3. Tyurin Yu.N., Makarov A.A. Statisticheskij analiz dannyh na komp'yutere [Statistical analysis of data on a computer]. Moscow: INFRA-M, 1998. 528 p.

INFORMATION ABOUT THE AUTHOR

KACHANOVSKY Felix Vjacheslavovich – Associate Professor of the Department of Hydraulics, Heat Engineering and Hydraulic Drive, Tver State Technical University, 22, embankment Af. Nikitin, Tver, 170026, Russia. E-mail: felix.kachanovscky@yandex.ru

CITATION FOR AN ARTICLE

Kachanovsky F.V. Analysis of the electrical conductivity of the precipitation in Tver during 2016–2020 years // Vestnik of Tver State Technical University. Series «Building. Electrical engineering and chemical technology». 2021. No. 2 (10), pp. 47–56.

УДК 621.316:005.334

УПРАВЛЕНИЕ РИСКАМИ И НАДЕЖНОСТЬЮ В СИСТЕМАХ ЭЛЕКТРОСНАБЖЕНИЯ

К.Б. Корнеев, Ю.М. Павлова, Р. Осеи-Овусу
Тверской государственный технический университет (г. Тверь)

© Корнеев К.Б., Павлова Ю.М.,
Осеи-Овусу Р., 2021

Аннотация. Отмечено, что функционирование развивающихся электрических сетей с распределенной генерацией и управлением спросом требует совершенствования подходов к управлению надежностью системы. Сделан вывод, что оценка рисков и эффективное планирование могут осуществляться только на основе высококачественного системного анализа существующей инфраструктуры, учета всех факторов. Рассмотрены некоторые риски (в первую очередь связанные с информационной безопасностью), которые требуют всестороннего исследования в целях недопущения возникновения аварийных ситуаций.

Ключевые слова: энергосистема, риски, надежность, «Интернет вещей», безопасность, управление, распределенная генерация, управление спросом, альтернативная энергетика.

DOI: 10.46573/2658-7459-2021-56-67

В настоящее время развитая электроэнергетическая система вынуждена обрабатывать растущее количество «субсекундных» событий, которые требуют времени отклика, слишком короткого для того, чтобы операторы системы (диспетчеры) могли отреагировать на них. Одной из современных тенденций, делающих «умные» сети необходимыми, является распространение «умных» устройств. При этом каждый элемент «умной» сети может быть подвержен микроскопическим сбоям частоты, что создает

новую проблему для системных операторов. Многие бытовые электронные устройства (например, мобильные телефоны, решения для домашней автоматизации на основе Wi-Fi и интеллектуальные развлекательные устройства) представляют собой конечные точки, которые могут влиять на работоспособность системы. Кроме того, устройства «Интернета вещей» (IoT) работают на микросекундных тактовых частотах. Эти устройства являются новым источником изменчивости нагрузки и информационных потоков на скоростях, намного превышающих те, которые традиционно используют в электрических сетях. Решение должно заключаться в использовании защитных реле и синхронизирующих устройств, работающих более или менее автономно в реальном времени. Перспективные решения для строящихся и реконструируемых сетей должны предусматривать процесс их функционирования. Отметим, что оцифровка сетевых операций на глубину менее секунды создает новые уязвимости в киберпространстве [1–3].

К сожалению, на данный момент технологический рост и внедрение новых автоматизированных систем значительно опережают развитие нормативной базы, регулирующей аспекты интеграции этих технологий в существующую инфраструктуру. Это приводит к тому, что технологические разработки проходят «обкатку на месте», при этом их функционирование далеко не всегда согласуется с действующими стандартами. Существует также явная проблема частичной или полной несовместимости конечных устройств разных производителей в плане информационного обмена [4].

С помощью современных систем управления сетью в настоящее время обрабатывают, определяют и контролируют огромное количество конечных устройств. Широкое распространение распределенной генерации и управление спросом на электроэнергию подразумевают, что будущим системам управления сетью, возможно, придется координировать миллионы устройств управления конечными точками для поддержания нормального функционирования сети. Эти устройства различают по типу: цифровые датчики и интеллектуальные платы, встроенные в трансформаторы; мобильные устройства, используемые полевыми операторами и менеджерами для управления сетями, и т. д.

Существующие системы управления сетью не структурированы для крупномасштабной оптимизации миллионов устройств и не оборудованы для обработки все возрастающих объемов и типов данных. Конечные пользователи (потребители, а также группы потребителей с разными профилями спроса на электроэнергию) могут захотеть осуществить оптимальное локальное управление для удовлетворения своих потребностей, которые могут вступать в конфликт с оптимальным общесистемным контролем [5].

