УДК 685.1

Е. В. БРЕЖНЕВ, В. С. ХАРЧЕНКО

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

МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ: КОНЦЕПЦИЯ И ПРИНЦИПЫ

В работе предлагаются элементы методологического подхода к обеспечению безопасности критических инфраструктур (КИ) в условиях неопределенности. Предложенный подход включает концепцию, принципы, модели и методы, а также основные этапы обеспечения безопасности. Показано, что проблема обеспечения безопасности может быть решена только с позиции системного подхода, в основе которого лежит представление КИ в виде сложной динамической системы из взаимосвязанных систем. В основу методологии положена концепция безопасной КИ из небезопасных и ненадежных систем, которая базируется на известной парадигме фон-Неймана. Оценки безопасности КИ должны быть получены с учетом влияния множества факторов безопасности (внешней среды, человеческого фактора), взаимовлияний между системами с учетом неопределенности. Сформулированы принципы оценивания и обеспечения безопасности КИ, основными из которых являются учет эмерджентных рисков, интеграция результатов априорного и апостериорного анализа безопасности, декомпозиция неопределенности при анализе безопасности и др.

***Ключевые слова**: методология, риск, критическая энергетическая инфраструктура, безопасность, концепция, принципы.*

Введение

Анализ проблемы оценивания и обеспечения безопасности критических инфраструктур. Развитие современного общества зависит от надежного и безопасного функционирования критических инфраструктур (КИ), под которыми понимаются жизненно важные физические или виртуальные системы (S_i,), аварии и сбои которых наносят ущерб экономике, окружающей среде, здоровью и жизни людей [1]. К КИ относятся системы телекоммуникаций, водо- и теплоснабжения, транспорта, др.

Анализ крупных техногенных аварий подтверждает важность проблемы обеспечения инфраструктурной безопасности. Существует множество подходов к трактовке понятия *безопасности* КИ. Безопасность рассматривается как состояние КИ, при котором риск нанесения вреда человеку, обществу, окружающей среде сокращается до приемлемого уровня путем постоянного процесса мониторинга и управления рисками. Кроме того, безопасность может рассматриваться как эмерджентное свойство КИ, связанное с полным отсутствием рисков или наличием приемлемых рисков ее опасных отказов или аварий вследствие отказов отдельных систем.

Безопасность КИ может обеспечиваться посредством улучшения свойств ее систем, компонентов и элементов, мониторингом и управлением рисками в период нормальной эксплуатации, восстановлением работоспособного состояния после аварии или сбоя, использованием избыточности – резервирования, диверсности (разнообразия), а также защитой в глубину. В соответствии с [2], данный подход является наиболее важным и иногда единственным способом обеспечения безопасности критических систем и инфраструктур в целом.

Анализ известных методологий обеспечения инфраструктурной безопасности.

Вопросы оценки безопасности КИ рассмотрены в различных работах по следующим направлениям:

1) системный подход к оценке безопасности [3 – 5];

2) моделирование КИ, формализация взаимовлияний между различными системами на основе теории игр, имитационного моделирования, теории сетей [6, 7]. Рассмотренный класс типов взаимовлияний не статичен. Для современных КИ типы взаимовлияния также размыты. Это позволяет рассматривать различные комбинированные типы влияния, например, информационно-физическое влияние. При таком влиянии информационное состояние одной из систем в КИ определяет физическое состояние другой системы. Изменение внутренней структуры и эволюция КИ приводят к появлению новых типов взаимовлияния;

3) обеспечение живучести КИ [8 – 10]. Оценка и обеспечение живучести КИ является мультидис-

циплинарным подходом. Существует множество подходов, позволяющих получить оценку живучести. Атрибуты живучести (Robustness, Redundancy, Resourcefulness, Rapidity) также не являются статическими. Увеличение живучести, снижение уязвимостей может быть достигнуто за счет диверсификации наиболее важных узлов и связей между ними;

4) оценка безопасности КИ в условиях неопределенности. Подходы к оценке безопасности КИ должны учитывать влияние человеческого фактора, уровень организации и подходы к инфраструктурному менеджменту [11 – 13];

5) подход к анализу функциональной и информационной безопасности (ФБ и ИБ) систем в КИ представлен в работе [14]. Безопасность систем в КИ, например, ИУС может рассматриваться как интегральная сумма ФБ и ИБ. Адекватная оценка ФБ может быть получена с учетом оценок ИБ и наоборот.

