УДК 685.1

Е.В. Брежнев

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

РАЗРАБОТКА ПОДХОДА К ОЦЕНКЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ С УЧЕТОМ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

К инфраструктурным авариям с тяжелыми последствиями приводят комбинации маловероятных событий, например, отказов программных и аппаратных средств, аномальных природных явлений, ошибок оператора. Человеческий фактор оказывает двойственное влияние на инфраструктурную безопасность. Существует множество подходов к оценке надежности оператора. Для получения достоверных оценок инфраструктурной безопасности необходимо проводить многофакторный анализ. В качестве основы многофакторного анализа предложено использовать байесовские сети доверия (БСД). Предложены два подхода для интеграции вероятностных оценок, представленных в различных квалиметрических шкалах. Рассмотрен пример применения БСД для оценки безопасности с учетом человеческого фактора на примере аварии на АЭС Фукусима-1.

***Ключевые слова**: человеческий фактор, критическая энергетическая инфраструктура, безопасность, байесовская сеть доверия, киберфизические системы.*

Введение

Постановка проблемы и анализ литературы. Критические энергетические инфраструктуры (КЭИ) являются основой жизнедеятельности любого государства. Под КЭИ понимается совокупность объектов энергетики аварии, сбои в работе которых могут привести к негативным последствиям для общества и всех зависимых инфраструктур. КЭИ включает в себя объекты электрогенерации (атомные и тепловые станции, объекты альтернативной энергетики, и пр.), линии передачи электроэнергии, распределенную сеть цифровых подстанций, а также информационно-управляющие системы (ИУС) для контроля и управления технологическими процессами.

Повышение надежности программных и аппаратных средств объектов КЭИ и ИУС, внедрение информационных технологий (ИТ) приводит к повышению их эффективности за счет скоординированного управления и двусторонних коммуникаций между элементами сети, подстанциями и потребителями. Внедрение новых ИТ положительно влияет на способность КЭИ к самовосстановлению после сбоев в подаче электроэнергии; повышает возможность активного участия потребителей в работе сети, а также ее устойчивость к физическому и кибернетическому вмешательству злоумышленников, и пр.

Вместе с тем, КЭИ и ИУС являются сложными кибер физическими системами, в которых влияние человеческого фактора на показатели их надежности и безопасности является определяющим на любом уровне их иерархии. Человеческий фактор остается одним из главных факторов безопасности КЭИ и ИУС, одним из основных причин аварий и сбоев в их работе.

Под аварией КЭИ (блэкаут, системная авария) понимается нарушение нормального режима всей или значительной ее части, связанное с повреждением оборудования, временным недопустимым ухудшением качества электрической энергии или перерывом в электроснабжении потребителей. На рис. 1 приведено распределение основных причин крупных аварий КЭИ. Так, например, около 8 процентов причин крупных аварий, произошедших в период с 1984 по 2011 гг. были связаны с ошибками диспетчерского персонала энергосистем.

Рис. 1. Основные причины крупных аварий КЭИ

На рис. 2 приведено распределение основных причин сбоев в работе ИУС АЭС. Так, около 11% нарушений работы ИУС АЭС также связаны с ошибками человека при проведении ремонтных работ и технического обслуживания (ТО) [1].

Вышеприведенная статистика подтверждает необходимость учета влияния человеческого фактора на безопасность КЭИ и ИУС.

В настоящее время существует множество подходов к оценке надежности оператора систем, важных для безопасности. Основную группу методов составляют методы HRA (human reliability assessment), используемые для оценки надежности оператора ИУС АЭС. Авария на АЭС Три-Майл-Айленд (Three Mile Island accident), произошедшая 28.03.79 г., обусловила дальнейший скачок в развитии методов оценки влияния человеческого фактора на безопасность АЭС.

Рис. 2. Распределение основных причин сбоев в работе ИУС АЭС

Исторически сложилось, что оценке надежности оператора ИУС АЭС уделялось больше внимания, чем надежности диспетчера энергосистем, что обусловлено прежде всего различной тяжестью последствий аварий. Специфической особенностью учета человеческого фактора в КЭИ является необходимость оценки взаимного влияния действий диспетчера энергосистемы на безопасность и оператора ИУС АЭС на надежность КЭИ. В настоящее время, появление адаптивно-активных сетей (smart grid), интеллектуализация энергосистем, не снижает актуальности проблемы влияния человеческого фактора на безопасность и надёжность КЭИ.

