Электрические станции и электроэнергетические системы (05.14.02)

УДК 621.311.001.57
DOI: 10.24160/1993-6982-2019-3-27-36

Повышение информационной безопасности автоматизированных систем диспетчерского управления в электроэнергетических системах

Д.Б. Гвоздев, О.Д. Архангельский

Рассмотрены основные тенденции развития автоматизированных систем диспетчерского управления (АСДУ) в электроэнергетике, проанализирован переход к концепции удаленно управляемых необслуживаемых подстанций. Показано, что в связи с интеллектуализацией электроэнергетики в настоящее время на первый план выходят вопросы обеспечения кибербезопасности энергообъектов. Возможные информационные воздействия и кибератаки на объекты электроэнергетической системы (ЭЭС) могут привести к нарушению работы не только автоматизированных систем и вторичного интеллектуального оборудования, но и первичного оборудования станций и подстанций. Основными вызовами и угрозами, возникающими в результате информатизации отрасли, являются несанкционированное управление оборудованием цифровых подстанций, отказы и сбои в работе первичного и вторичного оборудования подстанций в результате кибератак. Новые вызовы определяют актуальность задачи оценки рисков нарушения функционирования АСДУ в электроэнергетике.

Оценку рисков нарушения функционирования АСДУ предложено проводить в дополнение к оценке надежности электроэнергетических систем и их компонент. Показана актуальность разработки указанной методики оценки рисков, а также предложен один из вариантов ее практической реализации. Представленный вариант предполагает использование метода моделирования ЭЭС в реальном времени с включенным в контур моделирования вторичным оборудованием: терминалами релейной защиты и автоматики (РЗА), контроллерами и интеллектуальными устройствами. При этом остальная часть системы (первичное оборудование подстанции) может выглядеть как численная модель, реализуемая на симуляторе RTDS (такой подход носит название полунатурного моделирования). Моделирование участка ЭЭС с включенными в контур моделирования устройствами РЗА и АСУ ТП позволит оценить последствия для различных сценариев нарушения функционирования сложной электроэнергетической системы, в том числе в результате возможных несанкционированных информационных воздействий.

Разработанная методика оценки рисков нарушения функционирования АСДУ позволяет получить интегральные значения риска для рассматриваемого объекта или системы. Результаты расчетов могут быть использованы для принятия управленческих решений, а корректный и своевременный выбор мероприятий по управлению выявленными рисками позволяет обеспечить надежность и безопасность как отдельных объектов электроэнергетики, так и ЭЭС в целом.

Ключевые слова: автоматизированные системы управления, SCADA, безопасность автоматизированных систем, оценка рисков, киберфизические системы, полунатурное моделирование.

Для цитирования: Гвоздев Д.Б., Архангельский О.Д. Повышение информационной безопасности автоматизированных систем диспетчерского управления в электроэнергетических системах // Вестник МЭИ. 2019. № 3. С. 27—36. DOI: 10.24160/1993-6982-2019-3-27-36.

Enhancing the Information Security of Automated Dispatch Control Systems in Electric Power Systems

D.B. Gvozdev, O.D. Arkhangelsky

The main trends in the development of automated dispatch control systems (also known as SCADA — supervisory control and data acquisition systems) in the electric power industry are considered, and the shift to the concept of remotely controlled unattended substations is analyzed. It is shown that the introduction of smart computerized control systems in the electric power industry results in that the matters concerned with ensuring cybersecurity of power facilities are coming at the forefront. Possible information-related impacts and cyber-attacks on electric power system facilities can upset the operation of not only automated systems and secondary intelligent equipment, but also the main power equipment of power plants and substations. Unauthorized control of digital substation equipment, failures and malfunctions of primary and secondary substation equipment caused by cyber attacks are the main challenges and threats arising from the

fitting of the electric power industry with information technologies. These new challenges determine the relevance of assessing the risks of upsetting the operation of automated dispatch control systems in the electric power industry.
It is proposed to assess the risks of upsetting the automated dispatch control system operation in addition to evaluating the reliability of electric power systems and their components. The relevance of developing the above-mentioned risk assessment methodology is shown, and one of possible versions of its practical implementation is proposed. The proposed version implies application of the real-time power system simulation method with connecting the secondary equipment (relay protection and automatic control terminals, controllers and intelligent devices) into the simulation loop. The rest part of the system (primary substation equipment) can be represented by a numerical model implemented on an RTDS simulator (this approach is called hardware-in-the-loop simulation). Simulation of an electric power system area with the relay protection, automatic, and process control system devices connected in the simulation loop will make it possible to estimate the consequences for various scenarios of disturbing the operation of a complex electric power system, also as a result of possible unauthorized information attacks.
The developed methodology for assessing the risks of disturbing the operation of an automated dispatch control system makes it possible to obtain the integral risk values for the considered plant or system. The analysis results can be used for taking management decisions, and a correct and timely choice of measures for managing the identified makes it possible to ensure the reliability and safety of both individual electric power industry facilities and the electric power system as a whole.

Key words: automated control systems, SCADA, automated system security, risk assessment, cyber-physical systems, hardware-in-the-loop modeling.

For citation: Gvozdev D.B., Arkhangelsky O.D. Enhancing the Information Security of Automated Dispatch Control Systems in Electric Power Systems. Bulletin of MPEI. 2019;3:27—36. (in Russian). DOI: 10.24160/1993-6982-2019-3-27-36.

Введение

Для обеспечения надежности, повышения наблюдаемости и управляемости на объектах электроэнергетических систем (ЭЭС) активно внедряются различные автоматизированные системы управления. Автоматизируется большая часть функций, относящихся как к оперативно-технологическому, так и к оперативно-диспетчерскому управлению. Информационные системы (ИС) внедряются на всех уровнях иерархии электросетевых компаний: начиная с уровня объекта и заканчивая исполнительным аппаратом.

