УДК 614.84
DOI: 10.12737/2773

Особенности обеспечения безопасности критических инфраструктур

Н.А. Махутов, *главный научный сотрудник, чл.-корр. РАН, д-р техн. наук*
Д.О. Резников, *ведущий научный сотрудник, канд. техн. наук*
В.П. Петров, *ведущий научный сотрудник, канд. техн. наук*

Институт машиноведения им. А.А.Благонравова Российской академии наук, г. Москва

e-mail: mibsts@mail.ru

Ключевые слова:
критические инфраструктуры,
риск,
безопасность,
запроектное воздействие,
устойчивость.

В статье рассматривается ряд особенностей критических инфраструктур, которые определяют дополнительные требования к обеспечению их безопасности. Обоснована необходимость дополнить традиционные подходы к обеспечению защищенности критических инфраструктур по отношению к проектным воздействиям комплексом мер, направленных на обеспечение их устойчивости к запроектным воздействиям. Рассматриваются способы проведения количественной оценки устойчивости критических инфраструктур.

1. Введение

Критические инфраструктуры (энергетические, транспортные, телекоммуникационные, кредитно-финансовые системы, системы газо- и водоснабжения) представляют собой сложные, пространственно распределенные, многокомпонентные системы, устойчивая работа которых критически важна для функционирования экономики и жизнедеятельности людей. Критические инфраструктуры (далее КИ) имеют многоуровневую структуру, которая включает: уровень технических компонентов (машины, оборудование и аппаратура); социальный уровень (персонал, обслуживающий технические компоненты КИ); организационный уровень (взаимодействие служб компании, эксплуатирующей КИ) и уровень государственного управления (нормативные и контролирующие органы, осуществляющие надзор и государственное регулирование в сфере деятельности КИ). Сложность критических инфраструктур обусловливается: 1) сложностью их структуры (сложными взаимозависимостями и нелинейными связями между компонентами и уровнями системы, а также между различными КИ); 2) сложным характером явлений и процессов, имеющих место в ходе эксплуатации КИ (рис. 1) [1].

Элементы КИ представляют собой технические объекты, на которых осуществляются хранение, переработка/преобразование или транспортировка/передача опасных веществ, энергии и/или информационных потоков. Эти объекты могут служить источниками тяжелых аварий и катастроф, являющихся предметом традиционного анализа рисков, на основе которого строятся карты рисков для территорий размещения объектов критических инфраструктур и принимаются решения о строительстве или модернизации КИ.

Наличие тесных взаимосвязей между компонентами КИ является их принципиально важной осо-

Рис. 1. Структура взаимосвязей между элементами критических инфраструктур [20]

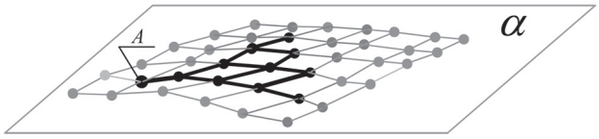

Рис. 2. Внутриинфраструктурный каскад отказов в критической инфраструктуре α. Каскад инициируется отказом элемента *A* и развивается далее по инфраструктуре, вызывая отказы выделенных черным цветом элементов

бенностью, которая оказывает определяющее влияние на характер их функционирования в штатных и нештатных ситуациях. С одной стороны, связанность элементов КИ повышает их эффективность, позволяя рационально использовать и перераспределять имеющиеся ресурсы и мощности, а с другой — делает их склонными к крупномасштабным катастрофам, огромный размер ущерба от которых не позволяет пренебрегать ими, несмотря на низкую вероятность реализации рисков.

Ключевым понятием в теории риска является понятие стохастической (вероятностной) зависимости. Это понятие рассматривается при оценке эффективности системы защитных барьеров. Два события *A* и *B* считаются вероятностно несвязанными, если вероятность события *A* не зависит от того, произошло ли событие *B*. Математически это может быть представлено с помощью выражения $\Pr(A \mid B) = \Pr(A)$. Наличие стохастической зависимости между событиями *A* и *B*, напротив, означает, что вероятность

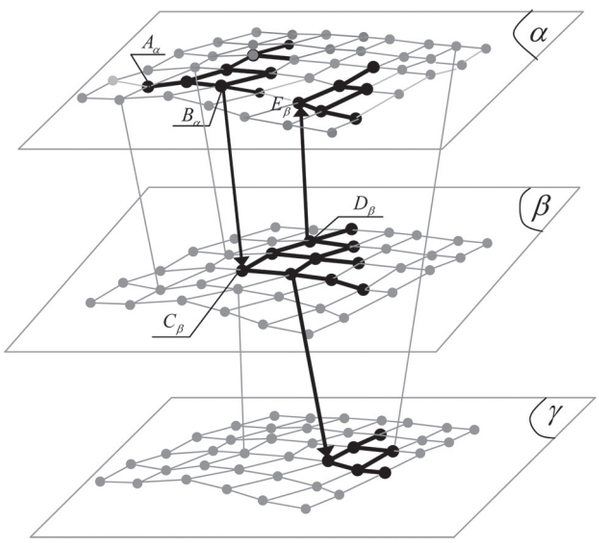

Рис. 3. Сценарий межинфраструктурного каскада в системе КИ. Каскад инициируется отказом компонента A_α и распространяется по инфраструктуре α до компонента B_α, отказ которого вследствие наличия межинфраструктурных связей приводит к отказу элемента C_β и инициации каскада в инфраструктуре β, с последующим распространением каскада на инфраструктуру γ

реализации события *A* изменяется, если появляется информация о том, что произошло событие *B*: $\Pr(A \mid B) \neq \Pr(A)$.

Особую роль в теории риска имеет положительная зависимость, при которой реализация события *B* повышает вероятность события *A*. Для инфраструктурных систем наличие положительной корреляционной связи особенно характерно, поскольку после отказа одного из элементов инфраструктуры и перенесения нагрузки, которую нес этот элемент, на смежные с ним элементы вероятность последующих отказов дополнительно нагруженных элементов возрастает.

Применительно к анализу рисков взаимосвязанных инфраструктурных систем приходится иметь дело с двухсторонними зависимостями между компонентами КИ, поэтому принято говорить о взаимозависимости элементов КИ. Причем эти взаимозависимости существуют как для элементов, принадлежащих к одной инфраструктуре, так и для элементов, относящихся к различным инфраструктурам. В последнем случае говорят о взаимозависимостях между различными КИ. Соответственно различают каскадные сценарии, реализующиеся внутри отдельных инфраструктур (рис. 2), и межинфраструктурные каскады (рис. 3), которые (благодаря наличию межинфраструктурных связей) могут распространяться по всей совокупности инфраструктурных систем и приводить к коллапсу в целом регионе.

Наличие сильных связей между элементами КИ делает их склонными к каскадным сценариям аварий, которые охватывают множество объектов инфраструктуры, причем ход реализации аварии определяется структурой связей между элементами. Помимо масштабов потенциальных аварий, наличие внутри- и межинфраструктурных зависимостей оказывает определяющее влияние на динамику распространения аварий, приводя к реализации комбинированных механизмов достижения предельных состояний, резкой интенсификации процессов деградации и потоку отказов элементов КИ.

