Оценка уязвимости технических систем и ее место в процедуре анализа риска

ISSN 1812-5220

Н.А. Махутов,
Д.О. Резников,
Институт машиноведения РАН, Москва

Аннотация

В настоящей работе представлены различные подходы к определению количественной меры уязвимости технических систем по отношению к природно-техногенным и террористическим воздействиям. Предложен подход к оценке уязвимости технических систем, основанный на использовании графовых моделей эскалации аварии. При этом оценка уязвимости рассматривается как один из ключевых этапов анализа риска, который следует за анализом угроз и предшествует калькуляции ущербов.

Ключевые слова: уязвимость, угроза, ущерб, риск, начальное состояние, инициирующее событие, конечное состояние, отказ, авария.

Technical System Vulnerability Assessment and its Role in the Framework of Risk Analysis

ISSN 1812-5220

N.A. Makhutov,
D.O. Reznikov,
Institute of Machine Sciences, Russian Academy of Sciences, Moscow

Abstract

The paper addresses different ways of quantitative assessment of technical systems vulnerabilities to various natural and manmade hazards. An approach to vulnerability assessment based on graph models of accident escalation is presented. Vulnerability assessment is considered as the key phase of risk analysis that follows hazards assessment and forms the basis for subsequent loss estimation.

Key words: vulnerability, hazard, loss, risk, initial state, initiating event, end state, failure, accident.

Содержание

Введение

В настоящее время понятие *уязвимость* все более широко используется при оценке рисков, которым подвергаются технические системы, для того, чтобы охарактеризовать реакцию рассматриваемых систем на экстремальные воздействия [1, 3, 4, 5, 6, 7, 12, 13]. Однако в теории рисков отсутствует одно установившееся определение понятия «уязвимость». Как правило, под уязвимостью понимают открытость системы к различным экстремальным внутренним и внешним событиям/воздействиям, которые способствуют развитию катастрофического процесса. Достаточно часто понятие «уязвимость» определяют через связанные с ним характеристики системы. Например, под уязвимостью системы понимают совокупность свойств, являющихся противоположными устойчивости и живучести системы, а также ее способности выполнять заданные функции в случае частичного повреждения.

В связи с тем что понятие «уязвимость» является многосторонним и должно отражать физические, организационные, технологические и функциональные аспекты состояния системы, весьма актуальной задачей является формирование единого методологического подхода к количественной оценке уязвимости, то есть определению меры уязвимости для технических систем.

В статье рассматриваются существующие в настоящее время подходы к оценке уязвимости технических систем и представляется подход к оценке уязвимости технических систем, основанный на использовании графовых моделей.

1. Определение и количественная мера уязвимости

Изменения, происходящие в технической системе, призванной обеспечить получение определенного результата (или реализацию заданного технологического процесса), могут быть представлены в виде траектории в пространстве состояния системы Ω, определяющей переход от начального состояния системы *НС* в ее конечное состояние $КС_0$ (рис. 1). В случаях когда удается обеспечить подобный переход, говорят, что в системе реализован заданный сценарий (или «сценарий успеха») S_0 [11,12]. Конечное состояние $КС_0$ определяет набор значений $x_0^1, x_0^2, \cdots, x_0^m$, которые должны принимать переменные состояния системы $x^1, x^2, \cdots, x^m$, чтобы система соответствовала предъявляемым к ней требованиям. К этим требованиям могут, например, относиться: структурная целостность системы, неповрежденность ее элементов, выполнение системой заданных функций, обеспечение заданной производительности и качества (продукции или услуг) и т. д. Перечисленные переменные состояния системы определяют размерность и конфигурацию пространства состояний системы.

Если в системе происходит инициирующее событие $ИС_*$, она может отклониться от сценария S_0 (рис. 2) и перейти к реализации некоторого нового сценария S_*, заканчивающегося конечным состоянием $КС_*$, отличным от заданного конечного состояния $КС_0$:

$$КС_*(x_*^1, x_*^2, \cdots, x_*^m) \neq КС_0(x_0^1, x_0^2, \cdots, x_0^m).$$

В этом случае можно сказать, что в системе произошел отказ, связанный с ее неспособностью обеспечить требуемое конечное состояние $КС_0$. То есть система оказалась уязвима к инициирующему событию $ИС_*$.

Вследствие высокого уровня неопределенности, касающейся типа и интенсивности инициирующих событий, а также способности системы «сопротивляться» инициирующим воздействиям, мера уязвимости должна быть вероятностной, то

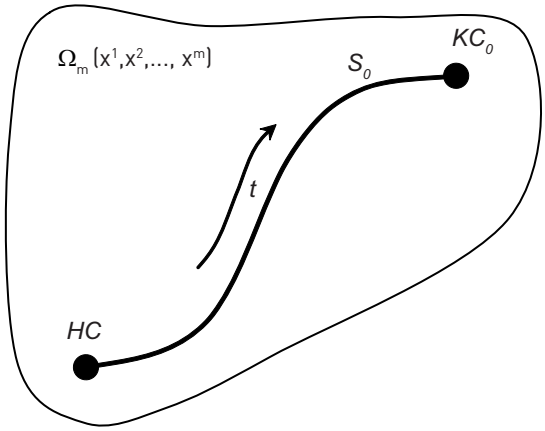


Рис. 1. Сценарий успеха S_0

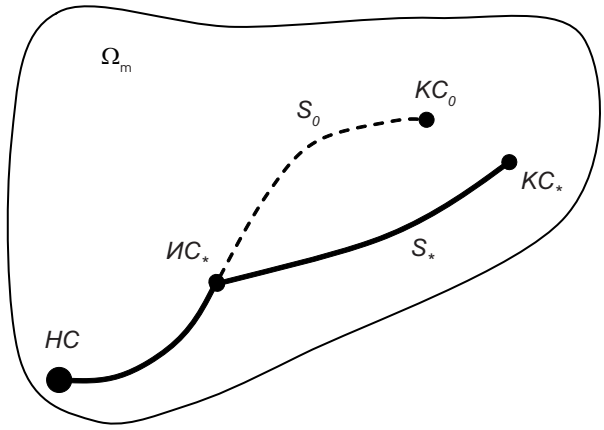


Рис. 2. Сценарий отказа S_*

есть определяться вероятностью отказа (O) системы[1]: $V = f(P[O])$.

В связи с тем, что свойства, характеризующие уязвимость системы, начинают проявляться только после того, как в ней произошло некоторое нештатное инициирующее событие (или система была подвергнута некоторому нештатному воздействию), то мера уязвимости должна определяться условной вероятностью отказа системы при условии, что система была подвергнута инициирующему воздействию $V = f(P[O \mid ИС])$.

Очевидно, что на практике невозможно бывает обеспечить абсолютно точное достижение системой заданного конечного состояния $КС_0$. Реальные системы всегда будут подвергаться некоторым, иногда слабым, инициирующим воздействиям, которые будут несколько отклонять траекторию системы от заданного сценария успеха S_0. Кроме того, отклонение от сценария успеха S_0 будет еще обуславливаться и естественной вариативностью параметров системы.

Поэтому при оценке уязвимости речь должна идти об условной вероятности выхода конечного состояния системы из заданной области ε_0 пространства состояний Ω_m. В частности, на рисунке 3 представлено слабое инициирующее событие $ИС_k$, которое приводит к конечному состоянию $КС_k$, лежащему в пределах заданной окрестности ε_0. При этом можно считать, что система не является уязвимой к инициирующему воздействию $ИС_k$.

Далее под отказом системы будет пониматься выход конечного состояния системы из заранее заданной области ε_0 пространства состояний системы Ω_m, вне которой система либо перестает существовать, либо не обеспечивает выполнение заданных функций или качества продукции (услуг и т. д.).

