

УДК 62-192:519.2

О. В. ИВАНЧЕНКО<sup>1</sup>, В. С. ХАРЧЕНКО<sup>2</sup><sup>1</sup>Севастопольский национальный технический университет, Украина<sup>2</sup>Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

## МЕТОД ПРИЧИННО-СЛЕДСТВЕННОЙ ДЕКОМПОЗИЦИИ АВАРИЙ И ИНЦИДЕНТОВ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

*Излагается систематизированная последовательность шагов, которые необходимо реализовать для решения задачи декомпозиции событий, наблюдаемых в ходе аварий и инцидентов критических инфраструктур (КИ). Рассмотрена возможность использования алгебры причинно-следственных комплексов для построения автоматной и стохастической моделей каскадных отказов компонентных составляющих КИ. Представлены таксономия и структурно-логическая схема совокупности негативных явлений, наблюдавшихся в ходе аварии Северо-Американской энергетической инфраструктуры, которые составили композиционную основу причинно-следственных звеньев разрабатываемых моделей.*

**Ключевые слова:** критическая инфраструктура, каскадные отказы, таксономия, причинно-следственные звенья.

### Постановка проблемы

Устойчивое экономическое развитие в значительной степени зависит от эффективного функционирования критических инфраструктур (КИ), являющихся ключевой составляющей национальной безопасности государства. Рост сложности и масштабов задач, решаемых с использованием различных инфраструктурных образований, является характерной особенностью современного этапа применения КИ по назначению. Этот процесс сопровождается стремлением улучшить функциональность, эффективность критических инфраструктур при приоритете их надежности и безопасности. Однако, достичь этого не всегда удается, о чем свидетельствуют последствия крупнейших аварий, произошедших за последние пятнадцать лет на АЭС Фукусима – 1 (Япония, 2011 г.), Саяно-Шушенской ГЭС (Россия, 2009 г.) и др. Поэтому без преувеличения можно утверждать, что энергетические инфраструктуры (ЭИ) относятся к КИ, а проблема обеспечения их безопасного, надежного использования по назначению носит глобальный характер.

Интерес представляют результаты анализа [1, 2] одной из наиболее крупных аварий объединенной ЭИ США и Канады (Blackout), которая произошла в августе 2003 г. Существуют различные подходы и математические методы анализа безопасности ЭИ, которые базируются на применении математического аппарата марковских, полумарковских случайных процессов, байесовских сетей, моделей риск-анализа. В частности, строятся иерархи-

ческие динамические матрицы критичности, учитывающие взаимное влияние отказов и эффекты «перетекания» рисков в рассматриваемом инфраструктурном образовании [1].

Одной из наиболее строгих в математическом отношении и конструктивных в прикладном смысле является методология описания и анализа сложных систем на основе алгебры причинно-следственных комплексов (ПСК), разработанная В. А. Твердохлебовым [1, 3]. Применение ПСК позволяет решать одну из ключевых проблем анализа безопасности КИ – проблему сложности моделей, обеспечивая исследователя более гибким инструментарием их представления по сравнению с традиционными методиками – деревьями отказов, HAZOP- и FME(C)A-анализом и другими.

**Целью статьи** является разработка аналитико-стохастического метода анализа аварий и инцидентов критических инфраструктур путем причинно-следственной декомпозиции последовательности негативных событий.

### 1. Изложение основного материала

Сформулируем основные положения метода причинно-следственной декомпозиции (ПСЛД) на примере ПСЛД одного из этапов аварии критической ЭИ (КЭИ) США и Канады (Blackout, 2003 г.) [2]. Будем полагать, что критическая энергетическая инфраструктура CrEI состоит из множества разнородных элементов, т.е.

