УДК 685.1

Е.В. Брежнев, В.С. Харченко

Национальный аэрокосмический университет имени М.Е. Жуковского "ХАИ", Харьков

МЕТОД ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ С УЧЕТОМ НАДЕЖНОСТИ ЦИФРОВОЙ ПОДСТАНЦИИ

Критическая энергетическая инфраструктура (КЭИ) является сложной иерархической киберфизической мегасистемой, состоящей из объектов энергогенерации (АЭС, ГЭС, ТЭС, пр.) и электросистемы (подстанций, линий передач, пр.). Безопасность АЭС является главной составляющей инфраструктурной безопасности. Смарт грид являются новым поколением КЭИ, в которой АЭС является неотъемлемой частью энергогенерации. Цифровая подстанция является интерфейсом между смарт грид и АЭС. Ее надежность является одним из основных факторов безопасности АЭС и КЭИ в целом. Работоспособность подстанции определяется надежностью и информационной безопасностью ее критических активов. В статье предложен подход к учету надежности цифровой подстанции при оценке инфраструктурной безопасности с использованием байесовской сети доверия и метода анализа дерева отказов. Проанализированы основные компоненты подстанции, отказы которых приводят к ее неработоспособности. Рассмотрен иллюстративный пример применения подхода.

Ключевые слова: *критическая энергетическая инфраструктура, смарт грид, цифровая подстанция, надежность, байесовские сети доверия, метод дерева отказов.*

Введение

Постановка проблемы и анализ литературы.Критическая энергетическая инфраструктура (КЭИ) [1]является сложной иерархической киберфизической мегасистемой, обеспечивающей энергетическую безопасность любого государства, благополучие его граждан. Она включает объекты генерации электричества (АЭС, ГРЭС, ТЭС), объекты альтернативной энергетики, линии передачи электроэнергии (ЛЭП), распределенную сеть подстанций, пр. Безопасность КЭИ определяется отсутствием недопустимых рисков, связанных с функционированием объектов энергетики, отказы и аварии которых приводит к наиболее тяжёлым последствиям.

Анализ инфраструктурных аварий показывает, что аварии на объектах генерации электричества, приводят к крупным техногенным катастрофам, гибели людей, загрязнению окружающей среды. Безопасность КЭИ определяется прежде всего безопаснымфункционированием АЭСв виду высокой тяжести последствий их аварий для общества и окружающей среды. Крупные техногенные катастрофы происходят и с другими объектами КЭИ. Так, например, ущерб от аварии на Саяно-Шушенской ГРЭС, произошедшей в 2009 году, превысил 7,338 млрд рублей.

Всоответствиис[2] безопасное функционирование АЭС определяется надежностью электросети, которая непосредственно обеспечивает внешнее энергоснабжение станции. Полная или частичная потеря внешнего энергоснабжения может привести к серьезным авариям и сбоям в работе станции. Для АЭС определяющим фактором безопасности является надежность оборудования трансформаторной подстанции, посредством которой обеспечивается внешнее электроснабжение, а также надежность линий электропередач, пр.

Безопасная эксплуатация АЭС выдвигает большие требования к качеству параметров электрической сети. Так, например, для нормальной работы всех систем безопасности реактора АЭС частота тока должна быть в пределах +3% и – 5%;напряжение в пределах +/ – 5%.Любые отклонения от этих параметров могут привести к остановке реактора АЭС. Так, например, в сентябре 2011 г., в Сан Диего, США, в результате отказа оборудования подстанции произошла аварийная остановка реактора АЭС в Сан Клименте, Калифорния.

В настоящее время активно развивается новое поколение КЭИ – smartgrid (смарт грид, адаптивно-активные сети, интеллектуальные сети)[3]. Под смарт грид понимается система передачи и распределения электрической энергии, которая сочетает в себе элементы обычной энергетики и новейшие энергетические технологии, комплексные инструменты контроля и мониторинга, а также информационные технологии (ИТ) и средства коммуникации, обеспечивающие более высокую производительность энергосети. Несмотря на повышение безотказностикомпонентой базысмарт грид, проблемы обеспечения ее надежности остаются актуальными. Это обусловлено прежде всего:

1) растущими требованиями энергетического рынка, обуславливающими функционирование электросети на грани ее предельных возможностей по току, напряжению, частоте, пр.;