Существуют качественные и количественные методы HRA. Качественные методы, например, Human Factor Process FMEA [1] и Human error HAZOP [2] ориентированы на выявление неблагоприятных событий на АЭС и оценке влияния на них действий оператора. Качественные методы не предусматривают определение вероятностей ошибок оператора (Human Error Probability (HEP)) и поэтому не могут быть интегрированы в рамках единого подхода к многофакторной оценке инфраструктурной безопасности.

Количественные методы HRA могут быть классифицированы с учетом: уровней принятой в модели детализации; учета когнитивных процессов; фактора времени; контекстуальных факторов и типов используемых входных данных. К основным количественным методам относят Technique for Human Error Rate and Prediction (THERP) [4], Technique for Human Event Analysis (ATHENA) [5]), Human Cognitive reliability HCR [6], и пр. При определении HEP эти методы учитывают действие внешних и внутренних факторов (performance shaping factors, PSFs). К основным внутренним факторам относят: индивидуальные особенности человека, уровень подготовки, устойчивость к стрессам, навыки, физическое состояние и пр. Внешние факторы связаны с объектом управления, условиями работы и т.д.

Оценки HEP интегрируются в рамках Probabilistic Reliability Assessment (PRA) с использованием, например, деревьев отказов (FTA). Вместе с тем, FTA не может быть использовано для комплексного анализа безопасности инфраструктур в виду большого числа систем и числа (типов) связей между ними. Это приводит к увеличению временных затрат, к снижению точности результатов. Кроме того, множество состояний систем в FTA ограничено двумя (работоспособное и неработоспособное).

Существует ряд альтернативных подходов к оценке надежности оператора, основанных на математическом моделировании сложных систем. Так, например, в работе [7] для оценки надежности оператора ИУС АЭС (human failure event) используются БСД. В работе предлагается интегрировать факторы, влияющие на ошибки оператора (Performance Influencing Factor) с использованием сети. Входные данные получены из Human Events Repository Analysis (HERA). В работе не указано на возможность и способы интеграции результатов с другими подходами с целью многофакторного анализа безопасности. В работе [8] байесовская сеть рассматривается для получения вероятностных оценок расплавления активной зоны реактора с учетом времени задержки по его аварийному останову. Вместе с тем факторы (PSFs), влияющие на время задержки, в подходе не учитываются.

Проведенный анализ подходов к оценке надежности оператора показывает отсутствие единой таксономии в классификации его ошибок. Различные методы оперируют с различными видами ошибок. Отсутствие единой классификации связано с особенностями областей анализа, с различием применяемых подходов. Поскольку анализ человеческого фактора на безопасность является сложной проблемой, для ее решения необходима интеграция различных подходов и входных данных в рамках единого подхода к оценке инфраструктурной безопасности.

Таким образом, можно сформулировать проблему, связанную с необходимостью учета человеческого фактора при анализе безопасности КЭИ, с одной стороны, и отсутствием подходов, направленных на комплексную оценку инфраструктурной безопасности с учетом человеческого фактора.

Цель статьи – разработка подхода к оценке безопасности КЭИ с учетом влияния человеческого фактора.

Основной материал

Анализ крупных инфраструктурных аварий позволил выделить ряд основных особенностей, связанных с человеческим фактором.

1. *Двойственность (негативное и позитивное) влияния человеческого фактора на безопасность КЭИ.* Негативное влияние оператора проявляется в совершении ошибок, которые влияют (или усугубляют) аварийную ситуацию в КЭИ. Качество и своевременность решений непосредственно влияют на безопасность КЭИ. Так, например, в ходе развития аварийной ситуации на АЭС Фукусима-1, работники второго энергоблока по неосторожности допустили

ряд ошибок (не была замечена остановка насоса, подававшего морскую воду в реактор, ошибке был перекрыт клапан, через который из контейнера реактора должен был высвобождаться пар, пр.)

Негативное влияние человеческого фактора на уровне менеджмента компании ТЕРСО в целом Позитивное, как и негативное влияние человеческого фактора на безопасность проявляется на всем жизненном цикле КЭИ.

2. Многоуровневое влияние человеческого фактора на безопасность КЭИ.