Системы управления сетью должны превратиться из централизованных в гибридные (центральных и распределенных платформ управления). Потребность в гибких сетевых операциях ставит под сомнение базовые предположения об управлении сетью, что предполагает изменение стандартов и операционных протоколов. Операции с большими энергосистемами входят в компетенцию регулирующих органов, таких как Министерство энергетики, но пока что имеется проблема информационного характера (в плане безопасности и надежности информационной составляющей сети), которая не может быть решена по причине значительной взаимосвязи с другими инстанциями, регламентирующими и регулирующими функции информационного обмена в общедоступных и закрытых сетях передачи данных.

К сожалению, в России стали утверждать стандарты, регулирующие «Интернет вещей» [6], на 5 лет позже, чем в США и других странах: 15 ноября 2016 года

Министерство внутренней безопасности США разработало стратегические принципы [7], направленные на сокращение числа уязвимостей, порождаемых «Интернетом вещей», с помощью признанных передовых методов обеспечения безопасности. Эти принципы призваны служить руководством для заинтересованных сторон в их стремлении избежать проблем безопасности «Интернета вещей». Суть состоит в следующем:

1. Обеспечение безопасности на этапе проектирования сокращает потенциальные сбои и позволяет избежать сложных и дорогостоящих попыток сделать продукты после их разработки и внедрения безопасными.

2. Обязательны обновления безопасности и управление уязвимостями: уязвимости могут быть обнаружены в продуктах уже после их развертывания. Эти недостатки можно и нужно устранять с помощью исправлений, обновлений безопасности и стратегий управления уязвимостями.

3. Необходимо основываться на проверенных методах обеспечения безопасности. Многие из них, используемые в традиционных информационных технологиях и сетевой безопасности, могут быть применены к IoT: они также помогают выявлять уязвимости, обнаруживать нарушения, реагировать на потенциальные инциденты и восстанавливаться после повреждения или сбоя в работе устройств IoT.

4. Требуется расставлять приоритеты для обеспечения мер безопасности в соответствии с потенциальным воздействием: модели рисков существенно различаются в экосистеме «Интернета вещей», поэтому последствия сбоя безопасности для разных клиентов также будут значительно различаться. Таким образом, сосредоточение внимания на потенциальных последствиях сбоев, взлома или злонамеренных действий для всего спектра потребителей имеет решающее значение при определении того, на что следует направить конкретные усилия по обеспечению безопасности и кто лучше всего сможет смягчить серьезные последствия возникших сбоев в функционировании электросетевого комплекса.

5. Бо́льшая прозрачность «Интернета вещей» означает, что повышение уровня осведомленности может помочь производителям и промышленным потребителям определить, где и как применить меры безопасности, обеспечить избыточность; производители и промышленные потребители будут лучше подготовлены для надлежащей минимизации угроз и уязвимостей, станут осуществлять ее как можно быстрее.

6. Подключаться требуется осторожно и осознанно. Иными словами, потребители «Интернета вещей» могут также помочь в устранении потенциальных угроз, создаваемых подключением к сети, благодаря тому, что будут подключаться осторожно и намеренно и взвешивать риски потенциального взлома или отказа устройства «Интернета вещей» с затратами на ограничение подключения конечных устройств к интернету.

Следует отметить, что даже издание нормативных и регламентирующих документов зачастую не приводит к существенным сдвигам в обеспечении кибер-безопасности объектов энергетики. Ярким примером являются попытки взлома энергетических объектов по всему миру [8–10]. При этом некоторые из этих попыток могут оказаться успешными и их не обнаруживают на протяжении достаточно большого количества времени [11].

Технология управления спросом дает потребителям возможность изменить обычные модели потребления электроэнергии и выступает, таким образом, гибким сетевым ресурсом, способным повысить надежность системы, снизить рыночные цены на электроэнергию, а также потребность в капитальных вложениях для удовлетворения

пикового спроса. Эта технология также может использоваться для минимизации нагрузки и формирования прироста нагрузки, а также для того, чтобы помочь сетям уменьшить изменчивость генерации.

Существует множество программ аварийного восстановления. Некоторые из них предлагаются непосредственно энергетическими компаниями или же операторами электросетей. Таким образом, внедрение управления спросом изменяет привычные понятия «разрешенная мощность» и «установленная мощность», так как каждая из этих величин в рамках реализации технологии может быть вариативной. Однако в плане тарифообразования и определения технологических норм для подключения к существующей электрической инфраструктуре (подстанциям и линиям электропередач) реализация такого подхода приводит к возникновению существенных рисков, связанных с неопределенностью. Тем не менее благодаря внедрению согласованного управления на базе распределенной генерации, систем интеллектуального управления потоками мощности, большей автоматизации производственных процессов с минимальной зависимостью от человеческого фактора станет возможным значительно сместить потребительский спрос с пиковых периодов на непиковые.