2) возрастающими потребностями в электричестве, стремлению стейкхолдеров энергокомпаний к получению максимальной прибыли; это приводит к

принятию технически необоснованных решений, например, попередаче электричества на большие расстояния, что ведет к росту нагрузки на оборудование этих сетей, и как следствие, к его износу;

3) использованием современных ИТдля повышения возможностей контроля за состоянием сети; однако, с одной стороны,ИТ повышают возможности по контролю за состоянием и самоадаптации, а с другой, – увеличиваюттребования к надежности оборудования;

4) высокой динамикой системы, что приводит к необходимости принятия качественных решений в режиме реального времени;

5) высокой географической распределенностью активов энергосистемы;6) интеграциейальтернативных источников в энергосистему, что вносит дополнительные риски в возможность поддержания ее стабильной работы и качества параметров сети, пр.

Анализ основных подходов к оценке надежности энергосистем. В настоящее время существует множество подходов к оценке влияния надежности энергосистемы на безопасность АЭС [4, 5]. Эти подходы к оценке надежности основаны на использовании моделирования методом Монте Карло для вычисления показателей надежности энергосистем.

Для оценки надежности также используется теория деградирующих систем [6, 7], как систем в которых при определенных условиях, по мере накопления отказов компонент, вызванных естественными (старение) или искусственными (внешнее воздействие) причинами, допускается деградация функций системы, когда выполнение части из них становится невозможным, или о деградации качества (точности, производительности и др.), когда ухудшаются основные его показатели.

Для оценки надежности подстанций используются вероятностные методы, имитационные модели [6, 7]. Эти методы и модели являются трудозатратными, требующими поддержки вычислительных средств и разработки специализированного ПО.

Кроме того, используются специализированные программные средства тестирования для оценки влияния отказов оборудования на надежность подстанции у целом, например, IEEEReliabilityTestSystem (IEEE-RTS) [8] или Roy Billinton TestSystem (RBTS) [9].Также применяются аналитические упрощенные модели оценки надежности подстанций [10].

В настоящее время одной из проблем обеспечения инфраструктурной безопасности является адекватное моделирование инфраструктур, учет влияния надежности систем и компонентов современной электрической сети на безопасность инфраструктуры. Для оценки безопасности КЭИ используются Марковские сети, сети Петри, Байесовские сети доверия (БСД). Отличие БСД от вышеназванных методов состоит в их способности проводить многофакторный анализ безопасности КЭИ, включая фактор надежности систем электрической сети.

Цель статьи – разработка подхода к оценке влияния надежности компонентов цифровой подстанции на безопасностьКЭИ с использованием БСД.

Показатели надежности КЭИ и подстанции

В соответствии с [10] под надежностью КЭИ понимается комплексное свойство, определяющее ее способность осуществлять электроснабжение потребителей путем выполнения функций по производству, передаче и распределению электрической энергии нормированного (требуемого) качества при едином технологическом взаимодействии генерирующих установок, электрических сетей и электроустановок потребителей, удовлетворять в любой момент времени спрос на мощность и электроэнергию (адекватность, балансовая составляющая системной надежности), противостоять возмущениям, вызванным отказами отдельных элементов энергосистемы (безопасность, оперативная составляющая системной надежности).

КЭИ состоит из генерирующих станций и электросистемы (рис. 1). Основной функцией электросистемы является передачи и распределение электроэнергии от генерирующих станций к потребителю.

