УДК 519

ВЛИЯНИЕ ВНУТРЕННЕЙ СТРУКТУРЫ СЛОЖНОЙ СИСТЕМЫ НА ЕЕ ИНТЕГРАЛЬНЫЙ РИСК НА ПРИМЕРЕ ЗАДАЧИ МИНИМИЗАЦИИ РИСКА В ДРЕВОВИДНОЙ СТРУКТУРЕ

А. А. Широкий*, А. О. Калашников**

*,**Институт проблем управления им. В. А. Трапезникова РАН, г. Москва

*✉ shiroky@ipu.ru, **✉ aokalash@ipu.ru

Аннотация. Одной из наиболее общих математических постановок задачи управления рисками является задача «Защитник – Атакующий». Ее суть состоит в том, что указанные игроки с противоположными целями назначают элементам рассматриваемой системы некоторые объемы ресурсов из ограниченного пула таким образом, чтобы значение наперед заданной функции риска было, соответственно, минимальным или максимальным. В предположении независимости элементов системы эта задача исследована достаточно подробно. Однако элементы сложных систем связаны и влияют друг на друга, что приводит к значительным отклонениям измеряемого риска от прогнозируемого значения. Модели риска, учитывающие взаимное влияние элементов системы друг на друга, периодически встречаются в литературе, но системного понимания характера и степени влияния структуры сложной системы на ее интегральный риск пока не сформировано. С этой целью авторами запланирована публикация серии работ, в которых изучается влияние структур все возрастающей сложности на интегральный риск защищаемой системы. В ранее опубликованных работах были рассмотрены простая цепная и звездообразная структуры. В настоящей работе ранее полученные результаты обобщены на случай произвольной древовидной структуры. Поставлена задача оптимального с точки зрения минимизации риска размещения элементов в древовидной структуре, рассчитаны верхние оценки относительной погрешности ее приближенного алгоритмического решения для деревьев с небольшим числом ветвей и листьев, проанализировано поведение полученных оценок при увеличении числа листьев и ветвей. Показано, что полученные значения оценок не превосходят аналогичных, полученных для звездообразных структур в предшествующих работах авторов.

Ключевые слова: сложные системы, риск, структура системы, управление рисками, алгоритмы минимизации риска, задача оптимального размещения элементов.

ВВЕДЕНИЕ

Сложность дисциплины управления рисками обусловлена, в первую очередь, ее мультидисциплинарностью. Так, в книге [1] выделены 15 «размерностей» (*dimensions*) управления рисками, включающих в себя как сравнительно узкие предметные области (управление риском в цепочках поставок, управление финансовыми рисками), так и глобальные – например, вопросы этики в управлении рисками. Во второй части той же книги обсуждаются шесть кросс-дисциплин, частично перекрывающих все предметные области, а именно (в скобках даны оригинальные названия на английском языке): риск-культура (*risk culture*), принятие решений на основе риска (*risk-based decision making*), управление рисками в сложных системах (*risk leadership in complexity*), устойчивость (*resilience*), информационная неопределенность (*communication uncertainty*), риск в управлении ор-

ганизационными изменениями (*organizational change management and risk*). Приведенная выше классификация не является ни полной, ни единственно возможной. Она иллюстрирует тот факт, что управление рисками можно обсуждать в привязке к специфике конкретной управляемой системы, а можно – применительно к процессам и свойствам, характерным для целых классов систем. При этом будут отличаться не только применяемые модели и методы, но и используемая терминология (в частности, многие фигурирующие в книге [1] термины не имеют устоявшегося русскоязычного эквивалента), и даже само определение риска.

В условиях отсутствия общепринятой универсальной модели управления рисками объединяющую роль играют базовые принципы, верные для любой управляемой системы. Этот факт нашел отражение в стандарте ГОСТ Р ИСО 31000–2019: «Менеджмент риска. Принципы и руководство» [2], который также предлагает достаточно общее определение риска как следствия влияния неопределенности на достижение поставленных целей. При этом отмечается, что под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и (или) негативное). Но для использования такого определения на практике необходимо научиться *измерять* цели, неопределенность и вызываемые ею отклонения. Отсюда следует необходимость исследования количественных соотношений для управления рисками с применением соответствующего математического аппарата.

Исходя из природы управления рисками, заключающегося в минимизации отклонений, математическая задача управления риском должна принадлежать к классу задач оптимизации (в случае наличия в системе игроков со стратегическим поведением постановка может также быть теоретико-игровой – см., например, работы [3–5]). Однако попытка поиска исследований, посвященных математическим моделям управления рисками, не привязанным к конкретному объекту, их классу или предметной области, скорее всего, будет неудачной. Причиной этого является то, что если работа посвящена математическим моделям оптимизации, применяемым в риск-менеджменте, то она будет относиться к соответствующему разделу математики, а не к управлению рисками. Если же речь идет именно об управлении рисками, то в работе будет обозначен управляемый объект, что привяжет работу к его специфике.

Тем не менее, вполне можно предположить существование моделей, достаточно универсальных, чтобы с их помощью можно было количественно рассматривать общие принципы управления рисками, но не привязанных к конкретным управляемым объектам, системам или их классам. По всей видимости, в наибольшей степени этому критерию отвечает модель защищаемой системы, представляющая собой взвешенный ориентированный граф, вершины которого являются элементами системы (объектами произвольной природы), а дуги с назначенными весами характеризуют направление и силу связей между элементами, имеющих значение для задачи управления рисками.

Отметим, что в общем случае такой граф является сложной сетью произвольной топологии. Моделируемый объект управления – защищаемая система – может представлять собой социальную сеть [6], сеть организаций [7], компьютерную сеть [8] или относиться к иному классу. Необходимо отметить, что в настоящей статье авторы работают с чисто математической постановкой задачи. Это означает, что структура защищаемой системы вовсе не обязательно отражает именно физическую или организационную структуру объекта, моделью которого является. В то же время дуги орграфа показывают взаимное влияние элементов друг на друга. Например, при решении задачи снижения рисков наступления авиационных происшествий в регионе модель будет скорее отражать структуру причинно-следственных связей между типами происшествий, их предпосылками и факторами влияния, нежели связи между элементами инфраструктуры управления воздушным движением. Если с точки зрения передачи риска друг другу все элементы системы независимы, то адекватной моделью такой ситуации будет частный случай безреберного графа.

В общем виде задачу управления рисками в сложных сетях можно сформулировать следующим образом.

Рассмотрим защищаемую систему, состоящую из конечного множества элементов (объектов, пока произвольной природы): $S = \{s_1, ..., s_i, ..., s_n\}$, $i \in N = \{1, ..., n\}$, $n \in \mathbb{N}$. Предположим, что существуют два субъекта (также пока произвольной природы), которых будем называть игрок *A* (иначе, Атакующий, *Attacker*) и игрок *D* (иначе, Защитник, *Defender*), имеющие несовпадающие интересы относительно состояния системы *S*.