Тогда может быть сформулировано следующее определение понятия «уязвимость»:

Под уязвимостью системы понимается условная вероятность выхода конечного состояния системы $КС_*$ за границы заданной области ε_0 пространства состояний системы Ω_m, в случае если произойдет инициирующее событие ИС:

$$V = P[(\|KC_* - KC_0\| > \varepsilon_0) \mid ИС] \ . \qquad (1)$$

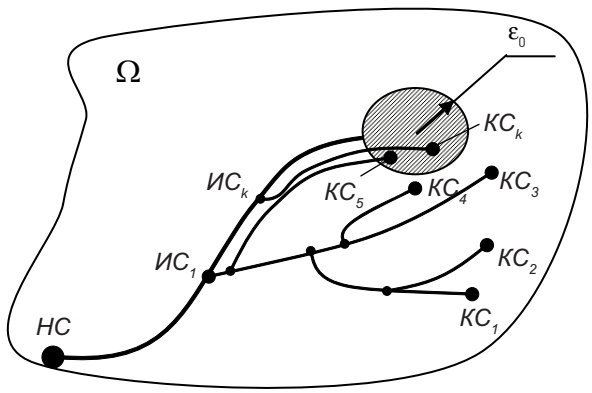


Рис. 3. Область условно неповрежденных состояний ε_0

[1] Здесь и далее под отказом будет пониматься получение системой определенной степени повреждения или невыполнение системой (полностью или частично) заданных функций.

Конкретный вид неравенства $\|KC_* - KC_0\| > \varepsilon_0$ зависит от выбора пространства состояний системы и от способа задания метрики в этом пространстве.

Может быть выбрана Евклидова метрика пространства Ω_m:

$$\|KC_* - KC_0\| = \sqrt{(x_*^1 - x_0^1)^2 + (x_*^2 - x_0^2)^2 + \cdots (x_*^m - x_0^m)^2} \quad (2)$$

или

$$\|KC_* - KC_0\| = \max_m \left\{ (x_*^1 - x_0^1); (x_*^2 - x_0^2); \cdots; (x_*^m - x_0^m) \right\}. \quad (3)$$

В частности, могут быть выбраны различные одномерные пространства состояний системы Ω_1, позволяющие описывать различные аспекты состояния системы (физические, экономические, функциональные и т. д.).

Различают физические, функциональные и экономические составляющие уязвимости, которые могут быть определены в соответствующих одномерных пространствах состояния системы.

Если в качестве пространства состояний системы выбирается одномерное пространство Ω_1^{ph}, единственная координата которого определяет физическую степень повреждения системы ($x^1 = DS$), то под физической уязвимостью V_{ph} системы понимается условная вероятность получения системой определенной степени повреждения (конечного состояния, которое соответствует определенной степени повреждения):

$$V_{ph} = P[(DS_* > DS_d) \mid ИС], \quad (4)$$

где DS_d — допустимая степень повреждения системы.

Если в качестве пространства состояний системы выбирается одномерное пространство Ω_1^U, единственная координата которого определяет уровень ущерба, который наступает при достижении системой конечного состояния KC_* ($x^1 = U$), то экономическая уязвимость системы определяется как условная вероятность того, что за время Δt в системе произойдет инициирующее событие, приводящее к ущербу, превышающему заданное пороговое значение U_d:

$$V_e = P[U_* > U_d \mid ИС]. \quad (5)$$

Величина V_e также называется экономической уязвимостью системы.

Если в качестве пространства состояний системы выбирается одномерное пространство Ω_1^{Φ}, единственная координата которого определяет степень выполнения системой заданных функций, которые реализуются системой при достижении ею конечного состояния KC_* ($x^1 = \Phi_*$), то под функциональной уязвимостью понимается условная вероятность потери системой способности выполнять определенные функции (степень утраты системой заданных функциональных обязанностей, при условии инициирующего воздействия)

$$V_f = P[(\|\Phi_* - \Phi_0\| > \delta) \mid ИС], \quad (6)$$

где Φ — заданный функциональный уровень.

При этом величины $V_{ph}\, V_e\, V_f$ могут рассматриваться как физическая, экономическая и функциональная компоненты вектора уязвимости системы.

Таким образом, оценка уязвимости системы предполагает определение условной вероятности отказа в системе при условии, что произошло инициирующее событие. Данная трактовка понятия «уязвимость» будет использоваться далее в этой работе. Следует, однако, отметить, что существуют и другие трактовки этого понятия; некоторые из них будут кратко представлены ниже.

Уязвимость системы часто определяется как величина противоположная (в вероятностном смысле — дополнение до 1) таким величинам как робастность/живучесть(англ. robustness) и способность к восстановлению (англ. resilience) [9].

Под робастностью системы понимается условная вероятность того, что в случае инициирующего воздействия *ИС* конечное состояние системы KC_* отклоняется в пространстве состояний от KC_0 на величину, не превосходящую заданной малой величины ε_0:

$$Rob = P\left[\left(\|KC - KC_0\| < \varepsilon_0\right) \mid ИС\right]. \quad (7)$$

Тогда можно прийти к сформулированному выше определению уязвимости вида (1) через понятие робастности:

$$V = 1 - Rob = 1 - P\left[\left(\|KC_* - KC_0\| < \varepsilon_0 \right) \mid ИС\right] = P\left[\left(\|KC_* - KC_0\| > \varepsilon_0 \right) \mid ИС\right]. \quad (8)$$

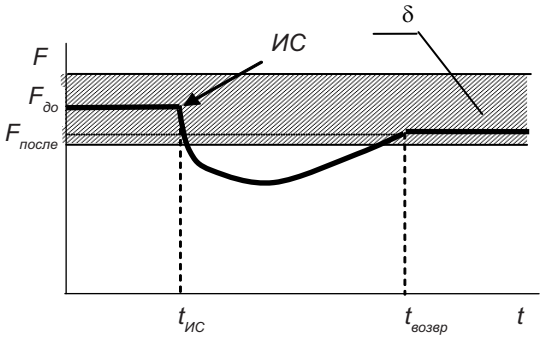


Рис. 4а. Система, способная адаптироваться после экстремального воздействия

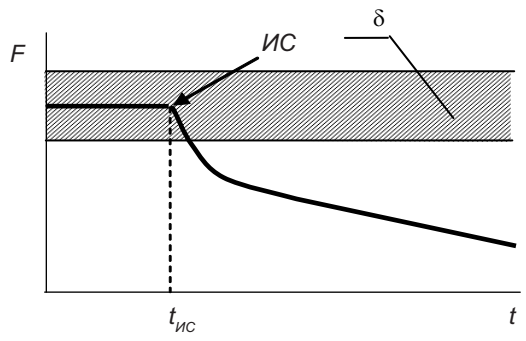


Рис. 4б. Система, неспособная адаптироваться после экстремального воздействия

В динамических системах следует опираться на понятие устойчивости (способности к восстановлению), которая характеризует способность системы адаптироваться и находить новое устойчивое положение, достаточно близкое к заданному, чтобы она смогла выполнять заданные функции, после возмущения.

