УЧЁТ ВЛИЯНИЯ СТРУКТУРЫ СЛОЖНОЙ СИСТЕМЫ ПРИ УПРАВЛЕНИИ РИСКАМИ

Широкий А. А.[1]

(*ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, Москва*)

Теоретико-игровые модели «Защитник – Атакующий» и «Защитник – Атакующий – Защитник» часто используются в качестве базовых для постановки задач управления рисками. При этом стратегии игроков обычно задаются на множествах допустимых распределений располагаемых игроками ограниченных ресурсов. Возможность дополнительного снижения риска Защитником путём управления составом или структурой защищаемой системы в классических постановках не рассматривается, поскольку на практике подобные действия для него нехарактерны или вовсе невозможны. В то же время вопрос о влиянии структуры системы на её уязвимость весьма актуален на этапе проектирования системы, в связи с чем возникает потребность в методах сравнения структур между собой. В статье предложена модификация классической постановки задачи минимизации интегрального риска сложной системы, позволяющая количественно учесть влияние размещения элементов системы внутри заданной структуры на значение её интегрального риска. Приведено решение поставленной задачи для наиболее простого частного случая – простой цепи, а также представлен алгоритм построения структуры сложной системы, минимизирующей риск. Полученный результат в дальнейшем будет использован для поиска решений этой задачи в случае структур более сложных топологий, в частности древовидных.

Ключевые слова: сложные системы, структура сложной системы, управление рисками.

1. Введение

Риск в семействе стандартов ISO 31000 [26] определяется как следствие влияние неопределённости на достижение поставленных целей. При этом отмечается, что под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное). В терминах системного анализа это определение можно переписать следующим образом:

[1] *Александр Александрович Широкий, к.ф.-м.н.* (*shiroky@ipu.ru*).

Определение 1. *Риск – системный параметр, свойство системы управления, в частности ЛПР, принимать решения в условиях неопределённости, которые могут повлечь за собой как нежелательные* (*опасные*)*, так и существенно выигрышные последствия* [4].

Управление риском (или менеджмент риска) в стандарте ГОСТ Р ИСО 31000-2019 [1] определено как скоординированные действия по руководству и управлению организацией в области риска. Действительно, исследования по управлению рисками преимущественно сосредоточены в областях теории менеджмента и теории управления.

В терминологии А.М. Новикова [5] первая из них относится к «слабым» наукам, работает преимущественно с качественными оценками рисков, а результаты в этой области получены с минимумом ограничивающих предположений. Вторая же является «сильной» наукой, активно использует математические модели, работает с количественными оценками рисков, а результаты применимы на практике лишь при соблюдении достаточно большого количества подчас трудновыполнимых ограничений.

Глобальной стратегической целью настоящего исследования является сближение этих подходов путём построения общих принципов, методов и технологий управления рисками на основе строгого математического обоснования.

Базовой моделью для постановки задачи управления рисками в данной работе является классическая модель «Защитник – Атакующий». В её рамках защищаемая (или атакуемая, в зависимости от точки зрения исследователя) система представляется в виде графа, вершины которого соответствуют элементам системы, а рёбра – связям между ними. Также вводится функция риска, зависящая от распределения ресурсов Защитником и Атакующим между элементами системы. Задача управления риском может быть поставлена в теоретико-игровой форме либо, в случае отсутствия одного из игроков, в оптимизационной форме.

Для ситуаций, когда связи между элементами неважны, получен ряд фундаментальных результатов. Так, в условиях отсут-

ствия атакующего и полной определённости относительно вида функций локального (соответствующего отдельным элементам системы) риска задача сводится к нахождению минимума (или точной нижней грани) аддитивной функции [2]. При отсутствии информации о конкретном виде функций локального риска решить задачу минимизации риска для системы в целом уже не получается. Однако можно воспользоваться принципом минимального гарантированного результата и перейти к задаче снижения максимума локальных рисков. В работе [3] доказана единственность её решения (если оно существует) и предложен алгоритм его нахождения с помощью арбитражных схем. Впоследствии этот алгоритм был обобщён для учёта вероятностной неопределённости («игры с природой», [2]).