Будем считать, что игрок D располагает некоторым объемом ресурса $X \geq 0$, который он может произвольным образом распределять между элементами системы S: $x = (x_1, \ldots, x_n)$, $x_i \geq 0$, $i \in N$, $\sum_{i=1}^{n} x_i \leq X$. Аналогично будем считать, что игрок A также располагает некоторым объемом ресурса $Y \geq 0$, который он может произвольным образом распределять между элементами системы S: $y = (y_1, \ldots, y_n)$, $y_i \geq 0$, $i \in N$, $\sum_{i=1}^{n} y_i \leq Y$.

В рамках рассматриваемой модели под ресурсом будем понимать любой измеримый и произвольно делимый ресурс, который может быть представлен неотрицательным действительным числом. В качестве ресурсов, в зависимости от контекста, могут пониматься финансовые, трудовые, временны́е, производственные и иные ресурсы (затраты).

Допустим, что воздействие в части передачи рисков описано взвешенным орграфом $G(S, W)$, $W \subseteq S \times S$, $w_{ij} = (s_i, s_j) \in W$, $i, j \in N$. Положим, что на $G(S, W)$ заданы функции

$$\rho : s \to \mathbb{R}_+^0, \ \sigma : W \to \mathbb{R}_+^0,$$

где ρ_i, $i \in N$ – «вес» узлов, отражающий текущее значение локального риска, а σ_{ij}, $i, j \in N$, – «вес» дуг, отражающий «интенсивность» передачи риска между элементами рассматриваемой системы. Матрица $\Sigma = \|\sigma_{ij}\|$ отражает степень (или силу) влияния i-го элемента системы S на j-й. Начальное (при $t = 0$) значение функций $\rho_i = \rho_i(x, y, t) = \rho_i(x, y, t = 0)$ определяется распределениями ресурсов x и y. Значения весов ρ_i при $t > 0$ зависят только от предшествующих по времени значений этих функций. Изменение значений весов элементов в результате их взаимного влияния друг на друга будет описываться следующим выражением:

$$\rho_i(t+1) = \rho_i(t) + \sum_{k=1}^{n} \sigma_{ik} \left(\rho_i(t) - \rho_i(t-1) \right), \quad t = 0, 1, \ldots; \ \rho_i(t = 0) = \tilde{\rho}_i. \tag{1}$$

Аргументы x, y в записи выше пропущены для компактности.

Обозначим $\mathcal{X}(X)$ множество допустимых распределений ресурса X между элементами системы S игроком D, а $\mathcal{Y}(Y)$ – множество допустимых распределений ресурса Y между элементами системы S игроком A:

$$\mathcal{X}(X) = \left\{ (x_1, \ldots, x_n) \in \mathbb{R}_+^n : x_i \geq 0, \ i \in N, \ \sum_{i=1}^{n} x_i \leq X \right\},$$

$$\mathcal{Y}(Y) = \left\{ (y_1, \ldots, y_n) \in \mathbb{R}_+^n : y_i \geq 0, \ i \in N, \ \sum_{i=1}^{n} y_i \leq Y \right\}.$$

Тогда задача игрока D («задача Защитника») заключается в нахождении распределения ресурса $x^* \in X$, минимизирующего интегральный риск (т. е. риск, характеризующий уязвимость системы в целом), и формально может быть записана в следующем виде:

$$x^* = \operatorname*{Argmin}_{x \in X} \lim_{t \to \infty} \rho(x, y, t) = \operatorname*{argmin}_{x \in X} \sum_{i=1}^{n} \lim_{t \to \infty} \rho_i(x, y, t). \tag{2}$$

Решение этой задачи с ограничениями на собственные значения матрицы взаимного влияния элементов приведено в работе [8]. При этом необходимо отметить, что для такой постановки задачи требуется с достаточной точностью идентифицировать не только текущие значения локальных рисков и функциональные зависимости $\rho(x, y, \cdot)$, но еще и количественно охарактеризовать взаимное влияние локальных рисков. Для реально существующих систем это может оказаться крайне трудоемко и даже невозможно. По этой причине актуальной становится задача нахождения общих принципов управления рисками системы, имеющей сложную сетевую структуру, которые позволили бы достигать эффекта снижения риска даже в условиях неполной информации. Решению этой задачи для древовидных структур и посвящена предлагаемая статья.

Структура изложения материала в работе следующая. В § 1 содержится краткий обзор математических моделей распространения отказов в сложных сетях. В § 2 приведена общая постановка задачи управления риском сложной системы с древовидной структурой. В § 3 предложено субоптимальное решение этой задачи. В заключении обсуждаются дальнейшие перспективы исследования.

1. КРАТКИЙ ОБЗОР МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ ОТКАЗОВ В СЛОЖНЫХ СЕТЯХ

В самом общем случае можно считать, что структура сложной системы является сложной сетью произвольной топологии. Успешной атакой

(или, по-другому, отказом) некоторого элемента системы будем считать наступление события, при котором этот элемент системы перестает выполнять свою функцию. Для простоты в настоящей работе будем рассматривать только бинарный случай – когда элемент функционален либо нефункционален полностью. Для исследования различных деструктивных эффектов (включая целенаправленные атаки на узлы и ребра) в таких сетях разработано достаточно много моделей и постоянно появляются новые. Весьма широко применяются модели оценки риска распространения отказов при исследовании сложных систем различной природы – в частности, киберфизических [9–17], вычислительных [18–19] и медико-социальных [20–22].

Ранние модели описывали развитие отказов, вызванных нецеленаправленными (например, случайными) воздействиями. Наиболее известными из них являются модель устойчивости к ошибкам [23–25], модель распространения лесного пожара [26–28] и ее производные, модели на базе клеточных автоматов [29–32], а также модели перколяции со случайными атаками [33]. Отметим, что последние имеют ряд модификаций, предполагающих, что деструктивные воздействия на узлы и ребра сети являются целенаправленными. К таковым относятся собственно перколяции с целенаправленными атаками [34–36], а также перколяции с локализованными атаками [37–40] и перколяции с *k*-ядром [41–43].

Упомянутые выше модели распространения отказов хорошо сочетаются с классическими моделями управления рисками в сложных сетях «Защитник – Атакующий» [44–46]. Напомним, что такие модели описывают конфликт между двумя игроками – Защитником и Атакующим – имеющими противоположные цели относительно рассматриваемой системы. Атакующий расходует ресурсы из некоторого доступного ему ограниченного пула с целью вывести систему из строя. Защитник, в свою очередь, пытается противостоять действиям Атакующего. В классических постановках Защитник решает задачу оптимального распределения ресурсов среди элементов системы с целью минимизации ее интегрального риска. Но он может выбрать и другой путь, а именно – модифицировать структуру самой системы с той же самой целью. Для описания такого сценария требуются другие модели.

