УДК 004.413.4
DOI:10.25729/ESI.2023.30.2.010

Анализ рисков при функционировании агрегатора управления спросом на электроэнергию

Колосок Ирина Николаевна, Коркина Елена Сергеевна

Институт систем энергетики им. Л.А. Мелентьева СО РАН,
Россия, Иркутск, *kolosok@isem.irk.ru*

Аннотация. В статье представлен граф-аналитический подход к проблеме минимизации рисков при функционировании агрегатора управления спросом на электроэнергию в условиях неблагоприятных внешних воздействий. Приведен пример составления диаграммы-бабочки, содержащей в себе проактивные (превентивные) и реактивные (восстановительные) меры защиты агрегатора. Предложен способ увеличения количества проактивных мер защиты с помощью перевода некоторых реактивных мер в разряд проактивных.

Ключевые слова: агрегатор спроса на электроэнергию, риски, непрерывность бизнеса, информационная безопасность

Цитирование: Колосок И.Н. Анализ рисков при функционировании агрегатора управления спросом на электроэнергию / И.Н. Колосок, Е.С. Коркина // Информационные и математические технологии в науке и управлении. – 2023. – № 2 (30). – С. 98-106. DOI:10.25729/ESI.2023.30.2.010.

Введение. В основе управления спросом (УС) на электроэнергию (ЭЭ) заложена возможность сокращения потребителями энергосистемы количества энергопотребления в период пиковой нагрузки вместо того, чтобы энергосистема увеличивала объем доступной мощности [1], это выгоднее и эффективнее. Потенциал этого решения оценивается значительной долей сокращения потребления в пиковые периоды (до 15 % от общего объема потребления) [2]. Для осуществления механизма УС нужно скоординировать действия множества розничных потребителей, с этой целью создана специальная структура – агрегатор спроса на ЭЭ (Demand Response, DR-Агрегатор) [3].

В условиях неблагоприятных внешних воздействий (НВВ) – крупного технического сбоя, аварийного события, кибератаки – необходимо сохранить функционирование DR-Агрегатора, а для этого – минимизировать риски от последствий НВВ. Как показано в [4], «…анализ риска является частью системного подхода к принятию практических мер в решении задач уменьшения опасности для жизни человека, ущерба имуществу и окружающей среде, называемого в нашей стране обеспечением промышленной безопасности, а за рубежом – управлением риском». Управление рисками начинается с выявления и оценки возможных угроз. Затем осуществляется поиск альтернатив, то есть рассматриваются менее рискованные варианты [5]. Применительно к задаче минимизации рисков DR-Агрегатора в статье рассматриваются операционные (технико-технологические) и информационные риски.

Во втором разделе статьи рассматриваются основные риски в электроэнергетике, а также риски, являющиеся угрозой функционированию DR-Агрегатора. В третьем разделе обсуждается проблема «непрерывности бизнеса» (НБ) применительно к DR-Агрегатору. Раздел 4 содержит предложения авторов статьи по снижению рисков при функционировании DR-Агрегатора, разработанные на основе граф-аналитического Bow-Tie (диаграмма «Галстук-бабочка»).

2. Риски в электроэнергетике. Типовыми рисками в электроэнергетике являются: превышение расчетных нагрузок, аварийные отключения, неплатежи, срыв поставок топлива, снижение качества ЭЭ и другие (риски инвестирования, кредитования и т.д.) [6]. Риском может обернуться и «…отсутствие достоверной информации о потенциальном объеме спроса на электроэнергию …» [7]. В [8] перечислены множество рисков в электроэнергетике, являющихся последствиями переходного периода в отрасли: риск снижения потребления энергии

из-за создания потребителями собственной генерации; риск нарушения нормальных режимов при выводе объемов сбыта ЭЭ из состава сетевых компаний; риск снижения надежности и резкого роста затрат на поддержание оборудования в период жизненного цикла и многие другие виды рисков.

В [9] показано, что возрастание интереса к управлению операционными рисками, в частности, рисками бизнес-процессов, объясняется изменением траекторий жизненных циклов в производстве благодаря новым технологиям, поиску внутренних ресурсов для оптимизации производства, совершенствованию систем управления. Для эффективного управления рисками необходимо ясное представление, какие риски являются угрозой для конкретного вида бизнеса (здесь – DR-Агрегатора). Согласно типологии рисков [7], главными угрозами в бизнесе названы рыночные, кредитные, риски ликвидности, операционные риски, риски события. Здесь, не рассматривая финансовую сторону, отметим, что «…риск события – это возможные потери, обусловленные форс-мажорными условиями, изменениями в законодательстве, действиями управляющих структур и пр., а операционный риск – это убытки вследствие технических ошибок и отказов, проблем человеческого фактора, аварий, несанкционированного доступа к информационным системам и т.д.». При уточнении, что такое операционный риск во всем многообразии рисков, применяют классическое определение из Базеля II «…операционный риск – это потенциальные потери организации из-за неадекватных или ошибочных внутренних процессов и/или систем, действий персонала, а также внешние события» [9].