Из-за сложной структуры КИ и сложного характера взаимодействий между значительным числом элементов возможности проведения сценарного анализа с помощью традиционного инструментария (деревьев событий, деревьев отказов, байесовых сетей) оказываются ограниченными. Для описания развития возмущений в критических инфраструктурах применяются сетевые модели, активно использующие математический аппарат теории графов. Сети представляют собой чрезвычайно гибкую абстракцию, которая может широко применяться при изучении инфраструктурных систем. При этом может

быть построена иерархия математических моделей различной сложности, позволяющих описать различные аспекты рисков инфраструктурных систем по отношению к возможным инициирующим воздействиям. С помощью указанных моделей удается описать многие свойства и особенности сетевых систем: хаос, самоорганизация, степенные распределения, критичность.

Принято выделять три типа взаимозависимостей между компонентами инфраструктурных систем, которые могут иметь место между компонентами как одной инфраструктуры, так и различных инфраструктур.

Физические взаимосвязи, которые имеют место, когда вещество, энергия или информация физически передается от одного компонента к другому компоненту (той же или другой) инфраструктуры. При этом выходной продукт, создаваемый или перерабатываемый одной инфраструктурой, используется как входной продукт компонентом другой инфраструктуры. Например, железнодорожная инфраструктура и электрогенерирующая сеть взаимосвязаны между собой физически, поскольку уголь, перевозимый по железной дороге, является исходным сырьем для генерации электроэнергии. При этом существует и обратная физическая зависимость, поскольку генерируемая электроэнергия потребляется локомотивным парком. Очевидно, что аварии в компонентах одной КИ могут вызвать каскады отказов, распространяющиеся на компоненты другой КИ.

Кибервзаимозависимости. КИ является информационно зависимой, если состояние ее элементов зависит от информации, передаваемой по телекоммуникационной сети. В связи с быстрым развитием информационных технологий система управления энергосистемой или система распределения вагонов железнодорожной инфраструктуры зависят от качества работы телекоммуникационной сети.

Территориальные взаимозависимости – инфраструктуры, компоненты которых размещаются территориально в непосредственной близости друг от друга, могут испытывать непосредственное воздействие при ЧС на компонентах другой инфраструктуры.

Особенность современных КИ в том, что они становятся трансграничными, а в ряде случаев — глобальными. Пространственная протяженность КИ, наряду с наличием тесных взаимосвязей между ними, делает их функционирование зависящим от огромного количества факторов, связанных с состоянием природно-техногенно-социальной среды в различных регионах мира. Значительный объем опасных веществ, энергии и информации, которые хранятся, транспортируются и перерабатываются критическими инфраструктурами, а также их огромная роль в экономике и жизни людей обусловливают возможность крупномасштабных аварий на КИ и тяжесть последствий, возникающих при таких авариях для населения и объектов экономики. Сложность критических инфраструктур значительно затрудняет создание эффективных систем защиты, поскольку становится практически невозможно провести детальный сценарный анализ системы, выявить все значимые опасные сценарии и определить набор мер и барьеров защиты, направленных на парирование всех возможных угроз.

Вместе с тем анализ сложившейся практики в сфере функционирования КИ свидетельствует, что их проектирование, строительство и эксплуатация осуществляются в соответствии с традиционной парадигмой обеспечения безопасности технических систем (ТС). Эта парадигма предполагает:

а) анализ возможных сценариев развития отказов в системе;
б) идентификацию наиболее значимых сценариев;
в) создание защитных барьеров, направленных на предупреждение этих сценариев.

Структурная сложность КИ, их исключительно важная роль в жизнедеятельности людей и функционировании экономики, а также тяжесть последствий, которые неизбежно возникают в случае аварий на КИ, должны определить особый порядок и специальные требования в сфере обеспечения их безопасности. Современные тенденции в сфере обеспечения безопасности критических инфраструктур предполагают формирование новой парадигмы, которая должна дополнить традиционные усилия по обеспечению безопасности КИ системой мер, направленных на повышение их устойчивости к возможным экстремальным воздействиям [10, 12, 13].

2. Проведение сценарного анализа для технических систем

2.1. Традиционный подход

Выполнение традиционного сценарного анализа для технических систем предполагает последовательный анализ:

- угроз, которым подвергается система;
- уязвимости системы по отношению к выявленным угрозам;
- ущерба от аварий, реализующихся, если система оказалась уязвимой к действующим на нее угрозам (рис. 4) [1, 2, 18].

Траекторию в пространстве состояний, описывающую эволюцию системы от исходного состояния *НС* до требуемого конечного состояния $КС_0$, принято называть сценарием успеха

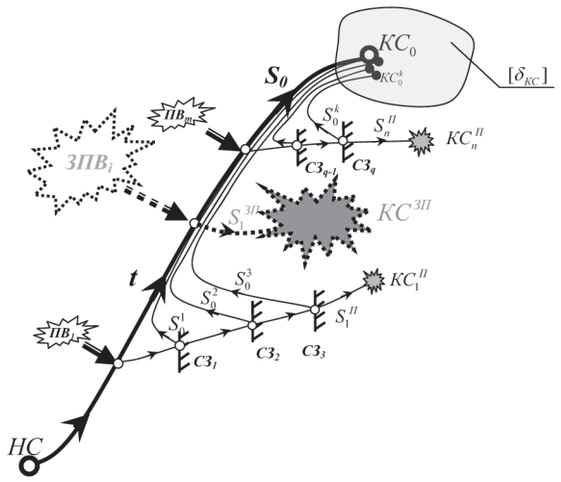

Рис. 4. Сценарное «дерево» ТС, содержащее сценарии проектных ($S_1^П$ и $S_n^П$) и запроектных ($S_1^{ЗП}$) катастроф
HC – начальное состояние системы, KC_0 – заданное конечное состояние системы, $[\delta_{KC}]$ – область допустимых конечных состояний, $ПВ_i$ – проектные воздействия на систему, $ЗПВ_j$ – запроектные воздействия на систему, KC_0^k – допустимые конечные состояния, в которые система приходит в случае срабатывания систем защиты $СЗ_l$, S_0 – заданный сценарий успеха, $S_j^П$ – проектные сценарии аварий, $S_j^{ЗП}$ – запроектные сценарии аварий, $KC_j^П$ – конечные состояния проектных аварий, $KC^{ЗП}$ – конечное состояние запроектной аварии

S_0 (рис. 4). В ходе эксплуатации система может быть подвержена проектным воздействиям $ПВ_i$ $(i=1,2,...,m)$, которые способны отклонить траекторию сценария успеха S_0, запуская тем самым последовательность событий, соответствующих сценариям проектных аварий $S_j^П (j=1,2,...,n)$. Такие сценарии реализуются, если не сработают системы защиты $СЗ_k$ $(k=1,2,...q)$, и будут приводить к достижению системой соответствующих конечных состояний проектных аварий $KC_1^П, KC_2^П, \ldots, KC_n^П$. В случае успешного срабатывания систем защиты система будет возвращаться на траектории S_0^k $(k=1,2,...,p)$, близкие к сценарию успеха S_0. Конечные состояния KC_0^k, соответствующие этим сценариям и попадающие в область допустимых конечных состояний $[\delta_{KC}]$, будут считаться тождественными заданному конечному состоянию KC_0.