На рисунке 1 изображена «пирамида автоматизации», в которой АСУ ТП на подстанциях — первый уровень системы управления электрической сетью, непосредственно связанный с технологическим оборудованием [1]. Основные задачи трехуровневой системы

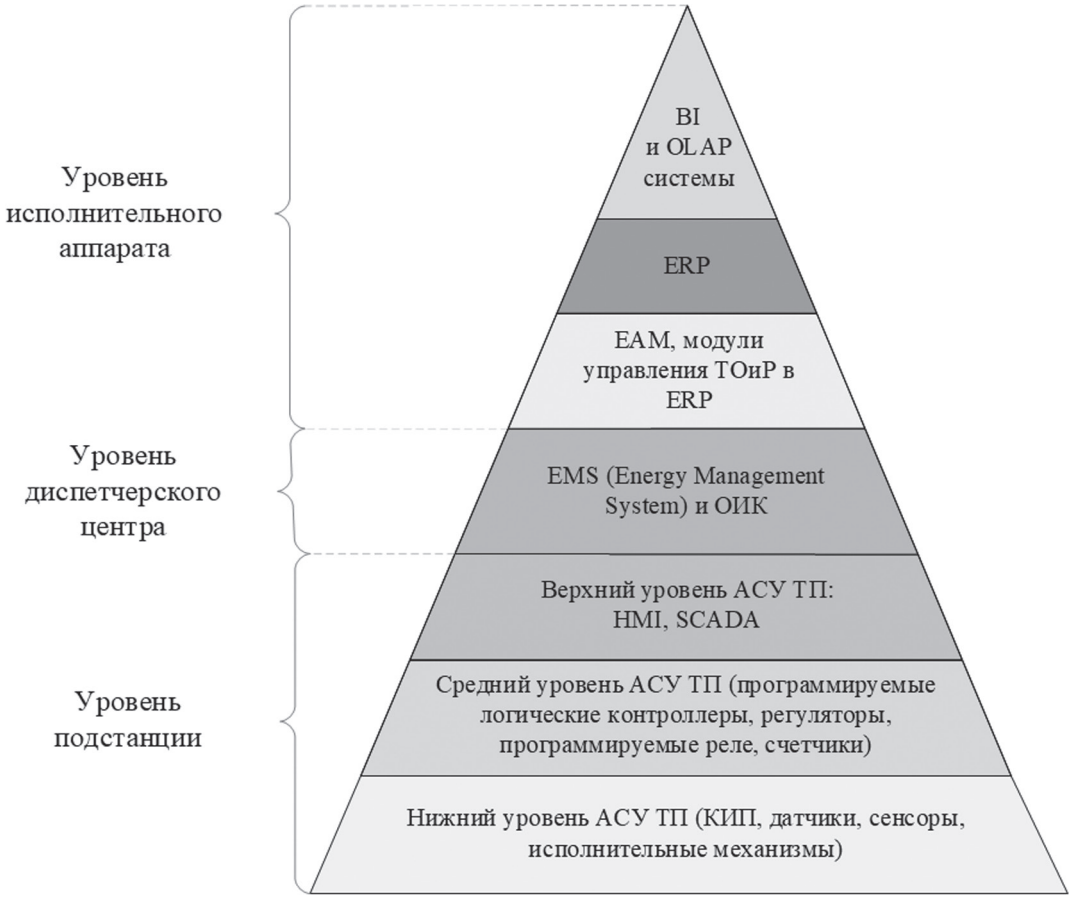

Рис. 1. Целевая архитектура АСДТУ

АСУ ТП — контроль состояния первичного оборудования энергообъекта, автоматическое и автоматизированное регулирование технологических параметров и дистанционное управление оборудованием ПС: коммутационными аппаратами, РПН трансформаторов и т. д. Именно уровень АСУ ТП во многом определяет эффективность управления всей электроэнергетической системой, поскольку является источником информации для верхних уровней управленческой структуры: системы диспетчерского управления ЭЭС (Energy Management System, EMS), а также систем управления активами (Enterprise Asset Management System, EAM) и управления ресурсами электросетевых компаний (Enterprise Resource Planning, ERP).

EMS-система, расположенная на уровне диспетчерского центра, обеспечивает проведение оперативных переключений, а также обладает широким спектром расчетно-аналитических функций: расчетом и планированием режимов сети, оптимизацией режимов, расчетом токов КЗ и поддержкой заданных уровней напряжения. В EMS могут быть реализованы и административно-технические функции по управлению работой оперативных выездных бригад, функции формирования отчетности и т. д. Помимо EMS на уровне диспетчерского центра могут использоваться операционные управляющие комплексы (ОИК). Как правило, в части управления режимом работы энергосистемы в ОИК реализованы те же функции, что и в EMS, однако они обладают меньшими возможностями в части дорасчета параметров, а также меньшим набором административно-технических функций. В настоящее время с целью создания единой системы управления проводится интеграция EMS и ОИК, т.е. реализуются не только вертикальная интеграция между системами различных уровней, но и горизонтальная интеграция систем, работающих на одном уровне. Так, в ПАО «МОЭСК» система EMS в Центре управления сетями (ЦУС) интегрирована с ОИК диспетчерских центров (рис. 2) [2].

На уровне исполнительного аппарата применяются информационные системы, обеспечивающие поддержку административно-хозяйственной деятельности электросетевой компании. Информация с уровня SCADA и EMS поступает в ERP-системы, отвечающие за автоматизацию и управление бизнес-процессами компании, а также на уровень высшего менеджмента предприятия (аналитические системы OLAP и BI).

Наличие различных информационных систем на нескольких уровнях иерархии свидетельствует о высоком уровне информатизации отрасли [3]. Если в части автоматизации бизнес-процессов взаимная интеграция систем позволяет более эффективно решать задачи, связанные с эксплуатационной деятельностью электросетевых компаний (например, организация ремонтов в системах EAM или ERP на основе данных, получаемых от SCADA и EMS), то интеграция систем объектового уровня (SCADA подстанций) с автоматизированными системами диспетчерских центров (ОИК, EMS) может говорить о качественных изменениях в процессе оперативно-диспетчерского управления и переходе к удаленному управлению электроэнергетическими объектами [4 — 7].

На примере объектов ПАО «ФСК ЕЭС» видно, что в настоящее время современными средствами телемеханики и телеуправления (ТУ), позволяющими удаленно контролировать оборудование подстанций из диспетчерского центра, оснащены более 70% ПС различных классов напряжения (рис. 3; данные приведены за 2018 г. [5]).

