Запобігання та ліквідація надзвичайних ситуацій

УДК 685.1

Е.В. Брежнев

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

МЕТОД ИНТЕГРАЦИИ РЕЗУЛЬТАТОВ АПРИОРНОГО И АПОСТЕРИОРНОГО АНАЛИЗА БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

В статье предлагается подход к оценке безопасности критических инфраструктур, который основан на интеграции результатов априорного и апостериорного анализа безопасности. Интеграция результатов рассматривается в качестве одного из основных принципов риск анализа инфраструктур и систем, отказы и аварии которых характеризуются высокой тяжестью последствий для человека и окружающей среды. Рассмотрены варианты отношений между априорной и апостериорной моделью анализа. Подход позволяет уточнить параметры априорной математической модели, используемой для анализа безопасности критических инфраструктур, а также повысить достоверность результатов оценки безопасности и обоснованность решений по снижению рисков до приемлемого уровня.

Ключевые слова: *критическая инфраструктура, безопасность, априорный и апостериорный анализ.*

Введение

Постановка проблемы и анализ литературы. Безопасность является одним из наиболее важных понятий анализа критических инфраструктур (КИ). Под безопасностью понимается состояние КИ, при котором на протяжении всего жизненного цикла (ЖЦ) риски аварий, отказов и сбоев в ее работе отсутствуют или являются приемлемыми с точки зрения субъекта анализа.

Субъект анализа – исследователь, проводящий оценку сценариев развития неблагоприятных событий, объект анализа – безопасность КИ.

Риск, связанный с функционированием КИ, определяется как комбинация вероятности неблагоприятного события (аварии, сбоя, и т.д.) и его тяжести. Тяжесть определяется с точки зрения ущерба окружающей среде, здоровью и жизни человека. Безопасность КИ и, соответственно, риски, связанные с ней, не являются статическими. Это означает, что под влиянием множества факторов как стохастической, так и нестохастической природы, величина рисков может изменяться. Это обуславливает необходимость проведения анализа безопасности КИ на протяжении всего ЖЦ.

Предметом анализа безопасности КИ является оценка факторов, приводящих к возникновению неблагоприятных событий, параметров риска, связанного с этими событиями, а также оценка превентивных мер, направленных на снижение вероятности и тяжести последствий.

Можно выделить три подхода к анализу рисков в КИ: детерминированный и вероятностный анализ, а также анализ, основанный на теории возможностей. Все вышеуказанные подходы к анализу безопасности КИ могут применяться как априорно, так и апостериорно [1, 2].

Априорный анализ безопасности проводится до возникновения неблагоприятного события. В его основе лежит сценарный анализ, при котором вводятся и анализируются множество возможных сценариев, связанных с событием и возможным поведением КИ как реакции на его возникновение. Последствия, характерные для различных сценариев, оцениваются с учетом ущерба, связанного с ними. Количественные и качественные характеристики каждого сценария определяются в рамках модели, принятой для анализа. Каждая модель строится с учетом допущений и ограничений, свойственных ей.

Априорный анализ проводится в условиях неопределенности. Существует множество подходов к классификации неопределенности при анализе безопасности КИ [3]. Классически выделяется две стороны неопределенности [4]: эпистомологическая неопределенность, связанная с отсутствием у субъекта анализа полных знаний об объекте исследований, алеаторная неопределенность, непосредственно связанная с объектом анализа. Алеаторная неопределенность обусловлена эволюцией свойств и поведения объекта. Данный вид неопределенности считается неотъемлемым свойством КИ, обусловленным действием случайных факторов. Классифици-

руется как стохастическая неопределенность. Алеаторную неопределенность невозможно снизить полностью. Можно лишь говорить о снижении неопределенности до определенного уровня, достаточного с точки зрения субъекта анализа.

Эпистомологическая неопределенность является свойством объекта анализа безопасности и может быть снижена за счет получения дополнительных сведений о характеристиках КИ, ее поведении.