2.1. Риски в работе DR-Агрегатора. Целью DR-Агрегатора как механизма УС является координация взаимодействия потребителей, не являющихся участниками оптового рынка, с Системным Оператором, дающим команду на выполнение снижения энергопотребления по запросу оптового рынка [1, 3]. DR-Агрегатор объединяет разных потребителей: промышленных, сельско-хозяйственных, жилой сектор и др. Их взаимодействие скрепляется договорными обязательствами. Таким образом, механизм DR-Агрегатора может быть представлен в виде бизнес-процесса [10], в котором объединены: цель (запрос рынка Системному Оператору ЕЭС), управление (СО ЕЭС, руководящие и договорные нормативно-правовые документы, DR-Агрегатор как координатор), ресурсы (потребители ЭЭ как объекты управления и избытки ЭЭ у потребителей за счет снижения потребления в пиковые периоды), конечный продукт (получение рынком избытков ЭЭ). Применительно к задаче минимизации рисков DR-Агрегатора в статье рассматриваются риски событий (НВВ) и операционные риски (отклонения в работе IT-систем и систем контроля, человеческий фактор, низкий уровень и нарушение процессов производства, сбои в работе оборудования, его физический и моральный износ, заимствованные технологии, вычислительная техника (ВТ), программное обеспечение (ПО) и т.п.) (рис.1).

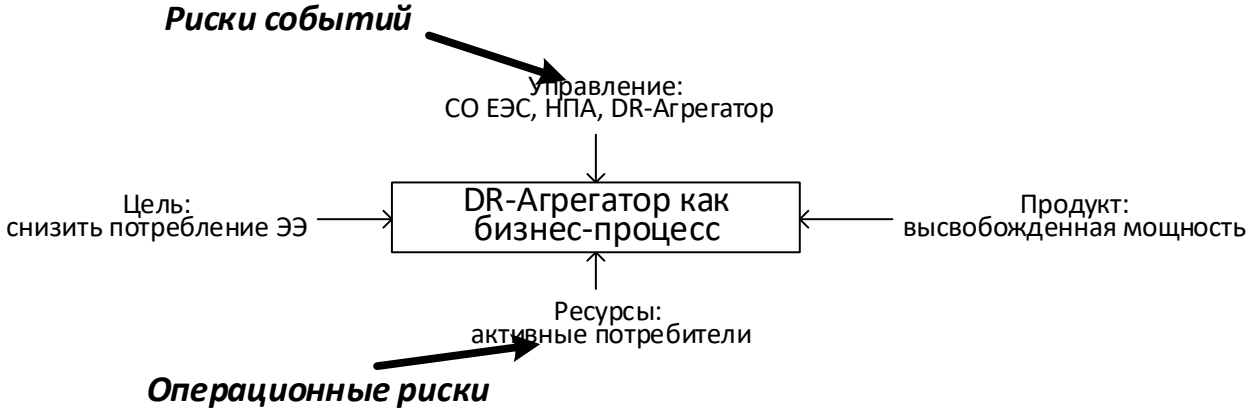

Рис. 1. Рассмотрение DR-Агрегатора как бизнес-процесса с учетом рисков

Для DR-Агрегатора и его участников существенными рисками из перечня [11] являются:

- в системе управления – риск неучета специфики местных условий и запаздывания принятия неотложных мер в аварийных ситуациях;
- в АСУ ТП – риск отставания отрасли по новейшим технологиям основного и вспомогательного оборудования и по информационному обеспечению (ПО полномасштабных АСУ ТП); риск снижения надежности и резкого роста затрат на поддержание оборудования из-за многочисленных остановов в АСУ ТП, например, вследствие ввода новых мощностей на основе зарубежных парогазовых установок, не подкрепленного отечественными запчастями; риск внедрения в аппаратуру незадокументированных функций из-за применения импортной электронно-компонентной базы;
- в разработке стандартов и регламентов – риск отставания в решении текущих проблем [11].

В [12] рассматривается связь между системой управления информационной безопасностью (ИБ) (плюс системой управления IT-инфраструктурой) и системой управления бизнесом. Обе системы управления используют анализ рисков, но в ИБ этот анализ проводится профилактически, а в бизнесе – во время чрезвычайной ситуации при аварийных процессах с точки зрения процесса обеспечения непрерывности бизнеса. «Кибер-риск – это первый шаг на пути понимания бизнесом важности кибербезопасности, как риска финансовых потерь» [13].

3. Непрерывность бизнеса. Как к бизнес-процессу к DR-Агрегатору применимо понятие «непрерывность бизнеса» (НБ) или BCM (Business Continuity Management), пришедшее на смену понятию «аварийное восстановление» (II-я половина 90х гг XX в.). НБ означает, что для сохранения функциональности недостаточно ограничиться созданием резерва оборудования (холодного, горячего или зеркального и т.п.), в НБ речь идет о бесперебойной работе всего предприятия (оборудование, технологические процессы, IT-системы, средства коммуникации и т.д.) [14]. В круг решаемых задач НБ входят только те инциденты, которые угрожают бизнесу. Так, критической является потеря доступа к IT-системам [15].