Реконструкция и модернизация подстанций с внедрением телеуправления — это только первый шаг в цифровизации электроэнергетики. Следующим шагом является строительство телеуправляемых цифровых подстанций (ЦПС) — одного из ключевых компонентов интеллектуальной сети SmartGrid [8]. Данные подстанции характеризуются применением интегрированных цифровых систем измерения, цифровых терминалов релейной защиты, контроллеров управления силовым

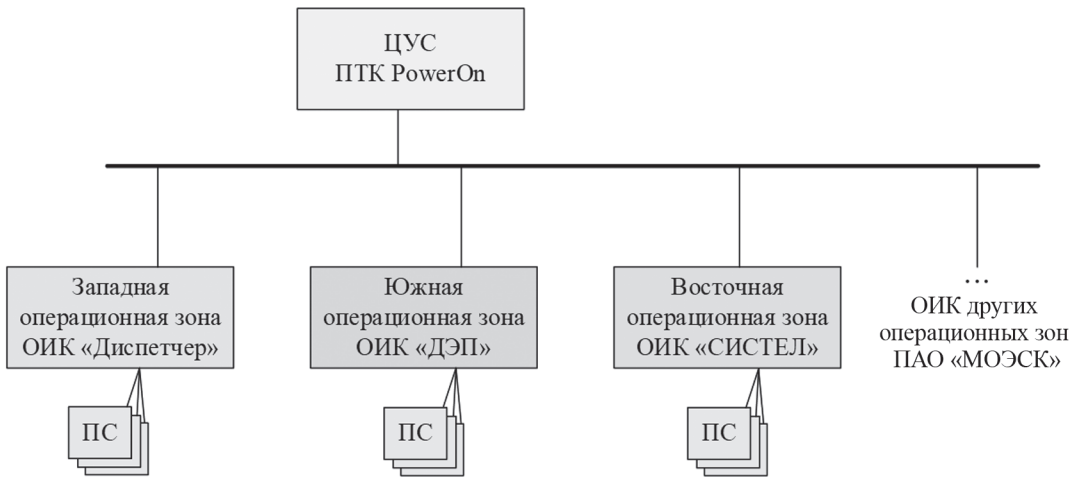

Рис. 2. Интеграция ОИК и EMS (на примере ПАО «МОЭСК»)

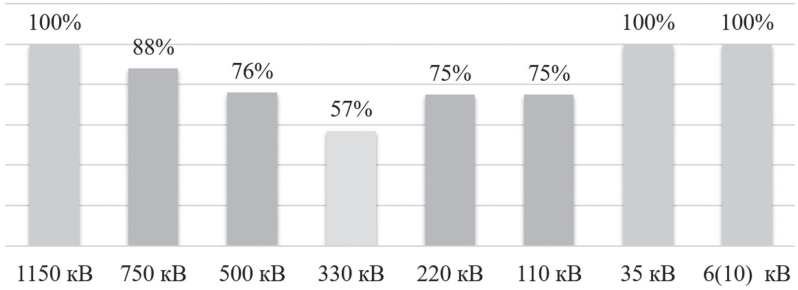

Рис. 3. Процентное отношение телеуправляемых подстанций ПАО «ФСК ЕЭС» к общему количеству подстанций с распределением по классам напряжений

оборудованием и оптических трансформаторов тока и напряжения, работающих на едином стеке протоколов стандарта МЭК 61850. Следует отметить, что вторичное оборудование цифровой подстанции имеет внешние интерфейсы, разрешающие удаленное подключение как для сервисного обслуживания (конфигурирования, обновления прошивок и т.д.), так и для оперативных задач: изменения группы уставок или выполнения переключений.

В рамках активного внедрения этой технологии ПАО «ФСК ЕЭС» планирует до 2025 г. построить 32 цифровые подстанции, а целый ряд электросетевых компаний заявил об успешном завершении пилотных проектов и начале масштабного строительства ЦПС [9, 10]. Сразу в нескольких электросетевых компаниях реализуются программы, предусматривающие модернизацию не только магистральных, но и распределительных электрических сетей с применением современных программных продуктов и телеуправляемого оборудования (информационные системы и интеллектуальные устройства внедряются в рамках программы «Цифровой РЭС» [11, 12]).

Таким образом, современные ЭЭС характеризуются интеграцией физической (электросетевой) и информационной инфраструктур, т. е.приобретают черты кибер-физических систем. В них обе составляющих (физическая и информационная) в равной степени сложны и взаимно влияют друг на друга [13]. Однако неизбежным следствием взаимной интеграции становится появление новых, ранее несвойственных для электроэнергетики угроз и уязвимостей.

Интеллектуализация сетей, с одной стороны, значительно упрощает как эксплуатационное обслуживание, так и оперативно-диспетчерское и оперативно-технологическое управления сетями. С другой стороны, наличие непосредственного взаимодействия с управляемым объектом, а также ряд других факторов, отмеченных в [14], значительно повышает критичность систем автоматизированного диспетчерского управления и сетей связи, в связи с чем особенно актуальной оказывается проблема потенциальных кибератак на объекты электроэнергетической инфраструктуры и, как следствие, нарушения управляемости ЭЭС.

Кибератаки могут быть направлены на инфраструктуру передачи и распределения электроэнергии, а также на объекты генерации электроэнергии. При этом, по мнению экспертов [14, 15], в обоих случаях наиболее уязвимым звеном являются именно системы управления и диспетчеризации электроэнергетических систем, причем их уязвимость возрастает по мере внедрения технологий интеллектуальных сетей.

В качестве основных возможных угроз в настоящее время исследователи отмечают следующие [14, 16]:

- кибератаки через внешние цифровые каналы связи энергообъекта (поскольку зачастую удаленное управление осуществляется через арендованные каналы связи), приводящие к искажению или подмене диспетчерских команд или значений телеметрии [17];
- невыявленные ошибки в программном обеспечении устройств цифровой подстанции, в том числе терминалов РЗА [18];
- кибератаки на серверы АСУ ТП подстанции и серверы SCADA-системы в центрах управления сетями и диспетчерских центрах;
- злонамеренные программные дефекты, встроенные в программное обеспечение микропроцессорных устройств.