На первом шаге сценарного анализа проводится оценка угроз для ТС, предполагающая составление закрытого/исчерпывающего перечня воздействий $ПВ_1, ПВ_2, ..., ПВ_m$, которым может быть подвергнута система в течение срока ее эксплуатации. Воздействия, включенные в этот перечень, принято называть проектными. К ним относят эксплуатационные нагрузки, отказы элементов системы, внешние экстремальные воздействия, ошибки операторов, несанкционированные воздействия на систему и т.д. Далее оценивается мера возможности реализации проектных воздействий. В простейшей постановке угроза неблагоприятного воздействия может характеризоваться вероятностью его реализации. Тогда сводной характеристикой угроз, которым подвергается рассматриваемая система, будет вектор проектных угроз $\overline{H^П}$. Его компонентами будет вероятности реализации различных проектных воздействий:

$$\overline{H^П} = \left\{P(ПВ_1); P(ПВ_2); ...; P(ПВ_m)\right\}.$$

Уязвимость системы характеризуется совокупностью сценариев случайных событий (отказов в системе) и причинно-следственных связей между этими событиями, т. е. структурой сценарного графа системы [2, 5, 6, 11, 12]. Обобщенными характеристиками уязвимости системы будут условные вероятности реализации различных конечных состояний системы, возникающих в случае эскалации аварии, развивающейся в системе вследствие идентифицированных в ходе анализа угроз проектных воздействий на систему. Анализ уязвимости предполагает исследование последовательности событий и причинно-следственных связей между событиями, происходящими вслед за проектным воздействием вплоть до достижения системой возможных конечных состояний. Иными словами, анализ уязвимости системы заключается в проведении качественного и количественного исследования структуры сценариев эскалации аварии. Таким образом, анализ уязвимости предполагает детальное изучение «дерева» сценариев рассматриваемой системы. Рассматриваемые в ходе анализа уязвимости сценарии принято называть проектными, а соответствующие им конечные состояния ТС – проектными. Соответственно вводится и понятие проектной уязвимости. Принципы построения сценарных «деревьев», описывающих сценарии эскалации аварий, подробно изучаются в рамках *теории структурирования сценариев*. Среди подходов этой теории центральное место занимают методы, базирующиеся на построении графовых моделей типа «дерево» событий, «дерево» отказов и байесовых сетей, описывающих вероятностные причинно-следственные связи между событиями в процессе эскалации аварии. Тогда уязвимость системы к проектным воздействиям может быть описана с помощью матрицы, компоненты $V_{i,j}^П$ которой будут представлять собой условные вероятности достижения системой конечного состояния $KC_i^П$ $(i=0,1,2,...,n)$ при условии, что система была подвергнута проектным воздействиям $ПВ_j$ $(j=1,2,...,m)$: $V_{i,j}^П = P[KC_i \mid ПВ_j]$:

$$\overline{\overline{\mathbf{V}^{\Pi}}} = \begin{bmatrix} P[KC_0^{\Pi}|\Pi B_1] & P[KC_1^{\Pi}|\Pi B_1] & P[KC_2^{\Pi}|\Pi B_1] \cdots P[KC_m^{\Pi}|\Pi B_1] \\ P[KC_0^{\Pi}|\Pi B_2] & P[KC_1^{\Pi}|\Pi B_2] & P[KC_2^{\Pi}|\Pi B_2] \cdots P[KC_m^{\Pi}|\Pi B_2] \\ P[KC_0|\Pi B_3] & P[KC_1|\Pi B_3] & P[KC_2^{\Pi}|\Pi B_3] \cdots P[KC_m|\Pi B_3] \\ & & \bullet \ \bullet \ \bullet \\ P[KC_0^{\Pi}|\Pi B_m] & P[KC_1^{\Pi}|\Pi B_m] & P[KC_2^{\Pi}|\Pi B_m] \cdots P[KC_m^{\Pi}|\Pi B_m] \end{bmatrix}$$

Реализация определенного сценария проектной аварии S_i^{Π} приводит к достижению системой соответствующего проектного конечного состояния KC_i^{Π}, сопряженного с ущербом $U(KC_i^{\Pi})$ [1, 3, 4, 19]. При этом *ущерб* от аварии на ТС как результат изменения состояния системы может иметь разное выражение — нарушение ее целостности или ухудшение других свойств; фактические или возможные экономические и социальные потери (отклонение здоровья человека от среднестатистического значения, т.е. его болезнь или смерть; нарушение процесса нормальной хозяйственной деятельности; утрата того или иного вида собственности; ухудшение природной среды и т.д.), возникающие в результате каких-то событий, явлений, действий; полная или частичная потеря здоровья либо смерть человека; утрата имущества или других материальных, культурных, исторических или природных ценностей.

Произведя последовательно оценку угроз, уязвимости и ущербов для ТС, можно оценить индексы дифференциальных рисков реализации различных проектных сценариев S_i^{Π}:

$R(S_i^{\Pi}) = P(\Pi B_j) \cdot P(KC_i|\Pi B_j) \cdot U(KC_i^{\Pi})$ для рассматриваемой системы с помощью трехфакторной модели «угроза—уязвимость—последствия».

Далее может быть оценен индекс проектного риска для рассматриваемой системы:

$$R_{\Sigma}^{\Pi} = \overline{H^{\Pi}} \cdot \overline{\overline{\mathbf{V}^{\Pi}}} \cdot \overline{U^{\Pi}},$$

где $\overline{H^{\Pi}} = \{P(\Pi B_1); P(\Pi B_2); ...; P(\Pi B_m)\}$ — вектор проектных угроз, компонентами которого являются вероятности реализации проектных воздействий ΠB_1, ΠB_2, ...; ΠB_m;

$\overline{\overline{\mathbf{V}^{\Pi}}} = \left[P(KC_i|\Pi B_j)\right]$ — матрица уязвимости, компоненты которой представляют собой вероятности реализации возможных поврежденных состояний KC_i^{Π} при условии оказания на систему различных проектных воздействий ΠB_j;

$\overline{U^{\Pi}} = \{U(KC_0^{\Pi}), U(KC_1^{\Pi}), U(KC_2), \cdots, U(KC_n)\}^T$ — вектор проектных ущербов, компонентами которого являются величины ущербов, соответствующих проектным конечным состояниям KC_0, KC_1^{Π}, KC_2^{Π}, ... , KC_n^{Π}.