Влияние человеческого фактора существует на всех уровнях иерархии инфраструктуры. Оператор индивидуально и в составе команды влияет на технологические процессы и объекты, важные для безопасности. Менеджмент компании-собственника влияет на безопасность инфраструктуры в целом, посредством политик и процессов управления активами (информационными и физическими).

Примером негативного многоуровневого влияния человеческого фактора на безопасность является авария на нефтяной платформе Deepwater Horizon, произошедшая 20 апреля 2010 года. Маловероятная комбинация многих факторов, а также негативное влияние человеческого фактора привело к авариям с тяжелыми последствиями.

Основными причинами аварии на платформе явились: многочисленные ошибки оператора на этапе развития аварийной ситуации; игнорирование персоналом процедур ТО систем (включая системы безопасности); игнорирование требований и руководств безопасности. Персонал отключил системы сигнализации и оповещения; отсутствовало согласованное взаимодействие внутри смены платформы; игнорирование процедур риск анализа на уровне организации; технические отказы систем мониторинга состояния герметичности скважины; недостаточная подготовка персонала; непонимание руководством компании BP отличий между индивидуальной и системной безопасностью. Основные особенности влияния человеческого фактора на инфраструктурную безопасность приведены в табл. 1.

Таблица 1

Основные особенности влияния человеческого фактора на инфраструктурную безопасность

Особенность человеческого фактора для КЭИ	КЭИ	
	АЭС (ИУС)	Энергогрид (линии, подстанции, SCADA)
Степень влияния на безопасность	Высокая - на функциональную безопасность ИУС Высокая - на безопасность АЭС Важная (но менее высокая) на ИБ	Высокая на ФБ и ИБ
Иерархичность влияния (на различных уровнях системы):	Влияние человеческого фактора существует на всех уровня иерархии АЭС	Влияние человеческого фактора существует на всех уровня иерархии энергосистемы
Влияние человека оператора	Да	Да
Влияние смены (команды)	Да	Да
Влияние организации	Да	Да
Двойственность влияния (позитив и негатив)	Да	Да
Методы HRA	Умышленные и неумышленные ошибки, их комбинации	

Разработка подхода к оценке безопасности КЭИ с учетом человеческого фактора.

В настоящее время БСД широко используется для анализа безопасности и надежности сложных систем. В БСД, вероятности пребывания системы S_3 в различных состояниях из множества Ω_{S3} в зависимости от состояний вершин родителей могут быть определены по соотношению вида:

$$P(S_3^{(k)}) = \sum_i \sum_j P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)}) \cdot P(S_1^{(i)}) \cdot P(S_2^{(j)}), \quad (1)$$

где $P(S_3^{(k)})$ - вероятность нахождения системы S_3 в k-м состоянии; $P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)})$ - условная вероятность нахождения системы S_3 в k-м состоянии при условии нахождения системы S_1 в i-м состоянии и системы S_2 в j – м состоянии; $P(S_1^{(i)})$ - вероятность нахождения системы S_1 в i-м состоянии; $P(S_2^{(j)})$ - вероятность нахождения системы S_2 в j-м состоянии.

Для получения достоверных оценок безопасности КЭИ необходимо учитывать множество факторов безопасности. Факторы безопасности представляются в различных квалиметрических шкалах, имеют различную природу и достоверность, пр. Входные вероятностные оценки для БСД могут быть получены на основе имеющихся статистических данных, в результате анализа опыта эксплуатации КЭИ, статистики отказов, аварийных ситуаций, пр.

Для оценивания безопасности КЭИ целесообразно использовать все имеющиеся данные, в том числе субъективные оценки экспертов, операторов систем, менеджеров и т.д Концепция использования субъективных вероятностей, в том числе представленных в виде выражений естественного языка, лежит в основе построения БСД. Это приводит к тому, что часть входных данных (таблицы условных вероятностей, вероятности исходных состояний узлов) могут быть представлены виде лингвистических переменных (ЛП). Возникает задача приведения всех входных данных к единой шкале, например, к абсолютной, с целью моделирования с использованием инструментальных средств.