Помимо возможных информационных воздействий, вызывающих сбои в работе АСДУ и ее подсистем (РЗА, АСУ ТП и т. д.), для сложных киберфизических систем следует принимать во внимание опасность последствий ошибочных действий персонала. С одной стороны, автоматизация технологических процессов позволяет свести к минимуму риск ошибки при штатных оперативных переключениях за счет программных блокировок, загружаемых типовых бланков переключений. С другой стороны, внедрение большого количества информационных систем на различных уровнях создает дополнительные «точки отказа»; с учетом непосредственного взаимодействия управляющих систем с физическим оборудованием энергообъекта это может привести к тому, что даже незначительная ошибка диспетчера или несоблюдение оперативным персоналом требований обеспечения информационной безопасности (ИБ) могут иметь серьезные последствия для энергосистемы [19 — 21]. Кроме того, значительно увеличивается информационная нагрузка на оперативный персонал [22], и это приводит к росту вероятности некорректных или ошибочных действий диспетчера.

Кибербезопасность подстанций и объектов электроэнергетической системы

Повышенное внимание к проблеме информационной безопасности и возможным нарушениям функционирования АСДУ в результате информационных воздействий не случайно. Согласно результатам исследований, проведенных в 2017 г. [23], наибольшее число кибератак пришлось именно на предприятия электроэнергетического комплекса (38,7% от общего числа атак). Известно о ряде успешных атак на электроэнергетические предприятия, приведших к ограничению (а в ряде случаев и полному прекращению) электроснабжения потребителей [24]. Очевидно, что с внедрением информационных систем проблема будет усугубляться, поскольку в рамках концепции цифровых подстанций программное обеспечение и информационные системы становятся одним из наиболее важных (и, в тоже время, уязвимых) элементов киберфизической ЭЭС.

Как отмечено в [14], проблема кибербезопасности объектов электроэнергетики — одна из ключевых с точки зрения обеспечения общей надежности ЭЭС, при этом в настоящее время ее масштаб явно недооценен.

Таким образом, чрезвычайно актуальной становится задача обеспечения безопасности функционирования создаваемой интеллектуальной электроэнергетической системы. Необходимо разработать методы и подходы, позволяющие проводить анализ по целому ряду факторов, многие из которых не характерны для «традиционных» ЭЭС, но оказывают значительное влияние на киберфизические системы.

Применение теории рисков для оценки безопасности электроэнергетической системы

В настоящее время в России как для первичного оборудования, так и для автоматизированных систем управления и интеллектуальных устройств применяется оценка надежности систем и их компонент [25]. Разработаны различные процедуры и методики расчёта нормативных показателей надёжности, в частности, создана математическая теория надежности (ТН) сложных систем. Однако использование данной теории на практике для оценки безопасности функционирования киберфизических систем в условиях возможных внешних информационных воздействий связано с определенными ограничениями.

Наиболее заметной проблемой является проблема «редких событий». Теория надежности рассматривает прогнозируемые отказы оборудования, в то время как кибератака на объекты ЭЭС является сложной комбинацией «маловероятных» отказов и событий, в итоге приводящих к опасному состоянию [26 — 28]. При использовании классической теории вероятностей, применяемой в ТН, «редкие события», попадающие в область крайне малых значений распределения вероятности, не рассматриваются [29]. Поскольку кибератаки можно отнести к внешним экстремальным возмущениям, приводящим к каскадному развитию аварии в ЭЭС (в англоязычной литературе для подобных явлений введено специальное обозначение HILF (от англ. High Impact & Low Frequency Events, т.е. события с малой частотой возникновения и высокой тяжестью последствий [30])), очевидно, что корректно оценить вероятность выхода из строя энергообъекта в результате данных событий с помощью классической теории вероятности невозможно [13].

Существует проблема с интерпретацией результатов анализа системы и последующим выбором соответствующих мероприятий, направленных на устранение выявленных недостатков. При использовании теории надёжности по результатам анализа предпринимаются меры, направленные на обеспечение «классической» надежности (например, резервирование и дублирование уязвимых элементов) [31]. Очевидно, что в большинстве случаев они не эффективны против возможных кибератак, поскольку не устраняют саму причину возможных отказов и нарушений в работе систем. Применение только мер и методик обеспечения ИБ также не позволит решить проблему обеспечения безопасности объекта, так как эта проблема не лежит в какой-то одной плоскости и является комплексной, требующей применения знаний из различных областей. В связи с этим основной задачей в настоящее время является разработка методики, позволяющей проанализировать возможные отказы АСДУ и учесть влияющие факторы различной природы (в том числе и внешнее вмешательство в работу системы).

Для решения указанной задачи может быть применена теория рисков. Риск-ориентированный подход успешно применяется (в основном в США и странах ЕС) в различных отраслях промышленности, в том числе и для объектов энергетической инфраструктуры [32].

Основное отличие анализа надежности от анализа рисков заключается в следующем. В первом случае изучается способность объекта выполнять заданные штатные функции (при определенных условиях эксплуатации) в установленных пределах, в то время как во втором случае рассматриваются влияющие факторы различной природы (в том числе, экстремальные и маловероятные внешние воздействия на систему) и взаимосвязи между ними, а также проводится всесторонний анализ последствий реализации выявленных угроз.

Подходы к решению задачи

Процедуру оценки рисков нарушения функционирования АСДУ в ЭЭС следует проводить в дополнение к существующим процессам оценки надежности электроэнергетической системы и ее компонентов. Аналогичный подход используется в различных высокорисковых отраслях. Широко распространена оценка безопасности для атомных станций, газо- и нефтепроводов [33, 34]. В [14] перечислены основные аспекты,

которые необходимо учесть при разработке методики для оценки рисков. Стоит отметить, что при разработке многофакторной методики анализа рисков нарушения функционирования АСДУ в электроэнергетике следует принять во внимание следующие моменты.

Используемые методы и подходы должны позволять учитывать различные влияющие факторы, взаимодействие информационных и технологических подсистем и системные свойства сложной киберфизической энергосистемы.

Выбор методов оценки рисков должен осуществляться с учетом проблемы «редких событий», т. е. при выборе методов необходимо исключить методы, основанные на классической теории вероятностей.