В России вопросы, связанные с обеспечением непрерывности бизнеса, рассматриваются, в основном, как проблемы информационной безопасности или часть задач IT-инфраструктуры [16]. Необходимость создания программы НБ возникает при намерении бизнеса повысить уровень управления IT-сервисами. При создании программы НБ удается оценить угрозы/чрезвычайные ситуации; оценить существующие уязвимости IT-инфраструктуры (управление рисками); минимизировать вероятность нештатных ситуаций и их воздействие на деятельность организации, проактивно идентифицировать возможные последствия нештатной ситуации.

При разработке стратегии НБ последовательно осуществляется ряд этапов, важным среди которых является анализ воздействия на бизнес (по сути – анализ рисков). Анализ воздействия на бизнес позволяет понять, какое влияние могут оказать различные виды негативных событий (нарушений, отказов или разрушений) на основные направления деятельности компании и ключевые бизнес-процессы. Принимая во внимание развитие информационных технологий и проникновение этих технологий в промышленность, в том числе, в электроэнергетику, мы рассматриваем участников DR-Агрегатора как кибер-физическую систему (КФС) [17], и нам важны обе подсистемы, составляющие любую КФС, – кибер- и физическая [18]. Поэтому мы должны рассматривать проблемы и кибербезопасности (кибер-риски), и производственной безопасности (операционные риски). В область кибер-рисков входит и цифровизация бизнеса, и зависимость областей безопасности друг от друга, например, физической безопасности от Интернета вещей. Риски, возникающие в IT-системах предприятий, являются относительно новыми, но неизменно присутствуют в их системах управления. Каким образом можно снизить эти риски? Например, в [19] предлагается разделить все риски бизнеса на 2 категории – те, которые зависимы от IT-систем, и те, которые от них не зависят.

4. Управление рисками DR-Агрегатора. Существуют различные подходы к анализу рисков. В [7] разработана графическая нотация процесса управления рисками, отображающая все его составляющие: источники рисков, риск-события, риск-ситуации, мероприятия по снижению рисков, мероприятия по устранению последствий реализации рисков и др. Для сохранности бизнеса создается система управления рисками (СУР), включающая в себя структурный, процессный и системный аспекты. Эти аспекты позволяют понять причины и обстоятельства, приводящие к риск-событиям. *Структурный* аспект иллюстрируется построением дерева отказов, на котором видны взаимосвязи элементов всей структуры объекта. *Процессный* аспект представлен бизнес-процессами. *Системный* аспект показывает взаимодействие объекта с окружающей средой. Координация этих аспектов позволяет выработать комплексный подход по управлению рисками, выполняющийся поэтапно во времени. На первом этапе проводятся *прелиминарные* (превентивные) мероприятия, выполняемые заранее для того, чтобы предотвратить риск-событие или снизить возможность его наступления, например, перестроить структуру системы (объекта). При осуществлении рисков проводятся *прецедентные* (восстановительные) мероприятия, к которым вынуждены прибегнуть с целью недопущения дальнейшего развития аварийных ситуаций, устранения последствий, восстановления работоспособности. Хорошо известными аналитическими методами при изучении аварийных ситуаций являются метод дерева отказов [20] и метод дерева событий [21]. Так, в [4] применен метод дерева отказов, определяющий структуру и последовательность вероятностных расчетов по оценке риска возникновения возможных аварий, метод анализа дерева событий, рассматривающий события, влекущие за собой аварию, и метод анализа причинно-следственных связей, предусматривающий построение расчетной диаграммы, которая связывает отказы и опасные события в причинно-следственные цепочки.

4.1. Проактивные защитные меры. Для иллюстрации проактивных защитных мер в статье рассматривается дерево угроз и уязвимостей DR-Агрегатора. В области ИБ и кибербезопасности ***деревья угроз и деревья атак*** строятся на основе дерева отказов**,** но от дерева отказов они отличаются наличием нижнего уровня – уровня защитных мер. С позиций ИБ риски функционирования DR-Агрегатора – это угрозы прерывания, искажения и потери информации, критически важной для управления функционированием всего бизнес-процесса и/или его отдельных звеньев (кибер- и физических подсистем его участников). На рис. 2 представлено ***дерево угроз*** с учетом всех компонентов DR-Агрегатора как бизнес-процесса. Структура дерева:

- верхний уровень (корень дерева, цель) – нарушение функционирования DR-Агрегатора (анализ рисков непрерывности бизнеса),
- второй уровень (основные компоненты) – представление DR-Агрегатора как КФС (подсистемы: управления спросом, техническая и информационно-коммуникационная),
- третий уровень – уровень возможных уязвимостей,
- четвертый уровень – проактивные меры защиты DR-Агрегатора.

В качестве проактивных мер (рис.2.) для подсистемы управления могут быть: четко работающий алгоритм назначения фиксированных или плавающих цен, свободный доступ потребителей к участию в управлении спросом, безукоризненно составленные договоры между потребителями и агрегатором. В технической подсистеме должен быть предусмотрен строгий порядок обновления оборудования, переход на импортозамещение, в части защиты от НВВ и ошибок персонала – метод логико-вероятностного анализа, позволяющий выразить логику безотказной работы компонентов технической подсистемы с помощью вероятностей работоспособности узлов подсистемы [18]. Для информационно-коммуникационной подсистемы проактивными мерами являются структура сетецентрического управления (СЦУ) и организация кибер-физического управления (КФУ) на нижнем уровне СЦУ, а также методы искусственного интеллекта (ИИ) и машинное обучение (МО).