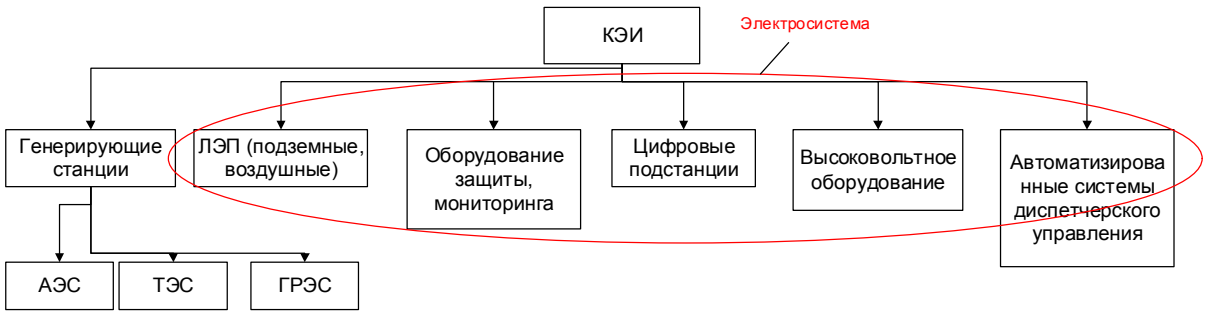

Рис. 1. Общая схема критической энергетической инфраструктуры

Основными компонентами электросистемы, надежность которых определяет безопасность АЭС, являются подвесные и подземные ЛЭП; цифровые подстанции; высоковольтное оборудование; автоматы защиты, системы мониторинга; системы связи и управления, пр.

Все показатели надежности КЭИ можно представить в виде групп частных и интегральных показателей. К основным интегральным показателям надежности относят:

– средний индекс длительности прерываний (SAIDI) в работе КЭИ. Этот индекс используется для измерения суммарной длительности прерывания для усредненного потребителя энергии за данный период времени. В качестве временного интервала используется месячный или годовой период. Этот показатель определяется по соотношению вида

$$\mathrm{SAIDI} = \sum r_i N_i \big/ N_T ,$$

где r_i – время восстановления системы после сбоя, мин; N_i – общее число потребителей, которые потеряли энергоснабжение; N_T – общее число потребителей;

– средняя величина эксплуатационной готовности (ASAI) определяется как отношение фактического времени наличия энергоснабжения к общему времени. Эта величина определяется как:

$$\mathrm{ASAI} = [1 - (\sum (r_i \cdot N_i) / (N_T \cdot T))] \cdot 100,$$

где T – общий период времени, ч; r_i – времявосстановления, ч; N_i - число потребителей без энергоснабжения; N_T – общее число потребителей.

Существуют также такие интегральные показатели как: суммарное время простоя оборудования, отключения энергопринимающих установок потребителей, недоотпуски электроэнергии, пр.

Цифровая подстанция является одним из важных активов электросистемы, обеспечивающим прием, преобразование и распределение электрической энергии. Фактически, она является интерфейсом между АЭС и электросистемой, расположенной в непосредственной близости к станции. Цифровая подстанция содержит комплекс цифровых устройств (терминалов) для решения задач релейной защиты и автоматики и АСУ ТП - регистрации аварийных событий, учёта и контроля качества электроэнергии, телемеханики. Все оборудование станции общается между собой и центральным сервером объекта по последовательным каналам связи на единых протоколах.

Частные показатели используются для оценки надежности цифровой подстанции. Для подстанции выделяют следующие частные показатели надежности: вероятность отказа оборудования подстанции, среднее время наработки на отказ, интенсивность отказа, время восстановления, коэффициент оперативной готовности, пр.

В рамках данного подхода в качестве показателя надежности цифровой подстанции предлагается использовать коэффициент оперативной готовности. Под коэффициентом оперативной готовности понимается вероятность того, что цифровая подстанция окажется работоспособной (обеспечит электроснабжение для АЭС) в произвольный момент времени и с этого момента будет работать безотказно в течение заданного промежутка времени. Предполагается, что рассматривается установившийся процесс эксплуатации, математической моделью которого является стационарный случайный процесс.

Оценка безопасности КЭИ с учетом параметров надежности подстанции

Для оценки влияния показателей надежности цифровой подстанции на безопасность КЭИ предлагается использовать метод, основанный на комбинированном использовании Байесовской сети доверия (БСД) и метода анализа деревьев отказов (МАДО).

БСД представляет собой полное описание рассматриваемой проблемной области. Каждый элемент в полном совместном распределении вероятностей может быть получен на основе информации, представленной в этой сети. Универсальным элементом в совместном распределении является вероятность конъюнкции конкретных присваиваний значений каждой переменной, такой как

$$P(X_1 = x_1 \wedge .... X_n = x_n).$$

БСД может быть представлено как

$$P(x_1, ..., x_n) = \prod_{i=1}^{n} P(x_1 / \mathrm{parents}(x_i)) ,$$

где $\mathrm{parents}(x_i)$ означает конкретные значения переменных в множестве вершин Parents (x_i). Поэтому каждый элемент в совместном распределении представлен в виде произведения соответствующих элементов в таблицах условных вероятностей БСД.

При построении БСД очень важно правильно задать априорные вероятности состояний узлов родителей. Для этого предлагается использовать метод анализа дерева отказов.