Учет изменения структуры подразумевают, например, модели каскадного распространения ошибки [47, 48], однако в их рамках такие изменения не предполагаются целенаправленными. Возможность намеренного изменения структуры предусмотрена в моделях, модифицированных для случая двух взаимосвязанных сетей [49–51], но именно в отношении ребер, связывающих сети между собой.

Таким образом, для решения задач управления структурой сложной системы, в том числе с целью минимизации ее интегрального риска, существующего аппарата моделирования недостаточно. В настоящей (и ряде предшествующих) работ авторы сконцентрировались на том, чтобы рассчитать влияние на риск собственно структуры, безотносительно выделяемых ресурсов.

С этой целью базовая задача (2) была переформулирована таким образом, чтобы вместо поиска оптимального назначения ресурсов элементам системы с зафиксированной структурой осуществлялись бы поиск оптимального размещения элементов в некоторой заданной структуре и сравнение структур между собой. Решать эту задачу «в лоб» не получается из-за высокой вычислительной сложности, поэтому авторы ищут приближенные решения для различных типов структур в порядке возрастания их сложности, а именно:

1) простая цепь – получено аналитическое решение, см. работу [52];

2) «звезда» – предложено приближенное решение с гарантированной погрешностью [53];

3) древовидная структура – рассматривается в настоящей работе;

4) произвольная структура – решение будет построено на основе обобщения результатов, полученных для более простых структур.

Отметим, что в общем виде задача эффективного управления сложной системой в условиях неопределенности эквивалентна задаче минимизации риска, где под риском понимается измеримое отклонение от максимально эффективного (целевого) режима функционирования рассматриваемой системы [2] – математическая эквивалентность постановок показана, например, в работе [54]. Поэтому, хотя проблема синтеза или совершенствования структуры, в частности, организационной системы управления, несомненно, не сводится только лишь к распределению ресурсов, а уровень риска – лишь один из ключевых показателей эффективности ее функционирования, в смысле обеспечения достижения целей системы управления его, по-видимому, следует считать наиболее важным.

2. ПОСТАНОВКА ЗАДАЧИ УПРАВЛЕНИЯ РИСКОМ СЛОЖНОЙ СИСТЕМЫ С ДРЕВОВИДНОЙ СТРУКТУРОЙ

Предположим, что защищаемая система включает в себя n элементов $s_1,..., s_n \in S$, $n \in \mathbb{N}$. Пред-

положим также, что каждому из них сопоставлены два числа: $p_i^0 \in (0, 1]$ – удельная вероятность успешной атаки на i-й элемент; $u_i > 0, u \in \mathbb{R}^+$ – величина ущерба, который будет нанесен в случае успешной атаки i-го элемента.

Определение 1. Удельным риском i-го элемента назовем величину $\rho_{s_i}^0 = u_i p_i^0$. ♦

Зададим структуру $W_m = \langle G(V, E), T \rangle, T \subseteq V,$ где $G(V, E)$ – ориентированный граф с множеством вершин V и множеством дуг E, а T – подмножество V, которое будем называть *периметром*. В настоящей работе будем рассматривать структуры с периметром, состоящим ровно из одной вершины.

Определение 2. Будем говорить, что последовательность векторов

$$B = \{(b_{01}, \ldots, b_{0q_0}), (b_{11}, \ldots, b_{1q_1}), \ldots, (b_{l1}, \ldots, b_{lq_l}), \ldots, (b_{L1}, \ldots, b_{Lq_L})\},$$
$$b, L, q_l \in \mathbb{N}, l \in \mathbb{N} \cup \{0\}$$

определяет направленное дерево с m листьями, если:

- число $b_{li}, i \in \{1, \ldots, q_l\}$, обозначает число дуг, выходящих из соответствующей вершины;
- число L равно длине максимального пути;
- число $q_l, l \le L,$ определяет число вершин яруса l (длина пути из корня до которых равна l);
- $q_0 = 1; q_l = \sum_{i=1}^{q_{l-1}} b_{(l-1)i} \; \forall l > 0; q_L = m;$
- $b_{L1} = b_{L2} = \ldots = b_{Lq_L} = 0$. ♦

Определение 3. Будем говорить, что порожденная последовательностью B структура системы имеет тип «дерево с m листьями», и записывать $W_m = \langle G(V, E), T \rangle$, если

$$V = \left\{ \{v_0\} \cup \bigcup_{j=1}^{b_{01}} \{v_{0j}\} \cup \bigcup_{i=1}^{q_1} \bigcup_{j=1}^{b_{1i}} \{v_{0ij}\} \cup \ldots \right.$$
$$\left. \ldots \cup \bigcup_{i=1}^{q_{L-1}} \bigcup_{j=1}^{b_{(L-1)i}} \{v_{0\ldots ij}\} \right\};$$

$$E = \left\{ \bigcup_{j=1}^{b_{01}} \{(v_0, v_{0j})\} \cup \bigcup_{i=1}^{q_1} \bigcup_{j=1}^{b_{1i}} \{(v_{0i}, v_{0ij})\} \cup \ldots \right.$$
$$\left. \ldots \cup \bigcup_{i=1}^{q_{L-1}} \bigcup_{j=1}^{b_{(L-1)i}} \{(v_{0\ldots i}, v_{0\ldots ij})\} \right\}; \; T = \{v_0\}. \blacklozenge$$

Пример дерева с четырьмя листьями на третьем ярусе приведен на рис. 1. Отметим, что частным случаем дерева, когда $b_{li} = 1, q_l = m \;\; \forall l < L, l \ne 0$, является структура типа «звезда с m лучами». Соответствующие типы структур рассматривались авторами ранее в работе [53].

Определение 4. Взаимно однозначное отображение $M^{-1} : S \to V$ будем называть размещением элементов S в древовидной структуре W_m. Соответствующее обратное отображение $M : V \to S$ будем называть проекцией дерева W_m на множество элементов S. ♦

Отметим, что для существования такого отображения необходимо равенство между числом вершин графа $G(V, E)$ и числом элементов защищаемой системы. В случае бесконечного числа вершин множества V и S должны быть счетными.