Анализ аварии на АЭС Фукусима-1 с использованием предложенного подхода. В рамках иллю-

стративного примера по комплексной оценке безопасности КЭИ с учетом человеческого фактора рассматривается авария на АЭС Фукусима-1, произошедшая 11 марта вблизи северо-восточного побережья Японии. Землетрясение с магнитудой 9 баллов вызвало разрушение внешней энергосистемы, что привело к длительному обесточиванию АЭС. Подача электрической энергии, необходимой для работы системы аварийного отвода остаточных тепловыделений активной зоны реакторов была обеспечена с помощью подключения аварийных дизель-генераторов. Цунами затопила машинные залы, где располагались аварийные генераторы, коммутаторы, доставлявшие электричество от генераторов к системам охлаждения, были также залиты в машинных залах. Защитная стена (для волны 6.5 м) не смогла защитить станцию (высота волны оценивалась в 15 метров).

Таким образом, цепочка, приведшая к аварии, состояла из комбинации маловероятных событий, обусловленных внутренними (связанными с проектными ошибками самой станции) и внешними факторами, связанными с возникновением неблагоприятных природных катаклизмов в районе площадки. Фрагмент БСД, описывающий причинно-следственные связи между основными системами АЭС и неблагоприятными внешними факторами, приведен на рис. 3.

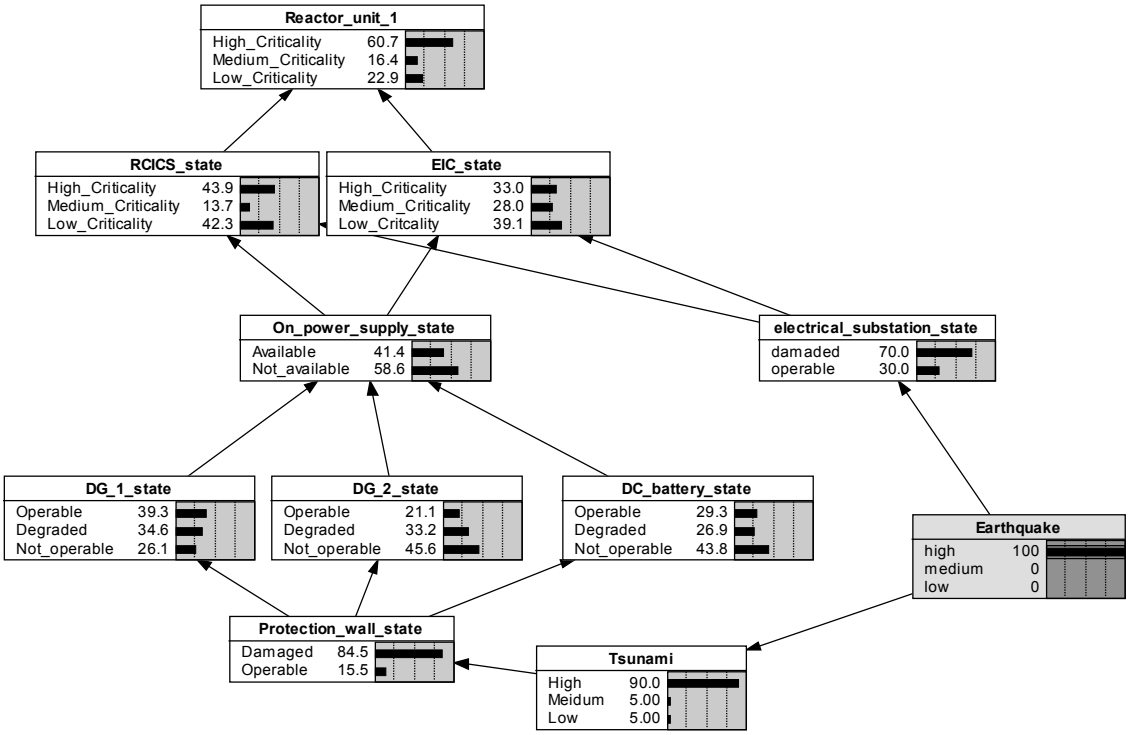

Рис. 3. Фрагмент БСД, описывающий причинно-следственные связи между основными системами АЭС и внешними факторами

Построение и оценка параметров сети проводилась с использованием Netica 5.12. В этом случае БСД описывает изменения состояний основных систем безопасности (RCICS, EIC) и реактора (RU1), внутреннего энергоснабжения (on_Power_Supply, включая дизель генераторы (DG_1(2), батареи (DC_battery), а также внешних факторов - цунами (Tsun) и землетрясения (Eartquake), защитной стены (Protection_Wall), электроподстанции (Electr_Substat). БСД не учитывает влияние человеческого фактора.