Или в развернутой форме:

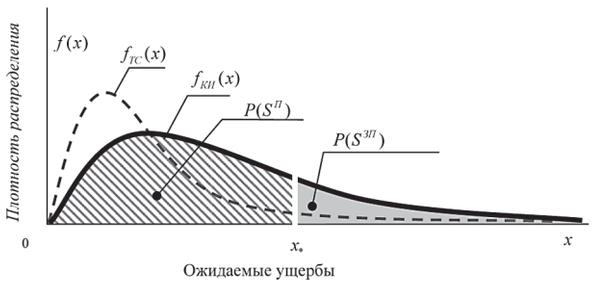

Рис. 5. Характер распределений ущербов для обычных технических систем и критических инфраструктур
$f_{ТС}(x)$ – функция плотности распределения ущерба для обычных технических систем; $f_{КИ}(x)$ – функция плотности распределения ущерба для КИ; $P(S^{\Pi})$ – вероятность реализации проектных сценариев для КИ; $P(S^{З\Pi})$ – вероятность реализации запроектных сценариев для КИ; x_* – пороговое значение экстремальных ущербов

$$R_{\Sigma}^{\Pi} = \underbrace{\{P(\Pi B_1); P(\Pi B_2); \ldots; P(\Pi B_m)\}}_{\text{Угрозы } \overline{H}} \times$$
$$\times \underbrace{\begin{bmatrix} P[KC_0|\Pi B_1] & P[KC_1^{\Pi}|\Pi B_1] & \cdots & P[KC_n^{\Pi}|\Pi B_1] \\ P[KC_0|\Pi B_2] & P[KC_1^{\Pi}|\Pi B_2] & \cdots & P[KC_n^{\Pi}|\Pi B_2] \\ & \ldots & & \\ P[KC_0|\Pi B_m] & P[KC_1^{\Pi}|\Pi B_m] & \cdots & P[KC_n^{\Pi}|\Pi B_m] \end{bmatrix}}_{\text{Уязвимость } \mathbf{V}} \times \underbrace{\begin{Bmatrix} U(KC_0) \\ U(KC_1^{\Pi}) \\ \ldots \\ U(KC_n^{\Pi}) \end{Bmatrix}}_{\text{Ущербы } \overline{U}}$$

При проведении сценарного анализа и оценки риска эксплуатации ТС необходимо иметь в виду, что в процессе эксплуатации на систему могут быть оказаны воздействия и запущены сценарии отказов, которые либо сознательно были исключены из перечня проектных, поскольку считались практически нереализуемыми, либо не были включены в рассмотрение из-за ограниченности знаний о системе и протекающих в ней и во внешней среде процессах. Подобные воздействия и инициируемые ими сценарии аварий получили название запроектных. Если не учитывать запроектные воздействия ($З\Pi B_i$) и запроектные сценарии аварий ($S_i^{З\Pi B}$), можно, с одной стороны, получить существенно заниженные оценки рисков, а с другой — разработанные для рассматриваемой ТС защитные барьеры окажутся недостаточно эффективными. Подобные ситуации особенно характерны для сложных систем, в частности для КИ.

Для сложных систем характерно наличие так называемых тяжелых хвостов распределений ущербов [4]. Это означает, что экстремальные ущербы, соответствующие запроектным авариям, в сложных системах реализуются не настолько редко, чтобы ими можно было пренебрегать (рис. 5).

2.2. Недостатки традиционного подхода

Представленный выше сценарный анализ выполняется в предположении, что для рассматриваемой системы может быть сформирован закрытый (ис-

черпывающий) перечень проектных воздействий, и изучены все возможные сценарии развития событий после каждого из этих воздействий; оценены ущербы, соответствующие всем проектным конечным состояниям. Далее выявляются наиболее катастрофичные сценарии, разрабатываются комплексы защитных мероприятий и строятся защитные барьеры, призванные предотвратить реализацию этих сценариев, тем самым обеспечив безопасность рассматриваемой ТС.

При этом делается допущение, что для рассматриваемой системы могут быть созданы закрытые перечни возможных воздействий на систему и сценариев эскалации аварии. В соответствии с этим допущением считается возможным создание комплексов защитных барьеров, обеспечивающих с требуемой достаточно высокой вероятностью блокировку сценариев проектных аварий. Этот закрытый перечень проектных воздействий включает события, происходящие при нормальной эксплуатации ТС, а также неординарные события (выход из строя различных компонентов ТС, ошибки операторов, экстремальные природные воздействия, а также несанкционированные воздействия), которые могут произойти, по крайней мере, один раз в течение цикла эксплуатации ТС.

При этом подходе ряд редких экстремальных событий, имеющих низкую вероятность реализации, но значительные последствия, выводятся за рамки рассмотрения как практически нереализуемые. Другие экстремальные события ввиду сложности системы вообще остаются неидентифицированными. Указанные события/воздействия относятся к категории запроектных. Таким образом, вопрос обеспечения безопасности ТС при запроектных воздействиях в рамках традиционного подхода не рассматривается. Однако подобные воздействия могут привести к крупномасштабным катастрофам, вызвать значительное число жертв и огромные материальные потери. Типичным примером запроектного воздействия на инженерную систему является авария на АЭС «Фукусима» — ее инициировало цунами, высота которого превышала заложенный в проекте уровень. Другим примером запроектной аварии является Чернобыльская катастрофа, причиной которой стала заранее не учтенная комбинация различных воздействий: технических отказов, ошибок операторов и нарушений на уровне управления станцией.

3. Учет особенностей критических инфраструктур при разработке стратегии обеспечения их защищенности

Современные критические инфраструктуры являются сложными техно-социальными системами, функционирование которых определяется взаимодействием технических, социальных, организационных и управленческих факторов. Традиционный подход к моделированию техно-социальных систем, широко используемый при обеспечении их безопасности, предусматривает декомпозицию системы на техническую, социальную и организационную подсистемы, которые затем рассматриваются отдельно в рамках соответствующих дисциплин. При этом не учитываются ни взаимные влияния подсистем, ни их взаимодействие на системном уровне.

Следует отметить, что усилия по защите критических инфраструктур традиционно фокусируются на технических аспектах. Благодаря этому достигнут значительный прогресс в сфере обеспечения надежности технических компонентов КИ. Однако возможности данного подхода близки к исчерпанию. Это связано с тем, что КИ более не могут рассматриваться как преимущественно технические системы, а становятся все в большей мере техно-социальными системами. Статистика чрезвычайных ситуаций на критических инфраструктурах свидетельствует о том, что в 70-90 случаях из 100 инициирующим фактором аварии являются ошибки человека, которые совершаются на этапах проектирования, строительства или эксплуатации системы. А это означает, что подобные аварии не могут быть предотвращены только путем реализации технических мер.

Благодаря бурному развитию в последние десятилетия, КИ становятся все более сложными. Это значит, что при оценке безопасности КИ появляется огромное число факторов, подлежащих учету, а некоторые режимы эксплуатации КИ становятся не полностью определенными. Это происходит вследствие сложных нелинейных взаимодействий между компонентами КИ, сильной связанности между различными подсистемами, а также того факта, что КИ и окружающая среда начинают изменяться быстрее, чем они могут быть описаны и исследованы. Поэтому возникает ситуация недостатка информации о КИ и, следовательно, ограниченности возможностей прогнозирования их поведения и управления ими. При этом на определенных режимах становится невозможно детально описать законы функционирования КИ и разработать правила управления.

Различие между полностью определенными и не полностью определенными системами становится чрезвычайно важным при разработке комплекса мер по обеспечению безопасности. Особенность не полностью определенных систем в том, что оказывается невозможным полное описание их поведения и прогнозирование их состояния при различных условиях и на различных режимах эксплуатации. Вследствие этого для таких сложных систем, как критические инфраструктуры, практически невозможно создать закрытый перечень проектных воздействий, которым система может подвергнуться в течение ее эксплуатации. В связи с этим

традиционная стратегия обеспечения безопасности КИ, основанная на разработке комплекса защитных барьеров, призванных парировать проектные воздействия, не может быть в должной степени успешной.