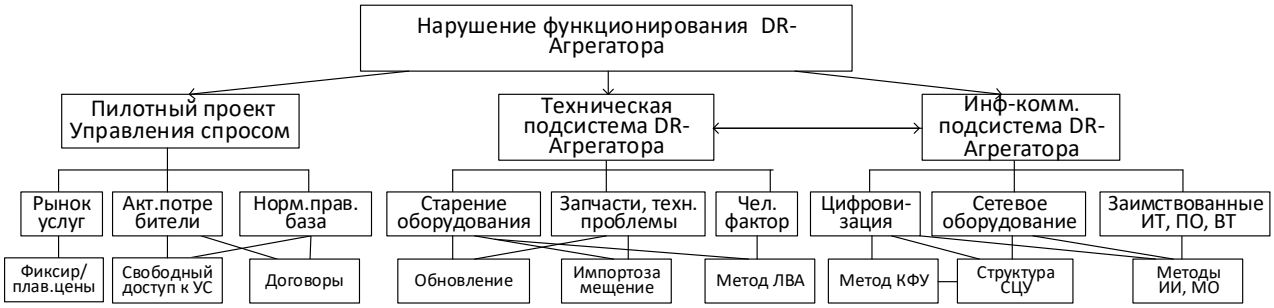

Рис. 2. Дерево угроз функционированию DR-Агрегатора

4.2. Реактивные меры защиты. Для анализа последствий от произошедших НВВ применяется метод *дерева событий* (ДС): типичное положение ДС – горизонтальное, в левой части ДС находится само событие, а справа от него располагаются реактивные меры защиты для восстановления DR-Агрегатора как бизнеса. Предположим, что в одном из кластеров DR-Агрегатора произошли два инцидента: у активного потребителя 1 – полное отключение электричества (сбой в физической подсистеме), у активного потребителя *n* – сработала зловредная закладка в операционной системе (сбой в информационной подсистеме) (рис.3).

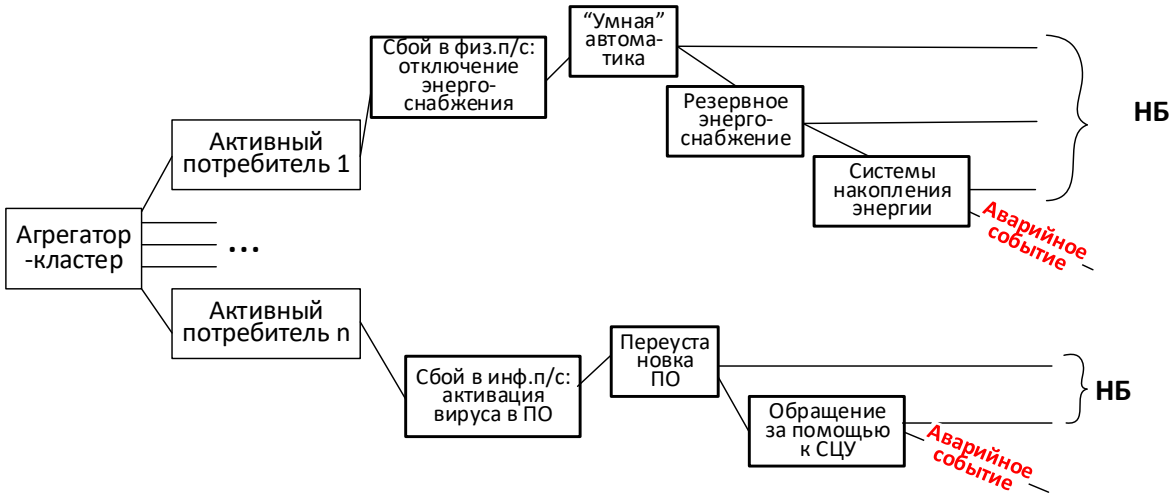

Рис. 3. Дерево событий DR-Агрегатора для восстановления НБ:
сбой в физической подсистеме активного потребителя *1*,
сбой в информационной подсистеме активного потребителя *n*.

Анализ мер по восстановлению этих потребителей с помощью ДС показывает, что если реактивные меры по восстановлению работоспособного состояния не привели к успеху, то возникает аварийное событие и реальная угроза бизнесу.

4.4. Снижение рисков при функционировании DR-Агрегатора. В [18] нами рассмотрен вопрос живучести DR-Агрегатора. В электроэнергетике под живучестью понимается свойство объекта противостоять возмущениям, не допуская их каскадного развития с массовым нарушением питания потребителей [22]. «Повышению живучести DR-Агрегатора могут способствовать такие факторы, как рационально сформированная структура, правильно организованная система сетецентрического управления (СЦУ) этой структурой и реализация киберфизического управления (КФУ) непосредственно на нижнем уровне иерархии СЦУ – на уровне потребителей ЭЭ (участников DR-Агрегатора)» [18] К выявлению слабых звеньев структуры в [12] применен логико-вероятностный анализ (ЛВА). Рациональная кластерная структура DR-Агрегатора и предложенные виды управления могут быть предупредительными (проактивными, или, как выше сказано, прелиминарными) мерами борьбы с операционными и кибер-рисками. Возможность разработать реактивные (или прецедентные) меры борьбы предлагается осуществить следующим образом.