В вероятностной постановке под способностью к восстановлению понимается условная вероятность того, что текущее состояние системы $F(t)$ в течение заданного интервала времени Δt после инициирующего воздействия должно прийти к некоторому устойчивому состоянию F_c, близкому к заданному состоянию (рис. 4а):

$$Rez = P[(F(t) \to F_c) \cap (F(t) \in \delta)]. \qquad (9)$$

Тогда уязвимость может быть определена как дополнение до 1 адаптивности системы:

$$V = 1 - Rez = 1 - P[(F(t) \to F_c) \cap (F(t) \in \delta)]. \quad (10)$$

Среди существующих трактовок уязвимости можно отметить понятие структурной уязвимости системы (англ. structural vulnerability), под которой понимается условная вероятность того, что сетевая структура не сможет выполнять свои функции (т. е. произойдет отказ структуры *ОС*), в случае если отдельные элементы структуры будут выведены из строя (отказ элемента — ОЭ):

$$V_{Str} = P[OC \mid O\Э]. \qquad (11)$$

В рамках подходов, базирующихся на построении деревьев отказов, уязвимость системы определяется совокупностью минимальных аварийных сочетаний (МАС)[2], которые приводят к различным конечным состояниям системы, отличающимся от заданного состояния $КС_0$.

2. Оценка уязвимости при различных уровнях описания неопределенности

В п. 1 анализ уязвимости основывался на так называемой точечной оценке условной вероятности отказа $V^0 = P[O \mid ИС]$. При этом не учитывались как неопределенности, связанные с интенсивностью воздействия, так и неопределенности, связанные со свойствами системы, определяющими ее способность сопротивляться экстремальным воздействиям (неопределенность механических свойств, геометрических размеров системы, условий во внешней среде, истории эксплуатационного нагружения и т. д.). С точки зрения описания неопределенностей определение типа V^0 принято называть определением уязвимости 0-уровня.

Если учесть, что интенсивность инициирующего события ω заранее неизвестна и может варьироваться, то уязвимость системы будет характеризоваться функцией условной вероятности отказа (под которым понимается выход конечного состояния системы за границы допустимой области ε_0) при

[2] Минимальное аварийное сочетание — наименьший набор исходных событий, при котором достигается аварийное конечное состояние системы. Полная совокупность МАС дерева представляет собой все варианты сочетаний событий, при которых может возникнуть авария. Минимальная траектория — наименьшая группа событий, при появлении которых происходит авария.

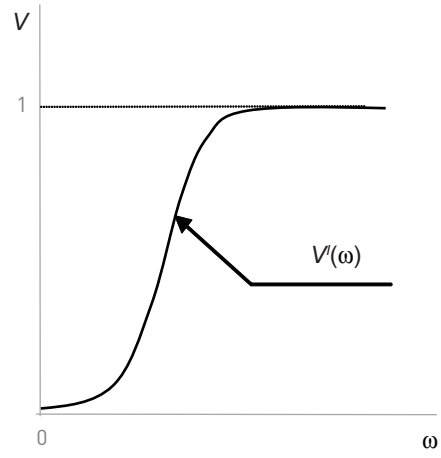


Рис. 5. Кривая уязвимости системы, отражающая неопределенность интенсивности воздействия ω

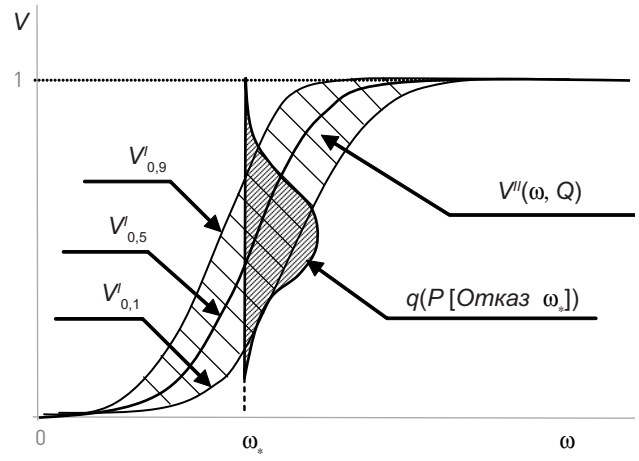


Рис. 6. Множество кривых уязвимости, отражающих неопределенность интенсивности воздействия и свойств системы

условии, что система подвергается инициирующему воздействию (рис. 5):

$$V^I(\omega) = P\left[\left\|KC_* - KC_0\right\| > \varepsilon_0 \mid \omega\right]. \qquad (11)$$

Учитывая принятое выше определение отказа, это выражение можно записать в более краткой форме:

$$V^I(\omega) = P[O \mid \omega]. \qquad (12)$$

Определение уязвимости типа V^I, учитывающее неопределенность, связанную с интенсивностью воздействия, называют определением уязвимости *I* уровня.

В еще более общей постановке наряду с неопределенностью, связанной с интенсивностью воздействия, необходимо учитывать неопределенность свойств самой системы (ее реакции на воздействие интенсивности ω). Эти неопределенности, например, могут быть связаны с разбросом механических свойств, геометрических размеров системы, условий во внешней среде, историей эксплуатационного нагружения и т. д.). Это означает, что определение уязвимости вида (12) также не является исчерпывающим. Описанный выше подход не учитывает неопределенность относительно вида кривой $V^I = P(O \mid \omega)$. В еще более общей постановке ордината точки кривой $V^I = P(O \mid \omega)$ при $\omega = \omega_*$ не является детерминированной величиной и должна описываться вероятностным распределением $q(P[O \mid \omega])$[3]. Это обстоятельство предполагает рассмотрение семейства кривых распределений ущерба вида $P_Q[O \mid \omega]$ (где параметр Q представляет собой интегральную вероятность для распределения q). В частности, ордината кривой $P_{0,9}$ при $\omega = \omega_*$ представляет собой 90%-квантиль случайной величины P. Запись $P_{0,9}$ говорит о том, что существует 90%-ная вероятность второго порядка (Q), что при заданной интенсивности воздействия ω_* вероятность первого порядка (P), с которой в системе возникает *Отказ*, не превосходит величины $V^I_{0,9}(\omega_*) = P_{0,9}[O \mid \omega_*]$: $Q\left(P[O \mid \omega_*] \le P_{0,9}[O \mid \omega_*]\right) = 0{,}9$.

В такой постановке под уязвимостью следует понимать множество кривых $V^I_Q(\omega) = P_Q[O \mid \omega]$, которое учитывает как неопределенности, связанные с вероятностями реализации различных интенсивностей воздействий ω, так и неопределенности, связанные с несущей способностью системы, обусловленной разбросом геометрических размеров системы, физико-механических свойств материалов и т. д., при рассматриваемой интенсивности воздействий ω_* (рис. 6). Данное определение можно счи-

[3] Здесь вводится вероятностное распределение $q(P)$ и соответствующая интегральная вероятность $Q(P)$, которая будет называться вероятностью второго порядка. Эти функции необходимо отличать от функции $P(\omega)$, которые будут далее именоваться вероятностью первого порядка.

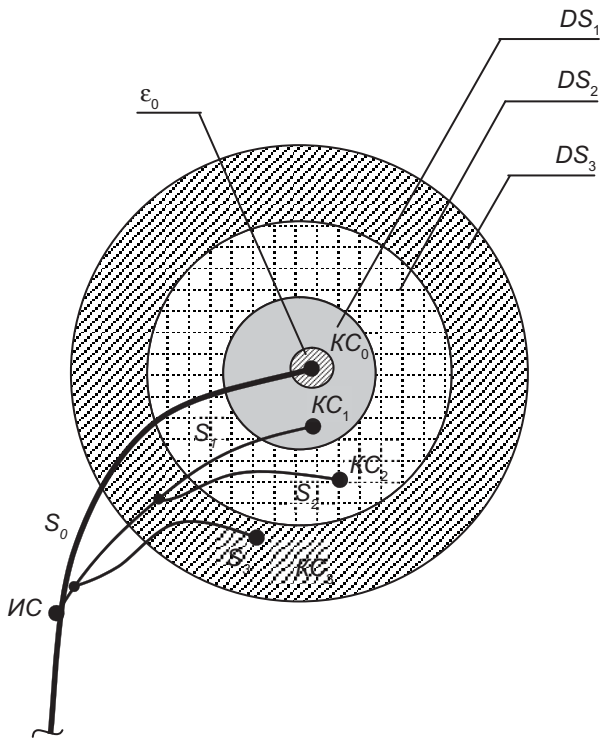


Рис. 7. Неопределенность конечного состояния системы

тать определением уязвимости *II* уровня и записать его в условном виде, как:

$$V^{II} = \left\{\bigcup V_Q^I(\omega)\right\} \qquad (13)$$

или в развернутой форме

$$V^{II} = \left\{\bigcup P_Q[O \mid \omega]\right\}. \qquad (14)$$

Представленный выше анализ неопределенности при описании уязвимости касается тех случаев, когда можно рассматривать только два состояния системы: «система не повреждена» и «система повреждена» (т. е. находится в состоянии отказа). В тех случаях, когда необходимо учитывать возможность реализации различных поврежденных конечных состояний системы (рис. 7), ее уязвимость должна описываться семейством кривых уязвимости, характеризующих зависимость вероятности реализации того или иного конечного состояния от интенсивности инициирующего события (рис. 8):

$$V_{KC_i}(\omega) = P\left[(KC = KC_i) \mid (\Omega = \omega)\right],\ i = 1,2,...,k.$$

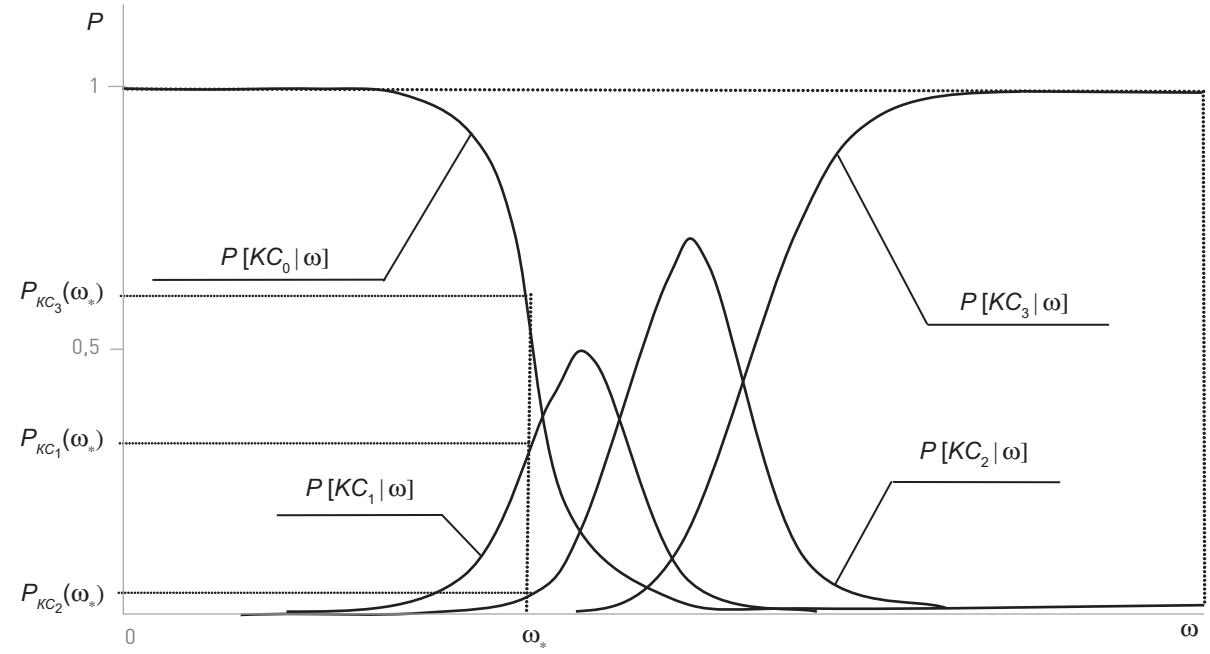


Рис. 8. Кривые уязвимости системы, соответствующие различным конечным состояниям системы. Кривая $P[KC_0 \mid \omega]$ ***характеризует вероятность того, что система не будет повреждена при воздействии на нее с интенсивностью*** ω***. Кривые*** $P[KC_i \mid \omega]$ ***(i = 1,2,3) характеризуют вероятности того, что система будет приведена в поврежденные состояния*** KC_1***,*** KC_2 ***и*** KC_3 ***в результате воздействия на нее с интенсивностью*** ω

Или в краткой форме

$$V_{KC_i}(\omega) = P\left[KC_i \mid \omega\right],\ i = 1,2,...,k.$$

Тогда с учетом неопределенности конечного состояния системы уязвимость может характеризоваться совокупностью кривых уязвимости, соответствующих различным конечным состояниям системы:

$$V^{III} = \left\{\bigcup_i P\left[KC_i \mid \omega\right]\right\}\ i = 1,2,...,k.$$

3. Место оценки уязвимости в процедуре оценки риска

Общий контекст анализа риска для рассматриваемой технической системы предполагает последовательный анализ угроз, которым подвергается система, анализ уязвимостей системы по отношению к этим угрозам и калькуляцию/оценку ущербов от аварий, реализующихся в тех случаях, когда система оказалась уязвима к действующим на нее угрозам (рис. 9).

Анализ уязвимости является ядром оценки риска. Он призван дать ответ на вопрос, как будут развиваться события после того, как рассматриваемая система будет подвергнута инициирующему воздействию, и насколько вероятно, что эта система окажется поврежденной.

В случае когда в системе возможны различные поврежденные состояния, анализ уязвимости предполагает анализ дерева сценариев и построение матрицы условных вероятностей достижения различных конечных состояний в случае различных инициирующих событий. Полученные данные о конечных состояниях системы далее становятся основой для проведения подсчета ущербов.

Очевидно, что анализ уязвимости должен проводиться во взаимоувязке с другими этапами анализа риска, поскольку он должен следовать за анализом угроз и предшествовать калькуляции ущербов, реализуемых в случае достижения системой различных поврежденных конечных состояний.

В качестве примера может быть рассмотрен анализ террористических рисков для некоторой технической системы. Анализ уязвимости системы по отношению к возможным террористическим атакам осуществляется совместно с оценкой террористических угроз с привлечением комбинирован-