Имеются серьезные проблемы, которые мешают сделать ресурсы аварийного восстановления надежными, предсказуемыми и устойчивыми, что могло бы способствовать их функционированию в роли резервного генератора. Для создания надежных, предсказуемых и устойчивых ресурсов нужны развитая система учета, наличие фактических возможностей у энергосистемы динамически управлять (не в одностороннем порядке отключать, а согласованно уменьшать расход электроэнергии) работой потребителей. До тех пор, пока не будут приняты единые стандарты, обеспечивающие точность и достоверность данных, получаемых операторами электросетей, сведения о мощности аварийного восстановления не будут учитываться операторами сети: предполагаемый ресурс аварийного восстановления мощностью 100 МВт, который теоретически может быть введен, не означает, что 100 МВт мощности потребителей будут быстро выведены из электрической сети. Существующий нормативный документ [12] предусматривает некоторые меры, улучшающие ситуацию, однако из-за низкой автоматизации и значительной потребности в согласованиях всех этапов процесс координирования мощностей является долгим (может занимать несколько часов), что нивелирует всю концепцию динамического управления (т. е. реагирования в течение секунд или нескольких минут).

Топографический и географический факторы могут оказывать дополнительное и очень важное влияние на возможность решения основных задач управления энергосистемой. Так, информационно-коммуникационные технологии (ИКТ) работают гораздо менее эффективно в гористой местности или городской инфраструктуре, так как не удается обеспечить надежность и необходимую скорость передачи беспроводного сигнала. Разработчикам интеллектуальных сетей приходится создавать избыточность, чтобы справиться с определенной топографической асимметрией (используют при этом несколько информационных каналов). Кроме того, переход на новые беспроводные стандарты (5G, WiFi) и одновременно повышение скорости передачи данных, уменьшение задержек сигнала снижают дальность передачи сигнала, что может отрицательно сказаться на функционировании сетей, а также увеличить капитальные затраты на информационную инфраструктуру. В данном случае отказ от перехода на современные стандарты не является выходом. Объясняется это также и тем, что в ряде существующих стандартов

связи выявлены неустранимые критические уязвимости, которые могут быть использованы для неавторизированного доступа и вмешательства в функционирование работы электрических сетей, что недопустимо.

Внедрение технологии распределенной генерации может привести в определенных городах к значительным нагрузкам на местную инфраструктуру, в том числе на трансформаторы и подстанции, что может породить серьезные проблемы для местных энергокомпаний. Особенно важным этот фактор становится, если элементы распределенной генерации и группы потребителей образуют своеобразные кластеры. В данном случае системные операторы должны будут более детально следить за состоянием сети, а изменения топологии сети для смягчения эффектов кластеризации станут важными путями адаптации сети к влиянию потребителя на нее и ее работу. Поскольку поведение потребителей может резко меняться, новые процессы проектирования сетей должны работать быстрее (начиная от процессов базовой архитектуры и заканчивая процессами, происходящими при фактическом развертывании) [13]. Регулирующие органы обязаны мгновенно учитывать дополнительные системные затраты, которые вызваны операторами сетей, предугадывающими проблемы и принимающими меры для их смягчения до того, как возникшие сбои приведут к отключениям сети.

Таким образом, надежность становится двусторонним процессом: в нем оказываются задействованы и операторы сети, и потребители. Надежность сети, предполагающая обеспечение долгого времени безотказной работы системы, теперь обусловливается «надежностью потребителей». Ранее понятие «надежность электроснабжения» обычно было синонимично понятию «надежность сети» (или «надежность системы»). Надежность потребителей формируется инициативами, реализуемыми на протяжении последних десятилетий. Эти инициативы направлены на постоянное повышение энергоэффективности, внедрение распределенной генерации, интеграцию «Интернета вещей», а также смещение приоритета потребителей (особенно коммерческого сектора) на услуги бесперебойного питания. Растущая взаимозависимость между операторами сети и потребителями – двусторонний поток информации и мощности – означает, что надежность сети может повыситься только в случае, если произойдет интеграция действий потребителей в работу сети.