Формализовано эта сеть представлена ниже в виде совместного распределения вероятностей:

$$P(\text{Eartquake}, \text{El\_subst}, \text{Tsun}, \text{Prot\_wall}, \text{DG\_1}, \text{DG\_2}, \text{DC\_bat}, \text{On\_power\_supply}, \text{RCICS}, \text{EIC}, \text{RU1}, \text{Electr\_Substat}) = P(\text{Eartquake}) \cdot P(\text{El\_subst} / \text{Earthquake}) \cdot P(\text{Tsun} / \text{Earthquake}) \cdot P(\text{Prot\_wall} / \text{Tsun}) \cdot P(\text{DG\_1} / \text{Protection\_Wall}) \cdot P(\text{DG\_2} / \text{Prot\_Wall}) \cdot P(\text{DC\_battery} / \text{Prot\_Wall}) \cdot P(\text{On\_Power\_supply} / \text{DG\_1}, \text{DG\_2}, \text{DC\_3}) \cdot P(\text{RCICS} / \text{On\_power\_supply}) \cdot P(\text{EIC} / \text{On\_power\_supply}) \cdot P(\text{RU1} / \text{RCICS}, \text{EIC}).$$

Анализ апостериорных вероятностей состояний всех узлов сети показывает, что при возникновении цунами, соответствующей состоянию High, вероятность нахождения реактора в предельном состоянии (High Criticality) становится равной 0,607.

Анализ аварии показал, что своевременное применение операторами АЭС процедур, предписанных инструкциями, могло бы снизить риски расплавления активной зоны и загрязнения окружающей территории. Вместе с тем, общепризнанной ошибкой операторов TEPCO, является несвоевременность в применении процедуры (emergency cooling procedures) для 1 и 3

Фрагмент БСД, в которой учтены все факторы безопасности, включая человеческий фактор, приведен на рис. 4. Формализовано эта сеть представлена ниже в виде совместного распределения вероятностей:

$$P(Eartquake, Electr\_subst, Tsun, Protection\_wall, DG\_1, DG\_2, DC\_battery,$$
$$On\_power\_supply, RCICS, EIC, RU1, Electr\_Substat, Delay\_to\_pump\_sea\_water,$$
$$Operator\_mor\_state, Operator\_Compt, Operator\_Fitness) =$$
$$= P(Eartquake) \bullet P(Electr\_subst / Earthquake) \bullet P(Tsun / Earthquake) \bullet$$
$$P(Protection\_wall / Tsun) \bullet P(DG\_1 / Protection\_Wall) \bullet$$
$$P(DG\_2 / Protection\_Wall) \bullet P(DC\_battery / Protection\_Wall) \bullet$$
$$P(On\_Power\_supply / DG\_1, DG\_2, DC\_3) \bullet P(RCICS / On\_power\_supply) \bullet$$
$$P(EIC / On\_power\_supply) \bullet P(RU1 / RCICS, EIC, Delay\_to\_pump\_sea\_water) \bullet$$
$$P(Operator\_moral\_state / Earthquake) \bullet$$
$$P(Delay\_to\_pump\_sea\_water / Operator\_mor\_st, Operator\_Compt, Operator\_Fitness).$$