Поэтому необходимо разработать методы обеспечения безопасности, позволяющие иметь дело с недоопределенными системами. При этом должны использоваться подходы, развиваемые в рамках новой дисциплины, получившей название *теория обеспечения устойчивости технических систем к экстремальным воздействиям* (англ. Resilience Engineering)[1] [7, 14, 15]. Эта дисциплина концентрирует внимание на создании систем, которые способны:

1) продолжать (по крайней мере частично) выполнять предписанные им функции после того, как они получают повреждения, подвергнувшись запроектным воздействиям;
2) достаточно быстро восстанавливать свой исходный функциональный уровень после запроектных воздействий.

4. Принципы обеспечения устойчивости КИ

Устойчивость к экстремальным воздействиям является ключевым понятием в случаях запроектных воздействий и запроектных сценариев аварий в сложных технических системах, к которым относятся КИ [7]. Современные инфраструктурные системы (системы водо-, электро- и газоснабжения, транспортные, телекоммуникационные сети) становятся все более сложными, взаимозависимыми, динамически изменяемыми, все более проявляющими нелинейные свойства. В связи с этим становится невозможно заранее — при проектировании — спрогнозировать многие неблагоприятные события или их сочетания, а также инициируемые ими сценарии отказов и, следовательно, заранее предусмотреть полный комплекс защитных мероприятий, позволяющий построить системы защиты от исчерпывающего перечня запроектных воздействий/сценариев. При этом на первый план выходит задача повышения устойчивости инфраструктурных систем к запроектным воздействиям. Традиционные меры по снижению риска и обеспечению безопасности ТС, предусматривающие создание систем защиты от проектных воздействий и аварий, должны дополняться мерами по обеспечению устойчивости к запроектным воздействиям и авариям. В такой постановке традиционные вопросы, на которые приходится отвечать при обеспечении безопасности технических систем — «какие проектные сценарии отказа могут произойти в системе?» и «какие защитные меры нужно предпринять, чтобы предотвратить эти сценарии?», должны дополняться вопросом: «Что нужно предпринять, чтобы обеспечить устойчивость системы по отношению к заранее неизвестным экстремальным воздействиям?».

Под устойчивостью ТС к экстремальным воздействиям понимается способность системы, подвергшейся запроектному воздействию, поддерживать определенный уровень эксплуатационных характеристик и возвращаться на нормальный уровень функционирования (т.е. восстанавливаться) в течение определенного интервала времени. Система, устойчивая к экстремальным воздействиям, должна отвечать следующим требованиям:

- живучесть, т. е. способность функционировать и в определенной мере выполнять предписанные функции при наличии локальных повреждений, возникающих вследствие экстремальных воздействий;
- избыточность, т. е. наличие резервных связей, альтернативных путей передачи нагрузки и дублирующих элементов, которые могут быть задействованы в чрезвычайной ситуации;
- ресурсообеспеченность, т.е. наличие в системе ресурсов, которые могут быть задействованы в случае экстремального воздействия;
- способность к быстрому восстановлению, определяемая интервалом времени, в течение которого повреждения могут быть ликвидированы, т. е. система будет восстановлена и выйдет на номинальный уровень.

Исторически в механике понятие устойчивости тесно связано со способностью системы, находящейся под действием нагрузки, деформироваться в упругой области, накапливать энергию при действии нагрузки, высвобождать накопленную энергию и возвращаться в первоначальное положение после снятия нагрузки. Со временем применительно к инфраструктурным системам понятие устойчивости к экстремальным воздействиям стало пониматься более широко. Инфраструктура считается устойчивой, если ей свойственны низкая вероятность отказа, незначительный ущерб, реализующийся в случае отказа (число пострадавших, экономический и экологический ущерб) и малое время восстановления системы (возвращение системы в нормальное состояние с выходом в штатный режим эксплуатации и на штатную мощность/производительность).

Концептуально понятие устойчивости инфраструктуры проиллюстрировано на рис. 6, на котором представлен профиль устойчивости системы [14, 21]. В момент времени t_* на систему оказывается экстремальное воздействие. В результате этого в течение малого временного интервала Δ_d происходит ее де-

[1] В настоящее время в русскоязычной литературе еще нет эквивалента английского термина Resilience Engineering.

градация, эксплуатационная характеристика снижается на величину ΔQ от номинального значения Q_n до значения $Q_{\min}$. Далее (начиная с момента времени $t_* + \Delta_d$) идет этап восстановления системы длительностью Δ_v. Этот этап завершается выходом на номинальный уровень эксплуатации Q_n (производительность восстанавливается до 100%) в момент времени t_v. Если $\Delta_d << \Delta_v$, то длительностью интервала деградации можно пренебречь. По сравнению с последующим интервалом восстановления, деградация будет считаться мгновенной (рис. 7). Величина ΔQ характеризует прямые последствия экстремального воздействия, связанные с потерями, которые обусловлены повреждениями, разрушениями и отказами в системе непосредственно после воздействия (точнее, отношение $\Delta Q/Q_n$ характеризует степень повреждения основных фондов, степень повреждения объекта, отношение прямых экономических потерь на рассматриваемом объекте к стоимости неповрежденного объекта).

Площадь криволинейной трапеции *ABB'C* (рис. 6) или криволинейного треугольника *ABC* (рис. 7) отражает косвенный ущерб, связанный с потерей производительности и частичным невыполнением системой заданных функций в течение периода времени от момента экстремального воздействия до момента полного восстановления системы. В качестве меры устойчивости системы может быть выбрано отношение площади под эксплуатационной характеристикой после момента экстремального воздействия t_* и до контрольного момента времени t_c, в который система должна вернуться на номинальный уровень (фигура *BCDEF*), к площади прямоугольника *ADEF* [9]:

$$Res = \frac{F_e}{F_n} = \frac{\int_{t_*}^{t_c} Q(t)dt}{(t_c - t_*)\cdot Q_n} \times 100\%. \qquad (1)$$

При этом можно вводить следующее ограничение: если период восстановления превышает предельно допустимую величину $[\Delta_v]$, то устойчивость системы полагается равной 0:

$$Res = \begin{cases} \dfrac{\int_{t_*}^{t_c} Q(t)dt}{(t_c - t_*)\cdot Q_n} \times 100\%, \ \textit{если} \ t_v - t_* < [\Delta_v]. \\ 0, \ \textit{если} \ t_v - t_* > [\Delta_v] \end{cases} \qquad (2)$$