$$CrEI = \bigcup_{\ell=1}^L \{CrS^\ell\},$$

где CrS – критические системы (КС) из состава КЭИ. Известен сценарий  $S_{CrEI} = \bigcup_{j=1}^J \{S_{CrS}^j\}$  протекания аварии CrEI, реализуемый в виде последовательности следующих событий:  $S_{CrS}^1$  – нарушение функционирования технологического оборудования критической системы из состава КИ;  $S_{CrS}^2$  – негативное событие, возникающее вследствие ошибочных действий обслуживающего персонала КС;  $S_{CrS}^3$  – уязвимость IT-компонентов КС;  $S_{CrS}^4$  – условие нарушения функционирования КЭИ, возникающее как результат совместного влияния нескольких негативных факторов и т.д. Предлагаемый метод реализуется в виде систематизированной последовательности шагов.

**Построение структурно-логической схемы протекания аварии КЭИ.** На первом шаге для известного сценария S строится структурно-логическая схема (СЛС) типа «нарушение-уязвимость» (рис. 1), которая отображает общий характер протекания первого этапа аварии.

На схеме (см. рис. 1), источник уязвимости, состояние которого влияет на безопасность КЭИ, изображен в форме эллипса; нарушения в функционировании стандартных операционных процедур отме-

чены прямоугольником. С помощью СЛС устанавливается последовательность и хронология событий. Однако, этой информации недостаточно для выполнения причинно-следственной декомпозиции. Поэтому на следующем шаге предлагается выполнить информационный анализ дополнительных факторов влияния и учесть их посредством построения таксономии аварии КЭИ.

**Построение таксономической схемы аварии КЭИ.** С целью детализации классификационных признаков дополним СЛС (рис. 1) таксономической схемой (ТКС) протекания аварии. На формальном уровне построению ТКС предшествует теоретическое представление объекта исследования в виде

$$TM = \{CrEIS, CrSS, CrEIF, CrEIR, CrSF, CrSR\}, \quad (1)$$

где  $CrEIS = \{CrEIS_i\}_{i=1}^N$  – множество основных технических состояний, в которых КЭИ выполняет заданные функции;

$CrSS = \{CrSS_j\}_{j=1}^M$  – подмножество технических состояний КС, влияющих на выполнение КЭИ заданных функций, т.е.  $CrSS \subset CrEIS$ ;

$CrEIF = \{CrEIF_p\}_{p=1}^Q$  – множество состояний отказов, неисправностей КЭИ;