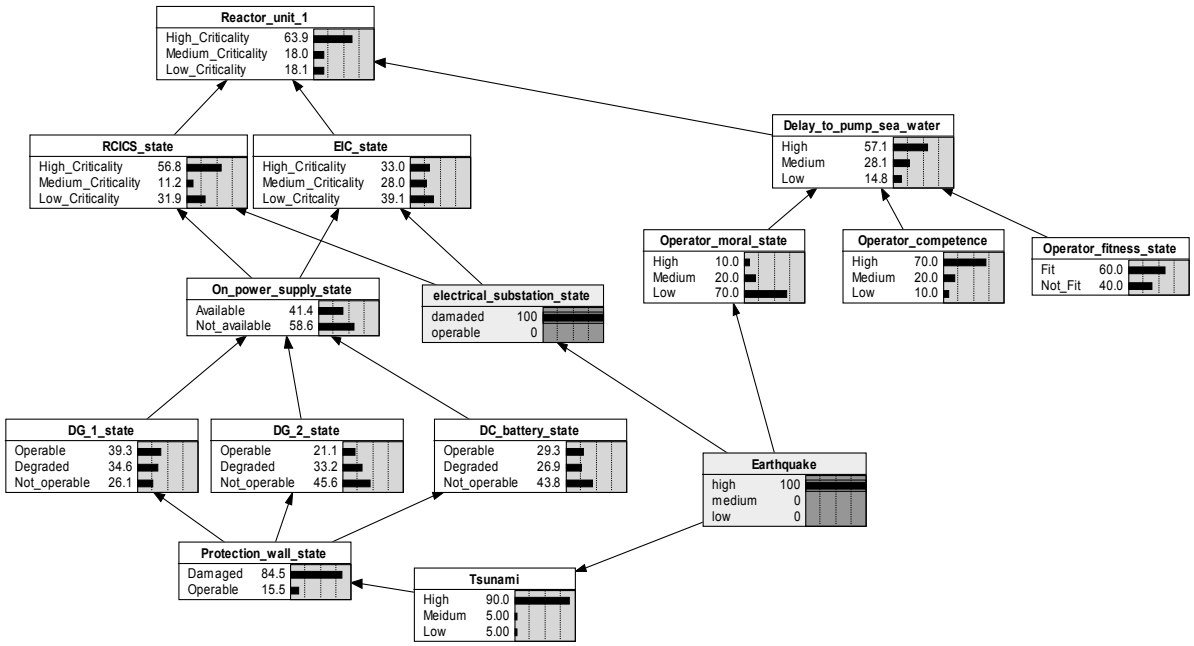

Рис. 4. Фрагмент БСД, в которой учтены все факторы безопасности, включая человеческий фактор

Анализ апостериорных вероятностей состояний всех узлов сети показывает, что при возникновении цунами, соответствующей состоянию High, вероятность нахождения реактора в предельном состоянии увеличивается к 0,639. Таким образом, моральное состояние операторов привело к задержке в подкачке морской воды для охлаждения активной зоны и повышению рисков для реактора.

Особенностью многофакторного анализа безопасности инфраструктур с использованием БСД является представление таблицы условных вероятностей (ТУВ), а также априорных маргинальных вероятностей в различных квалиметрических шкалах. Вместе с тем часть информации об PIFs, доступной для описания влияния человеческого фактора на безопасность, может быть доступна в виде экспертных оценок, представленных в виде выражений естественного языка, которые в свою очередь могут быть формализованы в виде ЛП. В соответствии с [9], ЛП представляет собой кортеж вида:

$$<в, T, X, G, M>,$$

где в - наименование ЛП; T - базовое терм-множество ЛП; X - область определения (универсум) нечетких переменных, которые входят в определение ЛП в; G - синтаксическая процедура, которая описывает процесс образования из множества T новых значений для данной ЛП; M - семантическая процедура, которая позволяет поставить в соответствие каждому новому значению данной ЛП, получаемому с помощью процедуры G, некоторое осмысленное содержание посредством формирования соответствующего нечеткого множества. Важно отметить, что одной из задач многофакторного анализа инфраструктурной безопасности является обработка вероятностей, представленных в различных квалиметрических шкалах. Задача может быть решена с использованием двух подходов. Первый подход связан с проведением фаззификации всех вероятностных метрик сети, второй с дефазификацией все переменных, представленных в виде ЛП. Выбор подхода обусловлен трудозатратами на выполнение каждой из задач. С учетом того,

что при анализе безопасности инфраструктур число узлов может быть очень велико, при выборе подхода может быть использован критерий вида:

$$k_1 \{<, >, \approx\} k_2 = \begin{cases} \text{fuzzific., if } k_2 < k_1; \\ \text{defuzzufic., if } k_2 > k_1; \\ \text{fuzzific. or defuzzufic., if } k_2 \approx k_1, \end{cases}$$

где коэффициент k_1 есть удельное число узлов $n_{linguist}$, ТУВ которых описаны с помощью ЛП, и определяемое как отношение $n_{linguist}$ к общему числу узлов БСД, $k_1 = n_{linguist}/N$.

Аналогично, коэффициент k_2 есть удельное число узлов $n_{probabl}$, ТУВ которых описаны с помощью числовых значений вероятностей, определяемое как отношение $n_{linguist}$ к общему числу узлов БСД, $k_2 = n_{probabl}/N$.

После проведения фаззификации (деффаззификации) все входные данные могут быть обработаны в рамках единой сети, построенной для многофакторного анализа безопасности КЭИ.