Управление рисками сложной системы в условиях взаимного влияния элементов друг на друга предлагается осуществлять по той же схеме, но только при условии, что при многошаговом линейном импульсном процессе (см., например, [6]) значения локальных рисков элементов системы (весов вершин ориентированного графа) становятся стационарными начиная с некоторого шага. Тогда Защитник распределяет ресурс так, как будто процесс уже стабилизировался. Отметим, что достаточное условие стабилизации при этом довольно сильное: все собственные значения матрицы весов рёбер, характеризующих интенсивность передачи риска между соответствующими элементами, должны оказаться внутри единичного круга на комплексной плоскости.

Таким образом, вопрос о влиянии структуры сложной системы на её интегральный риск всё ещё остаётся открытым. В настоящей статье представлен возможный путь для его решения.

Структура изложения материала в работе следующая.

Раздел 2 содержит краткий обзор математических моделей распространения отказов в сложных сетях. В разделе 3 приведена базовая постановка задачи управления риском сложной системы. Раздел 4 посвящён описанию модификации классической задачи для изучения влияния структуры защищаемой системы на её интегральный риск. В разделе 5 предложено частное решение мо-

дифицированной задачи для простой цепной структуры, а также алгоритм проектирования минимизирующей риск структуры мер безопасности на основе полученного результата. В заключении обсуждаются дальнейшие перспективы исследования.

2. Краткий обзор математических моделей распространения отказов в сложных сетях

В самом общем случае мы можем считать, что структура сложной системы является сложной сетью произвольной топологии. Для исследования различных деструктивных эффектов (включая целенаправленные атаки на узлы и рёбра) 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 [23, 31], вычислительных [15, 33] и медико-социальных [24, 27].

Ранние модели описывали развитие отказов, вызванных нецеленаправленными (например, случайными) воздействиями. Наиболее известными из них являются модель устойчивости к ошибкам [7], модель распространения лесного пожара [10] и её производные, модели на базе клеточных автоматов [28], а также модели перколяции со случайными атаками [20]. Отметим, что последние имеют ряд модификаций, предполагающих, что деструктивные воздействия на узлы и рёбра сети являются целенаправленными. К таковым относятся собственно перколяции с целенаправленными атаками [8, 14, 19, 25], а также перколяции с локализованными атаками [29] и перколяции с k-ядром [9, 11, 18, 22].

Упомянутые выше модели распространения отказов хорошо сочетаются с классическими моделями управления рисками в сложных сетях «Защитник – Атакующий» [12]. 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 це-

лью 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 её 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.

Учёт изменения структуры подразумевают, например, модели каскадного распространения ошибки [13, 21], однако в их рамках такие изменения не предполагаются целенаправленными. Возможность намеренного изменения структуры предусмотрена в моделях, модифицированных для случая двух взаимосвязанных сетей [16, 17, 32], но именно в отношении рёбер, связывающих сети между собой.

Таким образом, для решения задач управления структурой сложной системы, в том числе с целью минимизации её интегрального риска, существующего аппарата моделирования недостаточно. Поэтому далее мы обсудим один из возможных путей для частичного заполнения этого пробела.

3. Базовая постановка задачи управления риском сложной системы

Рассмотрим сложную систему, состоящую из конечного множества элементов (объектов, пока произвольной природы): $S = \{s_1, ..., s_i, ..., s_n\}$, $i \in N = \{1, ..., n\}$, $n \in \mathbb{N}$. Будем предполагать, что элементы $s_i \in S$ являются автономными и, в частности, не могут оказывать влияние на состояния друг друга.

Предположим также, что существуют два субъекта (также пока произвольной природы), которых мы будем называть игрок A (Атакующий, *Attacker*) и игрок D (Защитник, *Defender*), имеющие несовпадающие интересы относительно состояния системы S.

Будем считать, что игрок D располагает некоторым объёмом ресурса $X \geqslant 0$, который он может произвольным образом рас-

пределять между элементами системы S:

$$x = (x_1, ..., , x_n), x_i \geqslant 0, i \in N, \sum_{i=1}^{n} x_i \leqslant X. \quad (1)$$

Аналогично будем считать, что игрок A также располагает некоторым объёмом ресурса $Y \geqslant 0$, который он может произвольным образом распределять между элементами системы S:

$$y = (y_1, ..., y_n), y_i \geqslant 0, i \in N, \sum_{i=1}^{n} y_i \leqslant Y. \quad (2)$$

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, временные, производственные и иные ресурсы или затраты.