Метод анализа деревьев отказов интенсивно используется в различных отраслях, например, машиностроении, с целью выявления способов уменьшения рисков или определения частоты системного отказа. Предлагаемый метод учета надежности цифровой подстанции при оценке безопасности КЭИ с использованием комбинации БСД и МАДО включает следующие этапы:

- определение и структуризация всех активов подстанции;

- определение критичности (вероятность и тяжесть последствий) отказов всех активов подстанции;

- ранжирование активов подстанции по критичности влияния на работоспособностьцифровой подстанции. На этом этапе выявляются наиболее критичные активы, отказы которых приводят к потере готовности цифровой подстанции;

- построение БСД, включающей узел (узлы), учитывающий надежность цифровой подстанции в виде коэффициента готовности, а именно, вероятности нахождения подстанции в работоспособном состоянии. Параметры этого узла получают на основе МАДО с учетом критичности активов.

Пример оценки безопасности КЭИ

В качестве примера применения метода рассмотрен фрагмент БСД для оценки безопасности реактора АЭС с учетом состояния источников внешнего и внутреннего энергоснабжения (рис. 2).

В качестве основных узлов рассматриваются:узел состояния реактора (reactorstateunit), узлы учета состояния двух систем безопасности (RCIC, RPS), узлы учета состояния внешнего и внутреннего энергоснабжения (Off_site_power_state, On_site_power_state), узлы состояний трех цифровых подстанции (smart_substation_(1-3)), узлы для дизель-генератора (DG) и аккумуляторной батареи (DC_batteries). Данная БСД была построена с использованием инструментального средства Netica 512.

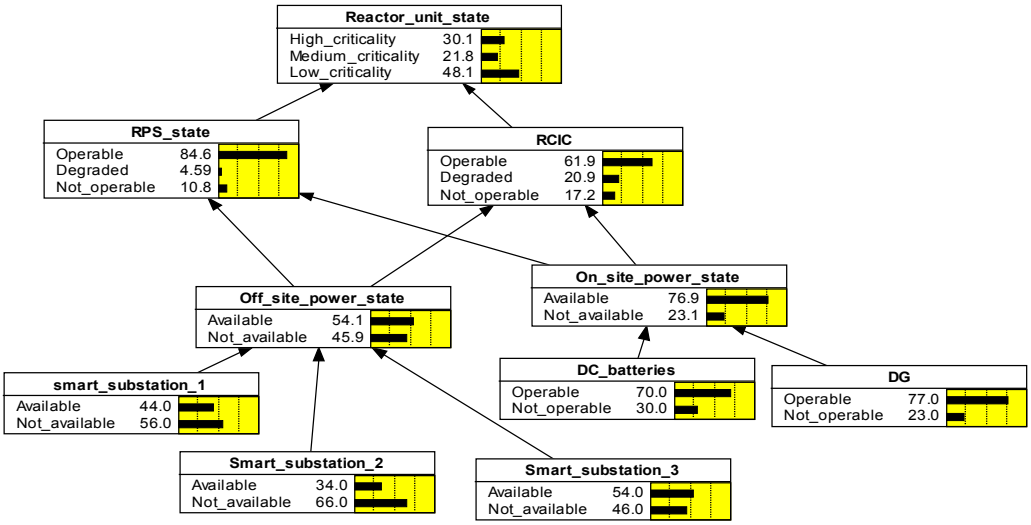

Рис. 2. Фрагмент БСД для оценки безопасности АЭС
с учетом работоспособности цифровых подстанций и внутреннего энергоснабжения

К основным причинам потери нагрузки (работоспособности)цифровой подстанции можно отнести:

- отказы полевого оборудования, датчиков сбора дискретной информации и передачи команд управления на удаленные коммутационные устройства (RTU);

- отказы датчиков для сбора аналоговой информации (цифровые трансформаторы тока и напряжения).

- отказы устройств управления и мониторинга (контроллеры присоединения, многофункциональные измерительные приборы, счетчики АСКУЭ, системы мониторинга трансформаторного оборудования и т.д.).

- выход из строя серверов верхнего уровня (сервер базы данных, сервер SCADA, сервер телемеханики, сервер сбора и передачи технологической информации и т.д., концентратор данных), пр.