Выводы

Таким образом, проведенный анализ позволяет сделать следующие выводы.

1. Человеческий фактор является основным риск фактором при оценке безопасности КЭИ и ИУС. Его влияние происходит не только на протяжении всего жизненного цикла, но и на всех уровнях иерархии, т.е. можно говорить о иерархичности влияния человека на безопасность.

2. Методы анализа надежности человека наиболее развиты для атомной энергетики. Для энергосистем методы оценивания надежности диспетчера адаптируют из атомной энергетики.

3. Для получения достоверных оценок безопасности КЭИ необходимо учитывать множество факторов, одним из которых является надежность оператора. При интеграции множества факторов в рамках одного подхода возникает задача обработки входных данных, представленных в различных квалиметрических шкалах. В работе предложены правила интеграции и критерий их выбора.

Список литературы

1. *Доклад ГНТЦ. SSTS NRC / www.sstc.kiev.ua.*
2. *Nancy G. Levenson Safeware: System safety and computers/ University of Washington. Addison – Wesley Publishing Company, 1995. – 679 p.*
3. *Madonna M. The human factor in risk assessment: methodological comparison between human reliability analysis technique / M. Madonna, G. Martella // Prevention Today. – Vol.5, ½. – P. 67-83.*
4. *Pekka P. Human reliability analysis methods for probabilistic safety assessment / P. Pekka. – Technical research centre of Finland, 2000. – 67 p.*
5. *Swain, A.D., "THERP", SC-R-64-1338, Sandia National Laboratories, Albuquerque, NM, August 1964.*
6. *US Nuclear Regulatory Commission (USNRC). Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). NUREG-1624. Division of Risk Analysis and Applications. Office of Nuclear Regulatory Research, Washington DC. May 2000.*
7. *Development and Use of Bayesian network to estimate Human Error Probability, K.Groth, etc. ANS PSA Int.l topical meeting on probabilistic safety assessment and analysis, 2011.*
8. *D .Marquez, etc., Improved reliability modeling using Bayesian Network and Dynamic Discretization, Reliability Engineering and System safety, 92, p. 412-425, 2010.*
9. *Заде Л. Нечеткая логика: Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – М. : Мир, 1976. – 167 с.*

Поступила в редколлегию 13.03.2014

Рецензент: д-р техн. наук проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

РОЗРОБКА ПІДХОДУ ДО ОЦІНЮВАННЯ БЕЗПЕКИ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ВПЛИВУ ЛЮДСЬКОГО ЧИНИКУ

Є.В. Брежнєв

До інфраструктурних аварій з важкими наслідками можуть привести комбінації множини мало ймовірних подій, таких як відмови програмних та апаратних засобів, виникнення незручних природних чинників, помилок оператора. Людський чинник має двоякий вплив на безпеку інфраструктури. Існує багато підходів щодо оцінки надійності оператора. Для отримання достовірних оцінок інфраструктурної безпеки необхідно проводити багатофакторний аналіз. В якості моделі багатофакторної оцінки безпеки запропоновано використовувати байесовські мережі довіри (БМД). Розглянуто приклад застосування БМД з урахуванням людського чинника на прикладі аварії на АЕС Фукусіма-1. Запропоновано два підходи щодо інтеграції ймовірнісних оцінок, які представлені в різних кваліметричних шкалах.

***Ключові слова**: людський чинник, критична енергетична інфраструктура, безпека, байєсовська мережа довіри, кіберфізичні системи.*

THE DEVELOPMENT OF APPROACH TO CRITICAL ENERGY INFRASTRUCTURE SAFETY ASSESSMENT TAKING INTO ACCOUNT HUMAN FACTOR INFLUENCE

Ye.V. Bregnev

The combination of set of remote probability events such as hardware and software failures, natural disasters, human mistakes lead to the infrastructure accidents with severe consequences. Human factor has a dual influence (positive and negative) on infrastructure safety. There is a set of approaches to human reliability assessment. The multifactorial assessment is needed to obtain the valid value of infrastructure safety estimate. This assessment shall incorporate the human factor. Bayesian Belief Network is suggested as a basis for multifactorial safety assessment. The example of BBN application for safety assessment considering the human factor is considered for Fukushima accident. Two approaches to integration of probabilistic estimates presented in different qualimetric scales are given in the paper.

***Keywords**: human factor, critical power infrastructure, safety, Bayesian network of trust, cyber physicals systems.*