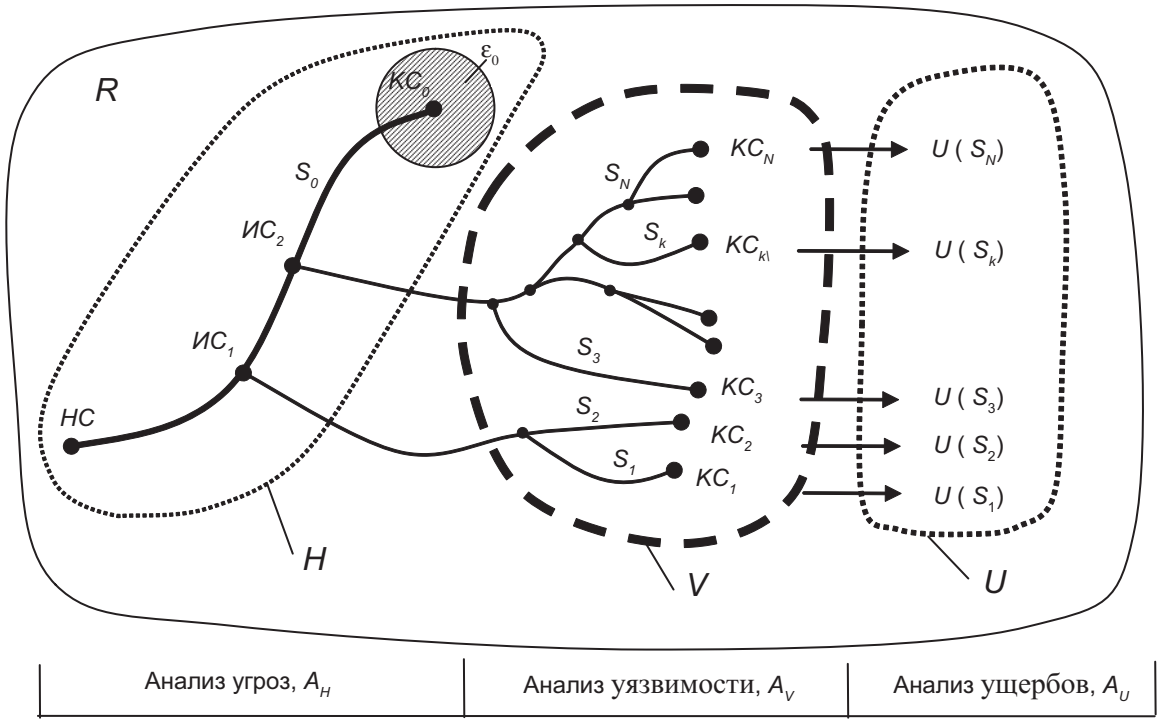


Рис. 9. Анализ уязвимости в структуре анализа риска

ных графовых моделей [7], объединяющих деревья событий и деревья отказов (рис. 10). На рисунке представлен сценарий успеха S_0 для рассматриваемой системы, связывающий ее начальное состояние *НС* и заданное конечное состояния $КС_0$, соответствующее успешному выполнению системой ее функций. Исходя из предварительного анализа ресурсов, которыми располагают террористы, и опыта предыдущих атак определяются элементы (или этапы функционирования) системы *k* и *l*, которые могут стать целями террористической атаки. Проведенный с помощью построения деревьев отказов анализ угроз позволяет идентифицировать возможные инициирующие события (сценарии атаки) $ИВ_k$ и $ИВ_l$.

Осуществляемый далее анализ уязвимостей проводится путем построения деревьев событий, исходящих из инициирующих воздействий *k* и *l*, позволяет определить возможные конечные состояния $КС_i$ и вероятности их реализации. Дерево событий описывает реакцию системы на инициирующее событие, в данном случае — террористическую

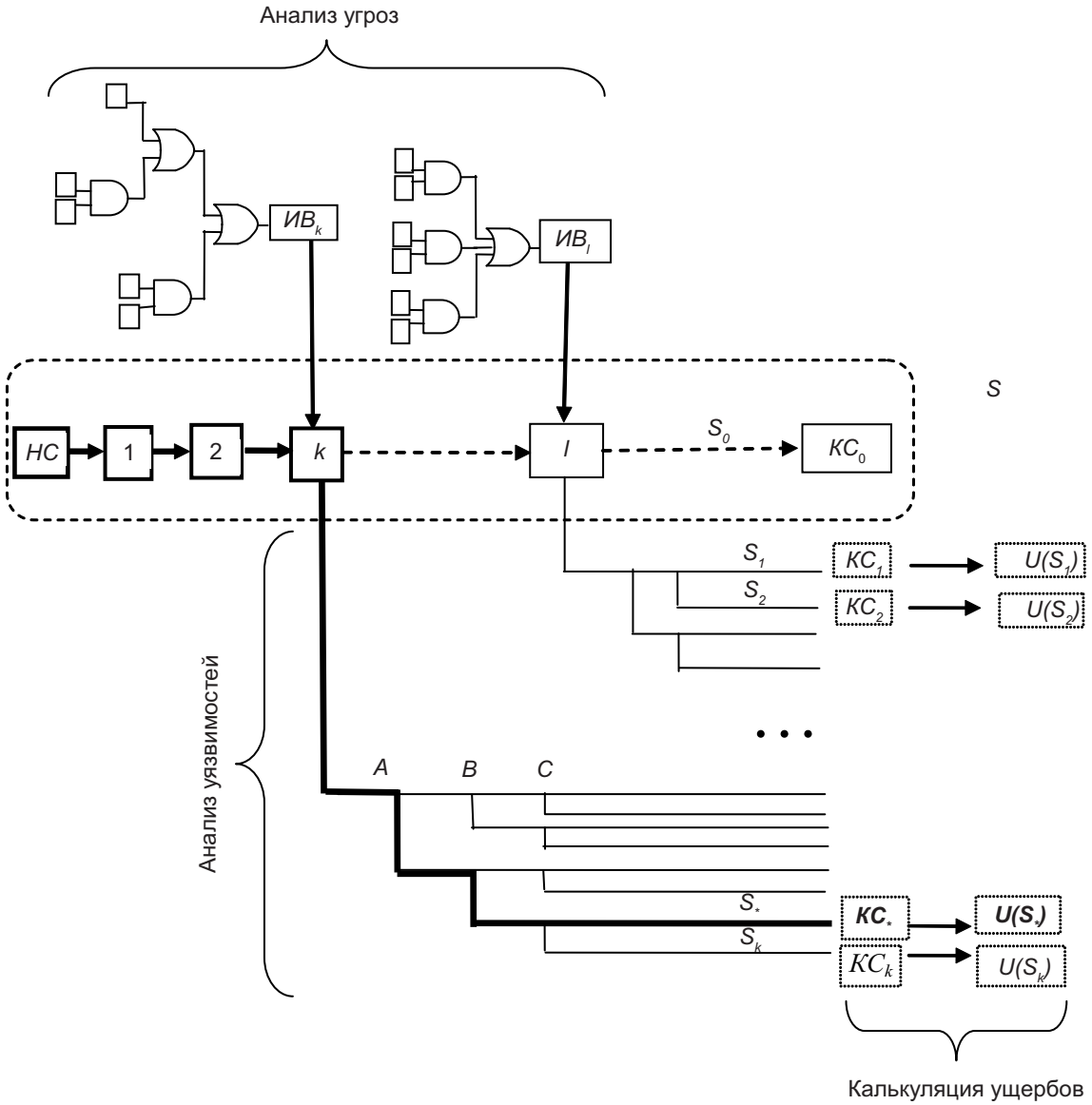


Рис. 10. Использование комбинированных графовых моделей для проведения анализа террористического риска

атаку, и позволяет проследить вероятностные связи между инициирующим событием и различными конечными состояниями системы. Структура дерева событий отражает вероятностные связи между случайными переменными системы (такими, как: вариант действий персонала, степень повреждения элементов системы, срабатывание механизма защиты). Сочетание возможных состояний случайных переменных определяет сценарий отказа в системе и, следовательно, конечное ее состояние. На рис. 10 литерами *A, B* и *C* обозначены такие случайные переменные. Выделенный сценарий S_* представляет собой последовательное выполнение событий $ИВ_k, \overline{A}, \overline{B}, C$ (черточка обозначает выполнение противоположного события, соответствующего нижней ветви, исходящей из узла). Вероятность реализации сценария S_* может быть подсчитана, как:

$$P[S_*] = P[ИВ_k] \cdot P[\overline{A} \mid ИВ_k] \cdot P[\overline{B} \mid (ИВ_k \overline{A})] \times \\ \times P[C \mid (ИВ_k \overline{A} \overline{B}).$$

Получив оценки вероятностей реализации различных сценариев отказа, можно построить матрицу уязвимости, характеризующую условные вероятности реализации различных сценариев при различных инициирующих воздействиях (см. п. 4, выражение (15)).