Сегодня многие категории потребителей так или иначе взаимодействуют с электросетями. У клиентов есть инструменты для изменения своих моделей потребления в ответ на ценовые сигналы (дифференцированные по времени и зонам тарифы), а также на запросы от сетевых операторов. Иными словами, произошло существенное изменение потребителя: из фигуры с пассивной нагрузкой он стал клиентом, который активно участвует в управлении спросом. В течение 10–15 лет многие новые устройства, которые, вероятно, станут частью нашей электроэнергетической системы (включая большие электростанции и собственные мощности малой энергетики, домашние накопители энергии и динамично управляемые светильники в составе уличного освещения, трансформаторы и электромобили), также будут иметь цифровую связь с сетью. Большинство этих устройств смогут «видеть» другие элементы в общей сети и динамически менять правила своего поведения. Двунаправленный обмен информацией с потребителями может привести либо к активному участию последних в сетевых операциях на многих уровнях (например, клиенты смогут реагировать на сигналы времени использования или цены в реальном времени), либо к пассивному, т. е. с помощью устройств, предназначенных для отображения информации о потребителях, которые

реагируют на изменения тарифов и оперативные сигналы. Прозрачность и одновременно защищенность этой связи являются ключевыми факторами работы и управления энергосистемой, имеют большое значение в плане надежности как для клиентов, так и для системы в целом.

Реакция потребителей на сигналы от энергосистемы может быть более точной, своевременной и предсказуемой благодаря улучшенным средствам обеспечения ИКТ и лучшей аналитике на стороне сети, ориентированной на управление общей надежностью системы, а не только на выравнивание графиков нагрузки. Например, имеется потенциальная возможность использования батарей электромобилей для формирования запасного актива мощности. Однако такое использование батарей потребует переоборудования зарядных станций с установкой в них инвертеров, а также изменения всей нормативной базы, поскольку хозяин электромобиля становится полноправным участником энергорынка и должен оплачивать отпущенную ему электроэнергию [14].

Чтобы увеличить степень участия потребителей в управлении спросом, в некоторых странах значительно развили распределенную генерацию (например, появились солнечные батареи на крыше или ветряки во дворе), позволяющую потребителям производить электроэнергию, которую они затем продают и отправят в сеть. В результате электричество и информация должны передаваться в двух направлениях через распределительную сеть, что реализуется посредством интеллектуальных счетчиков и облачных технологий. Это двустороннее взаимодействие становится все более сложным, поскольку распределенная генерация продолжает проникать в промышленные, коммерческие и жилые сегменты услуг электроснабжения. Тем не менее во многих странах установка собственных систем генерации в небольших домохозяйствах и появление устройств выработки электроэнергии в промышленных масштабах являются дотационными [15]. Из-за высоких тарифов, учитывающих необходимость окупаемости этих систем, возникает так называемая энергетическая бедность, когда свыше 10 % дохода тратится на оплату электрической энергии [16].

Оценить реальную степень проникновения распределенной зеленой генерации, т. е. не вызывающей в процессе работы выбросов парниковых газов (в первую очередь CO_2), оказывается достаточно сложно. Как правило, указывается суммарная максимальная мощность всех установок за все годы (что, конечно, далеко от количества фактически используемых установок, а также не учитывает выход некоторых из них из строя вследствие износа, поломок и т. п.). Кроме того, учет в зеленой энергетике работы гидроэлектростанций и тепловых электростанций на газе от переработки биомассы приводит к тому, что в обществе понятия «альтернативная энергетика» (энергия ветра и солнца) и «зеленая энергетика» (энергия солнца, ветра, биомассы и воды) становятся синонимами, а смешение понятий порождает завышенные показатели эффективности работы. Наконец, в публикациях можно встретить заявления о том, что более 50 % энергии страны было получено от солнечных батарей [17], однако не упоминается или упоминается вскользь, что погода в дни максимальной выработки была крайне благоприятной для функционирования батарей, т. е. солнечной, сухой, и что показатель энергопотребления в стране очень низок, так как доля возобновляемой энергии в общем энергопотреблении применительно к облачному дню с максимальной нагрузкой составит около 15–20 %.

Распространение распределенной генерации и улучшение управлением спросом приведут к тому, что энергосистеме для повышения надежности сети потребуются

усовершенствованные распределительные цепи и подстанции, которые будут допускать двусторонние перетоки электроэнергии, новые схемы защиты и новые парадигмы управления. Существующие и разрабатываемые технологии силовой электроники (интеллектуальные инверторы и интеллектуальные хранилища энергии) в сочетании с ИКТ могут предоставить операторам сетей гибкость, необходимую для управления смешанным набором распределенных генераторов.