Для решения этой задачи можно использовать подход Bow-Tie (диаграмма «Галстук-бабочка») [23]. Суть подхода заключается в анализе и отображении источников рисков. Главный узел (в центре) – это предмет обсуждения (проблема), здесь: непрерывность бизнеса DR-Агрегатора. Левое крыло включает в себя дерево угроз, при этом проактивные меры защиты переместились с нижнего уровня дерева угроз ближе к главному узлу – теперь это защитные барьеры. Правое крыло – это видоизмененное дерево событий с последствиями НВВ, обозначенного над главным узлом. Реактивные меры защиты также образуют защитные барьеры. Такую диаграмму удобно строить в процессе анализа рисков, а потом обновлять, достраивать и актуализировать в ходе всего жизненного цикла DR-Агрегатора как бизнес-процесса.

Практически, Bow-Tie объединяет оба дерева (угроз и событий) (рис.4).

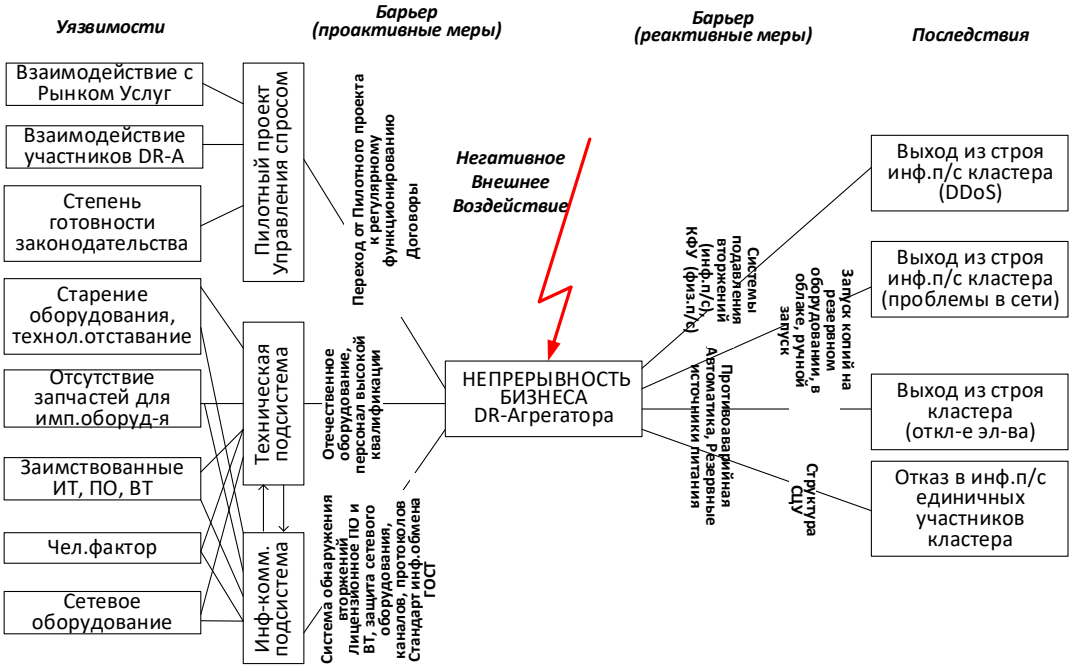

Рис. 4. Диаграмма «Галстук-бабочка» для непрерывности бизнеса DR-Агрегатора

В [24] показано, что в области ИБ реактивные механизмы защиты (реакция на происшедшую аварию) весьма распространены, и они признаются достаточно эффективными, но взаимодействие цифровых технологий и КФС становится всё сложнее, значит, растет необходимость в разработке новых проактивных мер или в переводе эффективных реактивных мер защиты в число проактивных мер.

Заключение. В статье DR-Агрегатор рассматривается как бизнес-процесс, поэтому требуется разработка методологии обеспечения непрерывности бизнеса (НБ). Специфика НБ заключается в том, что в круг задач НБ входят только инциденты, угрожающие бизнесу. В ходе работы с использованием диаграммы «Галстук-бабочка» сформулированы меры проактивной и реактивной защиты DR-Агрегатора в условиях негативных внешних воздействий. В рамках методологии обеспечения НБ при оценке рисков DR-Агрегатора можно определить его наиболее уязвимые компоненты и усилить упреждающие меры по их защите.

Благодарности. Исследование проводится в рамках проекта государственного задания (№ FWEU-2021-0001) программы фундаментальных исследований Российской Федерации на 2021-2030 годы (рег. № АААА-А21-121012190027-4).

