УДК 519.873

Е.В. Брежнев

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

ПОДХОД К МНОГОФАКТОРНОЙ ОЦЕНКЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ ДОВЕРИЯ

В статье предлагается подход к многофакторной оценке безопасности критических инфраструктур (КИ) в условиях неопределенности, основанный на использовании динамических байесовских сетей доверия (ДБСД). Применение ДБСД позволяет учесть динамику развития неблагоприятных событий, изменение состояний систем в КИ, а также их взаимовлияние между собой. ДБСД рассматривается в качестве основы многофакторного анализа безопасности, которая позволяет учесть множество внешних и внутренних факторов, влияющих на их безопасность КИ, независимо от их природы. Применение подхода позволит повысить достоверность оценок безопасности и обосновать комплекс мер по снижению рисков техногенных катастроф в КИ, а также расширить рамки вероятностного анализа рисков за счет учета субъективных вероятностей. В качестве примера показано использование ДБСД для анализа аварии на АЭС Фукусима-1.

***Ключевые слова**: критическая инфраструктура, многофакторный анализ безопасности, динамическая БСД.*

Введение

Планомерное развитие любого общества полностью определяется надежным и безопасным функционированием критических инфраструктур (КИ) [1]. Энергосистема является одной из наиболее важных КИ, обуславливающей развитие всех связанных с ней инфраструктур и систем. Энергосистема представляет совокупность электрических станций, электрических сетей и потребителей электроэнергии, характеризующихся общностью режима функционирования и единым управлением этим режимом. В общем виде энергосистема, как система из систем может быть представлена в виде совокупности программных средств (ПС), аппаратных средств (АС) и человека (на различных уровнях – оператор, организация, топ менеджент) в контуре управления этой системой.

Атомные электростанции (АЭС) являются интегральными составляющими электрической генерации, обеспечивающими производство экологически чистой энергетической продукции. АЭС получают электрическую энергию, обеспечивающую питание систем безопасности (СБ), от внешнего источника питания (offsite power), и собственных резервных источников (onsite power, дизель – генераторов и аккумуляторов). Безопасное функционирование АЭС выдвигает высокие требования к надежности энергосистемы (далее энергозоны), расположенной поблизости с АЭС. Любые риски и неблагоприятные события в энергозоне, например, сбои, отказы оборудования могут привести к колебаниям частоты, напряжения и тока, или к полной потере электричества, что в свою очередь обуславливает возникновение риск-событий для АЭС, например, автоматическое выключение реактора АЭС, переключение на другую силовую линию, включение дизель-генераторов (ДГ), и др.

Таким образом, любое неплановое изменение режима нормальной эксплуатации энергозоны может привести к появлению дополнительных рисков для АЭС поскольку:

– восстановление энергосистемы может занять время, превышающее время работы внутренних источников энергоснабжения. Потеря электроснабжения для систем контрольно-измерительных приборов и автоматики, приборов технологического контроля реактора и систем его управления и защиты, систем памяти и логики информационно-вычислительной машины блока, систем дозиметрии, и пр., может привести к потере контроля над критичностью реактора, и как результат, к аварии на АЭС;

– ненадежность ДГ (около 1 % отказов ДГ при включении), а также маловероятные комбинации событий – потеря внешнего энергоснабжения – отказы ДГ, длительный процесс восстановления энергосистемы – все это в совокупности может привести к аварии на АЭС с высокими последствиями.

Множество событий, например, сверхтоки, падение (флуктуации) напряжения, могут привести к изменению состояния АЭС (остановка реактора, включение резервных ДГ, и пр.). Вместе с тем, потеря внешнего энергоснабжения АЭС при одновременном аварийном отключении всех автономных систем ее энергоснабжения, может привести к аварии с катастрофическими последствиями для населения и окружающей среды.

На рис. 1 показаны виды основных сбоев в работе энергосистемы и возможные изменения состояния АЭС, связанные с ними.