Проведенный в соответствии с разработанной методикой анализ позволит получить интегральную оценку безопасности системы. При этом, за счет своевременно реализованных мер по управлению выявленными рисками, можно повысить безопасность автоматизированной системы диспетчерского управления и, соответственно, безопасность электроэнергетической системы в целом. Разработанная теоретическая методика оценки рисков нарушения управляемости АСДУ или отдельные ее компоненты могут быть реализованы в виде программного комплекса (например, информационно-аналитической системы анализа рисков).

Одним из наиболее интересных и перспективных направлений практической реализации концепции оценки рисков в сложных ЭЭС является полунатурное моделирование и создание специализированных испытательных лабораторий для исследования безопасности ЭЭС. Очевидно, что исследование киберугроз в реальной энергосистеме связано со значительными техническими трудностями и материальными затратами. В связи с этим полунатурное моделирование широко применяется в научных исследованиях в США и странах Европейского союза. В США функционирует несколько институтов и исследовательских лабораторий, изучающих вопросы возникновения различных сбоев и нарушений в работе автоматизированных систем диспетчерского управления (АСДУ), которые используют технологию полунатурного моделирования для построения испытательных стендов [35]. К ним относятся национальные лаборатории г. Сандия (Sandia National Laboratories), Аргоннская национальная лаборатория (Argonne National Laboratory, ANL), национальная лаборатория Айдахо (Idaho National Laboratory, INL) и исследовательская лаборатория TCIPG (Trustworthy Cyber Infrastructure for the Power Grid). Данные научно-исследовательские объединения проводят исследования в области противодействия угрозам информационной безопасности (ИБ) для интеллектуальных энергосистем и обладают значительными вычислительными и испытательными мощностями [36].

В рамках практической реализации методики оценки рисков подобный исследовательский комплекс для изучения безопасности электроэнергетических систем может быть разработан и в нашей стране. В нем необходимо смоделировать одновременно три взаимодействующих между собой уровня киберфизической системы, наиболее полно представляющих сложную ЭЭС (рис. 4): первичного (силового) оборудования, вторичного оборудования РЗА и АСУ ТП и систем связи, а также SCADA HMI (систем отображения и визуализации).

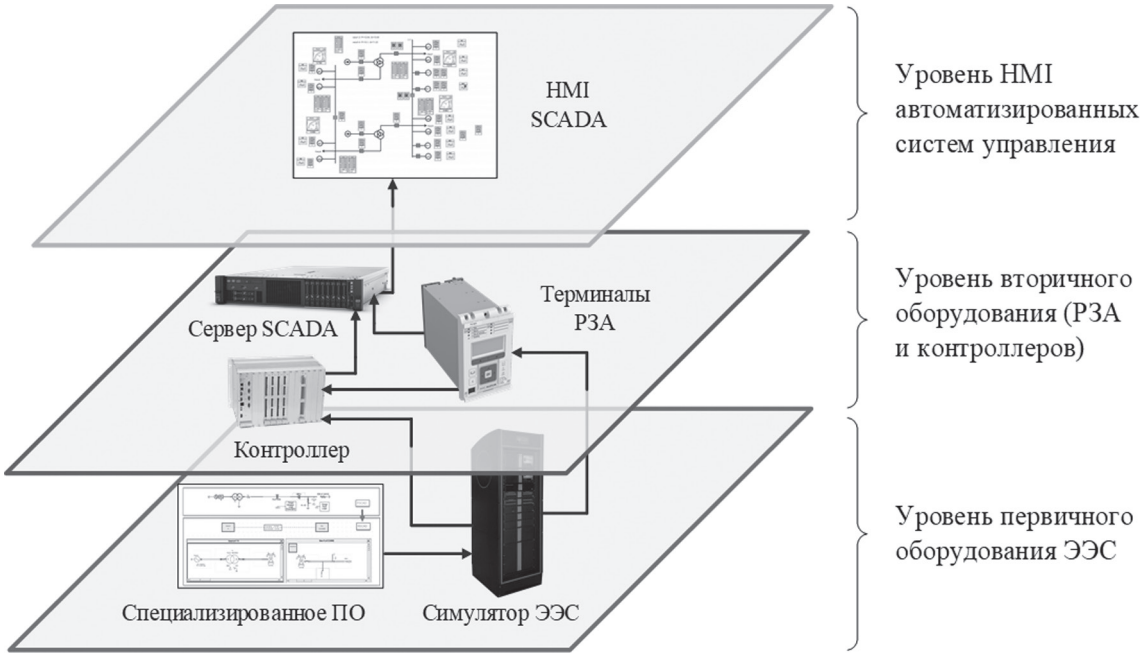

Рис. 4. Концепция модели киберфизической системы

Часть оборудования электроэнергетических объектов должна моделироваться математически, а остальные — с помощью реального оборудования, т.е. натурно. Наличие контура моделирования, включающего в себя оборудование различных подсистем сложной киберфизической ЭЭС, позволит эффективно решать задачи, связанные с оценкой безопасности объектов электроэнергетики, а также применять концепцию сценарного моделирования.

Заключение

Показана необходимость проведения анализа рисков для усложняющихся электроэнергетических систем. Поскольку существующие в настоящее время методики оценки надежности не позволяют проводить оценку безопасности киберфизических ЭЭС в силу своих ограничений, предложно в дополнение к оценке надежности проводить оценку рисков. Для ее проведения следует решить основные задачи, т. е. выбрать подходы, учитывающие взаимодействие различных информационных и технологических подсистем ЭЭС, и методы, позволяющие решить проблему «редких событий», для оценки которых неприменима классическая теория вероятностей.

В связи с этим основной научной задачей в настоящее время является многофакторный анализ рисков нарушения функционирования АСДУ в условиях неопределенности и разработка соответствующей методики. На базе данной методики могут быть созданы программные продукты для анализа рисков, позволяющие анализировать безопасность объектов ЭЭС и автоматизированных систем. Кроме того, концепция анализа рисков может служить базисом для создания лабораторий исследования безопасности электроэнергетических систем.

Литература

1. **Принципы** создания АСУТП на подстанциях ЕНЭС [Электрон. ресурс] http://www.cius-ees.ru/uploaded/document_files/58/Printsipy_postroeniya__ASUTP_PS.pdf (дата обращения: 14.12.2018).

2. **Чегодаев А.В.** Современная автоматизированная система технологического управления // Электроэнергия. Передача и распределение. 2012. № 4 (13). С. 76—80.

