обеспечения ее безопасности и устойчивости по отношению к отношению к намеренным кибератакам. Для этого она должна быть защищена по отношению к возможным кибератакам и уметь эффективно работать в условиях поступления сверхбольших потоков данных разного качества и достоверности. В противном случае уязвимая система управления станет причиной крупных техногенных аварий. Анализ системных

аварий свидетельствует о том, что несовершенство алгоритмов систем управления увеличивает масштаб последствий, когда локальные аварии переходят в общесистемные. Так, с 2010 года в 20 раз выросло число обнаруженных уязвимостей, при этом каждая пятая уязвимость устранялась дольше месяца [7].

Входящая в структуру АЭК на розничном рынке электроэнергии организация может быть самого разного вида деятельности, организационной структуры, количества и наличия подготовленного персонала, требований по кибербезопасности, в том числе понятие информационной безопасности и безопасности информационных технологий и распространяются на процессы в области информационных технологий, включая облачные сервисы, сервисы эксплуатации, технической поддержки, мониторинга и обслуживания сетевой инфраструктуры, вычислительных систем, комплексов и программного обеспечения, предоставляемых внешним и внутренним клиентам, которые обеспечивается эффективным сочетанием организационных, методических мер и программно-технических средств.

В сфере энергетического оборудования различных организаций существует чрезмерная зависимость от импорта многих видов технологий, систем автоматизированного контроля и управления оборудованием (датчики, контроллеры, микроэлектроника), программного обеспечения и различных приложений зарубежных производителей, усугубляющаяся монопольным положением их поставщиков. Так, например, у большого количества потребителей энергоресурсов основными производителями системы контроля и сбора данных SCADA являются иностранные компании, что также является одной из угроз кибербезопасности. Следует отметить, что это оборудование и программное обеспечение может давно не обновляться и не соответствовать современным требованиям кибербезопасности. Устаревшее ПО является идеальной мишенью для хакеров, поэтому производственные компании должны подготовить свои системы SCADA к потенциальным киберугрозам и внешним уязвимостям.

Помимо устаревшего ПО слабыми местами также можно назвать отсутствие безопасного удаленного доступа и регулярного контроля конфигураций, отсутствие разграничений

прав доступа, контроля над запуском различных приложений извне и многое другое.

В подавляющем большинстве случаев причиной возникающих киберугроз в настоящее время современных условиях являются не технологии, а человеческий фактор, который имеет часто большее значение, чем технические особенности атаки. Многие сотрудники организаций имеют возможность работать удаленно и могут использовать свой личный телефон для рабочих целей или получать доступ к электронной почте своей компании через личные устройства. Уязвимости пользователей начинаются с их цифрового поведения – как они работают и на что они кликают.

Смартфоны по своей сути являются персональными, они содержат ценную информацию о нашей деятельности, отношениях, финансах, симпатиях и антипатиях, все больше стирают грань между личным и профессиональным, что делает телефоны привлекательной целью для кибератак. Личные устройства могут не иметь такого же уровня защиты, как рабочие устройства, а сотрудники соответствующей подготовки в вопросах безопасности. Поэтому, с сотрудниками компаний должно регулярно проводиться обучение в области кибербезопасности с учетом всех изменений в деятельности компании.

Сегодня из-за нестабильной геополитической ситуации все это делает энергетическое оборудование удобным объектом для нападений киберпреступников и может стать причиной уязвимости участника АЭК для зарубежных хакеров и повлиять на надежность работы самой микроэнергосистемы в целом.

Тема технологической независимости отечественных решений стала одной из самых важных на российском рынке в последние годы. Киберугрозы представляют серьезную опасность для энергетического сектора, поэтому компании, занимающиеся технической поддержкой, активно внедряют новые решения для противодействия этим угрозам.

Тренд на импортозамещение в ключевых отраслях энергетики России активно развивается в последние годы, многие госпредприятия и корпорации переходят на отечественные технологии и внедряют современные импортонезависимые российские платформы для управления энергоресурсами. Это касается и инструментов защиты от кибератак.

Литература:

1. Энергетическая стратегия Российской Федерации на период до 2035 года. – URL: https://minenergo.gov.ru/node/1026 (дата обращения 20.09.2023).

2. *Стенников В.А*. Устойчивое развитие энергетики: тенденции и вызовы // Энергетическая политика. – 2023. – № 2. – С. 47-54.

3. Активные энергетические комплексы — первый шаг к промышленным микрогридам в России: экспертно-аналитический доклад / Под ред. Д. Холкина. – М.: Инфраструктурный центр «Энерджинет», 2020. – 58 с. – URL: https://www.np-sr.ru/ru/content/50156-aktivnye-energeticheskie-kompleksy-pervyy-shag-k-promyshlennym-mikrogridam-v-rossii (дата обращения 20.09.2023).

4. *Холкин Д., Чаусов И., Бурдин И., Рыбушкина А.* Архитектура Интернета энергии (IDEA). Версия 2.0 2021. – Инфраструктурный центр «Энерджинет», 2021. – 77 с. – URL: https://idea-go.tech/IDEAwhitepaper-ru.pdf (дата обращения 20.09.2023).

5. *Хохлов А., Мельников Ю., Веселов Ф., Холкин Д., Дацко К.* Распределенная энергетика в России: потенциал развития. – Энергетический центр Московской школы управления СКОЛКОВО, 2018. – 89 с. – URL: https://energy.skolkovo.ru/downloads/documents/SEneC/Research/SKOLKOVO_EneC_DER-3.0_2018.02.01.pdf (дата обращения 20.09.2023).

6. *Воропай Н.И., Колосок И.Н., Коркина Е.С., Осак А.Б.* Киберугрозы и кибербезопасность в электроэнергетических системах / Электроэнергетика глазами молодежи-2019: материалы юбилейной X Международной научно-технической конференции. Том 1. – Иркутск: Иркутский национальный исследовательский технический университет, 2019. – С. 32-37.

7. *Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Т.* Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. – 2016. – № 4. – С. 2-10.