Определение 5. Интегральным риском системы со множеством элементов S, размещенных в древовидной структуре W_m с помощью взаимно однозначного отображения $M^{-1} : S \to V$, будем называть величину

$$\rho\left(S, W_m, M^{-1}\right) = \rho_{M(v_o)} + \sum_{j=1}^{b_{01}} \rho_{M(v_{0j})} + \sum_{i=1}^{q_1} \sum_{j=1}^{b_{1i}} \rho_{M(v_{0ij})} + \ldots + \sum_{i=1}^{q_{L-1}} \sum_{j=1}^{b_{(L-1)i}} \rho_{M(v_{0\ldots ij})}. \blacklozenge \quad (3)$$

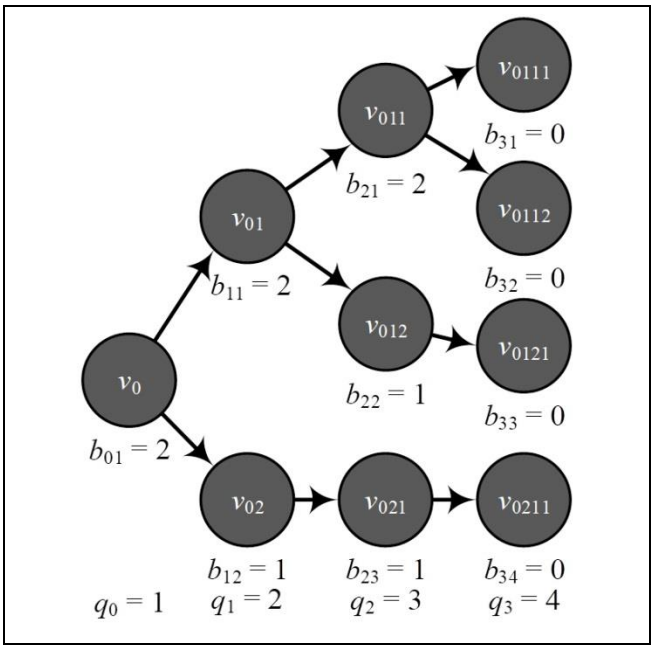

Рис. 1. Пример дерева с $m = 4$, $L = 3$. Индексы вершин являются уникальными и отражают простой путь до периметра – в него входят все вершины с индексами, являющимися подстроками индекса рассматриваемой вершины

Пусть защищаемая система включает в себя множество элементов $S=\{s_1, s_2,..., s_n\}$, $n\in\mathbb{N}$, с соответствующими им удельными вероятностями успешной атаки $P=\{p^0_{s_1}, p^0_{s_2}, p^0_{s_n}\}$ и ущербами $U=\{u_{s_1}, u_{s_2},..., u_{s_n}\}$. Предположим также, что возможные пути атаки задаются древовидной структурой $W_m=\langle G(V, E), T\rangle$, где $\sum_{l=1}^{L} q_l = n$. Тогда задача минимизации интегрального риска защищаемой системы заключается в нахождении такого размещения M^{-1} элементов S в структуре W_m, что

$$\rho(S, W_m, M^{-1})\to\min. \qquad (4)$$

Для частного случая $m = 1$ в работе [52] описано точное решение. Для случая $q_1 = m\ \forall l < L, l\neq 0$ в работе [53] получено субоптимальное решение с априорной оценкой относительной погрешности. Далее аналогичным образом найдем такую оценку для рассматриваемых в настоящей работе древовидных структур.

3. ПРИБЛИЖЕННОЕ РЕШЕНИЕ ЗАДАЧИ ОПТИМАЛЬНОГО РАЗМЕЩЕНИЯ ЭЛЕМЕНТОВ В ДРЕВОВИДНОЙ СТРУКТУРЕ

Предположим, что величины ущербов в случае успешной атаки для всех элементов системы оцениваются одинаково, т. е. $u_{s_i}=u\ \forall i\in\{1,..., n\}$. Тогда задача (4) принимает следующий вид:

$$\rho\left(S, W_m, M^{-1}\right)=u\left(p_{M(v_0)}+\sum_{k=0}^{L-1}\sum_{i=1}^{q_k}\sum_{j=1}^{b_{ki}}\left(p_{M(v_{0...ij})}\cdot\right.\right. \qquad (5)$$

$$\left.\left.\cdot p_{M(v_{0...i})}\cdot....\cdot p_{M(v_0)}\right)\right)\to\min.$$

Потребуем также, чтобы выражение

$$p_{M(v_0)}+\sum_{k=0}^{L-1}\sum_{i=1}^{q_k}\sum_{j=1}^{b_{ki}}\left(p_{M(v_{0...ij})}p_{M(v_{0...i})}\cdot....\cdot p_{M(v_0)}\right)$$

являлось конечным для любых значений L и $m=q_L$. С этой целью ограничим удельные риски элементов величиной, называемой предельно допустимым удельным риском и определяемой следующим образом (см. также работу [53]).

Определение 6. Предельно допустимым удельным риском элемента защищаемой системы, размещенного в структуре $W_m=\langle G(V, E), T\rangle$, назовем величину

$$\rho^0_{\max}=\frac{u}{1+\sqrt{m}}.\ \blacklozenge$$

Отметим, что при выполнении ограничения $p_i\le\frac{1}{1+\sqrt{m}}=p^0_{\max}$ справедливо следующее неравенство:

$$\rho\left(S, W_m, M^{-1}\right)\le$$

$$\le u\left(p^0_{\max}+\sum_{k=0}^{L-1}\sum_{i=1}^{q_k}\sum_{j=1}^{b_{ki}}\left(p^0_{\max}\right)^{k+1}\right)\le u. \qquad (6)$$

Равенство в формуле (6) достигается в случае $L = \infty$ для любого конечного m. Важным обстоятельством является то, что в силу построения величины (6), полученные ранее для звездообразной структуры [53, *табл. 2*] верхние оценки приращения значения интегрального риска по мере удаления от периметра остаются верными и для древовидных структур. Это позволяет рассчитывать на то, что приведенные в той же работе верхние оценки относительного отклонения от оптимального решения в случае произвольного размещения в структуре элементов на фиксированном удалении от периметра удастся использовать для деревьев.

Для того, чтобы это проверить, проведем серию численных экспериментов по аналогии с работой [53]. Введем следующие ограничения:

$$\begin{cases} u=1; \\ 0<p^0_{M(v_{0...i})}\le p^0_{M(v_{0...ij})} \\ \quad \forall i\in\{1,..., q_k\}, j\in\{1,..., b_{ki}\}, k\in\{0,..., L-1\}; \\ p^0_{M(v_{0...ij})}\le\frac{u}{1+\sqrt{m}} \\ \quad \forall i\in\{1,..., q_k\}, j\in\{1,..., b_{ki}\}, k\in\{0,..., L-2\}; \\ p^0_{M(v_{0...ij})}\le\sum_{l=L}^{\infty}\left(\frac{u}{1+\sqrt{m}}\right)^{l+1} \\ \quad \forall i\in\{1,..., q_{L-1}\}, j\in\{1,..., b_{(L-1)i}\}. \end{cases}$$

Будем генерировать выражения вида (3) для всех размещений, получаемых путем перестановки элементов, находящихся на первом и более дальних ярусах дерева, т. е. на фиксированном расстоянии k от периметра, начиная с $k = 1$. Для каждого k потребуется рассмотреть случаи $q_k = 2,..., m$, соответствующие деревьям с q_k вершинами k-го яруса. Затем рассмотрим все возможные модули разности этих выражений, для каждого из которых проведем поиск глобального максимума. Разделив найденное значение на минимум разности этих двух выражений, получим величину относительного отклонения. Максимум таких отклонений даст

верхнюю оценку относительной погрешности решения задачи (5).

Результаты вычисления величин относительной погрешности для небольших деревьев приведены в таблице.