Цель статьи – разработка структуры и элементов методологии обеспечения безопасности критических инфраструктур в условиях неопределенности.

1. Основные направления развития методологии обеспечения безопасности КИ

Несмотря на многообразие подходов к обеспечению безопасности, на сегодняшний день не в полной мере решен ряд весьма важных вопросов, связанных с такими важными теоретическими аспектами и практической реализацией обеспечения инфраструктурной безопасности:

- разработка методологии обеспечения инфраструктурной безопасности, основанной на положениях теории безопасности и риска, обобщающей аспекты безопасности КИ различного типа. Отсутствие единой методологии на сегодняшний день является препятствием на пути интеграции различных подходов и моделей, используемых для обеспечения безопасности систем и объектов, важных для безопасности. Отсутствие методологии также является препятствием на пути синтеза новых инфраструктур с различными требованиями по надежности и безопасности;

- разработка методов оценивания безопасности, позволяющих использовать априорные и апостериорные данные для уточнения и верификации результатов оценивания инфраструктурной безопасности;

- разработка методов обеспечения безопасности КИ, основанных на использовании инфраструктурной диверсности и защиты в глубину;

- разработка методов учета комплексного влияния человеческого фактора при оценивании безопасности КИ;

- моделирование аспектов безопасности КИ с учетом интеграции различной квалиметрической информации. Для задач практического оценивания безопасности КИ можно использовать частные и интегральные показатели безопасности. Частные показатели должны учитывать влияние других подсистем и внешней среды. Интегральный показатель безопасности должен учитывать все частные показатели безопасности;

- моделирование и оценка влияния внешних воздействующих факторов, проведение многофакторного анализа безопасности, при котором рассматриваются все факторы, независимо от частоты их проявления, приводящие к аварии.

На метауровне инфраструктура может быть представлена в виде системы из систем (SoS). Основными особенностями SoS являются:

- функциональная независимость систем. При виртуальной декомпозиции SoS все системы продолжают функционировать независимо от других систем полностью самостоятельно;

- целевая независимость систем. Каждая система имеет свою собственную цель функционирования. Если система отделена от SoS, то данная система продолжает выполнять свою собственную цель. Кроме того, системы управляются независимо друг от друга для достижения своих собственных целей.

Среди SoS можно выделить класс SoS критического применения, для которых можно выделить зависимости по безопасности. При этом уровень безопасности одной системы определяет уровень безопасности другой системы, а также безопасность SoS в целом.

Безопасность КИ определяется уровнем ФБ и ИБ систем, входящих в ее состав.

Традиционно, под ФБ понимается часть безопасности, относящаяся к управляемому оборудованию и управляющей системе, которая зависит от правильного функционирования электрических, электронных и программируемых электронных систем, связанных с безопасностью, других связанных с безопасностью технологических систем и оборудования для снижения внешнего риска [15]. Так, например, в атомной индустрии и авиации, ФБ традиционно является атрибутом информационно-управляющих систем (ИУС).

Тенденции развития КИ приводят к некоторому отставанию нормативной базы в сфере защиты КИ. Это обуславливает терминологические проблемы, двузначную трактовку одних и тех же понятий, что в свою очередь также является препятствием на пути интеграции различных практик обеспечения безопасности КИ. Кроме того, можно говорить и о проблеме гармонизации нормативной базы отдель-

ных инфраструктур при их синтезе. Так, например, интеграция АЭС и электросети должна поддерживаться согласованной и гармонизированной нормативной базой, единой терминологией, общими принципами оценивания надежности и безопасности, совместным подходом к риск-анализу.