Список источников

1. Концепция функционирования агрегаторов распределенных энергетических ресурсов в составе Единой энергетической системы России. Агрегаторы управления спросом на электроэнергию. – URL:

https://www.so-ups.ru/fileadmin/files/company/markets/dr/docs/dr_agregator_concept.pdf (дата обращения: 11.04.2023).
2. Moreton A. What is demand response? Available at: https://arena.gov.au/blog/what-is-demand-response/ (accessed: 04/11/2023).
3. Управление спросом в электроэнергетике России: открывающиеся возможности. – URL: https://www.so-ups.ru/fileadmin/files/company/markets/dr/publication/EnergyNet_2019.pdf (дата обращения: 10.02.2023).
4. Феоктистова О.Г. Актуальность оценки производственного риска на авиапредприятиях / О.Г. Феоктистова, И.К. Туркин, С.В. Баринов // Научный Вестник МГТУ ГА, 2017. – № 20(4). – С. 162-173.
5. Одинцова М.А. Методика управления рисками для малого и среднего бизнеса. – URL: https://cyber-leninka.ru/article/n/metodika-upravleniya-riskami-dlya-malogo-i-srednego-biznesa (дата обращения: 02.05.2023).
6. Колесников А.М. Анализ рисков предприятий электроэнергетики / А.М. Колесников, А.В. Баранов // Теория и практика сервиса: экономика, социальная сфера, технологии. СПбГЭУ, 2013. – № 4 (18). – С. 154-158.
7. Сеньков А.В. Графическая нотация для представления процесса управления комплексными рисками / А.В. Сеньков // Современные наукоемкие технологии, 2016. – № 12-1. – С. 72-81. – URL: https://top-technologies.ru/ru/article/view?id=36479 (дата обращения: 02/05/2023).
8. Жилкина Ю.В., Воденников Д.А. Риски в энергетике: анализ практики управления на рынке электроэнергии. – URL: http://cigre.ru/research_commitets/ik_rus/b3_rus/materials/library/%D0%96%D0%B8%D0%BB%D0%BA%D0%B8%D0%BD%D0%B0_.pdf (дата обращения: 11.04.2023).
9. Уварова Г. Карту рисков бизнес-процессов можно сделать практичной. – URL: https://www.eg-online.ru/article/274036/ (дата обращения: 15.05.2023).
10. Колосок И.Н. Demand Response агрегатор как бизнес-процесс в условиях цифровизации энергетики / И.Н. Колосок, Е.С. Коркина // Релейная защита и автоматизация, 2021. – № 4. – С. 22-27.
11. Кудрявый В.В. Риски и угрозы российской электроэнергетики. Пути преодоления. – URL: https://www.ruscable.ru/article/The_risks_and_threats_of_the_Russian_power_industry/ (дата обращения: 02.03.2023).
12. Boehmer W. Analysis of strongly and weakly coupled management systems in information security. 2010, available at: https://ieeexplore.ieee.org/document/5633657 (accessed: 03/02/2023).
13. Кибер-риски: как понимать и управлять. – URL: https://10guards.com/ru/articles/cyber-risks/ (дата обращения: 12.03.2023).
14. Роль информационной безопасности в обеспечении непрерывности бизнеса. – URL: http://www.interface.ru/home.asp?artId=40308 (дата обращения: 20.02.2023).
15. Качуров Е. Семь шагов к непрерывности бизнеса. 2015. – URL: https://habr.com/ ru/company/softline/blog/261053/ (дата обращения: 02.03.2023).
16. Мусатов К. Непрерывность бизнеса. Подходы и решения. – URL: https://www.jetinfo.ru/nepreryvnost-biznesa-podkhody-i/ (дата обращения: 15.05.2023).
17. Воропай Н.И. Проблемы уязвимости и живучести киберфизических электроэнергетических систем / Н.И. Воропай, И.Н. Колосок, Е.С. Коркина, А.Б. Осак // Энергетическая политика, 2018. – № 5. – С. 53-61.
18. Колосок И.Н. Применение логико-вероятностного анализа для повышения живучести Агрегатора управления спросом на электроэнергию / И.Н. Колосок, Е.С. Коркина // Энергетик, 2022. – № 12. – С. 9-12.
19. «Росэлектроника» представила киберзащищенную систему для цифровой электросети. – URL: https://www.cnews.ru/news/line/2019-07-09_roselektronika_predstavila_kiberzashchishchennuyu (дата обращения: 09.07.2019).
20. Гук Ю.Б. Расчет надежности электроэнергетических установок / Ю.Б. Гук. – Л.: Энергоатомиздат, 1988. – 224 с.
21. Надежность технических систем и техногенный риск. Дерево событий. – URL: http://www.obzh.ru/nad/6-9.html (дата обращения: 02.03.2023).
22. Руденко Ю.Н. Надежность систем энергетики / Ю.Н. Руденко, И.А. Ушаков. – Н-ск: Наука, 1989. – 328 с.
23. Анализ «галстук-бабочка». – URL: http://www.consultant.ru/document/cons_doc_LAW_406016/79d895387ec905fc042eccdcc6fce3b320e9b18d/ (дата обращения: 27.01.2023).
24. Уткин Н. Интервью с экспертом: «Безопасность кибер-физических систем: требуются комплексный подход и проактивные механизмы». – URL: https://safe-surf.ru/specialists/article/5291/668770/ (дата обращения: 02.03.2023).