В рамках примера, после ранжирования наиболее критичным активом определенRemote Terminal Unit (RTU). RTUпредставляет собой удаленное оконечное устройство, которое выполняет важные функции в обеспечении работоспособности цифровой подстанции. Устройство подключено к окончанию канала связи с центральным устройством системы.

Его отказы могут приводить к потере нагрузки (работоспособности) цифровой подстанции. В свою очередь, это событие приводит к потере одной из линий, обеспечивающей снабжение всех систем безопасности АЭС.

В качестве основных причин потери работоспособности RTU, могут быть: отказы терминалов ввода/вывода, отказы ПО, электропитания.

ОтказыRTU могут быть классифицированы первичные, вторичные. Причиной первичного отказа RTUявляются непосредственно его компоненты и элементы, т.е. он сам. Вторичныеотказы RTUобусловлены различного рода входными воздействиями (сигналами), лежащими вне диапазона, предусмотренного технической спецификацией на RTU. Эти внешние воздействия вызываются соседними элементами и окружающей средой, а также ошибочными действиями персонала подстанции. Вторичные отказы могут возникать вследствие успешных кибератак, проведенных опытным злоумышленником на уязвимости RTU.

Дерево отказов для события – потеря эксплуатационной готовности подстанции, построенное в рамках иллюстративного примера, приведено на рис.3.

Коэффициент оперативной готовности подстанции определен на основе метода анализа деревьев отказов. Расчеты показателей надежности подстанции были проведены с использованием средства Cafta 6.0 a.

Построение БСД и ее интеграция с методом анализа деревьев отказов приведена на рис. 4.