Глобальное внедрение информационных технологий (ИТ), расширение границ ИУС за счет передачи функций управления и контроля различным удаленным (полевым) устройствам, например, интеллектуальных цифровых устройств, приводит к тому, что ФБ становится не только специфичным свойством ИУС, но и свойством распределенных периферийных устройств. КИ постоянно развивается и не имеет статических границ. Изменяется функциональность и набор целей для систем.

2. Аспекты обеспечения безопасности КИ в условиях неопределенности

Неопределенность как естественный и существенный фактор обеспечения безопасности КИ. Неопределенность является неизбежным фактором, влияющим на безопасность КИ на протяжении всего ее жизненного цикла (ЖЦ). Неопределенность измеряется несоответствием знаний, представлений субъекта анализа (исследователя) о реальных процессах, поведении, структуре КИ.

Существенным препятствием на пути использования вероятностных методов является отсутствие статистической информации, позволяющей построить функции распределения отказов и аварий в работе КИ. Прежде всего это относится к эмерджентным рискам в КИ.

Разработка точной и полной модели оценивания безопасности КИ является сложной задачей, связанной с недостатком знаний о скрытых отказах и поведении КИ, наличием исходных данных представленных в разных квалиметрических шкалах, и пр. Все это неизбежно приводит к неопределенности при решении проблемы оценивания и обеспечения безопасности КИ.

Сложность характера инфраструктурного взаимодействия и взаимовлияния.

Функциональная и целевая независимость систем не исключает их зависимости по состояниям безопасности. Проблема оценки природы взаимосвязей между КИ и ее системами очень важна с точки зрения обеспечения безопасности. Эффект взаимозависимости между КИ очевиден, когда благодаря близости или различного рода влияниям (физическим, географическим, информационным, логическим и пр.), изменение состояния безопасности одной системы КИ вызывает изменения в состоянии безопасности всех зависимых КИ.

Следует отметить двойственность природы взаимодействия при оценивании безопасности КИ. С одной стороны, взаимозависимость обеспечивает живучесть КИ, обуславливая ее быстрое восстановление после воздействия неблагоприятных факторов, с другой, риски и последствия аварий, дефициты безопасности одной системы могут "перетекать" в другие зависимые КИ. В этом контексте уровень живучести КИ в целом обусловлен уровнем уязвимости самой слабой (незащищенной) системы в КИ.

Эволюция КИ и двойственность влияния ИТ. Важным аспектом, который необходимо учитывать при обеспечении безопасности КИ является ее эволюция. Существует множество факторов, обуславливающих эволюцию КИ. Наиболее важным фактором является развитие и внедрение ИТ. На сегодняшний день существует множество примеров успешной реализации ИТ для повышения эффективности управления КИ. Так, например, одним из них является развитие технологий smart grid, появление интеллектуальных энергосистем (адаптивно-активных сетей).

Вместе с тем, широкое внедрение ИТ создает дополнительные дефициты безопасности в подобных системах, обусловленные неадекватной оценкой их влияния не только на ФБ, но ИБ всех зависимых объектов, включая объекты критического применения, например, АЭС. Таким образом, возникает проблема оценивания безопасности КИ с учетом внедрения ИТ не только на уровне конкретной системы, но и в целом, когда вся КИ, а не только ее отдельные системы, становится *критической информационной инфраструктурой.*

Аспект учета влияние человеческого фактора в задачах риск анализа КИ. Роль человека оператора при управлении технологическими процессами в КИ чрезвычайно важна. Внедрение ИТ в практику обеспечения безопасности КИ приводит к уменьшению аварий и катастроф, обусловленных отказами технических систем. Стремление снизить негативное влияние человеческого фактора, с одной стороны, и появление новых возможностей для повышения информированности оператора приводит к автоматизации производства. Однако автоматизация не является универсальным средством снижения рисков в КИ. С одной стороны, она снижает влияние человеческого фактора, а с другой, - обуславливает формирование ошибочной линии поведения оператора. Решение проблемы оценивания и обеспечения безопасности КИ невозможно без учета влияния человеческого фактора.