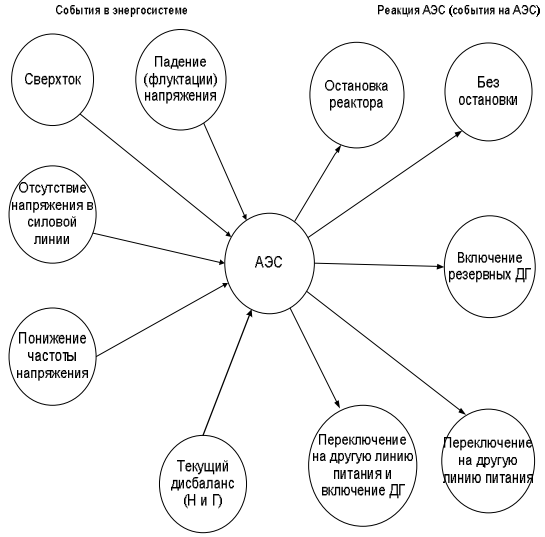

Рис. 1. Виды основных сбоев в работе энергосистемы и возможные изменения состояния АЭС, связанные с ними

В свою очередь, неплановая остановка АЭС может привести к дальнейшему падению напряжения, нарушению стабильности в энергозоне, что при неплановом увеличении нагрузки, может привести к полному “падению” энергосистемы и наступлению blackouts.

Анализ аварий в энергосистемах [2] показывает, что риски в энергозоне обусловлены: техническими отказами оборудования; недостаточной пропускной способность сетей, в том числе магистральных; ошибками в проектировании ПС и АС; природными катаклизмами (ураганные ветры, повышенное обмерзание проводов, катастрофические наводнения и т. п.); человеческим фактором (халатностью персонала); ошибками менеджмента (при формировании политики развития энергокомпаний и стратегий управления энергосистемой); политикой региональных властей в сфере энергоснабжения и пр.

Для интеллектуальных сетей (smart grid), концепция которых была разработана в 80 – 90 гг., причинами потери стабильности могут быть не только отказы оборудования и ошибки персонала и менеджмента, но и дефекты ПС, управляющих работой цифровых подстанций, устройствами связи с технологическими объектами (например, RTU), интеллектуальными устройствами (IDE). Следует отметить, что повышение управляемости и мониторинга *smart grid* обусловлено использованием большого объема данных, поэтому вопросы обеспечения информационной безопасности, снижение уязвимостей компонентов становятся актуальными для энергосистем нового поколения.

С учетом анализа аварий на АЭС, связанных с потерей внешнего энергоснабжения следует также отметить, что необходимым атрибутом этого анализа должна стать внешняя система S_{env}, как совокупность природных явлений с учетом их влияния на безопасность станции, так и другие системы в КИ, состояние которых обуславливает возможность оперативного проведения восстановительных мероприятий на АЭС.

Одним из извлеченных уроков аварии на АЭС Фукусима-1 является необходимость учета рисков, связанных с маловероятной возможностью аварий со значительными последствиями, которые могут привести к повреждению реактора. Это означает, что необходимо учитывать не только все маловероятные события с катастрофическими последствиями, но их комбинации, возникновение которых может привести к наступлению запроектной аварии на АЭС и радиоактивное загрязнение за ее пределами. Кроме того, необходимо учитывать множество всех внутренних и внешних факторов, влияние которых на КИ происходит на протяжении всего ее жизненного цикла (ЖЦ).

На рис. 2 показаны основные внешние и внутренние факторы, определяющие безопасность КИ. К основным внутренним факторам можно отнести:

надежность ПС и АС,

человеческий фактор на различных уровнях КИ от оператора,

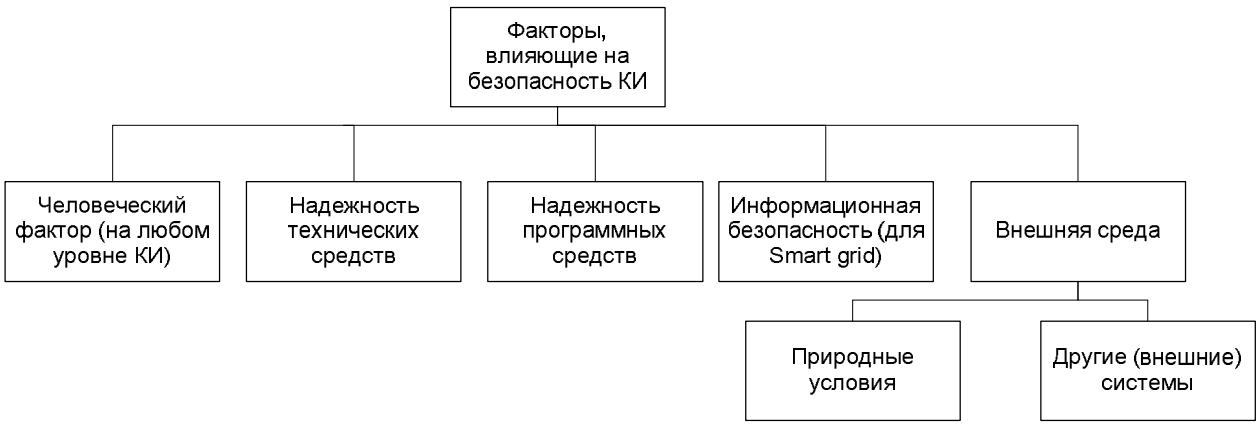

Рис. 2. Основные факторы, влияющие на безопасность КИ

качество подготовки которого является определяющим при возникновении аварии, заканчивая топменеджментом, действия которого определяют культуру безопасности, процедуры и политики компании, эксплуатирующей КИ,

влияние внешних природных факторов (природные катаклизмы),

влияние систем в рамках КИ.Таким образом, эффективное, безопасное и надежное функционирование АЭС требует, чтобы энергосистема, обеспечивающая ее работу, также была эффективной, надежной и безопасной. Это приводит к необходимости учета динамического взаимовлияния состояний элементов энергосистем и реактора АЭС. С учетом сложной природы и типов взаимовлияния между системами в рамках КИ данная задача не является тривиальной.

В этой связи, для снижения рисков энергосистемы для АЭС необходимо разработать подход, позволяющий оценивать безопасность АЭС в зависимости от событий, возникающих в энергосистеме, а также влияние множества неблагоприятных внутренних и внешних факторов. Кроме того, подход должен учитывать влияние человеческого фактора, ошибки менеджмента, и пр.

Цель статьи – разработка подхода к многофакторной оценке безопасности КИ в условиях неопределенности с целью повышения достоверности этих оценок и выработки адекватных мероприятий по снижению рисков возникновения событий с высокой тяжестью последствий.

Раздел основного материала

Традиционно байесовские сети доверия (БСД) [3] применяются для анализа безопасности сложных систем.

Вместе с тем, классические (статические) байесовские сети доверия не позволяют моделировать динамические объекты.

Динамика является основной особенностью КИ. Динамические БСД, напротив, позволяют моделировать любую нелинейную проблему (феномен), а также позволяют осуществлять факторизацию, что приводит к повышению вычислительной эффективности сети при снижении числа параметров анализа безопасности, при котором точность оценивания не снижается.

Развитие аварии на АЭС Фукусима-1 может быть представлено с помощью ДБСД. Динамика развития событий, факты, доступные для анализа, позволяют представить хронологию аварии в виде трех временных интервалов: фиксация подземных толчков – до цунами (интервал T_1); полная потеря энергоснабжения – после цунами (интервал T_2); полное обесточивание станции – взрывы водорода (интервал T_3).

В общем случае, для анализа аварии ДБСД должны быть построены для каждого энергоблока (1 – 3) отдельно.

В качестве примера, на рис. 3 показана ДБСД развития аварии, построенная для двух интервалов T_1 и T_2.