В настоящее время поддержание и повышение общей надежности энергосистемы не являются поводом для инвестирования и редко попадают в сферу интересов клиентов. В случаях, когда частью уравнения являются элементы распределенной генерации, действия клиентов могут увеличивать риски, связанные с обеспечением надежности энергосистемы. Кроме того, существующие энергосистемы изначально разрабатывались для передачи электроэнергии в одном направлении – от источников к потребителям. Появление обратного направления потоков мощности потребует значительных изменений в аппаратном парке, в устройствах релейной защиты и автоматики, а также в реализации учета отпущенной и полученной электроэнергии.

Как уже отмечалось ранее, для полноценного поддержания надежности сети требуется централизованное управление. Однако концентрация управления в одних руках (или у одного оператора электросети) и повышенная взаимосвязь энергопроизводящих и энергопотребляющих объектов одновременно способствуют успешности злонамеренных атак на элементы такой сети. Использование общедоступных сетей передачи данных приводит к тому, что эти сети выступают средством кибератаки. Последствия подобных атак могут распространяться не только на составные части электросети, но и на устройства клиентов, которые являются частью «Интернета вещей». Иными словами, существуют значительные пробелы в методической и технической части на стыке электричества и информации, которые требуют новых подходов, позволящих защитить критически важную инфраструктуру от упомянутых выше атак.

Риски, связанные с надежностью функционирования электросетей, – это сложное сочетание природных и человеческих угроз. Снижение рисков включает в себя разработку будущих проектов сетей, обеспечивающих максимальную гибкость, а также инвестиции в структурные, технические и технологические решения, которые повышают устойчивость сети и сокращают количество аварийных отключений. Некоторые стратегии могут помочь минимизировать риски различных угроз, в то время как другие стратегии могут привести к росту этих угроз. Среди мер минимизации рисков называют усиление элементов (например, защиту от ветра и наводнений); модернизацию (например, инвестиции в датчики, автоматизированные средства управления, базы данных и инструменты); общую готовность (например, техническое обслуживание оборудования, расчистку просек, создание резерва критически важного оборудования); совершенствование аналитики и безопасности в целом.

Владельцы и операторы сетей должны управлять рисками, связанными с широким спектром угроз. Эти угрозы определяют как все, что может нарушить работу системы или повлиять на нее (природные, экологические, человеческие или другие факторы). Многие угрозы для критически важной инфраструктуры электроснабжения являются универсальными (например, физические атаки), в то время как другие возникают в зависимости от географического положения и времени года (например, стихийные бедствия). Угрозы также различают по частоте возникновения: очень вероятные (например, погодные явления); менее вероятные (например, электромагнитный импульс).

Электроэнергетические компании обычно готовы к чрезвычайным ситуациям. Однако опасности, которые развиваются с течением времени, или комбинации опасностей, которые возникают одновременно, требуют усиленных или новых мер для предотвращения или смягчения. Например, аварийная ситуация на АЭС «Фукусима-1», возникшая из-за одновременного воздействия цунами и обесточивания собственных нужд после землетрясения, казалась чрезвычайно маловероятной, хотя к независимому воздействию каждого из этих факторов атомная электростанция была готова.

Понимание различных рисков для электроэнергетической системы, которое предполагает также характеристику исторических тенденций и прогнозирование, в том числе различных угроз, крайне важно для смягчения угроз и повышения устойчивости. Можно заметить, что многие эксперты в области энергетики оценивают состояние управления рисками в энергетике РФ как не очень высокое. При этом они ожидают, что многие риски усугубятся в будущем, следовательно, необходимы новые стратегии управления рисками. Текущие методы хорошо подходят для устранения общих угроз большинству компонентов системы, однако не всегда работают в отношении возникающих угроз, о которых имеется ограниченный объем данных и опыта. В энергетическом секторе существует множество хорошо зарекомендовавших себя методов управления рисками, порождаемыми различными текущими угрозами, но практики для других типов угроз только появляются, что вызывает необходимость в их дальнейшей разработке, развитии, совершенствовании и рассмотрении.

СПИСОК ЛИТЕРАТУРЫ

1. Bailey T., Maruyama A., Wallance D. The energy-sector threat: How to address cybersecurity vulnerabilities // *McKinsey & Company*. 2020. November. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20energy%20sector%20threat%20How%20to%20address%20cybersecurity%20vulnerabilities/The-energy-sector-threat-How-to-address-cybersecurity-vulnerabilities-F.pdf (date of access: 22.02.2021).