Формулировка проблемы. Таким образом, в настоящее время существует несоответствие между динамикой развития КИ, дефицитами ее безопасности вследствие изменения морфологии, эволюции,

негативного влияния факторов и их взаимовлияния, возрастанием затрат на обеспечение безопасности, с одной стороны, и уровнем развития моделей, методов и информационных технологий, необходимостью их объединения в единую методологию оценивания и обеспечения безопасности КИ в условиях неопределенности, - с другой стороны.

Это несоответствие позволяет сформировать научную проблему *разработки методологии оценивания и обеспечения безопасности КИ и их ИУС в условиях неопределенности.*

Для ее решения с позиции системного подхода необходимо разработать методологию обеспечения безопасности КИ. В основе методологии должен лежать системный подход как стратегия для решения проблемы в целом путем ее декомпозиции на подпроблемы анализа и синтеза с целью снижения инфраструктурных рисков и неопределенности с целью повышения безопасности и предупреждения инфраструктурных аварий.

3. Элементы методологии обеспечения безопасности КИ в условиях неопределенности

3.1. Логическая структура и этапы решения проблемы обеспечения безопасности КИ

В соответствии с [16] методология – это учение о структуре, логической организации, методах и средствах деятельности. Основываясь на данном определении, методология обеспечения безопасности КИ представляет собой целенаправленную деятельность субъекта анализа (исследователя) при получении нового знания, направленного на решение сложной проблемы по обеспечению безопасности КИ в условиях неопределенности. Это знание позволяет решать практические задачи управления инфраструктурной безопасностью, обеспечивая исследователя информацией, используемой для снижения риска до приемлемого уровня. Целенаправленная деятельность исследователя при анализе безопасности характеризуется логической структурой.

Основными элементами логической структуры являются:

- *субъект анализа* – организация (стейкхолдеры) или любая заинтересованная сторона, в интересах которой проводится исследование проблемы обеспечения безопасности КИ;

- *объект* – безопасность КИ;

- *предмет анализа* – модели, методы и ИТ обеспечения инфраструктурной безопасности;

- *методы анализа;* при проведении исследований использовались методы системного анализа, теории вероятностей, нечетких множеств и исследования операций, математический аппарат теории динамических байесовских сетей с дискретными состояниями, теории надежности и безопасности сложных систем и анализа рисков;

- *результат анализа* может быть представлен в виде нового знания, используемого для решения проблемы обеспечения безопасности КИ в условиях неопределенности.

Целью исследований является повышение безопасности КИ на основе развития методологии и разработки ИТ оценивания и обеспечения безопасности в условиях неопределенности.

Основные принципы, методы и модели, а также ИТ, поддерживающие процессы оценивания и обеспечения безопасности КИ в условиях неопределенности, представлены на рисунке 1.

3.2. Концепция и принципы обеспечения безопасности КИ

Концепция: безопасная инфраструктура из небезопасных и ненадежных независимых систем. Следует отметить, что одним из основных элементов методологии обеспечения безопасности КИ является разработка концепции как способа понимания, основной точки зрения на инфраструктурную безопасность. В основе данной работы лежит развитие концепции, разработанной Джоном фон Нейманом [1, 2]. Основная ее идея – создание надежной (безотказной) системы из ненадежных элементов. Развитие методов обеспечения надежности привело к эволюции данной концепции и появлению в 80-90 годы XX века парадигмы "надежные и безопасные системы из ненадежных и небезопасных компонент".

КИ является интегральной системой, состоящей из функционально независимых (слабо зависимых) систем, которые могут функционировать абсолютно независимо (слабо зависимо) друг от друга.