Колосок Ирина Николаевна. *Д.т.н., в.н.с., ИСЭМ СО РАН. Область научных интересов –математические модели, методы и алгоритмы для решения комплекса задач информационного обеспечения для мониторинга и диспетчерского управления интеллектуальной энергосистемой (ИЭС) на базе современных средств измерений*

и новых информационных технологий; кибербезопасность и киберфизическая устойчивость ИЭС и ее объектов. AuthorID: 48007871, ORCID: 0000-0002-2843-4455, kolosok@isem.irk.ru, 664033, Иркутск, ул. Лермонтова, 130.

Коркина Елена Сергеевна. *К.т.н., с.н.с. ИСЭМ СО РАН. Область научных интересов –кибербезопасность объектов электроэнергетики, синхронизированные векторные измерения, оценивание состояния электроэнергетических систем, кибер-физические системы. AuthorID: 24577537100, SPIN: 8084-7363, ORCID: 0000-0001-6488-5774, korkina@isem.irk.ru, 664033, Иркутск, ул. Лермонтова, 130.*

UDC 004.413.4
DOI: 10.25729/ESI.2023.30.2.010

Risk analysis of the Demand Response Aggregator

Irina N. Kolosok, Elena S. Korkina

Melentiev Energy Systems Institute SB RAS, Russia, Irkutsk, *kolosok@isem.irk.ru*

Abstract. The paper presents a graph-analytical approach to the problem of minimizing risks in the Demand Response (DR) Aggregator's operation under adverse external influences. An example of drawing up a Bow-Tie diagram containing proactive and reactive protection measures of the DR-Aggregator is given. That approach is proposed to increase the number of proactive protection measures by transferring some reactive measures to the category of proactive.

Keywords: demand Response Aggregator, risks, business continuity, information security

Acknowledgements: This study was carried out within the framework of the state assignment project (No. FWEU-2021-0001) of the program of fundamental research of the Russian Federation for 2021-2030 (Reg. No. AAAA-F21-121012190027-4).

References

1. Koncepciya funkcionirovaniya agregatorov raspredelennyh energeticheskih resursov v sostave Edinoj energeticheskoj sistemy Rossii. Agregatory upravleniya sprosom na elektroenergiyu [The concept of functioning of aggregators of distributed energy resources as part of the Unified Energy System of Russia. Aggregators of electricity demand management]. Available at: https://www.so-ups.ru/fileadmin/files/company/markets/dr/docs/dr_agregator_concept.pdf (accessed: 04/11/2023)
2. Moreton A. What is demand response? Available at: https://arena.gov.au/blog/what-is-demand-response/ (accessed: 04/11/2023)
3. Upravlenie sprosom v elektroenergetike Rossii: otkryvayushchiesya vozmozhnosti [Demand side management in the Russian electric power industry: emerging opportunities]. Available at: https://www.so-ups.ru/fileadmin/files/company/markets/dr/publication/EnergyNet_2019.pdf (accessed: 02/10/2023)
4. Feoktistova O.G., Turkin I.K., Barinov S.V. Aktual'nost' ocenki proizvodstvennogo riska na aviapredpriyatiyah [The relevance of the assessment of industrial risk in aviation enterprises]. Nauchnyj Vestnik MGTU GA [Scientific Bulletin of MSTU GA], 2017, no. 20 (4), pp. 162-173.
5. Odincova M.A. Metodika upravleniya riskami dlya malogo i srednego biznesa [Risk management methodology for small and medium-sized businesses]. Available at: https://cyberleninka.ru/article/n/metodika-upravleniya-riskami-dlya-malogo-i-srednego-biznesa (accessed: 02/05/2023).
6. Kolesnikov A.M., Baranov A.V. Analiz riskov predpriyatij elektroenergetiki [Risk analysis of electric power companies]. Teoriya i praktika servisa: ekonomika, social'naya sfera, tekhnologii, SPbGEU [Theory and practice of service: economics, social sphere, technology, SPbSUE], 2013, no. 4 (18), pp.154-158
7. Senkov A.V. Graficheskaya notaciya dlya predstavleniya processa upravleniya kompleksnymi riskami [Graphical notation for presenting the process of complex risk management]. Sovremennye naukoemkie tekhnologii [Modern High Technologies], 2016, no. 12 (1), pp. 72-81, available at: https://top-technologies.ru/ru/article/view?id=36479 (accessed: 02/05/2023).
8. Zhilkina Yu.V., Vodennikov D.A. Riski v energetike: analiz praktiki upravleniya na rynke elektroenergii [Risks in the energy sector: analysis of management practices in the electricity market]. Available at: http://cigre.ru/research_commitets/ik_rus/b3_rus/materials/library/%D0%96%D0%B8%D0%BB%D0%BA%D0%B8%D0%BD%D0%B0_.pdf (accessed: 04/11/2023).
9. Uvarova G. The risk map of business processes can be made practical [The risk map of business processes can be made practical]. Available at: https://www.eg-online.ru/article/274036/ (accessed: 05/15/2023).