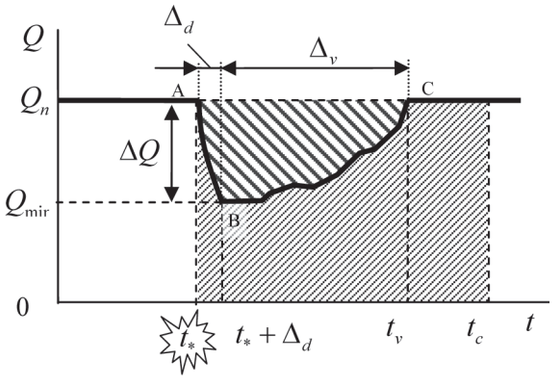

Рис. 6. Профиль устойчивости

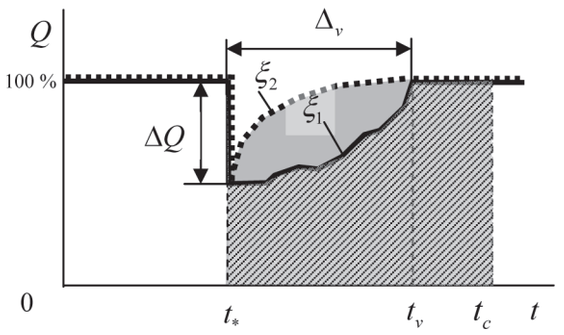

Рис. 8. Зависимость экстремальной устойчивости от характера функции восстановления

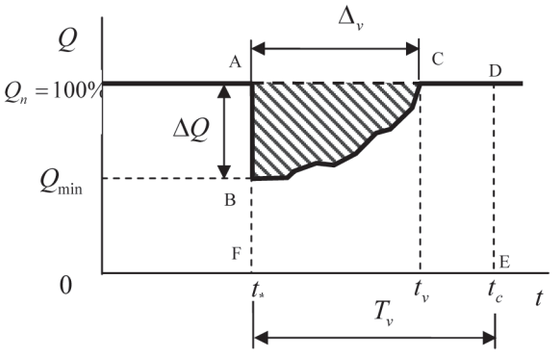

Рис. 7. Профиль устойчивости при допущении о мгновенном характере деградации эксплуатационной характеристики системы

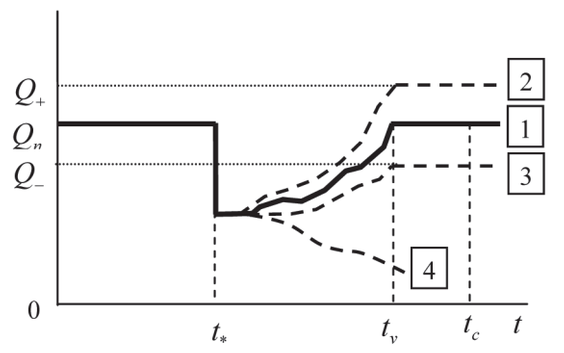

Рис. 9. Различные сценарии восстановления

Очевидно, что на величину экстремальной устойчивости системы влияют время восстановления $\Delta_v = t_v - t_*$ и падение эксплуатационной характеристики $\Delta Q = Q_n - Q_{\min}$. Кроме того, величина устойчивости будет определяться геометрией кривой восстановления (рис. 8). Действительно, система, имеющая кривую восстановления ξ_2, более устойчива, чем система с кривой восстановления ξ_1.

После крупномасштабной катастрофы окружающая среда может претерпеть существенные изменения, поэтому может возникнуть необходимость, чтобы рассматриваемая инфраструктурная система не возвращалась к исходному состоянию, а адаптировалась к изменившимся условиям и вышла на уровень, отличающийся от исходного (рис. 9). Поэтому помимо описанного выше сценария, который предполагает восстановление системы до номинального уровня (сценарий 1, рис. 9), возможны и другие сценарии:

- в результате проведенной модернизации система будет выведена на более высокий уровень эксплуатационной характеристики Q_+ (сценарий 2);
- вследствие невозможности (или нецелесообразности) полного восстановления системы она выводится на более низкий уровень эксплуатации (сценарий 3);
- вследствие катастрофических разрушений реализуется деградационный сценарий с падением эксплуатационных характеристик до нулевых значений (сценарий 4).

Ресурсы, направляемые на реализацию защитных мероприятий, обеспечивают повышение устойчивости системы к экстремальным воздействиям. При этом меняется профиль устойчивости (рис. 10): уменьшаются такие величины, как длительность периода восстановления Δ_v и падение эксплуатационной характеристики ΔQ.

Профиль устойчивости и, в частности траектория восстановления после экстремального воздействия, является случайным процессом, в начальном приближении его можно аппроксимировать линейной зависимостью (рис. 11). В этом случае выражение для устойчивости (1) может быть записано в виде, приведенном в [9]:

$$Res = \frac{(t_c - t_*)\cdot Q_n - \frac{\Delta Q \cdot \Delta_v}{2}}{(t_c - t_*)\cdot Q_n} = 1 - \frac{\Delta Q \cdot \Delta_v}{2\cdot(t_c - t_*)\cdot Q_n}. \quad (3)$$

Если вид функции восстановления считается заданным (линейным), то устойчивость системы будет характеризоваться параметрами ΔQ и Δ_v. При этом различные комбинации этих параметров, соответствующие разным случаям (1 — значительное падение эксплуатационной характеристики при малом периоде восстановления и 2 — незначительное падение эксплуатационной характеристики при большом периоде восстановления), могут иметь одинаковые индексы устойчивости. Таким образом, из выражения (2) можно получить гиперболические кривые равной устойчивости. Учитывая (2), можно записать [21]:

$$\Delta Q \cdot \Delta_v = 2 \cdot T_c \cdot Q_n \cdot (1 - Res)$$

$$(\Delta Q - 0)\cdot(\Delta_v - 0) = M, \text{ где } M = 2 \cdot T_c \cdot Q_n \cdot (1 - Res).$$

Тогда при фиксированном значении устойчивости *Res*, а также заданных значениях номинальной эксплуатационной характеристики Q_n и контрольного периода $T_c = t_c - t_*$ различным вариантам системы будут соответствовать точки плоскости (ΔQ; Δ_v), лежащие на одной гиперболе с центром в начале координат, асимптотами которой являются оси (0; ΔQ) и (0; Δ_v). Таким образом, для любого значения устойчивости *Res* множество возможных пар значений {ΔQ; Δ_v} будет лежать на гиперболе, расположенной в первом квадранте плоскости (ΔQ; Δ_v). Варьируя величину *Res*, можно получить множество равнобочных гипербол. Причем бóльшим значениям *Res* будут соответствовать меньшие значения *M* и, следовательно, гипербола,

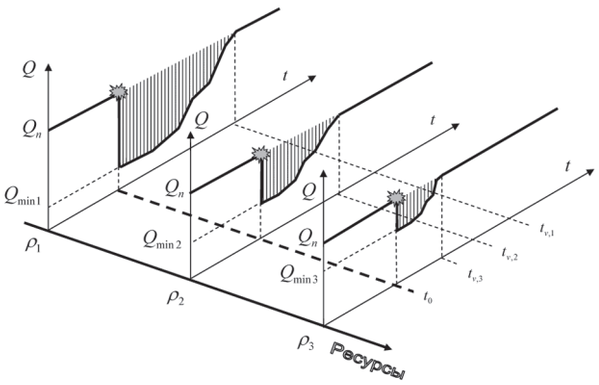

Рис. 10. Изменение профиля устойчивости системы в случае увеличения количества ресурсов, направляемых на защиту системы и ликвидацию последствий аварии [7]