Так, например, если рассматривать КИ, состоящую из АЭС и электрической системы, то безопасность КИ в данном случае определяется безопасностью систем АЭС, ФБ ИУС и надежностью работы электросети. Таким образом, оценка безопасности КИ определяется безопасностью одних систем и надежностью других, функционально и организационно независимых между собой. Предложенная концепция отличается от известных подходов к развитию и использованию концепции Д. Ф. Неймана переходом к инфраструктурному уровню с учетом независимости систем, интегрируемых в рамках КИ.

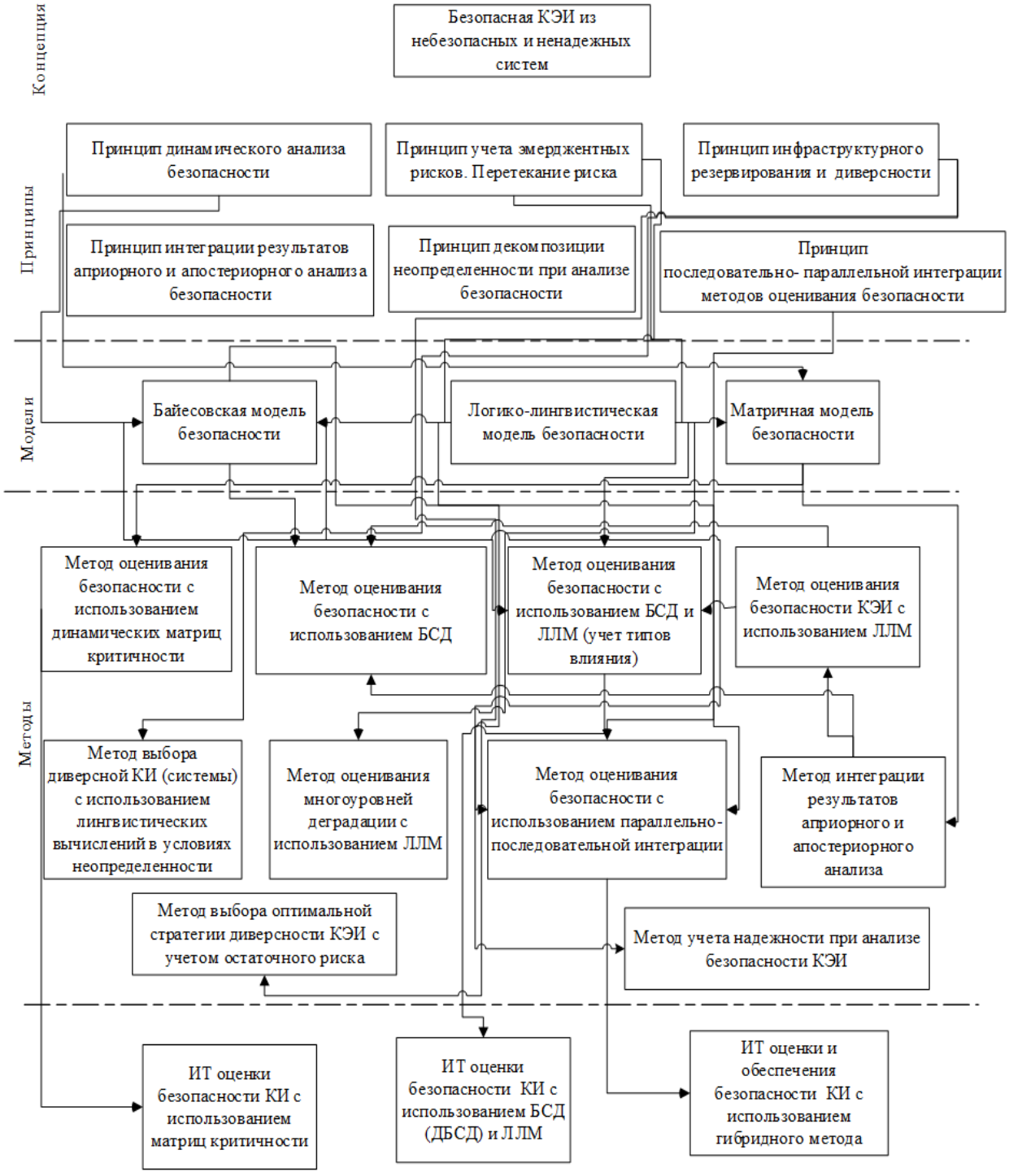

Рис. 1. Элементы методологии обеспечения безопасности КЭИ в условиях неопределенности

Принципы оценивания и обеспечения безопасности КИ. К основным принципам предложенной методологии обеспечения безопасности КИ относятся следующие.

Принцип динамического анализа безопасности, который предполагает, что подход к оценке безопасности КИ должен учитывать динамику рисков. Это означает, что мониторинг и управление рисками должны проводиться на протяжении всего ЖЦ безопасности КИ. ИУС выступает средством мониторинга и контроля. Отказы и сбои в работе КИ, не приводящие к крупным техногенным авариям, рассматриваются как индикаторы безопасности, которые используются для обновления вероятностей отказов, и, соответственно, рисков.

Кроме того, взаимовлияние между системами в

КИ приводит к появлению эмерджентных рисков, которые не были учтены на этапе разработки систем КИ. Сама КИ является динамическим объектом: изменяются параметры ее функционирования, состав систем, связи между ними, состояния, пр.

Принцип учета эмерджентного риска в КИ.

Взаимовлияние между системами приводит к феномену *эмерджентности рисков*, когда исходное множество рисков

$$R(t) = \{R_1(t), R_2(t), ...R_n(t)\},$$

определенное на этапе разработки, не совпадает с множеством текущих рисков

$$R^*(t) = \{R_1^*(t), R_2^*(t), ...R_n^*(t), R_{n+1}(t)\}.$$