Апостериорный анализ выполняется после того, как нежелательное событие уже произошло. Цель такого анализа – разработка рекомендаций, направленных на повышение уровня безопасности КИ, снижение рисков для аналогичных систем в будущем. Данный вид анализа связан с исследованием одного из предполагаемых сценариев, который был реализован. Неопределенность, свойственная априорному анализу, может привести к реализации последовательности событий, не принадлежащей исходному множеству сценариев.

Один вид анализа дополняет другой. Предпочтительность метода анализа зависит от сложности системы и от того, какие параметры КИ известны с приемлемой точностью. При изучении системы, характеристики, поведение и влияние окружающей среды которой детерминированы, предшествующий опыт позволяет осуществить детальный априорный анализ. При дополнении априорного анализа результатами, полученными при апостериорном анализе системы, анализ безопасности КИ становится более полным и достоверным.

Кроме того, апостериорный анализ может стать базой для последующего априорного анализа, т.к. субъект исследования делает выводы, выходящие за рамки единичного процесса, последствием которого стало неблагоприятное событие. При этом он одновременно анализирует различные события, которые могли бы привести к такому или подобным нежелательным событиям.

Таким образом, работы, связанные с риск анализом безопасности КИ, в которых указывается на необходимость интеграции априорного и апостериорного анализа, не содержат рекомендаций по формализации и выбору подходов к самой интеграции. Это является причиной существования методологических изъянов комбинации априорного и апостериорного анализа и трудностям, связанным с уточнением априорных моделей безопасности КИ.

Цель статьи – разработка подхода к интеграции результатов априорного и апостериорного анализа в интересах уточнения априорной модели анализа безопасности КИ аналогичного класса.

Основной материал

Для КИ априорный анализ безопасности проводится для снижения рисков, связанных с возникновением неблагоприятного события. Субъектом исследования может быть выбрана любая модель, позволяющая провести анализ поведения системы. Этот выбор определяется наличием исходной информации, целью анализа, сложностью самой системы, а также предпочтениями самого субъекта.

Любая модель анализа безопасности КИ формально может быть представлена как:

$$M = \{\{S_{ij}\}_{IJ}, \{L_k\}_K, \{St_g^{Sij}\}_G, \{M_h^{parametr}\}_H, \{y_m\}_M\},$$

где $\{S_{ij}\}_{IJ}$ – множество систем КИ, важных для безопасности;

$\{L_k\}_K$ – множество связей между системами КИ;

$\{St_g^{S_{ij}}\}_G$ – множество состояний систем КИ;

$\{y_m\}_M$ – комплексный показатель безопасности КИ, включающий М частных показателей;

$\{M_h^{parametr}\}_H$ – множество параметров, описывающих состояния систем КИ, например, вероятность нахождения системы в g-м состоянии.

Следует отметить, что в зависимости от используемой модели оценки безопасности, часть множеств может не использоваться.

Безусловно, невозможно рассматривать в рамках анализа безопасности все элементы, компоненты и системы КИ. Целесообразно из общего множества выделить подмножество элементов, компонентов и систем, важных для безопасности КИ.

С учетом формализованного представления модели анализа безопасности модель априорного анализа может быть записана как:

$$M^{Aprior} = \{\{S_{ij}^{aprior}\}_{IJ}, \{L_k^{aprior}\}_K, \{St_g^{Sij(aprior)}\}_G,$$
$$\{M_h^{parametr(aprior)}\}_H, \{y_m^{aprioor}\}_M\}.$$

Соответственно, модель апостериорного анализа может быть записана как:

$$M^{Aprior} = \{\{S_{ij}^{apost}\}_{IJ}, \{L_k^{apost}\}_K, \{St_g^{Sij(apost)}\}_G,$$
$$\{M_h^{parametr(apost)}\}_H, \{y_m^{apost}\}_M\}.$$

После возникновения аварии, сбоя в работе КИ исходная априорная модель может быть уточнена, вследствие снижения неопределенности. Могут быть представлены следующие варианты отношений между множествами, описывающими априорную (В) и апостериорную (А) модели.