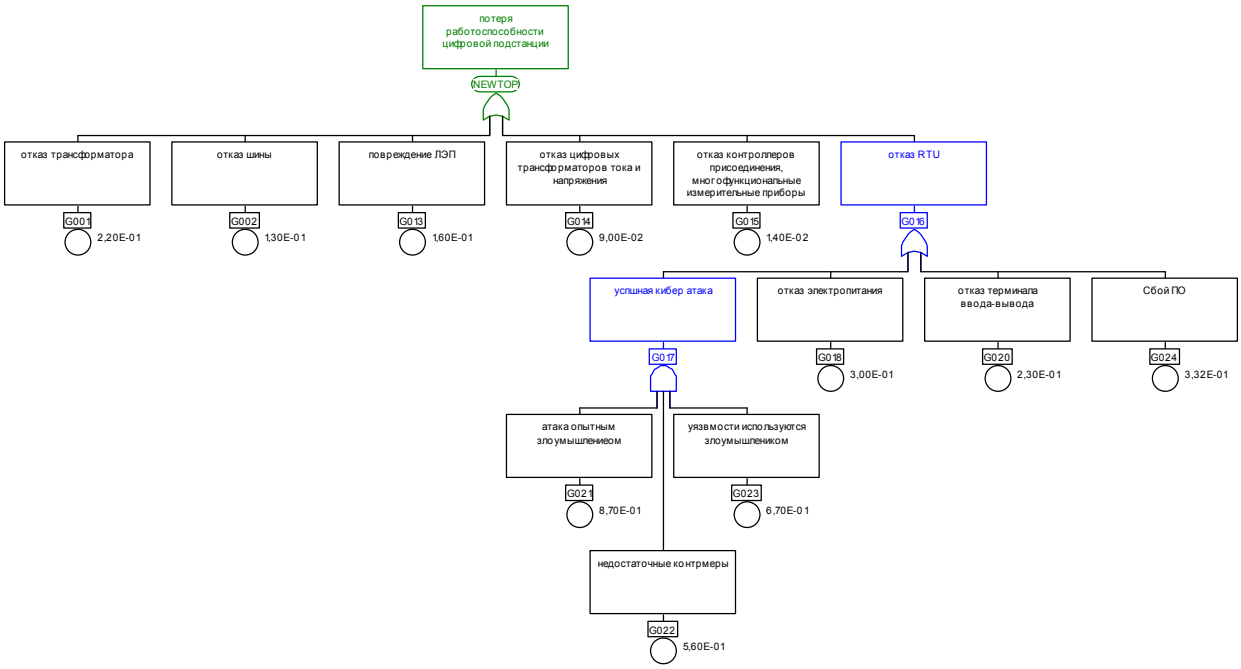

Рис. 3. Дерево отказов для RTU, построенное в рамках иллюстративного примера

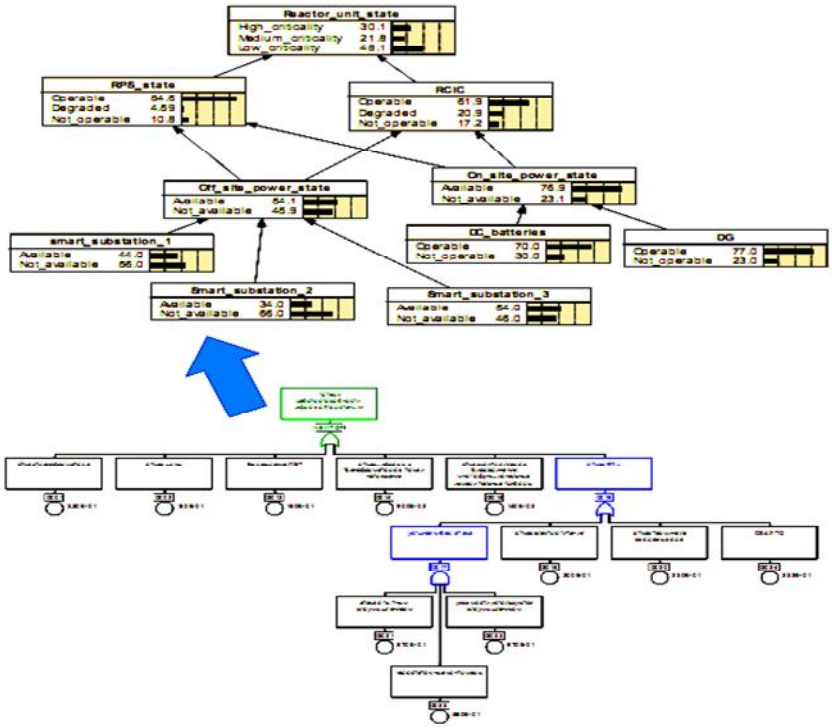

Рис. 4. Интеграция методов анализа деревьев отказов и БСД

Следует также отметить, что при совместном использовании БСД и МАДО могут возникнуть два случая:

- для оценки безопасности КЭИ используется комбинация лингвистической БСД и классического(вероятностного) метода анализа дерева отказов. В лингвистической БСД все параметры сети, включая условные вероятности, представлены в виде лингвистических переменных;

- для оценки безопасности КЭИ используется комбинация классической (вероятностной) БСД и метода анализа дерева отказов, в которой вероятности базовых событий могут частично или полностью быть представлены в виде лингвистических переменных. Нечеткое расширение метода анализа деревьев отказов применяется в случае наличия недостаточной статистики отказов, позволяющей определить параметры надежности сложной системы.

Для обоих случаев возникает вопрос интеграции входных и выходных данных двух методов. В качестве решения могут быть предложены существующие методы фазификации и дефазификации. Причем, оба

метода могут быть использованы в обоих случаях. Так, например, фазификация позволяет провести интеграцию вероятности в лингвистическую БСД. Теоритически возможно провести и дефазификацию лингвистической БСД. Однако эта задача может потребовать затрат ресурсов. Для второго случая можно использовать фазификацию классической БСД, что также является затратным процессом. Наиболее удобным подходом в этом случае является дефазификация выходных величин, полученных с использованием нечеткого метода анализа деревьев отказов.

Выводы

Смарт грид является новым поколением КЭИ, в которой АЭС является неотъемлемой частью энергогенерации. В этом случае можно говорить о КЭИ как о *киберфизической инфраструктуре*.Появление смарт грид приводит к появлению новых рисков для безопасности КЭИ и АЭС, в частности, рисков информационной безопасностии сложных отказов ее компонент. Подход к учету влияния надежности цифровых подстанций на безопасность КЭИможет быть основан на комбинированном применении БСД и МАДО. МАДО используется для получения показателей надежности подстанции с учетом вероятностей отказов наиболее критичных активов. Возможны два случая интеграции методов, для которых предложены варианты реализации.

Интеграция методов позволит получить обоснованные оценки вероятностей состояний цифровых подстанций, которые в дальнейшем интегрируются в БСД для получения оценок безопасности реактора АЭС.