То есть, на ЖЦ возникают эмерджентные риски, $R_{n+1}(t)$, определение вероятности и тяжести которых затруднительно в виду недостаточности данных для их анализа.

Таким образом, взаимовлияние приводит как к увеличению локальных рисков, идентифицируемых на этапе разработки КИ (рисков отказов оборудования, рисков ошибок персонала, пр.), так и к появлению новых рисков. Локальные и эмерджентные риски приводят к снижению безопасности КИ.

Принцип декомпозиции неопределенности требует рассматривать неполноту и неточность информации об условиях, которые приводят к возникновению аварийных ситуаций в работе КИ. В данной методологии неопределенность декомпозируется на неопределенность первого, второго рода и третьего рода.Декомпозиция проводится с целью снижения неопределенности и определения группы методов, которые могут быть использованы для получения показателей безопасности и определения на их основе стратегий обеспечения безопасности.

Неопределенность первого рода (стохастическая неопределенность) обусловлена случайностью, вероятностной природой факторов, определяющих безопасность КИ. Неопределенность второго рода обусловлена наличием нечеткости и расплывчатости в описании КИ, которые не учитываются в рамках традиционных вероятностных моделей.

В работе учитывается модельная неопределенность (третьего рода), которая включает параметрическую и структурную неопределенность. Параметрическая неопределенность модели связана с неточностью знаний исследователя о ее параметрах. Структурная неопределенность связана с возможным неучетом параметров модели. Этот вид неопределённости характеризуется невозможностью априорного задания параметров, входов и выходов модели оценивания безопасности КИ.

Принцип интеграции результатов априорного и апостериорного анализа безопасности. Априорный анализ безопасности КИ начинается на этапе разработки и продолжается на этапе эксплуатации системы. Для анализа рисков используется множество методов с допущениями, принятыми в рамках доступной для исследования информации.