Более общая постановка задачи анализа уязвимости предполагает учет неопределенностей, в частности неопределенности относительно вероятности реализации случайных событий $ИВ_k, \overline{A}, \overline{B}, C$. При этом необходимо рассматривать вероятностные кривые распределения $p(ИВ_k)$, $p(\overline{A} \mid ИВ_k)$, $p(\overline{B} \mid ИВ_k\ \overline{A})$, $p(C \mid ИВ_k \overline{A}\,\overline{B})$, которые строятся на основе анализа имеющихся сведений E_j о реализации указанных событий с привлечением байесовой процедуры (рис. 11):

$$\varphi(S_*) = p(ИВ_i) \cdot p(\overline{A} \mid ИВ_i) \cdot p(\overline{B} \mid ИВ_i\ \overline{A}) \times \\ \times p(C \mid ИВ_i \overline{A}\,\overline{B}).$$

В этом случае вероятность реализации сценария S_* оценивается с помощью вероятностного распределения частоты реализации рассматриваемого сценария.

Заключительный этап процедуры анализа риска, предусматривающий калькуляцию ущербов, соответствующих различным конечным состояниям системы, выполняется с учетом первичных, вторичных и каскадных разрушений в рассматриваемой системе, сопряженных инфраструктурах и окружающей среде.

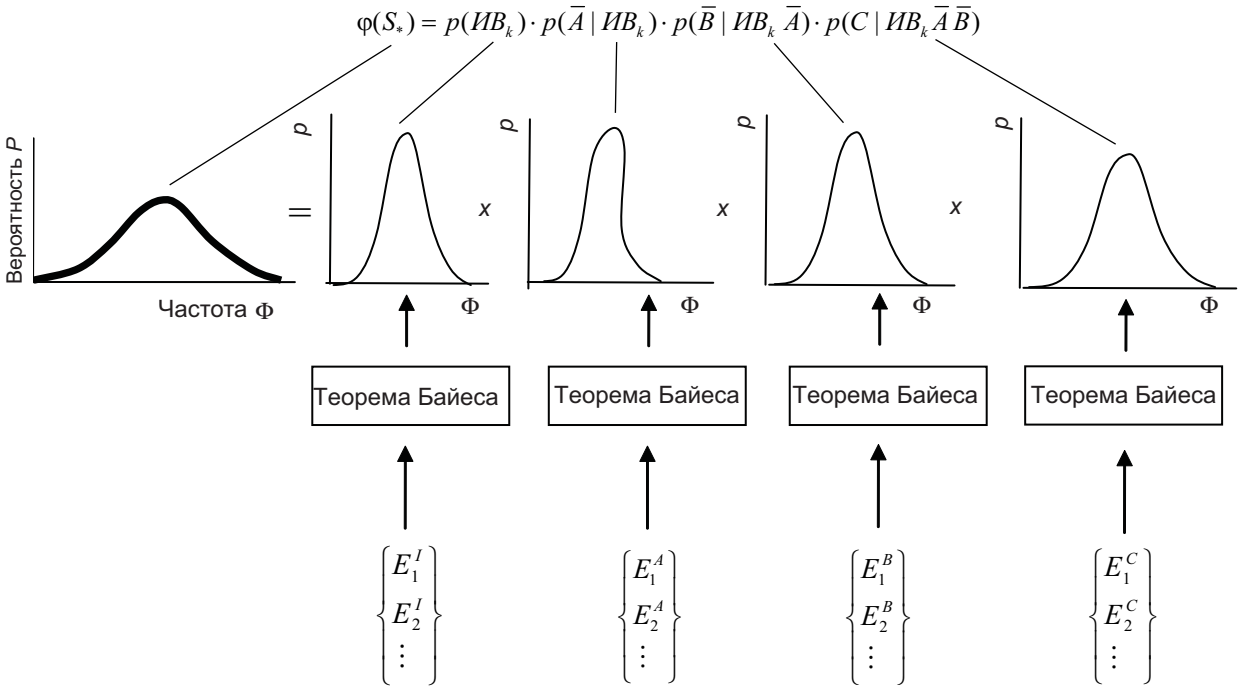


Рис. 11. Байесова процедура уточнения для получения оценки частоты реализации сценария отказов в виде кривой распределения

4. Анализ уязвимости системы в случае множественных сценариев отказов

Следует отметить, что если в системе могут быть реализованы различные сценарии отказов, развивающиеся после различных инициирующих воздействий и приводящие к различным конечным состояниям системы, то подход, базирующийся на определении уязвимости вида (1), не позволяет описать все многообразие вариантов невыполнения системой своих функций. В этом случае уязвимость системы не сводится к перечисленным выше индексам или отдельным характеристикам открытости системы к экстремальным воздействиям, а характеризуется структурой дерева сценариев отказов (рис. 12).

Иначе говоря, уязвимость системы характеризуется совокупностью сценариев случайных событий (отказов в системе) и причинно-следственных связей между этими событиями [11]. Уязвимость системы определяется вероятностями реализации различных конечных состояний системы, возникающих в случае эскалации аварии, развивающейся в системе после инициирующего события различного типа и интенсивности.

Анализ уязвимостей предполагает исследование последовательностей событий и причинно-следственных связей между событиями, происходящими вслед за инициирующим событием вплоть до достижения системой конечных состояний. Иными словами, анализ уязвимости системы заключается в проведении качественного и количественного исследования структуры сценариев эскалации аварии. Принципы построения сценарных деревьев, описывающих сценарии эскалации аварий, подробно изучаются в рамках *теории структурирования сценариев*, которая будет представлена ниже. Таким образом, анализ уязвимости предполагает детальное изучение дерева сценариев рассматриваемой системы.

Среди подходов теории структурирования сценариев центральное место занимают методы, базирующиеся на построении графовых моделей типа дерево событий или диаграмм влияния, описывающих вероятностные причинно-следственные связи между событиями в процессе эскалации аварии.