1. Равенство множеств, описывающих априорные и апостериорные модели. Равенство множеств может быть записано формально. Если А, В – множества, их равенство записывается как А=В.

При равенстве множеств априорная модель не может быть дополнена результатами апостериорного анализа. Идеальный случай с точки зрения риск анализа. В терминах формализованного представле-

ния моделей, все системы, их состояния, связи между ними и параметры учтены. Поскольку распределение ресурсов, направленных на снижение рисков, проводится на основе априорного анализа безопасности, данный случай может рассматриваться как рациональный с точки зрения использования ресурсов КИ для снижения рисков, связанных с ее системами. Характеризует полностью детерминированный случай, который не может быть реализован при анализе безопасности КИ.

2. Априорное множество является подмножеством апостериорного множества $A \subset B$. Множество А содержится во множестве В (множество В включает множество А), если каждый элемент А есть элемент В:

$$A \subset B : x \in A \Rightarrow x \in B.$$

В этом случае А называется подмножеством В, В – надмножеством А.

В качестве показателя неопределенности при анализе безопасности КИ может рассматриваться разность апостериорного и априорного множеств.

Разностью этих множеств является множество, которое состоит из элементов множества А (апостериорное множество), которых нет во множестве В (априорное множество), т.е.

$$A \setminus B = \{x | x \in A \wedge x \notin B\}.$$

Разность между этими двумя множества является результатом неопределенности анализа. Мощность множества может рассматриваться как метрика неопределенности. Чем больше (меньше) мощность, тем выше (ниже) неопределенность. Мощность апостериорного множества $|A|$ в этом случае больше мощности априорного множества $\| B|$, $|A| > |B|$. Данный вид отношений между множествами обусловлен тем, что не все системы, связи, параметры модели и состояния систем КИ были учтены при проведении априорного анализа. С точки зрения эффективности использования ресурсов на основе априорного анализа данный случай является нерациональным, поскольку часть рисков не была компенсирована.

3. Апостериорное множество является подмножеством априорного множества. Множество В содержится во множестве А (множество А включает множество В), если каждый элемент В есть элемент А:

$$B \subset A : x \in B \Rightarrow x \in A.$$

В этом случае А называется подмножеством В, В – надмножеством А. Данный случай возможен в случае избыточности ресурсов для компенсации рисков в КИ. Учтены и сбалансированы все возможные риски, независимо от вероятности неблагоприятных событий и тяжести их последствий.

В этом случае в априорную модель введены избыточные параметры, состояния систем, сценарии, которые не могут быть реализованы для данной системы.

Варианты этих отношений могут быть продемонстрированы на примере использования матрицы критичности, построенной для анализа рисков, связанных с отказами систем КИ. Матрица критичности позволяет указать и ранжировать все возможные риски, с учетом тяжести и вероятности их возникновения. Обычно используется двумерная матрица “вероятность – тяжесть”.

Поскольку любая КИ может быть представлена в виде иерархии уровней систем, подсистем, компонентов и элементов, то для каждой КИ может быть построено множество матриц критичности, описывающих риски, связанные с авариями (отказами) систем, подсистем, компонентов и элементов. В любой момент времени система характеризуется определенным уровнем критичности состояния, определяемым вероятностью аварий (отказов, сбоев) и тяжестью возможных последствий.

Так, например, матрица критичности КИ, построенная на этапе априорного анализа безопасности КИ для уровня систем, может быть представлена в виде табл. 1.

Исходными данными для построения матрицы критичности является: множество систем, важных для безопасности КИ; параметры, позволяющие определить риски неблагоприятных событий (вероятность аварии (отказа) и тяжесть последствий).