3. **Энергетика** глазами системных интеграторов [Электрон. ресурс] http://www.bcc.ru/press/publishing/pub07/Energy_in_syst_integrator_views (дата обращения 14.12.2018).

4. **«Россети»** и системный оператор совершенствуют технологию управления оборудованием подстанций ЕЭС России [Электрон. ресурс] http://www.rosseti.ru/press/news/?ELEMENT_ID=24828 (дата обращения 12.10.2018).

5. **Телеуправление** на подстанциях: ПС 330 кВ «Губкин» и ПС 500 кВ «Щёлоков» [Электрон. ресурс] http://digitalsubstation.com/blog/2018/06/27/teleupravlenie – na – podstantsiyah – ps – 330 – kv – gubkin – i – ps – 500 – kv – shhyolokov/ (дата обращения 12.10.2018).

6. **Впервые** в центральной России энергообъект высокого класса напряжения переведен на телеуправление [Электрон. ресурс] http://www.fsk-ees.ru/press_center/company_news/?ELEMENT_ID=227933 (дата обращения 12.10.2018).

7. **В энергосистеме** Республики Татарстан реализован проект модернизации системы телеуправления оборудованием подстанции 500 кВ Щёлоков [Электрон. ресурс] http://www.so-cdu.ru/index.php?id=odu_volga_news_view&no_cache=1&tx_ttnews[tt_news]=12680 (дата обращения 12.10.2018).

8. **Цифровая** подстанция — важный элемент интеллектуальной энергосистемы [Электрон. ресурс]

References

1. **Printsipy** Sozdaniya ASUTP na Podstantsiyakh ENES [Elektron. Resurs] http://www.cius-ees.ru/uploaded/document_files/58/Printsipy_postroeniya__ASUTP_PS.pdf (Data Obrashcheniya: 14.12.2018). (in Russian).

2. **Chegodaev A.V.** Sovremennaya Avtomatizirovannaya Sistema Tekhnologicheskogo Upravleniya. Elektroenergiya. Peredacha i Raspredelenie. 2012;4 (13):76—80. (in Russian).

3. **Energetika** Glazami Sistemnykh Integratorov [Elektron. Resurs] http://www.bcc.ru/press/publishing/pub07/Energy_in_syst_integrator_views (Data Obrashcheniya 14.12.2018). (in Russian).

4. **«Rosseti»** i Sistemnyy Operator Sovershenstvuyut Tekhnologiyu Upravleniya Oborudovaniem Podstantsiy EES Rossii [Elektron. Resurs] http://www.rosseti.ru/press/news/?ELEMENT_ID=24828 (Data Obrashcheniya 12.10.2018). (in Russian).

5. **Teleupravlenie** na Podstantsiyakh: PS 330 kV «Gubkin» i PS 500 kV «Schcelokov» [Elektron. Resurs] http://digitalsubstation.com/blog/2018/06/27/teleupravlenie – na – podstantsiyah – ps – 330 – kv – gubkin – i – ps – 500 – kv – shhyolokov/ (Data Obrashcheniya 12.10.2018). (in Russian).

6. **Vpervye** v Tsentral'noy Rossii Energoob′ekt Vysokogo Klassa Napryazheniya Pereveden na Teleupravlenie [Elektron. Resurs] http://www.fsk-ees.ru/press_center/company_news/?ELEMENT_ID=227933 (Data Obrashcheniya 12.10.2018). (in Russian).

7. **V energosisteme** Respubliki Tatarstan realizovan Proekt Modernizatsii Sistemy Teleupravleniya Oborudovaniem Podstantsii 500 kV Shchelokov [Elektron. Resurs] http://www.so-cdu.ru/index.php?id=odu_volga_news_view&no_cache=1&tx_ttnews[tt_news]=12680 (Data Obrashcheniya 12.10.2018). (in Russian).

8. **Tsifrovaya** Podstantsiya — Vazhnyy Element Intellektual'noy Energosistemy [Elektron. Resurs] https://

https://www.ruscable.ru/article/Tsifrovaya_podstantsiya__vazhnyj_element_intellektualynoj_energosiste/ (дата обращения 14.12.2018).

9. **«ФСК ЕЭС»** потратит на цифровизацию около 72 млрд руб. [Электрон. ресурс] https://www.vestifinance.ru/articles/97898 (дата обращения 10.10.2018).

10. **Цифровая** подстанция «Созвездие» введена в строй [Электрон. ресурс] https://www.comnews.ru/digital-economy/content/116697/news/2018-12-17/cifrovaya-podstanciya-sozvezdie-vvedena-v-stroy (дата обращения 14.12.2018).

11. **Энергетики** сформировали образ цифровой электроэнергетики [Электрон. ресурс] https://minenergo.gov.ru/node/9464 (дата обращения 10.10.2018).

12. **МОЭСК** представила пилотные проекты Москвы по цифровизации электрических сетей на Российской энергетической неделе [Электрон. ресурс] http://www.moesk.ru/press/company_news/item163415.php (дата обращения 10.10.2018).

13. **Воропай Н.И., Колосок И.Н., Коркина Е.С., Осак А.Б.** Киберфизические электроэнергетические системы: трансформация свойств и новые проблемы // Автоматизация и IT в энергетике. 2018. № 9 (110). С. 4—8.

14. **Массель Л.В., Воропай Н.И, Сендеров С.М., Массель А.Г.** Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17). С. 2—10.

15. **Куликов А.Л., Зинин В.М.** Создание системы кибербезопасности в электроэнергетике РФ с учётом реализации концепции ИЭС ААС // Электроэнергия. Передача и распределение. 2015. № 5 (32). С. 122—126.

16. **Byres E., Eng P.** SCADA Security in a Post Stuxnet World [Электрон. ресурс] https://www.tofinosecurity.com/sites/default/files/SCADA-Security-in-a-Post-Stuxnet-World.pdf (дата обращения 10.10.2018).

17. **Осак А.Б., Панасецкий Д.А., Бузина Е.Я.** Аспекты надежности и безопасности при проектировании цифровых подстанций // Современные направления развития систем релейной защиты и автоматики энергосистем: Сб. докл. Междунар. конф. Сочи, 2015. С. 1—7.