После возникновения аварии проводится апостериорный анализ безопасности, который позволяет уточнить модели безопасности, множество рисков, ограничений, принятых на этапе априорного анализа безопасности. Это позволит повысить качество риска анализа на этапе разработки систем КИ.

Принцип последовательно-параллельной интеграции методов оценки безопасности. Принцип состоит в интеграции различных методов для получения множества параметров безопасности КИ (множество методов – множество различных параметров безопасности КИ), а также интеграция различных групп методов для получения идентичных параметров безопасности (множество методов – один параметр безопасности КИ). Кроме того, интеграция методов рассматривается как процесс валидации используемых математических методов и моделей. При параллельной интеграции методов возникает возможность получения одного и того же показателя безопасности различными способами. Степень различия между ними рассматривается в качестве валидационной метрики.

Принцип инфраструктурного резервирования и диверсности для обеспечения безопасности КИ состоит в использовании избыточности и разнообразия на инфраструктурном уровне. Под инфраструктурным резервированием понимается избыточность, реализованная на инфраструктурном уровне, для повышения безопасности КИ, выполнения критических сервисов, снижения рисков для ИУС. Так, если критический сервис не может быть обеспечен одной из систем, эта функция передается другой системе, способной к ее выполнению. Данный вид резервирования приводит к увеличению робастности КИ, как способности к выполнению критических сервисов в условиях работы, отличных от нормальной эксплуатации.

Под инфраструктурной диверсностью понимается разнообразие между системами КИ и связями между ними. Инфраструктурная диверсность позволяет снизить риски множественных аварий, поскольку снижается множество общих уязвимостей.

Заключение

Высокая тяжесть последствий техногенных

аварий, сбоев в работе системы из систем (КИ) требует разработки методологии, которая бы обеспечила решение этой проблемы с точки зрения системного подхода, интегрируя задачи оценивания и обеспечения в рамках единого системного подхода. Предложенная методология включает концепцию, принципы, модели и методы, а также этапы применения этих методов и моделей. На наш взгляд концепция, базирующаяся на известной парадигме фон-Неймана, является сердцевиной системного подхода к решению проблемы обеспечения безопасности. На ее основе предложены принципы, которые позволят принять рациональные решения в сфере инфраструктурного менеджмента безопасности и таким образом повысить безопасность существующих и синтезируемых КИ.

Литература

1. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения [Текст]: учебник / под редакцией В. С. Харченко. – Х. : 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 [Текст] : книга / В. В. Скляр, Е. В. Брежнев ; под общей редакцией В. С. Харченко. – Г. : Palmarium Academic Publishing, 2013. – 529 с.

3. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies [Text] / M. Steven, et al. // IEEE Control System Magazine. – 2001. – P. 11-25.

4. North, M. Agent-based modeling of complex infrastructures [Text] / M. North // Proceedings of Workshop Simulation of Social Agents: Architectures and Institutions, Chicago, 12 December, 2000. – P. 239-251.

5. Energy interdependence modeling and simulation [Text] / C. Unal et al. // Tech. Rep. LAUR-01-1879, Los Alamos National Laboratory. – 2001. – P. 34 – 45.

6. Leontief-based model of risk in complex interconnected infrastructures [Text] / Y. Haimesand et al. // Journal of Infrastructure Systems. – 2001. – P. 67 -78.

7. Learning the critical infrastructure Interdependencies through an ontology-based information system [Text] / R. McNally et al. // Environment and Planning. – 2007. – V. 1. – P. 1103–1124.

8. A place-based model for understanding community resilience to natural disasters [Text] / S. Cutter, et al. // Global Environmental Change. – 2008. – № 18. – P. 598–606.

9. An exploratory framework for the empirical measurement of resilience [Text] / G. S Cumming et al. // Ecosystems. – 2005. – № 8. – P. 78 – 89.