На рис. 2 показано поведение полученных значений относительной погрешности на ярусах 1–4 в зависимости от числа выходящих из вершин (речь идет, соответственно, о подмножествах $\{v_{0j}\}_{j=1}^{b_{01}}$ (рис. 2, *а*), $\left\{\{v_{0ij}\}_{j=1}^{b_{1i}}\right\}_{i=1}^{q_1}$ (рис. 2, *б*), $\left\{\{v_{0...ij}\}_{j=1}^{b_{2i}}\right\}_{i=1}^{q_2}$ (рис. 2, *в*) и $\left\{\{v_{0...ij}\}_{j=1}^{b_{3i}}\right\}_{i=1}^{q_3}$ (рис. 2, *г*)) текущего яруса дуг и числа листьев в дереве. Отметим, что оно сходно с поведением, демонстрируемым величинами максимального прироста риска при заданной величине предельного собственного риска (подробнее см. табл. 2 из работы [53]). А именно, на первом ярусе погрешность растет вместе с числом листьев в дереве. На втором и более дальних ярусах, при числе листьев $m \geq 5$, погрешность монотонно убывает. При небольшом числе листьев монотонность нарушается. Природа этого явления кратко описана в работе [53]. Более подробно исследовать этот вопрос авторы не планируют, поскольку их задачей является разработка методов управления рисками в сложных сетевых структурах с тысячами вершин и ребер.

Отметим, что поскольку полученные в эксперименте значения относительного отклонения монотонно убывают с удалением от периметра, для построения системы с интегральным риском, не превышающим минимально возможный более, чем на 6,07 % (оценка на рис. 2, *б*), достаточно оптимальным образом выбрать элемент системы для помещения в вершину-периметр, а также элементы для размещения в вершинах первого яруса. При введенном ранее условии $u_{s_i} = u \ \forall i \in \{1,...,n\}$ это будут вершины с наименьшими удельными локальными рисками. Такая погрешность допустима для достаточно широкого класса систем. В случае, когда требуется более высокий уровень защищенности, потребуется дополнительно отобрать из оставшихся неразмещенными элементов q_2 с наименьшими удельными локальными рисками, а оставшиеся разместить в вершинах $V \setminus \left\{\{v_0\} \cup \bigcup_{j=1}^{b_{01}} \{v_{0j}\} \cup \bigcup_{i=1}^{q_1} \bigcup_{j=1}^{b_{1i}} \{v_{0ij}\}\right\}$ произвольным образом. Затем потребуется найти оптимальное

Численные оценки относительной погрешности решения задачи оптимального размещения элементов в подмножествах вершин древовидной структуры, округление до четвертого знака с избытком

Число вершин в подмножестве	Подмножество вершин			
	$\{v_{0j}\}_{j=1}^{b_{01}}$	$\left\{\{v_{0ij}\}_{j=1}^{b_{1i}}\right\}_{i=1}^{q_1}$	$\left\{\{v_{0...ij}\}_{j=1}^{b_{2i}}\right\}_{i=1}^{q_2}$	$\left\{\{v_{0...ij}\}_{j=1}^{b_{3i}}\right\}_{i=1}^{q_3}$
Три листа (m = 3)				
2	0,3095	0,0585	0,0119	0,0030
3	0,1548	0,0434	0,0088	0,0022
Четыре листа (m = 4)				
2	0,3750	0,0571	0,0107	0,0025
3	0,2500	0,0461	0,0086	0,0020
4	0,2000	0,0607	0,0107	0,0024
Пять листьев (m = 5)				
2	0,4223	0,0553	0,0097	0,0021
3	0,3168	0,0468	0,0082	0,0018
4	0,2563	0,0591	0,0098	0,0021
5	0,1709	0,0515	0,0085	0,0018
Шесть листьев (m = 6)				
2	0,4588	0,0535	0,0089	0,0018
3	0,3671	0,0466	0,0077	0,0016
4	0,2997	0,0574	0,0090	0,0018
5	0,2248	0,0512	0,0080	0,0016
6	0,1899	0,0607	0,0091	0,0018