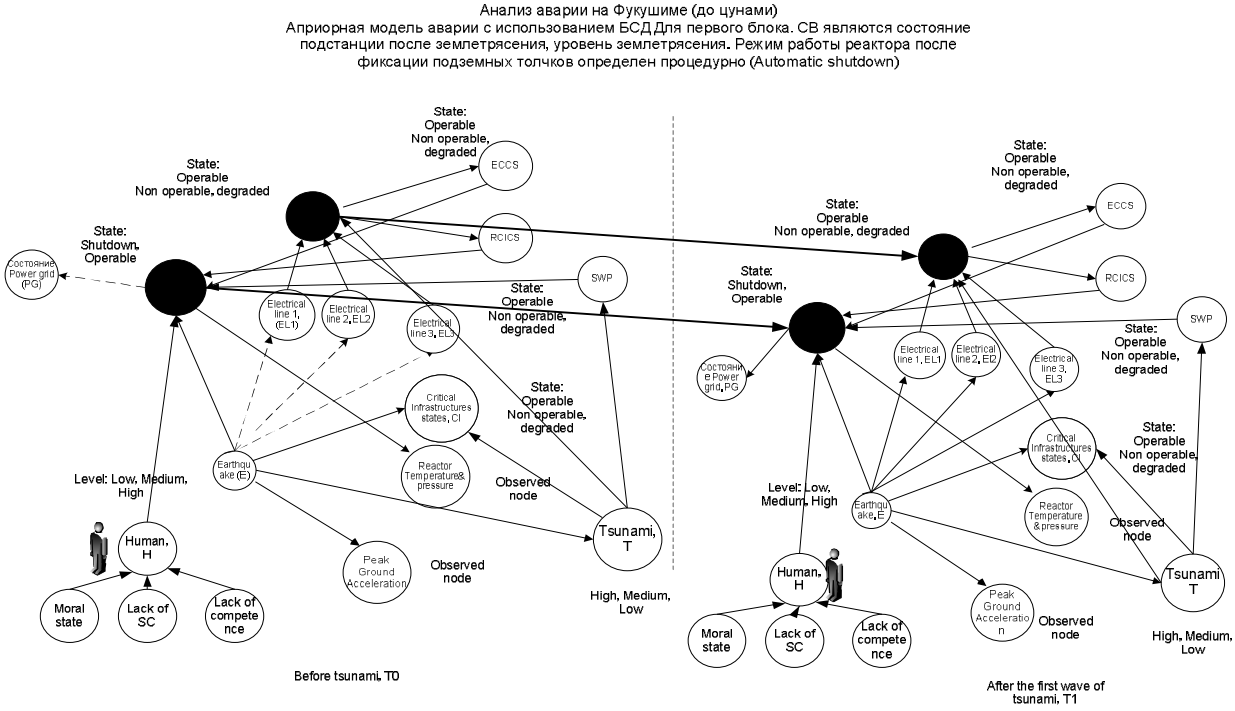

Рис. 3. Динамическая БСД развития аварии, построенная для двух интервалов T1 и T2

ДСБД включает различные узлы, которые, вместе с соответствующими связями, описывают влияние множества факторов безопасности, приведенных на рис. 2. Так, ДСБД содержит узлы, описывающие влияние действий человека оператора, состояние подстанции, самого реактора, СБ, и пр. Таким образом, в рамках ДБСД проводится интеграция множества факторов безопасности, определяющих состояния систем в КИ, причем текущее состояние систем обусловлено не только влиянием множества факторов в данный момент T_1, а также состоянием самой системы в момент времени T_0.

Следует отметить, что, традиционно, построение ДБСД основано на знаниях и опыте эксперта [3]. Между тем, построение ДБСД, описывающей аварию на АЭС Фукусима-1, может быть проведено с использованием двух множеств узлов (т.н. "технических" и "исторических"). Первое множество узлов и причинно-следственные связи между ними описывают процедурно-технологические события, протекающие на АЭС и в энергосистеме согласно принятым процедурам, алгоритмам и правилам. Так, например, автоматическая остановка реактора при появлении признаков землетрясения происходит в соответствии с принятыми процедурами обеспечения безопасности и является частью технологического процесса АЭС. Другое множество узлов и связи между ними обусловлены наличием исторической (статистической) информации, связанной с объектом анализа. Так, например, при анализе рисков цунами вблизи Фукусимы-1 не учитывалась возможность появления гигантского цунами. Тем не менее, узел, характеризующий появление цунами должен быть включен в ДБСД аварии поскольку существуют исторические данные о 16 случаях цунами в течение последних 500 лет в районе Японии и Курильских островов с высотой волны, превышавшей 10 м.

Для полноты анализа безопасности "исторический" узел – влияние оператора на состояние реактора – также может быть включен в ДБСД, поскольку в ядерной энергетике процент аварий по вине персонала достаточно велик. Так, например, в 80е годы он составлял в США 21%, в Японии 19% от общего числа аварий.