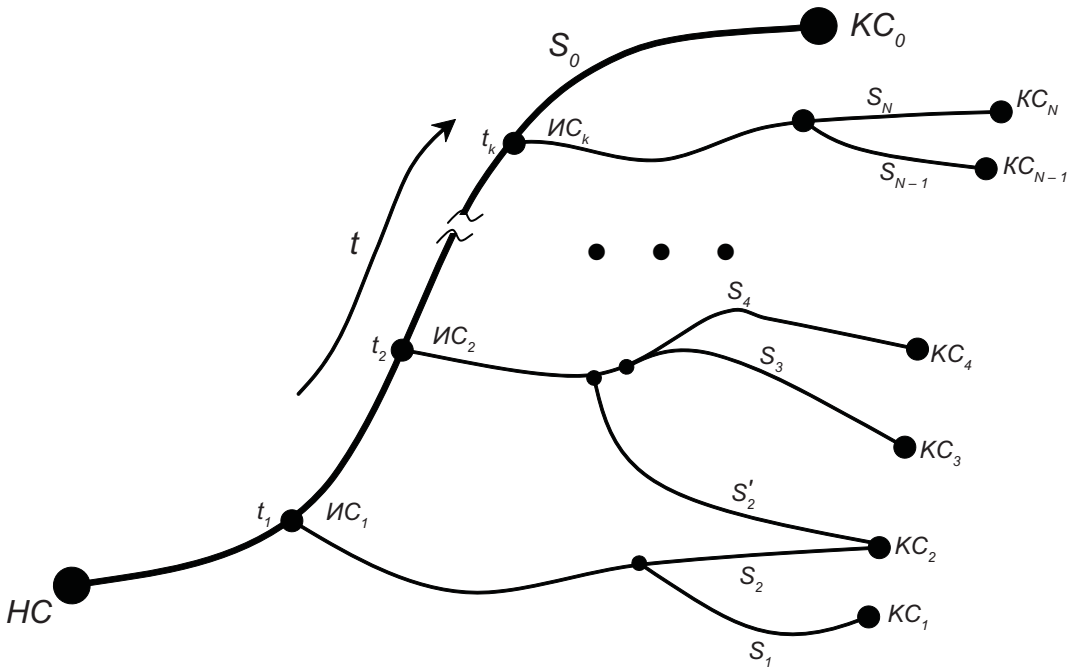


Рис. 12. Дерево сценариев отказов

Рассмотрим некоторую техническую систему, которая призвана обеспечить выполнение заданной функции или достижение определенного конечного состояния. Траектория в пространстве состояний, описывающая эволюцию системы от исходного состояния *НС* до требуемого конечного состояния $КС_0$, будет называться сценарием успеха S_0 (рис.12). В моменты времени t_1, t_2, ..., t_k в системе могут произойти инициирующие события ($ИС_i$), которые способны отклонить траекторию сценария S_0, запуская тем самым последовательность событий, соответствующих сценариям отказов S_1, S_2, ..., S_N, которые будут приводить к достижению системой соответствующих конечных состояний $КС_1$, $КС_2$, ..., $КС_N$. При этом следует иметь в виду, что различные сценарии отказа могут приводить к одному и тому же конечному состоянию системы. (В частности, сценарии S_2 и S_2' приводят к конечному состоянию $КС_2$.) Тогда уязвимость системы может быть представлена как матрица, компоненты которой $V_{ij,}$ будут представлять собой условные вероятности достижения системой конечного состояния $КС_i$ при условии того, что произошло инициирующее событие $ИС_j$: $V_{i,j} = P[КС_i \mid ИС_j]$.

$$V = \begin{bmatrix} P[КС_0 \mid ИС_1] & P[КС_1 \mid ИС_1] & P[КС_2 \mid ИС_1] & \cdots & P[КС_N \mid ИС_1] \\ P[КС_0 \mid ИС_2] & P[КС_1 \mid ИС_2] & P[КС_2 \mid ИС_2] & \cdots & P[КС_N \mid ИС_2] \\ P[КС_0 \mid ИС_3] & P[КС_1 \mid ИС_3] & P[КС_2 \mid ИС_3] & \cdots & P[КС_N \mid ИС_3] \\ & & \bullet\ \bullet\ \bullet & & \\ P[КС_0 \mid ИС_k] & P[КС_1 \mid ИС_k] & P[КС_2 \mid ИС_k] & \cdots & P[КС_N \mid ИС_k] \end{bmatrix} \quad (15)$$

Построив матрицу уязвимости, можно далее оценить индекс риска для рассматриваемой системы:

$$R = \overline{H} \cdot [V] \cdot \overline{U}\,, \quad (16)$$

где $\overline{H} = \{P[ИС_1]; P[ИС_2]; \ldots; P[ИС_m]$ — вектор угроз, компонентами которого являются вероятности реализации инициирующих событий $ИС_1, ИС_2, ...; ИС_m$.

$\overline{U} = \{U(КС_1); U(КС_2); \ldots; U(КС_N)\}$ — вектор ущербов, компонентами которого являются величины ущербов, соответствующих конечным состояниям $U(КС_1); U(КС_2); \ldots; U(КС_N)$.

Матрица уязвимости системы, представленной на рис. 13, может быть получена с помощью различных методов исследования графовых моделей (деревьев событий, деревьев отказов, байесовых сетей). В настоящей работе для построения матрицы уязвимо-

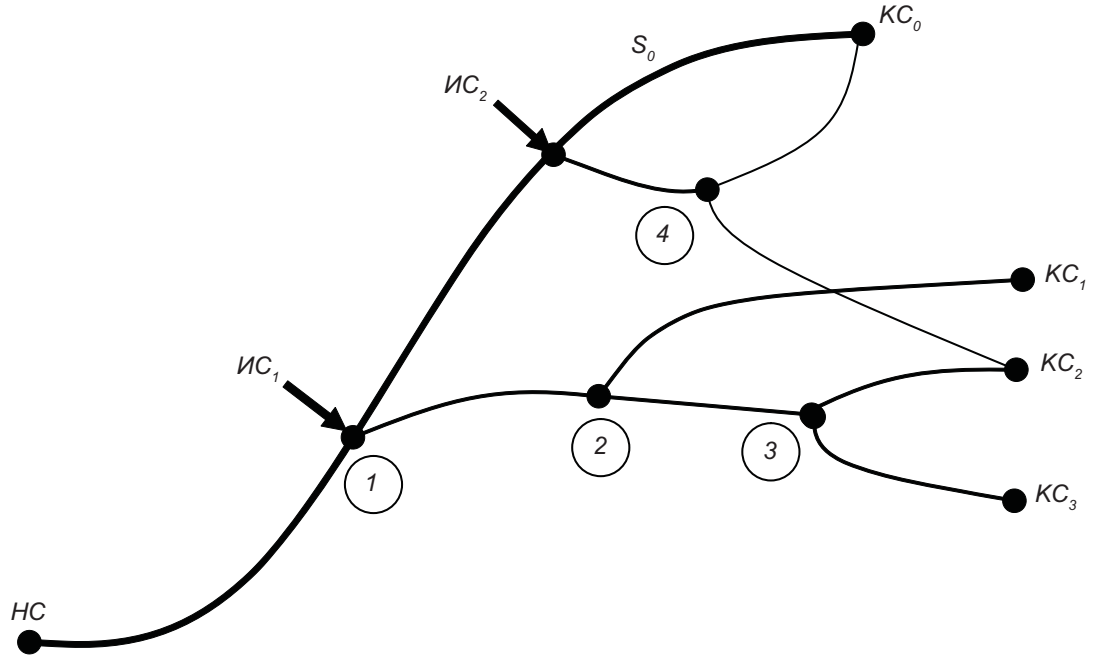


Рис. 13. Пример дерева сценариев отказов

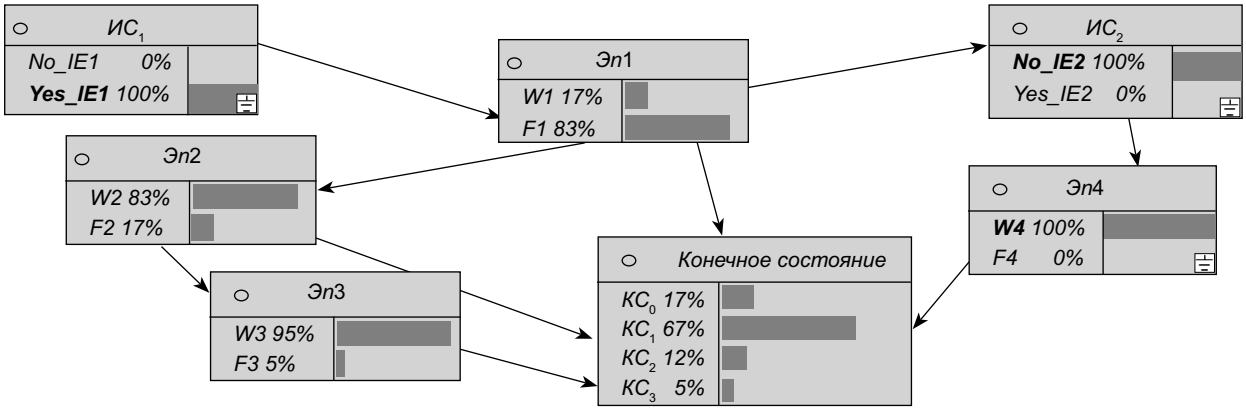
сти используется программный комплекс исследования байесовых сетей GeNie 2.0, разработанный в Питсбургском университете (США) [5]. Результаты численных расчетов представлены на рис. 14а , 14б и могут быть сведены в матрицу уязвимости системы

$$V = \begin{bmatrix} 0,17 & 0,67 & 0,12 & 0,05 \\ 0,52 & 0 & 0,48 & 0 \end{bmatrix}.$$