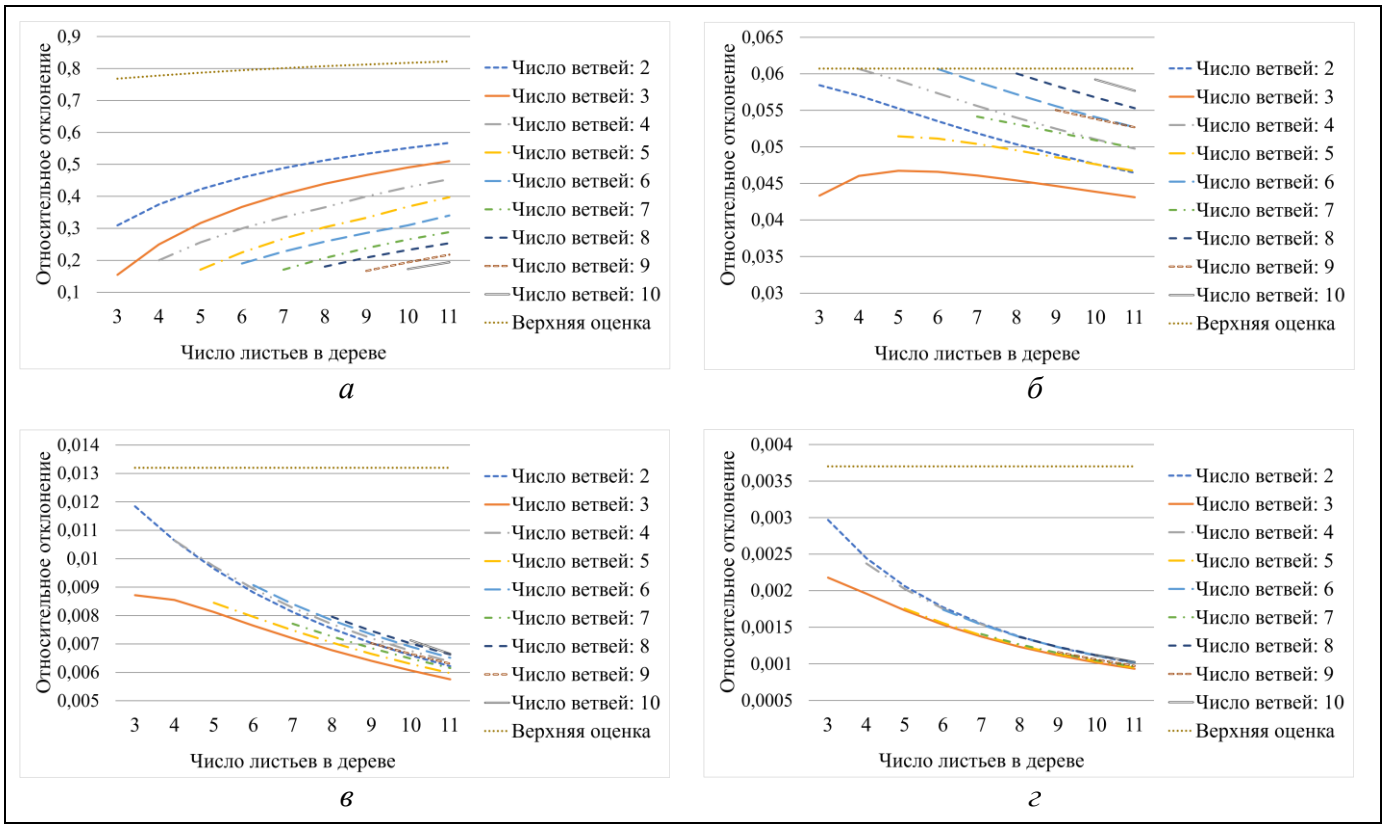

Рис. 2. Поведение численных оценок относительного отклонения от решения задачи оптимального размещения элементов в подмножествах древовидной структуры в зависимости от числа листьев в дереве: значения верхней оценки в подмножестве вершин первого яруса (*а*), соответствуют максимальному приращению риска в звездообразной структуре, т. е. при совпадающем числе ветвей и листьев; значения верхней оценки для подмножеств вершин ярусов 2–4 (*б*–*г*) равны значениям, полученным в работе [53] для звездообразной структуры с четырьмя лучами (для *б*), и двумя лучами (для *в* и *г*)

размещение отобранных элементов в вершинах $\bigcup_{i=1}^{q_1}\bigcup_{j=1}^{b_{1i}}\{v_{0ij}\}$, например, путем вычисления $q_3!$ значений интегрального риска для всех возможных перестановок элементов, размещенных в вершинах второго яруса. В этом случае погрешность полученного решения составит менее 1,32 %.

ЗАКЛЮЧЕНИЕ

Настоящая статья является частью серии работ, посвященных изучению влияния внутренней структуры сложной системы на ее интегральный риск. Для достижения цели исследования была сформулирована задача об оптимальном размещении элементов защищаемой системы внутри заданной структуры. Такая постановка позволяет изучать влияние структуры на риск безотносительно выделяемых для изменения последнего ресурсов (как это предусмотрено в классической постановке «Атакующий – Защитник»). В связи с тем, что прямой путь к решению поставленной задачи не просматривался, авторы приняли решение последовательно рассматривать отдельные виды структур в порядке возрастания сложности.

В предшествующих работах были рассмотрены цепные структуры [52], для которых было найдено общее решение в виде критерия предпочтения выбора того или иного элемента системы для размещения в вершине простой цепи в зависимости от ее положения относительно периметра. Для звездообразной структуры, включающей в себя единственную вершину-периметр и произвольное конечное число исходящих из нее простых цепей (в том числе бесконечной длины), были найдены [53] верхние оценки относительной погрешности решения поставленной задачи в случае, если начиная с некоторого расстояния от периметра размещение элементов будет произвольным.

В настоящей статье полученные для звездообразных структур оценки были обобщены на случай произвольных древовидных структур. Для этого была введена система обозначений вершин в дереве, в явном виде указывающих путь к текущей вершине от периметра, поставлена задача оптимального размещения элементов в древовидной структуре, рассчитаны численные оценки относи-

тельной погрешности решения этой задачи для деревьев с небольшим числом ветвей и листьев. Было проанализировано поведение полученных оценок при увеличении числа листьев и ветвей, сделан вывод о том, что погрешности решения не превосходят верхних оценок, полученных ранее для звездообразных структур.

Полученные результаты могут быть применены, например, при решении задач управления рисками в компьютерных сетях с переменной топологией, таких как туманные вычислители [55] или беспроводные mesh-сети [56], при проектировании систем охраны [57] и многих других. Предложенный подход позволяет оценить, в какой мере перестроение топологии компьютерной сети (или, как в другом примере, структуры системы охраны) влияет на ее защищенность в целом, а полученные верхние оценки позволяют быстро оценить величину интегрального риска рассматриваемой системы.

Следующим этапом работы станет рассмотрение структур произвольной топологии с одновершинным периметром.