Таблица 1

Априорная матрица критичности КИ (уровень систем)

		Вероятность отказа			
		Оч. Н	Н	Ср.	В
Тяжесть отказа	В	Отказ S_1			Отказ S_3
	Ср		Отказ S_2		
	Н			Отказ S_4	
	Оч. Н				

Если после возникновения неблагоприятного события в критической инфраструктуре матрица критичности, построенная по результатам апостериорного анализа, имеет аналогичный вид, то можно говорить о наступлении первого случая, когда результаты апостериорного и априорного анализа совпадают.

Если по результатам апостериорного анализа матрица критичности имеет вид, представленный в табл. 2, то можно утверждать о наступлении второго случая, когда априорное множество является подмножеством апостериорного множества $A \subset B$.

Таблица 2

Апостериорная матрица критичности КИ (уровень систем)

		Вероятность отказа			
		Оч. Н	Н	Ср.	В.
Тяжесть отказа	В	Отказ S_1			
	Ср		Отказ S_2	*Отказ S_5*	*Отказ S_6*
	Н			Отказ S_4	*Отказ S_3*
	Оч. Н				

В этом случае не были учтены возможные отказы систем S_5 и S_6, а также риски, связанные с ними. Кроме того, параметры риска, связанного с отказом системы S_3, были завышены.

Если по результатам апостериорного анализа матрица критичности имеет вид, представленный в табл. 3, то можно утверждать о наступлении третьего случая, в котором апостериорное множество является подмножеством априорного множества.

Таблица 3

Матрица критичности КИ (уровень систем)

		Вероятность отказа			
		Оч. Н	Н	Ср.	В
Тяжесть отказа	В	Отказ S_1			Отказ S_3
	Ср		*Отказ S_2*		
	Н			Отказ S_4	
	Оч. Н				

В этом случае, при априорном анализе система S_2 и параметры риска, связанного с ее отказом, были введены избыточно. Данная система не оказывает влияние на безопасность КИ.

Минимизация разности множеств апостериорного и априорного анализа может рассматриваться как критерий необходимости уточнения априорной модели по результатам апостериорного анализа. Графически схема уточнения априорной и апостериорной моделей представлена на рис. 1.

После наступления неблагоприятного события $T_{curr} > T_{accid}$ проводится апостериорный анализ безопасности КИ.

Проводится сравнение априорных и апостериорных результатов.

В качестве параметров сравнения могут быть использованы:

– качественный и количественный состав систем КИ, важных для безопасности, выделяемых на этапе априорного и апостериорного анализа. При проведении апостериорного анализа может быть определено, что качественный и количественный состав систем, рассматриваемых на этапе априорного анализа, является не полным;

Рис. 1. Схема уточнения априорной и апостериорной моделей

– множество связей между элементами, типы связей. Для КИ рассматриваются физические, географические, логические, информационные и др. При проведении апостериорного анализа безопасности может быть определено, что не были учтены все возможные типы связей между системами;

– множество состояний систем и элементов, важных для безопасности. По результатам апостериорного анализа безопасности КИ может быть определено, что множество состояний систем, используемых при проведении априорного анализа, являлось неполным;

– множество параметров, описывающих состояния систем, используемых для проведения априорного анализа и апостериорного анализа.

Сравнение множеств, описывающих априорную и апостериорную модели анализа безопасности, позволяет определить три возможных случая отношений между ними.

Принцип уточнения подходов и моделей анализа безопасности КИ, используемых при проведении априорного анализа, по результатам апостериорного анализа может быть применен для любой

модели оценки безопасности. При этом происходит уточнение параметров модели.

Разница между множествами характеризует уровень неопределенности.

Результаты апостериорного анализа могут быть использованы для снижения неопределенности и повышения обоснованности решений, направленных на снижение рисков в КИ.

Выводы

Таким образом, можно выделить следующие особенности интеграции результатов априорного и апостериорного анализа безопасности КИ.

1. Апостериорный анализ проводится в условиях определенности, после наступления неблагоприятного события в КИ. Это означает, что на данном этапе целесообразно уточнить все множества (см. формулу 1).