Плотность совместного распределения всех переменных (факторов безопасности), описанных ДБСД, приведенной на рис. 3, представлена ниже:

$$\begin{aligned}
&P(PG,E,R1^{1:T},EL_1,EL_2,EL_3,CI,RPT^{1:T},PGA^{1:T},PES^{1:T},T,H,SWP,MS,LSC,LC,PG) = \\
&= P(E)\times P(EL_1/E)\times P(SWP/T)\times P(EL_2/E)\times P(EL_3/E)\times P(CI/E,T)\times P(RTP/R1)\times \\
&\times P(PGA/E)\times P(PG/R1)\times P(RCICS/PES)\times P(ECCS/PES)\times P(T/E)\times P(H/MS,LSC,LC)\times \\
&\times P(MS)\times P(LSC)\times P(LC)\times P(PG/R1)\times \prod_{j=2}^{N} P(R1^{(j)}/E,RCICS,ECCS,SWP,H,R1^{(j-1)})\times \\
&\times P(PES^{j}/PES^{(j-1)},EL_1,EL_2,EL_3,T)\times \prod_{j=2}^{K} P(RTP^{(i,j)}/R1^{(j)})\times P(PGA^{(i,j)}/E^{(i)}).
\end{aligned}$$

Одним из основных свойств динамических байесовских сетей доверия является возможность факторизации плотности совместного распределения через плотности условного распределения одних величин, входящих в выражение, и маргинальную плотность других величин.

Так, вероятность нахождения реактора ($R1^{(j,k)}$) в k-м возможном состоянии в j-м временном интервале в зависимости от состояний СБ (узлов-родителей) ECCS, RCICS, уровня землетрясения E, подготовки оператора H в текущем (j-м) интервале и m-го состояния узла R1 в предыдущем (j-1) временном интервале может быть определена по соотношению вида:

$$\begin{aligned}
&P(R1^{(j,k)}) = \sum_{R1^{j-1},ECCS,RCICS,E} P(R1^{(j,k)}/R1^{(j-1,m)},ECCS^{(j,w)},RCICS^{(j,t)},E^{(j,h)},H^{(j,d)})\times \\
&\times P(ECCS^{(j,w)})\times P(RCICS^{(j,t)})\times P(E^{(j,h)})\times\times P(R1^{(j-1,m)})\times P(H^{(j,d)}),
\end{aligned}$$

где $P(R1^{(j,k)})$ – вероятность нахождения реактора в k-м состоянии в j-м временном интервале; $P(R1^{(j,k)}/R1^{(j-1,m)},ECCS^{(i)},RCICS^{(j)},E^{(h)})$ – условная вероятность нахождения реактора R1 в k-м состоянии в j-м временном интервале при условии нахождения системы ECCS в i – м состоянии и системы RCICS в j – м состоянии, системы E в h-м состоянии, с учетом m-го состояния реактора в предыдущем j-1 временном интервале; $P(ECCS^{(j,w)})$ – вероятность нахождения системы ECCS в w-м состоянии в j-м временном интервале.

Величина $P(ECCS^{(j,w)})$ может быть найдена по соотношению вида:

$$P(ECCS) = \sum_{ECCS,PES} P(ECCS/PES)\times P(PES),$$

где $P(ECCS/PES)$ – условная вероятность зависимости состояния системы ECCS от состояния аварийного энергоснабжения (PES); P(PES) – вероят-

ность нахождения системы аварийного энергоснабжения в одном из возможных состояний; $P(RCICS^{(j,t)})$ – вероятность нахождения СБ RCICS в t-м состоянии в j-м временном интервале, определяется аналогично, как для системы ECCS; $P(E^{(j,h)})$ – вероятность нахождения системы E в h–м состоянии в j-м временном интервале; $P(H^{(j,d)})$ – вероятность ошибки оператора H в j-м интервале.

Эта величина определяется по соотношению вида:

$$P(H) = \sum_{ECCS,PES} P(H/MS,LSC,LC) \times P(MS) \times P(LSC) \times P(LC),$$

где $P(H/MS,LSC,LC)$ – условная вероятность ошибки оператора в зависимости от его морального состояния (MS), уровня культуры безопасности (LSC), уровня его профессиональных знаний (LC).