ЛИТЕРАТУРА

1. *The Risk* Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk / Ed by D. Hillson. – London, UK: Kogan Page Publishers, 2023. – 416 p.
2. *ГОСТ* Р ИСО 31000–2019: «Менеджмент риска. Принципы и руководство». – М.: Стандартинформ, 2020. – I–IV, 13 с. [*ISO* 31000: Risk Management-Principles and Guidelines. – Geneva, Switzerland: International Organization for Standardization, 2018. – 24 p.]
3. *Rass, S.* On Game-Theoretic Risk Management (Part One) – Towards a Theory of Games with Payoffs that are Probability-Distributions. – arXiv:1506.07368, 2015. – DOI: https://doi.org/10.48550/arXiv.1506.07368
4. *Rass, S.* On Game–Theoretic Risk Management (Part Two) – Algorithms to Compute Nash-Equilibria in Games with Distributions as Payoffs. – arXiv:1511.08591, 2015. – DOI: https://doi.org/10.48550/arXiv.1511.08591
5. *Rass S.* On Game–Theoretic Risk Management (Part Three) – Modeling and Applications. – arXiv:1711.00708, 2017. – DOI: https://doi.org/10.48550/arXiv.1711.00708
6. *Остапенко А.Г., Паринов А.В., Калашников А.О.,* и др. Социальные сети и деструктивный контент / под. ред. Д.А. Новикова. – М.: Горячая линия – Телеком, 2017. – 276 с. [*Ostapenko, A.G., Parinov, A.V., Kalashnikov, A.O.,* et al. Sotsial'nye seti i destruktivnyi kontent / pod. red. D.A. Novikova. – M.: Goryachaya liniya – Telekom, 2017. – 276 s. (In Russian)]
7. *Калашников А.О.* Модели и методы организационного управления информационными рисками корпораций. – М.: ИПУ РАН, 2011. – 312 с. [*Kalashnikov, A.O.* Modeli i metody organizatsionnogo upravleniya informatsionnymi riskami korporatsii. – M.: IPU RAN, 2011. – 312 s. (In Russian)]
8. *Калашников А.О., Аникина Е.В.* Управление информационными рисками сложной системы с использованием механизма «когнитивной игры» // Информация и безопасность. – 2020. – Т. 38, № 4. – С. 2–10. [*Kalashnikov, A.O., Anikina, E.V.* Upravlenie informatsionnymi riskami slozhnoi sistemy s ispol'zovaniem mekhanizma «kognitivnoi igrY» // Cybersecurity Issues. – 2020. – Vol. 38, no 4. – P. 2–10. (In Russian)]
9. *Deng, S., Zhang, J., Wu, D.,* et al. A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack // IEEE Transactions on Industrial Informatics. – 2023. – Vol. 19, no. 3. – P. 2899–2908.
10. *Hu, B., Zhou, C., Tian, Y.–C.,* et al. Attack Intention Oriented Dynamic Risk Propagation of Cyberattacks on Cyber-Physical Power Systems // IEEE Transactions on Industrial Informatics. – 2023. – Vol. 19, no. 3. – P. 2453–2462.
11. *Xiaoxiao, G., Tan, Y., Wang, F.* Modeling and Fault Propagation Analysis of Cyber-Physical Power System // Energies. – 2020. – Vol. 13, no. 3. – Art. no. e539.
12. *Gao, X., Peng, M., Tse, C.K., Zhang, H.* A Stochastic Model of Cascading Failure Dynamics in Cyber-Physical Power Systems // IEEE Systems Journal. – 2020. – Vol. 14, no. 3. – P. 4626–4637.
13. *Marashi, K., Sarvestani, S.S., Hurson, A.R.* Identification of Interdependencies and Prediction of Fault Propagation for Cyber-Physical Systems // Reliability Engineering & System Safety. – 2021. – Vol. 215. – Art. no. e107787.
14. *Yan, K., Liu, X., Lu, Y., Qin, F.* A Cyber-Physical Power System Risk Assessment Model Against Cyberattacks // IEEE Systems Journal. – 2023. – Vol. 17, no. 2. – P. 2018–2028.
15. *Pelissero, N., Laso, P.M., Puentes, J.* Impact Assessment of Anomaly Propagation in a Naval Water Distribution Cyber–Physical System // Proceedings of 2021 IEEE International Conference on Cyber Security and Resilience (CSR). – Rhodes, Greece, 2021. – P. 518–523.
16. *Islam, M.Z., Lin, Y., Vokkarane, V.M., Venkataramanan, V.* Cyber–Physical Cascading Failure and Resilience of Power Grid: A Comprehensive Review // Frontiers in Energy Research. – 2023. – Vol. 11. – Art. no. e1095303.
17. *Zhang, C., Xu, X., Dui, H.* Analysis of Network Cascading Failure Based on the Cluster Aggregation in Cyber-Physical Systems // Reliability Engineering & System Safety. – 2020. – Vol. 202. – Art. no. e106963.
18. *Xing, L.* Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience // IEEE Internet of Things Journal. – 2021. – Vol. 8, no. 1. – P. 44–64.
19. *Wang, Q., Jia, G., Jia, Y, Song, W.* A New Approach for Risk Assessment of Failure Modes Considering Risk Interaction and Propagation Effects // Reliability Engineering & System Safety. – 2021. – Vol. 216. – Art. no. e108044.
20. *Khoshakhlagh, A., Moradi Hanifi, S., Laal, F.,* et al. A Model to Analyze Human and Organizational Factors Contributing to Pandemic Risk Assessment in Manufacturing Industries: FBN–HFACS Modelling // Theoretical Issues in Ergonomics Science. – 2023. – Vol. 25, no. 4. – P. 369–390.
21. *Moore, S., Rogers, T.* Predicting the Speed of Epidemics Spreading in Networks // Physical Review Letters. – 2020. – Vol. 124, no. 6. – P. 685–689.
22. *Nasution, H., Jusuf, H., Ramadhani, E., Husein, I.* Model of Spread of Infectious Diseases // Systematic Reviews in Pharmacy. – 2020. – Vol. 11, no. 2. – P. 685.

23.*Albert, R., Jeong, H., Barabasi, A.-L.* Error and Attack Tolerance of Complex Networks // Nature. – 2000. – Vol. 406. – P. 378–382.

24.*Artime, O., Grassia, M., De Domenico, M.,* et al. Robustness and Resilience of Complex Networks // Nature Reviews Physics. – 2024. – Vol. 6, no. 2. – P. 114–131.

25.*Ming, L., Run-Ran, L., Linyuan, L.,* et al. Percolation on Complex Networks: Theory and Application // Physics Reports. – 2021. – Vol. 907. – P. 1–68.

26.*Bak, P., Chen, K., Tang, C.* A Forest-Fire Model and Some Thoughts on Turbulence // Physics Letters A. – 1990. – Vol. 147, no. 5–6. – P. 297–300.

27.*Palmieri, L., Jensen, H.J.* The Forest Fire Model: The Subtleties of Criticality and Scale Invariance // Frontiers in Physics. – 2020. – Vol. 8. – Art. no. e00257.

28.*Rybski, D., Butsic, V., Kantelhardt, J.W.* Self-organized Multistability in the Forest Fire Mode // Physical Review E. – 2021. – Vol. 104, no. 1. – Art. no. eL012201.

29.*Newman, D.E., Nkei, B., Carreras, B.A.,* et al. Risk Assessment in Complex Interacting Infrastructure Systems // Proceedings of 38th Annual Hawaii International Conference on System Sciences (HICSS'05). – Big Island, HI, USA, 2005. – DOI: 10.1109/HICSS.2005.524

30.*Li, X., Ji, L., Zhu, H.,* et al. Cellular Automata–Based Simulation of Cross-space Transmission of Energy Local Area Network Risks: A Case Study of a Power Supply Station in Beijing // Sustainable Energy, Grids and Networks. – 2021. – Vol. 27. – Art. no. e100521.

31.*Torres, M.A., Chávez-Cifuentes, J.F., Reinoso, E.* A Conceptual Flood Model Based on Cellular Automata for Probabilistic Risk Applications // Environmental Modelling & Software. – 2022. – Vol. 157. – Art. no. e105530.

32.*Sequeira, J.G.N., Nobre, T., Duarte, S.,* et al. Proof–of–Principle That Cellular Automata Can Be Used to Predict Infestation Risk by *Reticulitermes grassei* (Blattodea: Isoptera) // Forests. – 2022. – Vol. 13, no. 2. – Art. no. e237.

33.*Gallos, L.K., Cohen, R., Argyrakis, P.,* et al. Stability and Topology of Scale-Free Networks under Attack and Defense Strategies // Physical Review Letters. – 2005. – Vol. 94, no. 18. – Art. no. e188701.

34.*Gallos, L.K., Cohen, R., Argyrakis, P.,* et al. Network Robustness and Fragility: Percolation on Random Graphs // Physical Review Letters. – 2000. – Vol. 85, no. 25. – Art. no. e5468.

35.*Wang, F., Dong, G., Tian, L., Stanley, H.E.* Percolation Behaviors of Finite Components on Complex Networks // New Journal of Physics. – 2022. – Vol. 24, no. 4. – Art. no. e043027.

36.*Dong, G., Luo, Y., Liu, Y.,* et al. Percolation Behaviors of a Network of Networks under Intentional Attack with Limited Information // Chaos, Solitons & Fractals. – 2022. – Vol. 159. – Art. no. e112147.

37.*Shao, S., Huang, X., Stanley, H.E., Havlin, S.* Percolation of Localized Attack on Complex Networks // New Journal of Physics. – 2015. – Vol. 17, no. 2. – Art. no. e023049.