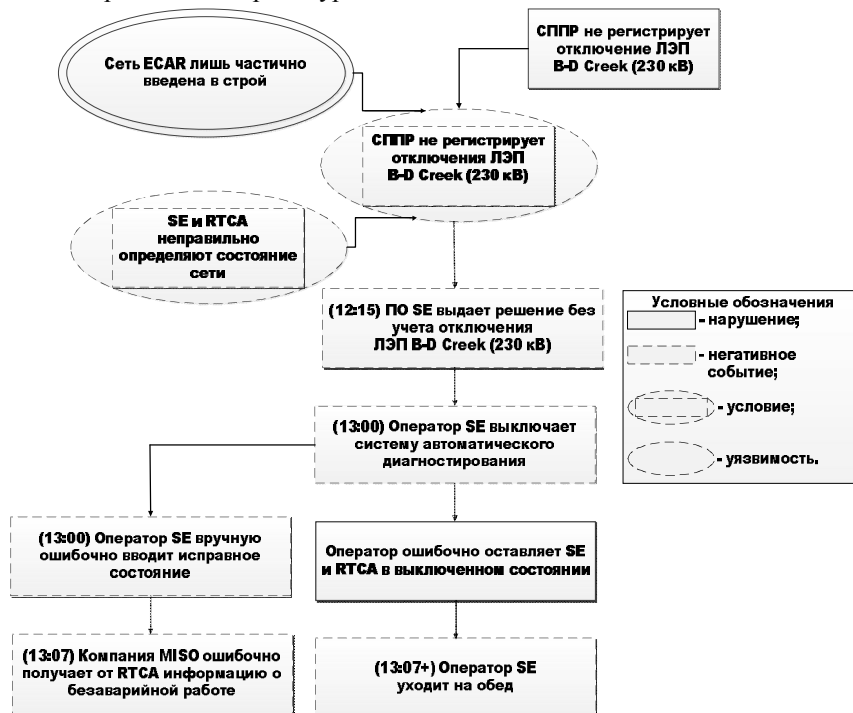


Рис. 1. Структурно-логическая схема протекания первого этапа Blackout

$CrEIR = \{CrEIR_d\}_{d=1}^U$  – множество состояний, в которых реализуется процесс восстановления КЭИ, влияющих на выполнение КЭИ заданных функций;

$CrSF = \{CrSF_g\}_{g=1}^H$  – множество состояний уязвимостей для ИТ-компонентов, нарушений и отказов технологического оборудования КС;

$CrSR = \{CrSR_z\}_{z=1}^V$  – множество состояний, в которых реализуется процесс восстановления КС, влияющих на выполнение КЭИ заданных функций.

Учет соответствующих классификационных признаков в сочетании с детальным анализом внутренних, внешних объективных и субъективных факторов негативного влияния на процессы функционирования КЭИ (КС) позволяет построить таксономическую схему протекания аварии (Blackout, 2003 г.), изображенную на рис. 2.

На следующем этапе строится автоматная модель аварии с использованием алгебры причинно-следственных комплексов (ПСК).

**Разработка причинно-следственного комплекса аварии КЭИ.** В соответствии с принципами построения, изложенными в [1, 3], структурно-логическая схема (см. рис. 1), дополненная таксономией последовательности негативных событий для КС (см. рис. 2), трансформируется в схему ПСК

протекания аварии критической ЭИ. В частности, на рис. 3 изображена схема ПСК протекания первого этапа Blackout 2003 г.

Для получения результирующих соотношений, элементарные звенья причинно-следственных связей (ПСС) (см. рис. 3) рассматриваются как модели трех простейших операций:  $\omega$  – совмещения,  $h$  – преобразования,  $\kappa$  – расщепления [1]. Операции композиции звеньев реализуются на основе отождествления узлов. Каждая операция композиции дает новую структуру взаимосвязей звеньев [5]. Охарактеризуем их.

1. Для рассматриваемой структуры первое и второе звенья (см. рис. 3) представляют собой стандартную операцию ( $O_2$ ) для параллельного соединения звеньев ПСС по группам причины и следствия, которая определяется тождеством  $v_1 \equiv \beta_2$ . А именно, для первого и второго звена  $O_2(H_1, H_2)$  определяются следующие операторы:

1.1)  $\omega_3(\alpha_1, \alpha_2)$  – причина;  $\beta_1$  – условие 1;

1.2)  $\omega_4(\eta_1, pr_1(\kappa_2(h_2(\omega_2(\alpha_2, \beta_2^*))))))$  – следствие;  $pr_2(\kappa_2(h_2(\omega_2(\alpha_2, \beta_2^*))))$  – условие 2 при  $\beta_2^* = pr_2(\kappa_1(h_1(\omega_1(\alpha_1, \beta_1))))$ .