Следует также отметить, что ДБСД может использовать субъективные вероятности в качестве параметров и исходных данных. Эти оценки могут быть в дальнейшем уточнены при накоплении достаточного объема статистических данных.

Выводы

Таким образом, ДБСД позволяет провести многофакторный анализ безопасности КИ, а также учесть множество факторов, влияющих на ее безопасность. В рамках рассматриваемого примера по многофакторному анализу безопасности для аварии на АЭС Фукусима-1, ДБСД позволяет учесть: влияние состояний аварийного энергоснабжения на состояния СБ реактора, посредством введения условных вероятностей; влияние внешней среды (природы) на состояние реактора, посредством введения условных вероятностей между величиной цунами и состоянием аварийного энергоснабжения, а также насосов забора морской воды (SWP). Кроме того, учитывается влияние внешней среды на состояние КИ в районе расположения АЭС и влияние величины землетрясения на состояния линий электроснабжения станции; влияние действий человека – оператора на состояние реактора, определяется своевременностью принятия решений важных с точки зрения безопасности реактора.

Список литературы

1. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / Под ред. Харченко В.С. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2011. – 641 с.

2. Харченко В.С. Безопасность информационно-управляющих систем и инфраструктур. Модели, методы и технологии / В.С. Харченко, В.В. Скляр, Е.В. Брежнев. – Германия: Palmarium Academic Publishing, 2013. – 528 с.

3. Brezhnev E.V. BBN-based Approach For Assessment of Smart Grid And Nuclear Power Plant Interaction / E.V. Brezhnev, V.S. Kharchenko // IEEE East-West Design & Test Symposium 2012, Kharkov, Ukraine, September 14-17, 2012.

Поступила в редколлегию 6.08.2013

Рецензент: д-р техн. наук проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ПІДХІД ДО БАГАТОФАКТОРНІЙ ОЦІНЦІ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ІЗ ЗАСТОСУВАННЯМ ДИНАМІЧНИХ БАЙЕСОВСЬКИХ МЕРЕЖ ДОВІРИ

Е.В. Брежнев

В статті пропонується підхід до багатофакторній оцінці безпеки критичних інфраструктур, що ґрунтується на застосуванні динамічних байесовських мереж довіри (ДБСД). Застосування ДБСД дозволяє врахувати динаміку розвитку несприятливих подій, зміни станів систем в КІ, а також взаємний вплив меж ними. Динамічні БСД розглядаються в якості основи багатофакторного аналізу безпеки, яка дозволяє врахувати множину внутрішніх та зовнішніх факторів, які впливають на безпеку КІ, незалежно від їх природи. Застосування підходу дозволяє підвищити достовірність оцінок безпеки та обґрунтувати комплекс заходів щодо зниження ризиків техногенних катастроф в КІ, а також збільшити межі імовірнісного аналізу ризиків за рахунок врахування суб'єктивних імовірностей, отриманих від експерта. В якості прикладу показано застосування ДБСД для аналізу аварії на АЕС Фукусіма-1.

Ключові слова: *критична інфраструктура, багатофакторний аналіз безпеки, динамічна БСД.*

APPROACH TO MULTIFACTORIAL ANALYSIS OF CRITICAL INFRASTRACTURE SAFETY BASED ON APPLICATION DYNAMIC BAYESIAN BELIEF NETWORK

E.V. Brezhnev

The approach to multifactorial safety assessment of critical infrastructure based on application of dynamic Bayesian belief network (DBBN) is suggested in the paper. Application of DBBBN allows taking into consideration the complicated dynamic of accident propagation, changes of critical infrastructure states and systems mutual influence as well. Also DBBN allows considering the set of external and internal factors which determine CI safety level. Thus, DBBN is suggested as a basis for multifactorial safety assessment of CI. The application of the approach proposed in this paper helps to increase the accuracy of CI safety indexes and ground the measures to decrease the risks of CI –related technological catastrophes. Beside, the application of this approach increases the scope of probabilistic safety assessment (PSA) due to accounting of subjective probabilities taken from experts. As an example of DBBN application Fukushima NPP accident is considered.

Keywords: *critical infrastructure, multifactorial safety assessment, dynamic Bayesian belief network.*