2. Cyber security in the energy sector. Recommendations for the European commission on a european strategic framework and potential future legislative acts for the energy sector // *EECSP Report*. February 2017. URL: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (date of access: 22.02.2021).

3. Корнеев К.Б., Окунева В.В., Павлова Ю.М. Открытость и защищенность протоколов передачи критической информации на объектах энергетики // *Вестник Тверского государственного технического университета. Серия «Строительство. Электротехника и химические технологии»*. 2019. № 2 (2). С. 50–57.

4. Корнеев К.Б., Окунева В.В., Ковалева Ю.В. Моделирование цифровой автоматики подстанций для защиты межподстанционных линий // *Вестник Тверского государственного технического университета. Серия «Строительство. Электротехника и химические технологии»*. 2021. № 1 (9). С. 50–57.

5. Herrera L.Á., Rosellón J. On distributive effects of optimal regulation for power grid expansion // *Energy Policy*. 2014. Vol. 69, pp. 189–204. DOI: 10.1016/ j.enpol.2014.02.011

6. ГОСТ Р ИСО/МЭК 29161-2019. Информационные технологии. Структура данных. Уникальная идентификация для «Интернета вещей». М.: Стандартинформ, 2019.

7. Strategic principles for securing the Internet of things (IoT) Version 1.0 (Washington, DC: DHS, November 15, 2016). URL: https://www.dhs.gov/sites/default/files/publications/Strategic_

Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (date of access: 22.02.2021).
8. Greenberg A. The highly dangerous «Triton» hackers have probed the US grid // *Wired.* 2019. June, 14. URL: https://www.wired.com/story/triton-hackers-scan-us-power-grid/ (date of access: 22.02.2021).
9. Vasquez C. Huge federal hack ripples across energy industry // *E&E News.* 2020. December 17. URL: https://www.eenews.net/stories/1063720933 (date of access: 22.02.2021).
10. «Интернет вещей» в электроэнергетике России // *PricewaterhouseCoopers*. 2018. Март. URL: https://www.pwc.ru/ru/iot/Stapran_D_IoT_in_energy.pdf (date of access: 22.02.2021).
11. Undetected hacks of IoT devices may be straining our power system & strangling our economy // *Meemoori Research.* 2018. May 28. URL: https://memoori.com/undetected-hacks-iot-devices-may-straining-power-system-strangling-economy/ (date of access: 22.02.2021).
12. Об утверждении требований к обеспечению надежности электроэнергетических систем, надежности и безопасности объектов электроэнергетики и энергопринимающих установок «Правила предотвращения развития и ликвидации нарушений нормального режима электрической части энергосистем и объектов электроэнергетики»: приказ Министерства энергетики Российской Федерации от 12.07.2018 № 548. URL: https://www.garant.ru/products/ipo/prime/doc/71924756/ (дата обращения: 22.02.2021).
13. Окунева В.В., Агамирзоев А.А., Корнеев К.Б. Реализация распределенной генерации посредством создания виртуальных электростанций // *Вестник Тверского государственного технического университета. Серия «Строительство. Электротехника и химические технологии»*. 2020. № 3 (7). С. 51–59. DOI: 10.46573/2658-7459-2020-3-51-59
14. Тычинин А. Как заработать с помощью электромобиля Nissan, не проехав ни единого лишнего километра? // *Авторевю.* № 11 (589). С. 26–28.
15. Кинкарц С., Евдокимова О. В Германии спорят о госдотациях на развитие альтернативной энергетики. URL: https://www.dw.com/ru/в-германии-спорят-о-госдотациях-на-развитие-альтернативной-энергетики/a-14844622 (дата обращения: 22.02.2021).
16. Tverberg G. How renewable energy models can produce misleading indications // *Our Finite World*. 2019. October 24. URL: https://ourfiniteworld.com/2019/10/24/how-renewable-energy-models-can-produce-misleading-indications/comment-page-9/ (date of access: 22.02.2021).
17. German solar breaks three records within two weeks // *Germany Trade and Invest.* URL: https://www.prnewswire.com/news-releases/german-solar-breaks-three-records-within-two-weeks-263664861.html (date of access: 22.02.2021).