10. Assessing power substation network security and survivability: A work in progress report [Text] / C. Taylor et al. // Proceedings of Int. Conf. on Security and Management, Las Vegas, 17-18, January, 2003. – P. 123 – 129.

11. Uncertainty Analysis of Interdependencies in Dynamic Infrastructure Recovery: Applications in Risk-Based Decision Making [Text] / K. Barker et al. // Journal of Infrastructure systems. – 2008. – № 15 (4). – P. 231 – 241.

12. Reckhow, K. Water-Quality Simulation Modeling and Uncertainty Analysis for Risk Assessment and Decision-Making [Text] / K. Reckhow // Ecological Model. – 1994. – P. 1-20.

13. Goodman, D. Extrapolation in risk assessment: Improving the quantification of uncertainty, and improving information to reduce the uncertainty [Text] / D. Goodman // Human Ecological Risk Assessment. – 2002. – № 8. – P. 177-192.

14. Скляр, В. В. Методологія та інформаційні технології забезпечення функціональної безпеки інформаційно-управляючих систем [Текст] : дис. ... д-ра техн. наук : 05.13.06 ; защищена 06.06.11 ; утв. 30.08.11 / Скляр Владимир Владимирович. – Х., 2011. - 324 с.

15. Smith, D. Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards [Text] / D. Smith. – Elsevier Butterworth-Heinemann, Oxford, UK, 2004. – 263 p.

16. Новиков, А. М. Методология научного исследования [Текст] / А. М. Новиков. – М. : Либроком, 2009. – 280 с.

Поступила в редакцию 03.02.2015, рассмотрена на редколлегии 20.03.2015

МЕТОДОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНИХ ІНФРАСТРУКТУР В УМОВАХ НЕВИЗНАЧЕНОСТІ: КОНЦЕПЦІЯ ТА ПРИНЦИПИ

Є. В. Брежнєв, В. С. Харченко

В роботі пропонуються елементи методологічного підходу щодо забезпечення безпеки критичних інфраструктур (КІ) в умовах невизначеності. Підхід ґрунтується на концепції, принципах, містить моделі та методи, а також основні етапи забезпечення безпеки. Показано, що проблема забезпечення безпеки може бути вирішена тільки на підставі системного підходу, в основі якого лежить подання КІ як складної

динамічної системи із взаємопов'язаними підсистемами. В основі методології покладено концепцію побудови безпечної КІ з небезпечних та ненадійних систем, як розвиток парадигми фон-Неймана. Показано, що оцінки безпеки КІ повинні враховувати множину чинників безпеки (зовнішнє середовище, людський чинник, тощо), взаємовплив між системами та невизначеності. Сформовано основні принципи методології.

Ключові слова: методологія, ризик, критична енергетична інфраструктура, безпека, концепція, принципи.

METHODOLOGY OF CRITICAL INFRASTRUCTURE SAFETY ASSURANCE UNDER UNCERTAINTIES: CONCEPT AND PRINCIPLES

E. V. Brezhnev, V. S. Kharchenko

The methodology basis of safety assessment and assurance of critical infrastructure under uncertainties are suggested in this paper. This basis includes safety concept, principles, models and methods, and safety assurance stages as well. It is shown that problem of infrastructure safety assurance might be solved only with systematic approach, with consideration of critical infrastructure as system of systems. The safety concept is a main pillar of this methodology. It is based on John von Neumann's paradigm and implies the development of safe infrastructure out of unsafe and unreliable systems. It is shown that infrastructure safety assurance shall take into account safety factors (external environment, humans, etc.), mutual influences between systems and uncertainties. The safety principles are also introduced in this paper.

Key words: methodology, critical energy infrastructure, safety, concept, principles.

Брежнев Евгений Витальевич – канд. техн. наук, доцент кафедры компьютерных сетей и систем, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: milestone@list.ru.

Харченко Вячеслав Сергеевич – д-р техн. наук, профессор, заведующий кафедрой компьютерных сетей и систем, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: v_s_kharchenko@ukr.net.