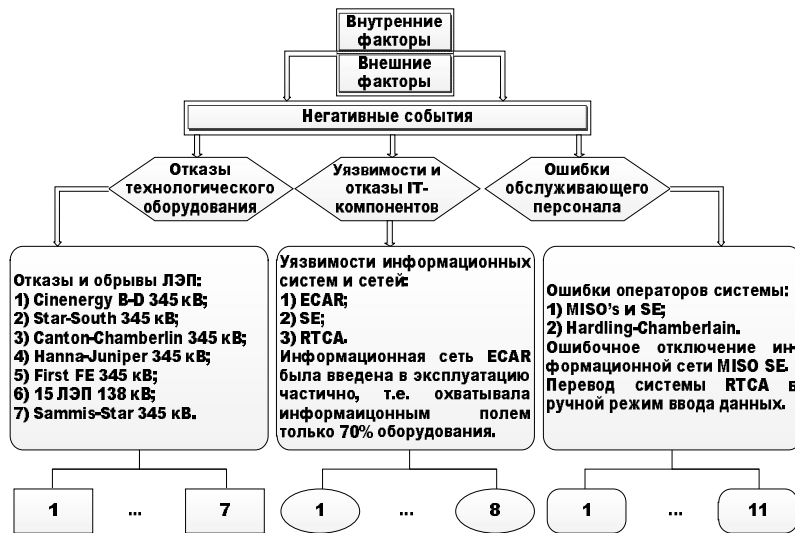


Рис. 2. Таксономия аварии Blackout

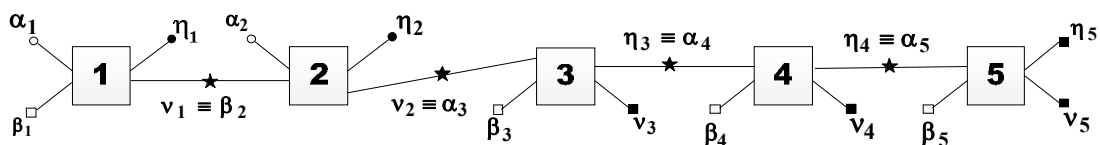


Рис. 3. Общая схема ПСК протекания первого этапа Blackout

2. Свертка первого и второго звеньев с третьим звеном представляют собой стандартную операцию ( $O_3$ ) для параллельного соединения звеньев ПСС по группам причины и следствия, которая определяется тождеством  $v_1 \equiv \alpha_2$ . Для этих звеньев  $O_3(H_1, H_2)$  задаются следующие операторы:

2.1)  $\alpha_1$  – причина;  $\omega_3(\beta_1, \beta_2)$  – условие 1;

2.2)  $\omega_4(\text{pr}_1(\kappa_2(h_2(\omega_2(\alpha_2^*, \beta_2))))))$  – следствие;  $\text{pr}_2(\kappa_2(h_2(\omega_2(\alpha_2^*, \beta_2))))$  – условие 2 при  $\alpha_2^* = \text{pr}_2(\kappa_1(h_1(\omega_1(\alpha_1, \beta_1))))$ .

3. Для рассматриваемой структуры свертка первого, второго, третьего звеньев и четвертое звено представляют собой стандартную операцию ( $O_1$ ) для параллельного соединения звеньев ПСС по группам причины и следствия, которая определяется тождеством  $\eta_1 \equiv \alpha_2$ . А именно в звене  $O_1(H_1, H_2)$ , для свертки первого, второго, третьего звеньев и четвертого звена определяются следующие операторы:

3.1)  $\alpha_1$  – причина;  $\omega_2(\beta_1, \beta_2)$  – условие 1;

3.2)  $\beta_1$  – условие 1;  $\text{pr}_1(\kappa_2(h_2(\text{pr}_1(\kappa_1(h_1(\omega_1(\alpha_1, \beta_1)))))))$  – следствие;  $\omega_4(v_1, v_2)$  – условие 2.

4. Свертка первого, второго, третьего, четвертого и пятого звеньев представляет собой стандартную операцию ( $O_1$ ) и записывается по аналогии с пунктом 3.

Записанная таким образом математическая интерпретация ПСК позволяет: а) устранить неопределенность и систематизировать взаимосвязи, взаимодействие компонентов (КС), процессов для рассматриваемой критической инфраструктуры; б) использовать звенья ПСС (см. рис. 3) для перехода к аналитико-стохастическому моделированию.

**Аналитико-стохастическое моделирование аварии КЭИ.** Воспользуемся структурированными, логически обоснованными связями между звеньями ПСС (см. рис. 3) для построения полумарковской модели протекания аварии. Построение модели реализуем в два этапа.