Пусть согласно экспертным оценкам вероятности реализации инициирующих событий для рассматриваемой в данном примере системы в течение года составляют $P[ИС_1] = 10^{-3}$ и $P[ИС_1] = 10^{-4}$, а величины ущербов, соответствующих возможным конечным состояниям, равны: $U(КС_0) = 0$, $U(КС_1) = 1 \cdot 10^6$ у. е., $U(КС_2) = 5 \cdot 10^6$ у. е. и $U(КС_3) = 1 \cdot 10^7$ у. е. В этом случае векторы угроз и ущербов принимают вид соответственно: $\overline{H} = [10^{-4}; 10^{-5}]$ и $\overline{U} = \{0; 1 \cdot 10^6; 5 \cdot 10^6; 1 \cdot 10^7\}$. Тогда согласно выражению (16) индекс риска для рассматриваемой системы будет составлять величину

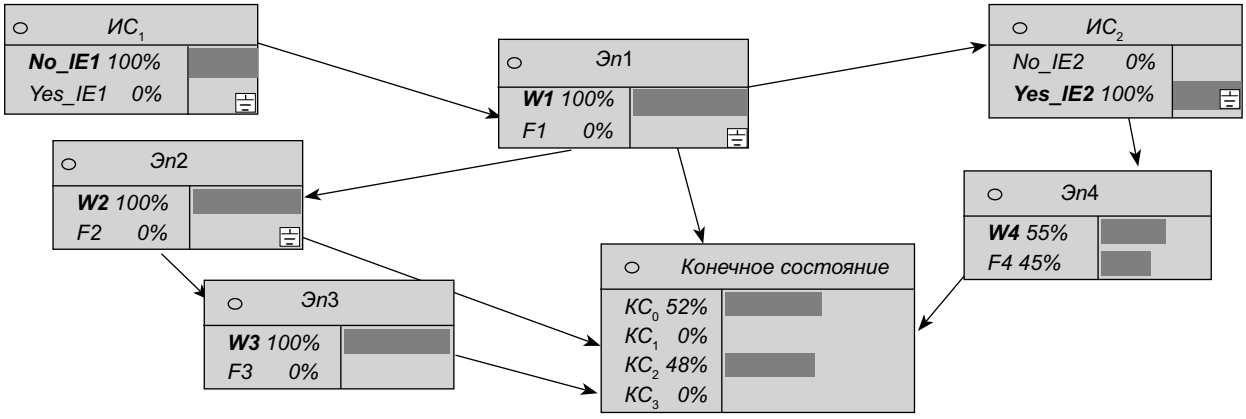
$$R = \{P[ИС_1]; P[ИС_2]\} \bullet \begin{bmatrix} P[КС_0 \mid ИС_1] & P[КС_1 \mid ИС_1] & P[КС_2 \mid ИС_1] & P[КС_3 \mid ИС_1] \\ P[КС_0 \mid ИС_2] & P[КС_1 \mid ИС_2] & P[КС_2 \mid ИС_2] & P[КС_3 \mid ИС_2] \end{bmatrix} \bullet \begin{Bmatrix} U(КС_0) \\ U(КС_1) \\ U(КС_2) \\ U(КС_3) \end{Bmatrix},$$

$R = 2010$ у. е. в год.



а) Вид графа при инициирующем воздействии $ИС_1$

$P[КС_0 \mid ИС_1] = 0,17$, $P[КС_1 \mid ИС_1] = 0,67$, $P[КС_2 \mid ИС_1] = 0,12$, $P[КС_3 \mid ИС_1] = 0,05$



б) Вид графа при инициирующем воздействии $ИС_2$

$P[КС_0 \mid ИС_2] = 0,52$, $P[КС_1 \mid ИС_2] = 0$, $P[КС_2 \mid ИС_2] = 0,48$, $P[КС_3 \mid ИС_2] = 0$

Рис. 14. Пример подсчета компонентов матрицы уязвимости системы

Заключение

Представленный анализ позволяет сформулировать принципы, которые необходимо учитывать при оценке уязвимости технических систем:

1. Для рассматриваемой системы должны быть детально описаны сценарий успеха, требования, предъявляемые к системе, и искомое конечного состояния $КС_0$, обеспечивающее выполнение системой заданных функций.

2. Оценка уязвимости технической системы должна быть вероятностной. Причем поскольку понятие «уязвимость» характеризует реакцию системы на инициирующие воздействия, то уязвимость должна определяться как условная вероятность отказа в случае осуществления инициирующего события.

3. В случае если в системе могут реализовываться различные инициирующие события и множественные сценарии отказов, уязвимость системы должна характеризоваться сценарным графом, описывающим вероятностные причинно-следственные связи между событиями в процессе эскалации аварии (от инициирующих событий до конечных состояний).

Оценка уязвимости системы является ключевым этапом анализа риска. Она следует за оценкой угроз, которым подвергается техническая система, и формирует основу для последующей оценки ущербов. Результатами оценки уязвимости являются условные вероятности достижения системой тех или иных конечных состояний в случае осуществления различных инициирующих воздействий на систему.

Литература

1. Махутов Н.А., Резников Д.О. Использование байесовых сетей для оценки террористических рисков и выбора оптимальной стратегии противодействия террористической угрозе// Проблемы безопасности и чрезвычайных ситуаций, 2007, № 5, с. 43—63.
2. Петров В.П., Резников Д.О., Куксова В.И., Дубинин Е.Ф. Оценка террористического риска и принятие решений о целесообразности построения систем защиты от террористических воздействий//Проблемы безопасности и чрезвычайных ситуаций, 2007, № 1, с. 89—105.
3. Рогозин А.Л., Ларионов В.И., Фролова Н.И. и др. Оценка и управление природными рисками. М.: «КРУК», 2003, 315 с.
4. Apostolakis G. Infrastructure Vulnerabilities due to Random Failures and Malevolent Acts. Presented at Decision and Risk Analysis Conference. University of Texas. USA, Dallas. 2007.
5. Decision System Laboratory, University of Pittsburg, USA. http://genie.sis.pitt.edu
6. Einarssonl S., Rausand M.. An Approach to Vulnerability Analysis of Complex Industrial Systems. Risk Analysis, Vol. 18, No. 5. 1998.
7. Garrick B., , Hall J., Kilger M., McDonald J., O'Toole T, Probst P., Rindskopf Parker E., Rosenthal R., Trivelpiece A., Van Arsdale L., Zebrosk E. Confronting the risks of terrorism: making the right decisions. Reliability Engineering and System Safety 86, 2004.
8. Haimes Y. On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. Risk Analysis, Vol. 26, No. 2, 2006.
9. Holmgren A. Using Graph Models to Analyze the Vulnerability of Electric Power Networks. Risk Analysis, 2006, Vol. 26, No. 4.
10. Jenelius E. Graph Models of Infrastructures and the Robustness of Power Grids. Master of Science Thesis. 2004
11. Kaplan S., Visnepolschi S., Zlotin B., Zusman A. New Tools for Failure and Risk Analysis. Anticipatory Failure Determination and the Theory of Scenario Structuring.
12. Kaplan S., Y. Haimes , B. Garrick. Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinery of the Definition of Risk. Risk Analysis, 2001, Vol. 21, No. 5.
13. Lind N. A measure of vulnerability and damage tolerance, Reliability analysis and safety systems. 1995, N48.
14. Moselhi O, Hammad A, Alkass S., Vulnerability Assessment of Civil Infrastructure Systems: A Network Approach. 1st CSCE Specialty Conference on Infrastructure Technologies, Management and Policy. Toronto, Ontario, Canada. June 2-4, 2005.