2. Уточненная априорная модель может быть использована для анализа безопасности аналогичных КИ. Это положение основано на подходе к анализу аварий сложных систем Левицки [5]. Первый уровень этой модели представляет собой цепочку событий, приводящих к аварии. Именно на этом уровне можно говорить об уникальности аварии, о неповторимости цепочки событий, приводящих к аварии.

Второй уровень представляет собой условия, которые обусловили возникновение инициирующего события первого уровня. Третий уровень представляет собой ограничения (либо их отсутствие), которые обусловили проявление условий второго уровня. Для второго и третьего уровня можно говорить об общности анализа безопасности для аналогичных КИ и, соответственно, о возможности применения уточненной априорной модели для аналогичных систем КИ.

3. Разность апостериорного и априорного множества обусловлена наличием неопределенности. Отсутствие неопределенности, полностью детерминированный случай для анализа КИ является исключением.

Список литературы

1. Шереметьева У.М. Охрана труда на производстве и в учебном процессе: Конспект лекций / У.М. Шереметьева, ГОУ ВПО «Томский государственный педагогический университет». – Томск: Издательство ТГПУ, 2009. – 160 с.

2. Безопасность жизнедеятельности: Учебник / Под ред. Э.А. Арустамова; 10-е изд., перераб. и доп. – М.: Издво «Дашков и К°», 2006. – 476 с.

3. Брежнев Е.В. Анализ подходов к оценке безопасности критических инфраструктур в условиях неопределенности / Е.В. Брежнев // Системи обробки інформації. – Х.: ХУ ПС, 2011. – Вип. 2 (92). – С. 277-281.

4. Terje Aven. Some considerations on the treatment of uncertainties in risk assessment for practical decision making / Terje Aven, Enrico Zio // Reliability Engineering and System Safety, 96 (2011). – P. 64-74.

5. Risk and Vulnerability Analysis of Complex Systems. A basis for proactive emergency management, Department of Safety Engineering and System Safety Faculty of Engineering. – 2007. – 123 p.

Поступила в редколлегию 12.11.2012

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

МЕТОД ІНТЕГРАЦІЇ РЕЗУЛЬТАТІВ АПРІОРНОГО ТА АПОСТЕРІОРНОГО АНАЛІЗУ БЕЗПЕКИ КРИТИЧНИХ ІНФРАСТРУКТУР

Є.В. Брежнєв

В статті запропоновано підхід до оцінки безпеки критичних інфраструктур, який базується на інтеграції результатів апріорного та апостеріорного аналізу безпеки. Інтеграція результатів розглядається в якості одного з основних принципів ризик аналізу безпеки інфраструктур та систем, відмови та аварії яких характеризуються великою важкістю наслідків для людини та навколишнього середовища. Розглянуто варіанти відношень між апріорною та апостеріорною моделями. Даний підхід дозволяє уточнити параметри апріорної математичної моделі, яка використовується для аналізу безпеки інфраструктур. Це дозволить підвищити достовірність результатів оцінки безпеки та обгрунтованність рішень щодо зниження ризиків до прийнятного рівня.

Ключові слова: *критична інфраструктура, безпека, апріорний та апостеріорний аналіз.*

THE INTEGRATION METHOD OF A PRIORI AND A POSTERIORI RESULT OF CRITICAL INFRASTRUCTURE SAFETY ANALYSIS

Ye.V. Brezhnev

The approach to critical infrastructure's safety assessment based on integarion of a priori and a posterioti safety analysis results is considered in the paper. The result integration is suggested as a main principle of risk analysis of infrastructure and systems characterized by high accident consequences severity for human beings and natural environment. The possible relations between a priori and a posterioti models are considered. This approach allows adjusting the parameters of a priori model used for infrastructure safety analysis. It allows increasing a credibility of safety analysis results and validity of decisions to decrease risk to acceptable level.

Keywords: *critical infrastructure, safety, a priori and a posterioti analysis.*