На первом этапе с использованием полученной схемы ПСК устанавливается последовательность логических переходов, на основе которой строится ситуационный граф состояний. В качестве наглядного примера рассмотрим схему, представленную на рис. 3, для которой запишем следующую последовательность логических переходов (ПЛП):

1)  $\beta_1 \rightarrow v_1 \equiv \beta_2 \rightarrow v_2 \equiv \alpha_3 \rightarrow \eta_3 \equiv \alpha_4 \rightarrow \eta_4 \equiv \alpha_5 \rightarrow \eta_5$  ;

2)  $\alpha_1 \rightarrow \eta_1$  ,  $\alpha_2 \rightarrow \eta_2$  ;

3)  $\beta_3 \rightarrow v_3$  ,  $\beta_4 \rightarrow v_4$  ,  $\beta_5 \rightarrow v_5$  .

Охарактеризуем каждую из полученных последовательностей. Как мы видим, первая последовательность реализуется в виде структуры причинно-следственных звеньев и комплексов (ПСК1) [3]. Вторая группа переходов представлена причинно-следственными звеньями  $\alpha_1 \rightarrow \eta_1$  (ПС31) и  $\alpha_2 \rightarrow \eta_2$  (ПС32) без учета групп условий. Напротив, третья группа переходов представлена условными звеньями  $\beta_3 \rightarrow v_3$  (УЗ3),  $\beta_4 \rightarrow v_4$  (УЗ4),  $\beta_5 \rightarrow v_5$  (УЗ5) без учета групп причин и следствий.

Каждая из указанных групп ПЛП описывает конкретные ситуации развития аварии КЭИ и может быть использована для реализации следующего этапа аналитико-стохастического моделирования.

На втором этапе с использованием полученных ПЛП строятся марковские (ММ), полумарковские модели (ПММ) для последовательности негативных событий с участием различных КС, и выполняется оценка показателя функциональной безопасности (ФБ) КЭИ.

В качестве показателя ФБ предлагается использовать коэффициент готовности КИ ( $K_{ГКЭИ}$ ), значение которого определяется с использованием следующего соотношения:

$$K_{ГКЭИ} = \prod_{j=1}^m K_{Гj} , \quad (2)$$

где  $j=1, \dots, m$  – совокупность КС из состава КЭИ, подверженных воздействию  $i$ -й последовательности негативных событий;  $K_{Гj}$  – коэффициент готовности  $j$ -й КС из состава КЭИ.

Результаты оценки КГ критических систем из состава КЭИ для различных законов распределений отказов, неисправностей, уязвимостей технологического оборудования и ИТ-компонентов представлены на рис. 4

После выполнения аналитико-стохастического моделирования, являющегося достаточно трудоемким и сложным с математической точки зрения процессом, целесообразно разработать аппарат логико-цифрового представления результатов причинно-следственной декомпозиции.

**Логико-цифровое представление результатов причинно-следственной декомпозиции аварии КЭИ.** Необходимость реализации данного шага связана со стремлением авторов разработать соответствующую информационную технологию, которую можно было бы использовать в различных сферах применения КИ. Логической основой аппарата цифрового представления результатов причинно-следственной декомпозиции аварии КЭИ является использование уникальных свойств операции сум-

мирования по модулю два, что фактически позволяет получить коды для разработанных ПСК, ПСЗ и УЗ (рис. 5).