18. **Харламов В.А.** Вопросы восстановления работы систем РЗА после успешных кибератак // Релейщик. 2016. № 2. С. 3—7.

19. **Дьяков А.Ф.** Надежная работа персонала в энергетике. М.: МЭИ, 1991.

20. **Integrated** Bulk Power System Risk Assessment Concepts. Atlanta: NERC, 2013.

21. **Снижение** рисков каскадных аварий в электроэнергетических системах / под ред. Н.И. Воропая. Новосибирск: Изд-во СО РАН, 2011.

22. **Гвоздев Д.Б.** Разработка критерия оптимальной информационной нагрузки диспетчера ЦУС предприятия электрических сетей // Вестник МЭИ. 2013. № 2. С. 55—58.

23. **Ландшафт** угроз для систем промышленной автоматизации [Электрон. ресурс] https://ics-cert.kaspersky.

www.ruscable.ru/article/Tsifrovaya_podstantsiya__vazhnyj_element_intellektualynoj_energosiste/ (Data Obrashcheniya 14.12.2018). (in Russian).

9. **«FSK EES»** Potratit na Tsifrovizatsiyu Okolo 72 mlrd rub. [Elektron. Resurs] https://www.vestifinance.ru/articles/97898 (Data Obrashcheniya 10.10.2018). (in Russian).

10. **Tsifrovaya** Podstantsiya «Sozvezdie» Vvedena v Stroy [Elektron. Resurs] https://www.comnews.ru/digital-economy/content/116697/news/2018-12-17/cifrovaya-podstanciya-sozvezdie-vvedena-v-stroy (Data Obrashcheniya 14.12.2018). (in Russian).

11. **Energetiki** Sformirovali Obraz Tsifrovoy Elektroenergetiki [Elektron. Resurs] https://minenergo.gov.ru/node/9464 (Data Obrashcheniya 10.10.2018). (in Russian).

12. **MOESK** Predstavila Pilotnye Proekty Moskvy po Tsifrovizatsii Elektricheskikh Setey na Rossiyskoy Energeticheskoy Nedele [Elektron. Resurs] http://www.moesk.ru/press/company_news/item163415.php (Data Obrashcheniya 10.10.2018). (in Russian).

13. **Voropay N.I., Kolosok I.N., Korkina E.S., Osak A.B.** Kiberfizicheskie Elektroenergeticheskie Sistemy: Transformatsiya Svoystv i Novye Problemy. Avtomatizatsiya i IT v Energetike. 2018;9 (110):4—8. (in Russian).

14. **Massel' L.V., Voropay N.I, Senderov S.M., Massel' A.G.** Kiberopasnost' kak Odna iz Strategicheskikh Ugroz Energeticheskoy Bezopasnosti Rossii. Voprosy Kiberbezopasnosti. 2016;4 (17):2—10. (in Russian).

15. **Kulikov A.L., Zinin V.M.** Sozdanie Sistemy Kiberbezopasnosti v Elektroenergetike RF s Uchetom Realizatsii Kontseptsii IES AAS. Elektroenergiya. Peredacha i Raspredelenie. 2015;5 (32):122—126. (in Russian).

16. **Byres E., Eng P.** SCADA Security in a Post Stuxnet World [Elektron. Resurs] https://www.tofinosecurity.com/sites/default/files/SCADA-Security-in-a-Post-Stuxnet-World.pdf (Data Obrashcheniya 10.10.2018).

17. **Osak A.B., Panasetskiy D.A., Buzina E.Ya.** Aspekty Nadezhnosti i Bezopasnosti pri Proektirovanii Tsifrovykh Podstantsiy. Sovremennye Napravleniya Razvitiya Sistem Releynoy Zashchity i Avtomatiki Energosistem: Sb. Dokl. Mezhdunar. Konf. Sochi, 2015: 1—7. (in Russian).

18. **Kharlamov V.A.** Voprosy Vosstanovleniya Raboty Sistem RZA Posle Uspeshnykh Kiberatak. Releyshchik. 2016;2:3—7. (in Russian).

19. **D'yakov A.F.** Nadezhnaya Rabota Personala v energetike. M.: MEI, 1991. (in Russian).

20. **Integrated** Bulk Power System Risk Assessment Concepts. Atlanta: NERC, 2013.

21. **Snizhenie** Riskov Kaskadnykh Avariy v Elektroenergeticheskikh Sistemakh / pod Red. N.I. Voropaya. Novosibirsk: Izd-vo SO RAN, 2011. (in Russian).

22. **Gvozdev D.B.** Razrabotka Kriteriya Optimal'noy Informatsionnoy Nagruzki Dispetchera TSUS Predpriyatiya Elektricheskikh Setey. Vestnik MEI. 2013;2: 55—58. (in Russian).

23. **Landshaft** Ugroz Dlya Sistem Promyshlennoy Avtomatizatsii [Elektron. Resurs] https://ics-cert.kaspersky.

ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/#_Toc508825243 (дата обращения 12.09.2018).

24. **Осак А.Б., Панасецкий Д.А., Бузина Е.Я.** Человеческий фактор при обеспечении кибербезопасности объектов электроэнергетики // Современные направления развития систем релейной защиты и автоматики энергосистем: Сб. докл. Междунар. конф. Сочи, 2015.

25. **Фадеев М.И.** Надежность технических систем и техногенный риск. М.: Деловой экспресс, 2002.

26. **Mehrdad S., Mousavian S., Madraki G., Dvorkin Yu.** Cyber-physical Resilience of Electrical Power Systems Against Malicious Attacks: a Review // Current Sustainable / Renewable Energy Rep. 2018. V. 5. Iss. 1. Pp 14—22.

27. **Колосок И.Н., Коркина Е.С., Гурина Л.А.** Анализ надежности результатов оценивания состояния по данным PMU при кибератаках на WAMS // Методические вопросы исследования надежности больших систем энергетики: Сб. науч. статей. Минск: БНТУ, 2015. Вып. 66. С. 231—237.

28. **Папков Б.В., Куликов А.Л., Осокин В.Л.** Киберугрозы и кибератаки в электроэнергетике. Нижний Новгород: НИУ РАНХиГС, 2017.