38.*Dong, G., Xiao, H., Wang, F.,* et al. Localized Attack on Networks with Clustering // New Journal of Physics. – 2019. – Vol. 21, no. 1. – Art. no. e013014.

39.*Shang, Y.* Percolation of Attack with Tunable Limited Knowledge // Physical Review E. – 2021. – Vol. 103, no. 4. – Art. no. e042316.

40.*Qing, T., Dong, G., Wang, F.,* et al. Phase Transition Behavior of Finite Clusters under Localized Attack // Chaos: An Interdisciplinary Journal of Nonlinear Science. – 2022. – Vol. 32, no. 2. – Art. no. e023105.

41.*Goltsev, A.V., Dorogovtsev, S.N., Mendes, J.F.F.* K-Core (Bootstrap) Percolation on Complex Networks: Critical Phenomena and Nonlocal Effects // Physical Review E. – 2006. – Vol. 73, no. 5. – Art. no. e056101.

42.*Burleson-Lesser, K., Morone, F., Tomassone, M.S., Makse, H.A.* K-core Robustness in Ecological and Financial Networks // Scientific Reports. – 2020. – Vol. 10, no. 1. – Art. no. 3357.

43.*Shang, Y.* Generalized K-cores of Networks under Attack with Limited Knowledge // Chaos, Solitons & Fractals. – 2021. – Vol. 152. – Art. no. e111305.

44.*Al Mannai, W.I., Lewis, T.G.* A General Defender-Attacker Risk Model for Networks // The Journal of Risk Finance. – 2008. – Vol. 9, no. 3. – P. 244–261.

45.*Peng, R., Wu, D., Sun, M., Wu, S.* An Attack-Defense Game on Interdependent Networks // Journal of the Operational Research Society. – 2021. – Vol. 72, no. 10. – P. 2331–2341.

46.*Ren, J., Liu, J., Dong, Y.,* et al. An Attacker-Defender Game Model with Constrained Strategies // Entropy. – 2024. – Vol. 26, no. 8. – Art. no. e26080624.

47.*He, S., Zhou, Y., Yang, Y.,* et al. Cascading Failure in Cyber-Physical Systems: A Review on Failure Modeling and Vulnerability Analysis // IEEE Transactions on Cybernetics. – 2024. – P. 1–19. – DOI: 10.1109/TCYB.2024.3411868

48.*Zhou, F., Xu X., Trajcevski, G., Zhang, K.* A Survey of Information Cascade Analysis: Models, Predictions, and Recent Advances // ACM Computing Surveys (CSUR). – 2021. – Vol. 54, no. 2. – P. 1–36.

49.*Cui, P., Zhu, P., Wang, K.,* et al. Enhancing Robustness of Interdependent Network by Adding Connectivity and Dependence Links // Physica A. – 2018. – Vol. 497. – P. 185–197.

50.*Xu, X., Fu, X.* Analysis on Cascading Failures of Directed-Undirected Interdependent Networks with Different Coupling Patterns // Entropy. – 2023. – Vol .25, no. 3. – Art. no. e471.

51.*Yang, X.H., Feng, W.H., Xia, Y.,* et al. Improving Robustness of Interdependent Networks by Reducing Key Unbalanced Dependency Links // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2020. – Vol. 67, no. 12. – P. 3187–3191.

52.*Shiroky, A., Kalashnikov, A.* Mathematical Problems of Managing the Risks of Complex Systems under Targeted Attacks with Known Structures // Mathematics. – 2021. – Vol. 9, no. 19. – Art. no. e2468.

53.*Shiroky, A., Kalashnikov, A.* Influence of the Internal Structure on the Integral Risk of a Complex System on the Example of the Risk Minimization Problem in a «Star» Type Structure // Mathematics. – 2023. – Vol. 11, no. 4. – Art. no. e998.

54.*Широкий А.А., Калашников А.О.* Применение методов естественных вычислений для управления рисками сложных систем // Проблемы упраления. – 2021. – № 4. – С. 3–20. [*Shiroky, A.A., Kalashnikov, A.O.* Natural Computing with Application to Risk Management in Complex Systems // Control Sciences. – 2021. – No. 4. – P. 2–17.]

55.*Shiroky, A.A.* A Method for Rapid Risk Assessment of a Fog Computing System with a Star–Shaped Topology // Proceedings of 17th International Conference Management of

Large–Scale System Development (MLSD). – Moscow, Russia, 2024. – P. 1–5.
56. *Shiroky, A.A.* Risk Management in the Design of Computer Network Topology / In: Lecture Notes in Computer Science. Ed. by V.M. Vishnevskiy, K.E. Samouylov, and D.V.Kozyrev. – Cham: Springer, 2024. – Vol. 14123. – P. 375–385.
57. *Shiroky, A.A.* Risk Management in the Design of Security Systems with Nested Security Zones // Proceedings of 16th International Conference Management of Large-Scale System Development (MLSD). – Moscow, Russia, 2023. – P. 1–4.

Статья представлена к публикации членом редколлегии В. Н. Бурковым.

Поступила в редакцию 06.11.2024,
после доработки 21.03.2025.
Принята к публикации 21.03.2025.

Широкий Александр Александрович – канд. физ.-мат. наук,
✉ shiroky@ipu.ru
ORCID ID: https://orcid.org/0000–0002–9130–5541

Калашников Андрей Олегович – д-р техн. наук,
✉ aokalash@ipu.ru
ORCID ID: https://orcid.org/0000–0001–5204–1398

Институт проблем управления им. В.А. Трапезникова РАН, г. Москва.

HOW DOES THE INTERNAL STRUCTURE OF A COMPLEX SYSTEM INFLUENCE ITS OVERALL RISK? RISK MINIMIZATION FOR TREES

A. A. Shiroky* and A. O. Kalashnikov**

*,**Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

*✉ shiroky@ipu.ru, **✉ aokalash@ipu.ru

Abstract. The Defender–Attacker problem is often employed as a mathematical framework in risk management. In this problem, the above players with opposite goals allocate limited resources to system elements to minimize or maximize a risk function. It has been well-studied under the assumption of independent system elements. However, in complex systems, elements interact, causing significant differences between the measured and predicted risks. Although models with the interdependence of system elements are regularly considered in the literature, no comprehensive understanding has been formed of how the structure of a complex system influences its overall risk. We address this issue in a series of papers by investigating system structures of increasing complexity. Chains and stars have been analyzed previously; in this paper, the findings are extended to arbitrary trees. We optimize the placement of elements within a tree to minimize risk; derive upper bounds for the relative error of an approximate algorithmic solution of this problem for trees with a few branches and leaves; and explore the dynamics of these bounds when increasing the number of leaves and branches. As demonstrated, the resulting upper bounds do not exceed their counterparts for stars from the previous works.

Keywords: complex systems, risk, system structure, risk management, risk minimization algorithms, the problem of optimal element placement.