СВЕДЕНИЯ ОБ АВТОРАХ

КОРНЕЕВ Константин Борисович – канд. техн. наук, доцент кафедры электроснабжения и электротехники, ФГБОУ ВО «Тверской государственный технический университет», 170026, г. Тверь, наб. Аф. Никитина, д. 22. E-mail: energy-tver@mail.ru

ПАВЛОВА Юлия Михайловна – старший преподаватель кафедры электроснабжения и электротехники, ФГБОУ ВО «Тверской государственный технический университет», 170026, г. Тверь, наб. Аф. Никитина, д. 22. E-mail: sokolhawk98@gmail.com

ОСЕИ-ОВУСУ Раймонд – аспирант кафедры электроснабжения и электротехники, ФГБОУ ВО «Тверской государственный технический университет», 170026, г. Тверь, наб. Аф. Никитина, д. 22. E-mail: orajmond2008@mail.ru

БИБЛИОГРАФИЧЕСКАЯ ССЫЛКА

Корнеев К.Б., Павлова Ю.М., Осеи-Овусу Р. Управление рисками и надежностью в системах электроснабжения // Вестник Тверского государственного технического университета. Серия «Строительство. Электротехника и химические технологии». 2021. № 2 (10). С. 56–67.

RISK AND RELIABILITY MANAGEMENT IN POWER SUPPLY SYSTEMS

K.B. Korneev, Yu.M. Sokolova, R. Osei-Ovusu
Tver State Technical University (Tver)

Abstract. It is noted that the functioning of developing electric networks with distributed generation and demand management requires improving approaches to managing the reliability of the system. It is concluded that risk assessment and effective planning can be based only on a high-quality system analysis of the existing infrastructure, taking into account all factors. Some risks (primarily related to information security) that require a comprehensive study in order to prevent the occurrence of emergency situations are considered.

Keywords: power system, risks, reliability, Internet of Things (IoT), security, management, distributed generation, demand management, alternative energy.

REFERENCES

1. Bailey T., Maruyama A., Wallance D. The energy-sector threat: How to address cybersecurity vulnerabilities. *McKinsey & Company*. 2020. November. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20energy%20sector%20threat%20How%20to%20address%20cybersecurity%20vulnerabilities/The-energy-sector-threat-How-to-address-cybersecurity-vulnerabilities-F.pdf (date of access: 22.02.2021).
2. Cyber security in the energy sector. Recommendations for the European commission on a european strategic framework and potential future legislative acts for the energy sector. *EECSP Report*. February 2017. URL: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (date of access: 22.02.2021).
3. Korneev K.B., Okuneva V.V., Pavlova Yu.M. Openness and security of protocols for the transfer of critical information at energy facilities. *Vestnik Tverskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Stroitelstvo. Elektrotekhnika I Himicheskie Tekhnologii»*. 2019. No. 2 (2), pp. 50–57. (In Russian).
4. Korneev L.B., Okuneva V.V., Kovalyova Yu.V. Simulation of digital substation automation to protect inter-substation lines. *Vestnik Tverskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Stroitelstvo. Elektrotekhnika I himicheskie tekhnologii»*. 2021. No. 1 (9), pp. 50–57. (In Russian).
5. Herrera L.A., Rosellón J. On distributive effects of optimal regulation for power grid expansion. *Energy Policy*. 2014. Vol. 69, pp. 189–204. DOI: 10.1016/ j.enpol.2014.02.011
6. GOST R ISO/IEC 29161-2019. Informacionnie tekhnologii. Struktura dannyh. Unikalnaya identifikaciya dlya interneta veschey [Information technology. Data structure. Unique identification for the Internet of Things]. Moscow: Standartinform, 2019. (In Russian).