10. Kolosok I.N., Korkina E.S. Response agregator kak biznes-protsess v usloviyakh tsifrovizatsii energetiki [Demand Response Aggregator as a business process under the energy digitalization]. Relejnaya zashchita i avtomatizaciya [Relay protection and automation], 2021, no. 4, pp. 22-27.
11. Kudrjavyj V.V. Riski I ugrozy rossijskoj electroenergetiki. Puti preodolenija [Risks and threats of the Russian electric power industry. Ways to overcome]. Available at: https://www.ruscable.ru/article/ The_risks_ and_ threats_of_the_Russian_power_industry/ (accessed: 03/02/2023).
12. Boehmer W.Analysis of strongly and weakly coupled management systems in information security. 2010, available at: https://ieeexplore.ieee.org/document/5633657 (accessed: 03/02/2023).
13. Kiber-riski: kak ponimat' i upravlyat' [Cyber risks: how to understand and manage]. Available at: https://10guards.com/ru/articles/cyber-risks/ (accessed: 03/12/2023)
14. Rol' informacionnoj bezopasnosti v obespechenii nepreryvnosti biznesa [The role of information security in ensuring business continuity]. Available at: http://www.interface.ru/home.asp?artId=40308 (accessed: 02/20/2023).
15. Kachurov E. Sem' shagov k nepreryvnosti biznesa [Seven steps to the business continuity], 2015, available at: https://habr.com/ru/company/softline/blog/261053/ (accessed: 03/02/2023).
16. Musatov K. Nepreryvnost' biznesa. Podhody i resheniya [Business continuity. Approaches and solutions]. Available at: https://lib.itsec.ru/articles2/control/ot-ypravleniya-incidentami-ib-cherez-neprerivnost (accessed: 15/05/2023)
17. Voropai N.I., Kolosok I.N., Korkina E.S., Osak A.B. Problemy uyazvimosti i zhivuchesti kiberfizicheskih elektroenergeticheskih sistem [Problems of vulnerability and survivability of cyberphysical electric power systems]. Energeticheskaya politika [Energy policy], 2018, no. 5, pp. 53-61.
18. Kolosok I.N., Korkina E.S. Application of logical-probabilistic analysis to increase the survivability of the Demand Response Aggregator [Primenenie logiko-veroyatnostnogo analiza dlya povysheniya zhivuchesti Agregatora upravleniya sprosom na elektroenergiyu]. Energetik [Power & Electrical engineering], 2022, no. 12, pp. 9-12.
19. "Roselektronika" predstavila kiberzashchishchennuju sistemu dlya cifrovoj electroseti ["Roselektronika" presented a cyber-protected system for the digital power grid]. Available at: https://www.cnews.ru/ news/line/ 2019-07-09_roselektronika_predstavila_kiberzashchishchennuyu (accessed: 07/09/ 2019).
20. Guk Yu.B. Raschet nadezhnosti electroenergeticheskih ustanovok [Calculation of the reliability of electric power plants], Leningrad, Energoatomizdat, 1988, 224 p.
21. Nadezhnost' tekhnicheskih sistem i tekhnogennyj risk. Derevo sobytij [Reliability of technical systems and technogenic risk. Event Tree]. Available at: http://www.obzh.ru/nad/6-9.html (accessed: 03/02/2023).
22. Rudenko Yu.N., Ushakov I.A. Nadezhnost' sistem energetiki. [Reliability of energy systems]. Novosibirsk, Nauka [Novosibirsk, Science], 1989, 328 p.
23. Bow Tie Analysis, available at: http://www.consultant.ru/docment/cons_doc_LAW_406016/79d895387 ec905 fc042 eccdcc6fce3b320e9b18d/ (accessed: 27/01/2023).
24. Utkin N. nterv'yu s ekspertom: «Bezopasnost' kiber-fizicheskikh sistem: trebuyutsya kompleksnyy podkhod i proaktivnyye mekhanizmy» [Interview with an expert: "Security of cyber-physical systems: an integrated approach and proactive mechanisms are required"]. Available at: https://safe-surf.ru/specialists/article/5291/668770/ (accessed: 03/02/2023).

Kolosok Irina Nikolaevna. *Doctor of Sciences, Leading Researcher, MESI SB RAS. Scientific interests area – mathematical models, methods and algorithms for solving complex tasks of information support for monitoring and dispatching control of an intelligent power system (IES) based on modern measuring instruments and new information technologies, cybersecurity and cyberphysical stability of the IES and its objects. AuthorID: 48007871, ORCID: 0000-0002-2843-4455, kolosok@isem.irk.ru, 664033, Irkutsk, Lermontov str.,130.*

Korkina Elena Sergeevna. *PhD, Senior Researcher, MESI SB RAS. Scientific interests area – cybersecurity of electric power facilities, synchronized vector measurements, assessment of the state of electric power systems, cyber-physical systems. AuthorID: 24577537100, SPIN: 8084-7363, ORCID: 0000-0001-6488-5774, korkina@isem.irk.ru, 664033, Irkutsk, Lermontov str.,130.*

Статья поступила в редакцию 06.04.2023; одобрена после рецензирования 16.05.2023; принята к публикации 16.06.2023.
The article was submitted 04/06/2023; approved after reviewing 05/16/2023; accepted for publication 06/16/2023.