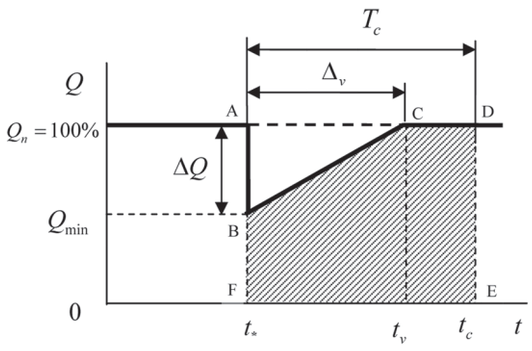

Рис. 11. Аппроксимация кривой восстановления с помощью линейной функции

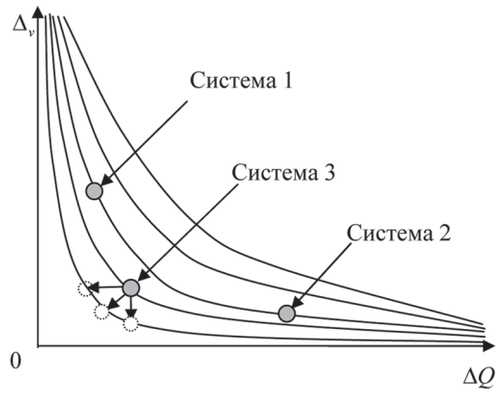

Рис. 12. Контуры равной устойчивости

Рис. 13. Области допустимых и недопустимых состояний по критерию устойчивости к экстремальным воздействиям

которая будет располагаться ближе к координатным осям. То обстоятельство, что всем точкам гиперболы будет соответствовать одно и то же значение устойчивости, позволяет в явной форме сопоставить влияние параметров ΔQ и Δ_v на устойчивость системы.

Система 1 имеет тот же индекс устойчивости, что и система 2, но при этом первоначальное падение эксплуатационной характеристики (прямые ущербы) у системы 1 больше, а период восстановления меньше, чем у системы 2. Система 3 имеет несколько большее падение эксплуатационной характеристики, чем система 1, и больший период восстановления, чем система 2, но более устойчива, чем системы 1 и 2. На рис. 12 представлены различные способы повышения устойчивости системы 3: снижение ΔQ, снижение Δ_v и комбинированный способ.

Может быть сформирован вероятностный индекс устойчивости системы. Пусть $[\Delta Q]$ и $[\Delta_v]$ соответственно предельно допустимое значение падения эксплуатационной характеристики после экстремального воздействия на систему и предельно допустимый интервал восстановления до номинального уровня эксплуатационной характеристики. Тогда под экстремальной устойчивостью будем понимать вероятность того, что система не выйдет за предельные границы по ΔQ и Δ_v, то есть будет соответствовать заданным эксплуатационным стандартам *S*. Тогда, если на систему оказывается экстремальное воздействие интенсивности ω, ***у***стойчивость системы к воздействию данной интенсивности может быть определена как:

$$Res_{\omega} = P(S \mid \omega) = P\left\{\left(\Delta Q < [\Delta Q]\right) \cap \left(\Delta_v < [\Delta_v]\right)\right\}$$

$$Res_p(\omega) = P(S \mid \omega) = P\left\{\left(\Delta Q < [\Delta Q]\right) \cap \left(\Delta_v < [\Delta_v]\right)\right\}. \quad (4)$$

Если учитывать возможность варьирования интенсивности воздействия по различным уровням, то по теореме о полной вероятности «интегральная» устойчивость может быть записана в виде

$$Res_p = \sum_{\omega} P(S \mid \omega) P(\omega).$$

Если рассматривается не дискретное, а непрерывное распределение:

$$Res_p = \int_{\omega} p_{S|\omega}(\omega) p_{\omega}(\omega) d\omega,$$

где $p_{(S|\omega)}(\omega)$ — условная плотность распределения вероятности реализации события *S*; $p_{(S|\omega)}(\omega)$ — функция распределения.

Используя понятие функции предельных состояний, можно определить понятие устойчивости исходя из подходов системной теории надежности. Пусть для данной системы, подвергающейся запроектному воздействию, рассматриваются два предельных состояния:

- прямой ущерб ΔQ превышает предельно допустимую величину ущерба $[\Delta Q]$;
- время восстановления превышает предельно допустимую величину $[\Delta_v]$.

Используя подходы теории надежности и, в частности понятие функции предельных состояний, можно рассматривать выражение (2) как условие нахождения системы в допустимой области, ограниченной двумя функциями предельных состояний:

$$g_1 = \frac{\Delta Q}{[\Delta Q]} - 1 \text{ и } g_2 = \frac{\Delta_v}{[\Delta_v]} - 1. \quad (5)$$

Тогда двухмерная функция предельных состояний, требующая одновременного выполнения условий $g_1 > 0$ и $g_2 > 0$, будет иметь вид:

$$g\left(\Delta Q, \Delta_v\right)=\left(\frac{\Delta Q}{[\Delta Q]}\right)^{a_1}+\left(\frac{\Delta_v}{[\Delta_v]}\right)^{a_1}-1, \qquad (6)$$

где a_1 и a_2 — показатели степени, определяемые в каждом конкретном случае.

На ее основе можно построить (рис. 13) области допустимых и недопустимых состояний объектов инфраструктуры в координатах «ΔQ — Δ_v».

5. Заключение

Существующие в настоящее время методики обеспечения безопасности технических систем разработаны для систем, имеющих четкие границы и хорошо определенные перечни угроз. Для этих систем могут быть созданы базы данных по статистике аварий, которые позволяют количественно оценивать и верифицировать модели. Эти методики, базирующиеся на построении сценарных «деревьев» (модели типа «дерево» событий, «дерево» отказов), были разработаны без учета запроектных воздействий и не позволяют в должной мере учесть сложность критических инфраструктур, функционирование которых определяется взаимодействием технических, организационных и социальных факторов.

В указанных методиках аварии, развивающиеся в технических системах, рассматриваются как линейные последовательности событий. Эти модели имеют ограниченные возможности, когда приходится описывать развитие аварий в таких сложных техно-социальных системах, как критические инфраструктуры, которые предполагают нелинейные взаимодействия между компонентами, петли обратных связей, множественные источники аварий и т.д. Традиционный подход к моделированию аварий не позволяет описывать сценарии отказов в сложных системах, которые, как правило, происходят не вследствие отдельного инициирующего события (технического отказа элемента системы или ошибки оператора), а являются следствием нескольких взаимосвязанных факторов, действующих на различных уровнях системы. К этим факторам относятся технические отказы, человеческие ошибки, внешние экстремальные воздействия, латентные условия, связанные с таким аспектами, как действующая практика управления системой или этнокультурные особенности персонала, внешние инициирующие события.