7. Strategic principles for securing the internet of things (IoT) Version 1.0 (Washington, DC: DHS, November 15, 2016). URL: https://www.dhs.gov/sites/default/files/publications/ Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (date of access: 22.02.2021).
8. Greenberg A. The highly dangerous «Triton» hackers have probed the US grid. *Wired.* 2019. June 14. URL: https://www.wired.com/story/triton-hackers-scan-us-power-grid/ (date of access: 22.02.2021).
9. Vasquez C. Huge federal hack ripples across energy industry. *E&E News.* 2020. December 17. URL: https://www.eenews.net/stories/1063720933 (date of access: 22.02.2021).
10. Internet of things in Russian electricity. *PricewaterhouseCoopers*. 2018. March. URL: https://www.pwc.ru/ru/iot/Stapran_D_IoT_in_energy.pdf (date of access: 22.02.2021). (In Russian).
11. Undetected hacks of IoT devices may be straining our power system & strangling our economy. *Meemoori Research.* 2018. May 28. URL: https://memoori.com/undetected-hacks-iot-devices-may-straining-power-system-strangling-economy/ (date of access: 22.02.2021).
12. Ob utverzhdenii trebovanij k obespecheniyu nadezhnosti elektroenergeticheskih sistem, nadezhnosti i bezopasnosti ob’ektov elektroenergetiki i energoprinimayushchih ustanovok «Pravila predotvrashcheniya razvitiya i likvidacii narushenij normal'nogo rezhima elektricheskoj chasti energosistem i ob"ektov elektroenergetiki»: prikaz Ministerstva energetiki Rossijskoj Federacii ot 12.07.2018 № 548 [On approval of requirements for ensuring the reliability of electric power systems, reliability and safety of electric power facilities and power receiving installations «Rules for preventing the development and elimination of violations of the normal operation of the electrical part of power systems and electric power facilities»: order of the Ministry of Energy of the Russian Federation of July 12, 2018 No. 548]. URL: https://www.garant.ru/products/ipo/prime/doc/71924756/ (date of access: 22.02.2021). (In Russian).
13. Okuneva V.V., Agamirzoev A.A., Korneev K.B. Implementation of distributed generation by creating virtual power plants. *Vestnik Tverskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya «Stroitelstvo. Elektrotekhnika I Himicheskie Tekhnologii»*. 2020. No. 3 (7), pp. 51–59. (In Russian). DOI: 10.46573/2658-7459-2020-3-51-59
14. Tychinin A. How to make money with a Nissan electric car without driving a single extra kilometer? *Autoreview.* No. 11 (589), pp. 26–28. (In Russian).
15. Kinkartz S., Evdokimova O.V. In Germany, they argue about state subsidies for the development of alternative energy. URL: https://www.dw.com/ru/в-германии-спорят-о-госдотациях-на-развитие-альтернативной-энергетики/a-14844622 (date of access: 22.02.2021). (In Russian).
16. Tverberg G. How renewable energy models can produce misleading indications. *Our Finite World*. 2019. October 24. URL: https://ourfiniteworld.com/2019/10/24/how-renewable-energy-models-can-produce-misleading-indications/comment-page-9/ (date of access: 22.02.2021).
17. German solar breaks three records within two weeks. *Germany Trade and Invest.* URL: https://www.prnewswire.com/news-releases/german-solar-breaks-three-records-within-two-weeks-263664861.html (date of access: 22.02.2021).

INFORMATION ABOUT THE AUTHORS

KORNEEV Konstantin Borisovich – Candidate of Technical Sciences, Associate Professor of the Department of Power Supply and Electrical Engineering, Tver State Technical University, 22, embankment of Af. Nikitin, Tver, 170026, Russia. E-mail: energy-tver@mail.ru

PAVLOVA Yulia Mikhailovna – Senior Lecturer, Department of Power Supply and Electrical Engineering, Tver State Technical University, 22, embankment of Af. Nikitin, Tver, 170026, Russia. E-mail: sokolhawk98@gmail.com

OSEI-OWUSU Raymond – Graduate Student, Department of Power Supply and Electrical Engineering, Tver State Technical University, 22, embankment of Af. Nikitin, Tver, 170026, Russia. E-mail: orajmond2008@mail.ru

CITATION FOR AN ARTICLE

Korneev K.B., Sokolova Yu.M., Osei-Ovusu R. Risk and reliability management in power supply systems // Vestnik of Tver State Technical University. Series «Building. Electrical engineering and chemical technology». 2021. No. 2 (10), pp. 56–67.

УДК 44.31.03:53.07.00:45.43.00

ВЛИЯНИЕ ЗАДЫМЛЕННОСТИ АТМОСФЕРЫ И ВЫСОТЫ ШЛАКА НА ТЕПЛООБМЕН В ДУГОВЫХ СТАЛЕПЛАВИЛЬНЫХ ПЕЧАХ. ЧАСТЬ I. ВЛИЯНИЕ ЗАДЫМЛЕННОСТИ АТМОСФЕРЫ НА ПОТЕРИ С ГАЗАМИ И ВОДОЙ

А.Н. Макаров

Тверской государственный технический университет (г. Тверь)

© Макаров А.Н., 2021

Аннотация. Состав пылегазовой атмосферы влияет на теплообмен в дуговой сталеплавильной печи. При значительной запыленности атмосферы печи тепловой поток дуг, излучаемый ими в свободное, не заполненное шихтой, пространство в основном поглощается пылегазовой средой и уносится из печи в виде тепловых потерь с отходящими газами. В лучепрозрачной атмосфере печи тепловой поток дуг, излучаемый ими в свободное пространство, достигает стен, поглощается водой водоохлаждаемых панелей и уносится из печи в виде тепловых потерь с охлаждающей водой.

Ключевые слова: электросталь, электрическая дуга, теплообмен, тепловое излучение, печь.

DOI: 10.46573/2658-7459-2021-67-77