29. **Nair J., Wierman A., Zwart B.** The Fundamentals of Heavy-tails: Properties, Emergence, and Identification // Proc. Intern. Conf. Measurement and Modeling of Computer Systems. N.-Y., 2013. P. 387.

30. **High-impact** Low-frequency Event Risk to the North American Bulk Power System. Atlanta: NERC, 2010.

31. **Плешко Д.Ю.** Влияние кибербезопасности объектов электроэнергетики на надежность функционирования ЭЭС // Актуальные проблемы энергетики: Материалы студенческой науч.-техн. конф. Минск: БНТУ, 2018. С. 564—567.

32. **Wenyuan Li.** Risk Assessment of Power Systems: Models, Methods, and Applications. N.-Y.: Wiley-IEEE Press, 2014

33. **Месенжник Я.З., Прут Л.Я., Горбунов С.И.** Оценка технических рисков погружных электроцентробежных нефтенасосов при переходе к внешнему сервисному обслуживанию // Электро. 2008. № 6 (20). С. 38—41.

34. **Горбунов С.И.** Развитие теории и методов оценки рисков для обеспечения промышленной безопасности объектов нефтегазового комплекса: автореф. дис. … докт. техн. Уфа: Ин-т проблем транспорта энергоресурсов, 2006.

35. **Kuipers D.** Cybersecurity for Energy Delivery Systems [Электрон. ресурс] www.sans.org/cyber-security-summit/archives/file/summit-archive-1493741208.pdf (дата обращения 14.12.2018).

36. **Bergman D.C., Jin D., Nicol D.M., Yardley T.** The Virtual Power System Testbed and Inter-Testbed Integration // Proc. USENIX Conf. Cyber Security Experimentation and Test. Berkeley, 2009.

ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017/#_Toc508825243 (Data Obrashcheniya 12.09.2018). (in Russian).

24. **Osak A.B., Panasetskiy D.A., Buzina E.Ya.** Chelovecheskiy Faktor pri Obespechenii Kiberbezopasnosti Ob′ektov Elektroenergetiki. Sovremennye Napravleniya Razvitiya Sistem Releynoy Zashchity i Avtomatiki Energosistem: Sb. Dokl. Mezhdunar. Konf. Sochi, 2015. (in Russian).

25. **Fadeev M.I.** Nadezhnost' Tekhnicheskikh Sistem i Tekhnogennyy Risk. M.: Delovoy Ekspress, 2002. (in Russian).

26. **Mehrdad S., Mousavian S., Madraki G., Dvorkin Yu.** Cyber-physical Resilience of Electrical Power Systems Against Malicious Attacks: a Review. Current Sustainable / Renewable Energy Rep. 2018;5;1:14—22.

27. **Kolosok I.N., Korkina E.S., Gurina L.A.** Analiz Nadezhnosti Rezul'tatov Otsenivaniya Sostoyaniya po Dannym PMU pri Kiberatakakh na WAMS. Metodicheskie Voprosy Issledovaniya Nadezhnosti Bol'shikh Sistem Energetiki: Sb. Nauch. Statey. Minsk: BNTU, 2015;66: 231—237. (in Russian).

28. **Papkov B.V., Kulikov A.L., Osokin V.L.** Kiberugrozy i Kiberataki v Elektroenergetike. Nizhniy Novgorod: NIU RANKHiGS, 2017. (in Russian).

29. **Nair J., Wierman A., Zwart B.** The Fundamentals of Heavy-tails: Properties, Emergence, and Identification. Proc. Intern. Conf. Measurement and Modeling of Computer Systems. N.-Y., 2013:387.

30. **High-impact** Low-frequency Event Risk to the North American Bulk Power System. Atlanta: NERC, 2010.

31. **Pleshko D.Yu.** Vliyanie Kiberbezopasnosti Ob′ektov Elektroenergetiki Na Nadezhnost' Funktsionirovaniya EES. Aktual'nye Problemy Energetiki: Materialy Studencheskoy Nauch.-tekhn. Konf. Minsk: BNTU, 2018: 564—567. (in Russian).

32. **Wenyuan Li.** Risk Assessment of Power Systems: Models, Methods, and Applications. N.-Y.: Wiley-IEEE Press, 2014

33. **Mesenzhnik Ya.Z., Prut L.Ya., Gorbunov S.I.** Otsenka Tekhnicheskikh Riskov Pogruzhnykh Elektrotsentrobezhnykh Neftenasosov pri Perekhode k Vneshnemu Servisnomu Obsluzhivaniyu. Elektro. 2008;6 (20): 38—41. (in Russian).

34. **Gorbunov S.I.** Razvitie Teorii i Metodov Otsenki Riskov dlya Obespecheniya Promyshlennoy Bezopasnosti Ob′ektov Neftegazovogo Kompleksa: Avtoref. Dis. … Dokt. Tekhn. Ufa: In-t Problem Transporta Energoresursov, 2006. (in Russian).

35. **Kuipers D.** Cybersecurity for Energy Delivery Systems [Elektron. Resurs] www.sans.org/cyber-security-summit/archives/file/summit-archive-1493741208.pdf (Data Obrashcheniya 14.12.2018).

36. **Bergman D.C., Jin D., Nicol D.M., Yardley T.** The Virtual Power System Testbed and Inter-Testbed Integration. Proc. USENIX Conf. Cyber Security Experimentation and Test. Berkeley, 2009.

Сведения об авторах:

Гвоздев Дмитрий Борисович — кандидат технических наук, доцент кафедры электроэнергетических систем НИУ «МЭИ», e-mail: GvozdevDB@mpei.ru
Архангельский Олег Денисович — аспирант кафедры электроэнергетических систем НИУ «МЭИ», e-mail: ArkhangelskyOD@mpei.ru

Information about authors:

Gvozdev Dmitriy B. — Ph.D. (Techn.), Assistant Professor of Power Electrical Systems Dept., NRU MPEI, e-mail: GvozdevDB@mpei.ru
Arkhangelsky Oleg D. — Ph.D.-student of Power Electrical Systems Dept., NRU MPEI, e-mail: ArkhangelskyOD@mpei.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов
Conflict of interests: the authors declare no conflict of interest

Статья поступила в редакцию: *04.05.2017*
The article received to the editor: *04.05.2017*