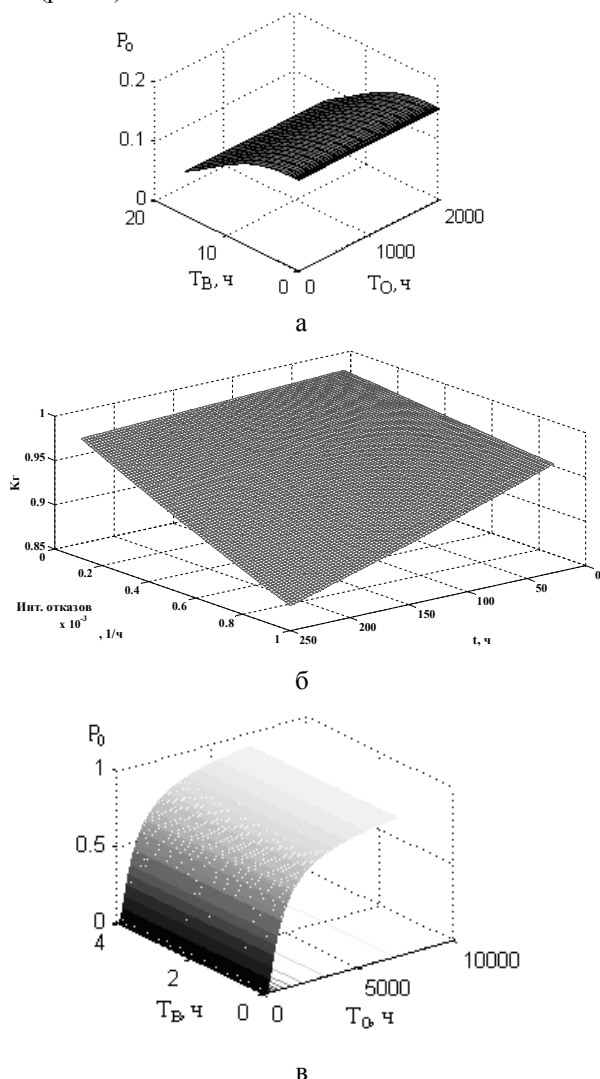


Рис. 4. Зависимости  $K_T = P_0(\lambda, T)$  для ПММ КС

Ниже представлены результаты выполнения этой операции.

1. Для ПСЗ1 и ПСЗ2, соответственно, получаем следующие значения:  $\alpha_1 \oplus \eta_1 = 0$ ,  $\alpha_2 \oplus \eta_2 = 0$ .

2. Для УЗ3, УЗ4, УЗ5, соответственно, справедливы следующие выражения вида:  $\beta_3 \oplus v_3 = 0$ ,  $\beta_4 \oplus v_4 = 0$ ,  $\beta_5 \oplus v_5 = 0$ .

3. Для ПСК1 получаем следующие соотношения:  $\beta_1 \oplus v_1 = 0$ ,  $\beta_2 \oplus v_2 = 1$ ,  $\alpha_3 \oplus \eta_3 = 0$ ,  $\alpha_4 \oplus \eta_4 = 1$ ,  $\alpha_5 \oplus \eta_5 = 0$ .

Схемы суммирования по модулю два представлены на рис. 5. Результатом сложения являются следующие кодовые последовательности:

1) 00010 – код причинно-следственного комплекса ПСК1;

2) 01000 – код для причинно-следственных

звеньев ПСЗ1 и ПСЗ2, условных звеньев УЗ3, УЗ4 и УЗ5.

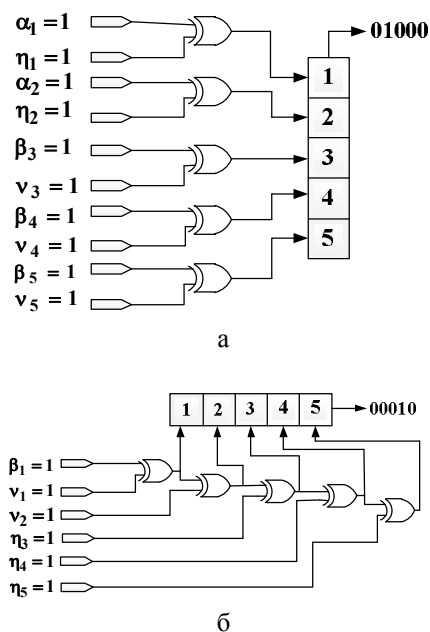


Рис. 5. Схемы логико-цифрового представления: а – ПСЗ1, ПСЗ2, УЗ3, УЗ4 и УЗ5; б – ПСК1

Не составляет труда заметить, что при изменении конфигурации ПСК, ПСЗ и УЗ изменяются кодовые последовательности, что свидетельствует о чувствительности предложенной операции для решения задач причинно-следственной декомпозиции аварий и инцидентов КИ.