Исследование критических инфраструктур как социо-технических систем требует оценки сложных взаимодействий между техническими, социальными и организационными уровнями системы. Поэтому КИ нужно рассматривать как единое целое. При этом необходимо делать акцент на одновременном совместном рассмотрении технических, организационных и социальных факторов, определяющих состояние системы и динамику ее развития. Чтобы обеспечить безопасность таких систем, необходимо выйти за рамки традиционного подхода к оценке проектных рисков и перейти к новой парадигме, основанной на обеспечении безопасности КИ по критерию устойчивости к запроектным воздействиям. В связи с необходимостью включить в рассмотрение запроектные аварии на КИ, рамки исследований должны быть существенно расширены. Меры по обеспечению безопасности должны быть направлены не только на создание защитных барьеров, призванных предупредить реализацию постулируемых проектных аварий, но и на повышение устойчивости и живучести КИ в случае запроектных воздействий, т. е. сосредоточиться на предотвращении крупномасштабных катастроф и длительных перерывов в функционировании КИ.

Возможность запроектных воздействий, имеющих низкую вероятность реализации и тяжелые последствия, должна учитываться при проведении оценок защищенности критических инфраструктур. Это потребует реализации дополнительных мер, направленных на повышение устойчивости КИ при запроектных воздействиях.

Необходимо выйти за рамки традиционных моделей оценки рисков, основанных на построении «деревьев» отказов и «деревьев» событий, которые ограничиваются рассмотрением проектных воздействий и проектных сценариев развития аварий, и начать изучать реакции КИ на возможные запроектные воздействия [10, 11]. Новая парадигма обеспечения безопасности КИ и других сложных систем должна концентрировать внимание не только на создании защитных барьеров и реализации охранных мероприятий, направленных на парирование проектных аварий, но и на повышении устойчивости КИ по отношению к запроектным авариям. Причем разрабатываемый новый подход к обеспечению безопасности КИ должен рассматриваться не как замена, а скорее как дополнение традиционного подхода.

ЛИТЕРАТУРА

1. *Махутов Н.А., Ахметханов Р.С., Резников Д.О. и др.* Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Безопасность и защищенность критически важных объектов. Часть 1. Научные основы безопасности и защищенности критически важных объектов. — М.: МГФ «Знание», 2012.
2. *Махутов Н.А., Петров В.П., Резников Д.О., Куксова В.И.* Обеспечение защищенности критически важных объектов на основе снижения их уязвимости//

Проблемы безопасности и чрезвычайных ситуаций. 2009. № 2.
3. *Махутов Н.А., Резников Д.О.* Сопоставительная оценка нормативного и основанного на управлении риском подходов к оценке защищенности сложных технических систем//Проблемы машиностроения и надежности машин. 2011. № 6. С. 92–98.
4. *Махутов Н.А., Резников Д.О., Петров В.П.*Оценка риска аварий на КВО с учетом возможности реализации экстремальных ущербов//Проблемы безопасности и чрезвычайных ситуаций. 2008. № 5. С. 57–73.
5. *Махутов Н.А., Резников Д.О.* Оценка уязвимости технических систем и ее место в процедуре анализа риска//Проблемы анализа риска. 2008. Том 5, № 3. — С. 76–89.
6. *Махутов Н.А., Резников Д.О., Петров В.П., Куксова В.И.* Обеспечение защищенности и минимизация общих эксплуатационных затрат и ущербов в течение жизненного цикла критически важных объектов путем выбора оптимальной стратегии проведения технических инспекций и ремонта//Проблемы безопасности и чрезвычайных ситуаций. 2010. № 3. С. 34–67.
7. *Bruneau M., Reinhorn A.* Overview of the Resilience concept // Proceedings of the 8-th U.S. National Conference on Earthquake Engineering, USA. 2006.
8. *Bruneau M., Reinhorn A.* Seismic resilience of communities — conceptualization and operationalization //Proceedings of International workshop on Performance based seismic-design. Bled — Slovenia, 2004.
9. *Cimellaro G., Reinhorn A., Bruneau M.* Quantification of Seismic Resilience // Proceedings of the 8-th U.S. National Conference on Earthquake Engineering, USA. 2006 (индексы устойчивости, теория надежности, предельные состояния).
10. Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience // Critical Infrastructure protection Program. Discussion Paper Series. George Masson University. 2007. 109 p.
11. *Gheorghe A., Vamanu D.* On the Vulnerability of Critical Infrastructures: 'Seeing it Coming'// Int. J. Critical Infrastructures. 2004. Vol. 1, Nos. 2/3. P. 216–246.
12. *Haimes Y.* On the Definition of Vulnerabilities in Measuring Risks to Infrastructures // Risk Analysis. 2006. Vol. 26, No 2.
13. *Hollnagel E.* From protection to resilience: Changing views on how to achieve safety/ 8-th International Symposium of the Australian Aviation Psychology Association. Australia, 2008.
14. *Hollnagel E., Woods D., Leveson N.* Resilience Engineering: Concepts and Precepts. Ashgate, Great Britain, 2006. 397 p.
15. *Hollnagel E., Sidney D., Woods D., Cook R.* Resilience Engineering: New directions for measuring and maintaining safety in complex systems / Lund University School of Aviation. 2008. P. 63.
16. *Makhutov N., Reznikov D., Petrov V.* Engineering Infrastructures: Problems of Safety and Security // Proceedings of the international Workshop "European perspectives on security research"/ Acatech, Gemany. 2011. P. 93-106.
17. *McDaniels T., Chang S. E., Cole D., Mikawoz J., Longstaff H.* Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. Global Environmental Change, 18, 310–318. 2008
18. *Makhutov N., Petrov V., Reznikov D.* Multivariant Risk Analysis of Critical Facilities and Infrastructures in Russia / 2nd International Disaster and Risk Conference, Davos, 2008. P. 118–119.
19. *Makhutov N., Reznikov D., Petrov V.* Development of the Open Database on Risk Assessment in Technical Systems / International Conference on Open Risk Analysis. University of Cambridge, UK. 2009.
20. *Pederson P., Dudenhoeffer D., Hartley S., Permann M.* Critical Infrastructure Interdependency Modelling: A Survey of U.S. and International Research / Idaho National Laboratory Critical Infrastructure Protection Division Idaho Falls, Idaho 83415. 2006.
21. *Zobel C.* Comparative Visualization of Predicted Disaster Resilience // Proceedings of the 7-th International ISCRAM Conference. USA, 2010.

Specific Futures of Critical Infrastructures Safety Ensuring

N.A. Makhutov, Chief Research Associate, RAS Member Correspondent, Doctor of Engineering, Institute of Machines Science named after A.A. Blagonravov of Russian Academy of Sciences, Moscow
D.O. Reznikov, Leading Research Associate, Ph.D. of Engineering, Institute of Machines Science named after A.A. Blagonravov of Russian Academy of Sciences, Moscow
V.P. Petrov, Leading Research Associate, Ph.D. of Engineering, Institute of Machines Science named after A.A. Blagonravov of Russian Academy of Sciences, Moscow

A number of critical infrastructures' distinctive features which define additional requirements to these infrastructures' safety ensuring are considered in this paper. Need of addition of traditional approaches to ensuring the safety of critical infrastructures in relation to design impacts by a complex of measures, aimed at providing their stability to beyond design basis influences is proved. Means related to carrying out of critical infrastructures' stability quantitative assessment are considered.

Key words: critical infrastructures, risk, safety, resilience, beyond design basis impact, stability.