Список литературы

1. Харченко В.С. Безопасность информационно-управляющих систем и инфраструктур. Модели, методы и технологии / В.С. Харченко, В.В. Скляр, Е.В. Брежнев. – Palmarium academic publishing, ФРГ, 2013. – 529 с.

2. IAEA Nuclear Energy Series No. NG-T-3.8

3. Janaka Ekanayake, etc. Smart grid technology and applications, A John Wiley & Sons, Ltd., Publication, 2012. – 293 p.

4. Billinton R., Allan R. N., Reliability Evaluation of Power Systems (2nd Edition). New York: Plenum, 2006.

5. Billinton R., BagenI., Generating capacity adequacy evaluation of small stand-alone power systems containing solar energy. Reliability Engineering & System Safety, 91(4), 2010. – P.438-443.

6. Billinton, R., Allan, R. N. Reliability Evaluation of Power Systems. Plenum Press, New York, 1996. – 534 p.

7. Meeuwsen, J. J., Kling, W. L. Substation reliability evaluation including switching actions with redundant components // IEEE Transactions on Power Delivery. 1997. Vol. 12, No. 4. – P. 1472 - 1479.

8. IEEE Committee Report. IEEE reliability test system // IEEE Transactions on Power Apparatus and Systems. 1979. Vol. PAS-98, No. 6. – P. 2047 -2054.

9. Billinton, R., Kumar, S., Chowdhury, N., Chu, K., Khan, E., Kos, P., Nourbakhsh, G., Oteng-Adjei, J. A reliability test system for educational purposes ñ Basic results // IEEE Transactions on Power Systems. 1990. Vol. 5, No. 1. – P. 319-325.

10. P. RAESAAR Simplified assessing of substation-originated outages in analysis of transmission system reliability/ Oil Shale, 2007, Estonian Academy Publishers,Vol. 24, No. 2, Special ISSN 0208-189X. – P. 308–317.

Надійшла до редколегії 28.08.2014

Рецензент: д-р техн. наук проф. Ю.В. Стасев, Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков.

МЕТОД ОЦІНЮВАННЯ БЕЗПЕКИ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ НАДІЙНОСТИ ЦИФРОВОЇ ПІДСТАНЦІЇ

Є.В. Брежнев, В.С. Харченко

Критична енергетична інфраструктура (КЕІ) є складною ієрархічною кіберфізичною мегасистемою, що складається із об'єктів енергогенерації (АЕС, ГЕС, ТЕС, пр.) та електросистеми. Безпека АЕС є головною складовою інфраструктурної безпеки. Смарт грид (адаптивно-активні мережі) є новим поколінням КЕІ, в якій АЕС являє собою невід'ємну складову енергогенерації. Цифрова підстанція є інтерфейсом між смарт грид та АЕС. Її надійність є одним із головних чинників безпеки АЕС та інфраструктури в цілому. Працездатність підстанції визначається надійністю та інформаційною безпекою її критичних активів. В статті пропонується підхід до урахування надійності цифрової підстанції при оцінюванні інфраструктурної безпеки з використанням байєсівської мережі довіри та метода аналізу дерев відмов. Проаналізовано основні компоненти підстанції відмови яких можуть призвести до втрати її працездатності. Розглянуто приклад застосування підходу.

Ключові слова: *критична енергетична інфраструктура, смарт грід, цифрова підстанція, надійність, байєсівські мережі довіри, метод дерева відмов.*

CRITICAL ENERGY INFRASTRUCTURE SAFETY ASSESSMENT WITH CONSIDERATION OF DIGITAL SUBSTATION RELIABILITY

E.V. Brezhnev, V.S. Kharchenko

Critical energy infrastructure (CEI) is complex hierarchical cyber physical system that consists of power generation systems (sush as NPP, HPP, etc.) and power grid. NPP safety is important and inherent part of infrastructure safety. Smart grid is a new generation of CEI, where NPP is one of main power suppliers. Smart substation is interface between smart grid (its electrical network) and NPP. Substation reliability is an important factor for NPP and infrastructure safety as well. The substation operability is determined by its components' reliability and cyber security. This paper suggests approach for consideration of substation reliability during infrastructure safety assessment based on joint application of Bayesian Belief Network and Fault Tree Analysis. The most critical substation assets that are important for substation operability are considered. The example of approach application is considered in the paper.

Keywords: *critical energy infrastructure, smart grid, digital substation, the reliability, the Bayesian network of trust, fault tree method.*