## Заключение

Комплексное использование разработанного авторами метода для решения задач декомпозиции событий на основе алгебры причинно-следственных комплексов позволяет получить формализованное описание аварии КИ и построить таким образом математическую модель ее протекания с применением как детерминистского, так и стохастического подходов.

Перспективы дальнейших исследований связаны с разработкой: а) метода инфраструктурной компаративистики, который может базироваться в том числе и на моделях ПСК; б) модельного ряда с целью получения количественных оценок безопасности; в) информационных технологий обеспечения безопасности КИ.

## Литература

1. *Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения [Текст]/ Под ред. В. С. Харченко. – Министерство образования и науки Украины, На-*

циональный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», 2011. – 641 с.

2. U.S.-Canada power system outage task force: final report on the August, 14, 2003 Blackout in the United States and Canada: causes and recommendations [Текст] / April 2004. – 228 p.

3. Резчиков, А. Ф. Принцип причинно-следственной декомпозиции динамических систем [Текст] / А. Ф. Резчиков, В. А. Твердохлебов. – Саратов : ООО Издательский Центр «Наука», 2013. – 56 с.

Поступила в редакцию 12.02.2014, рассмотрена на редколлегии 24.03.2014

**Рецензент:** д-р техн. наук, проф. А. А. Серков, Национальный технический университет «ХПИ», Харьков, Украина.

## МЕТОД ПРИЧИННО-НАСЛІДКОВОЇ ДЕКОМПОЗИЦІЇ АВАРІЙ ТА ІНЦИДЕНТІВ КРИТИЧНИХ ІНФРАСТРУКТУР

*О. В. Іванченко, В. С. Харченко*

Викладається систематизована послідовність кроків, які необхідно реалізувати для вирішення завдання декомпозиції подій, котрі спостерігаються під час аварій та інцидентів критичних інфраструктур (КІ). Розглянуто можливість застосування алгебри причинно-наслідкових комплексів для побудови автоматної та стохастичної моделей каскадних відмов компонентних складових КІ. Представлено таксономію і структурно-логічну схему сукупності негативних подій, які спостерігалися під час аварії Північно-Американської енергетичної інфраструктури, котрі слід розглядати як композиційну основу причинно-наслідкових ланцюгів розроблених моделей.

**Ключові слова:** критична інфраструктура, каскадні відмови, таксономія, причинно-наслідкові ланцюги.

## METHOD OF CAUSAL AND COSEQUENCE CRITICAL INFRASTRUCTURES DECOMPOSITION OF ACCIDENTS AND INCIDENTS

*O. V. Ivanchenko, V. S. Kharchenko*

The systematic sequence of steps describe that should be implemented to solve the task of decomposition of different events observed during the accidents and incidents of critical infrastructure (CI). The possibility of using algebra causal and consequence complexes in order to build an automaton and stochastic models of cascading failures of the critical infrastructures components. Presented taxonomy and structural logic of the aggregate negative events, which we observed during the accident of the North American energy infrastructure. These negative events constituted the basis of a composite causal links is being developed models.

**Keywords:** critical infrastructure, cascading failures, taxonomy, causal and consequence links.

**Іванченко Олег Васильевич** – канд. техн. наук, доцент, доцент кафедри кібернетики и вычислительной техники, Севастопольский национальный технический университет, Севастополь, Украина, e-mail: vmsu12@gmail.com.

**Харченко Вячеслав Сергеевич** – д-р техн. наук, профессор, Заслуженный изобретатель Украины, зав. кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: v.kharchenko@khai.edu.