Под *локальным риском* в рамках рассматриваемой модели будем понимать некоторую *локальную характеристику отдельного элемента* $s_i \in S$, зависящую от количества ресурсов, распределенных на указанный элемент игроками D и A, и связанную с возможными потерями (ущербом) от негативного или позитивного (в каком-то смысле) изменения состояния указанного элемента.

В свою очередь, под *интегральным риском* будем понимать некоторую *интегральную характеристику всей системы* S в целом, зависящую от количества ресурсов, распределённых на все элементы системы S игроками D и A, и связанную с возможными потерями (ущербом) от негативного или позитивного (в каком-то смысле) изменения состояния каждого элемента.

В случае, когда элементы системы S являются автономными, локальный риск любого элемента $s_i \in S$ будет зависеть от величины распределённых игроками D и A ресурсов на этот элемент. Определим для каждого элемента $s_i \in S$ функцию локального риска $\rho_i(x_i, y_i) : \mathbb{R}_0^+ \times \mathbb{R}_0^+ \to \mathbb{R}_0^+$, где $\mathbb{R}_0^+$ – множество действительных неотрицательных чисел.

Далее, в рамках рассматриваемой модели будем полагать, что функции локального риска $\rho_i(\cdot,\cdot)$, $i \in N$, обладают следующими свойствами.

Неотрицательность риска:

$$\forall i \in N, x_i, y_i \geqslant 0 : \rho_i(x_i, y_i) \geqslant 0. \tag{3}$$

Нестрогая монотонность риска:

$$\forall i \in N : \frac{\partial \rho_i(x_i, y_i)}{\partial x_i} \leqslant 0, \frac{\partial \rho_i(x_i, y_i)}{\partial y_i} \geqslant 0. \tag{4}$$

Ограниченность риска:

$$\forall i \in N, x_i, y_i \geqslant 0 \; \exists \rho_i^x = \text{const}, \rho_i^y = \text{const} : \rho_i^x \leqslant \rho_i(x_i, y_i) \leqslant \rho_i^y. \tag{5}$$

Свойство неотрицательности риска означает, что потенциальный ущерб, связанный с реализацией локального риска, для любого элемента $s_i \in S$ не может быть отрицательным.

Свойство монотонности риска означает, что для любого элемента $s_i \in S$ *дополнительное* выделение ресурса Защитником не должно приводить к *росту* локального риска этого элемента системы S и, с другой стороны, *дополнительное* выделение ресурса Атакующим не должно приводить к *снижению* локального риска этого элемента системы S.

Свойство ограниченности риска означает, что для любого элемента $s_i \in S$ никакое *дополнительное* выделение Защитником ресурса не позволяет снизить *остаточный риск* для данного элемента «до нуля» и, с другой стороны, вне зависимости от объёмов затраченных Атакующим ресурсов для любого элемента $s_i \in S$ всегда имеет место конечный положительный *предельный риск*.

Пусть $x = (x_1, ..., x_n), y = (y_1, ..., y_n)$ – некоторые допустимые распределения ресурсов между вершинами – элементами системы S игроками D и A соответственно. Будем рассматривать функции локального риска вида

$$\rho_i(x, y) = u_i(x, y) \cdot p_i(x, y) \tag{6}$$

для каждой вершины $s_i \in S$. Здесь $u_i(x, y) : \mathbb{R}_n^+ \times \mathbb{R}_n^+ \to \mathbb{R}_0^+$ – функция, описывающая зависимость ожидаемого ущерба в случае успешной атаки элемента s_i в зависимости от распределений

ресурсов x и y, а $p_i(x,y) : \mathbb{R}_n^+ \times \mathbb{R}_n^+ \to (0,1]$ – вероятность успешной атаки элемента s_i в зависимости от распределений ресурсов x и y.

Зададим функцию интегрального риска $\rho(x,y) : \mathbb{R}_n^+ \times \mathbb{R}_n^+ \to \mathbb{R}_0^+$:

$$\rho(x,y) = \sum_{i=1}^{n} \rho_i(x,y). \tag{7}$$

Тогда базовая модель управления рисками сложной системы со структурой и периметром задаётся следующим кортежем:

$$\langle S = \{s_i\}_{i \in N}, D, A, X, Y, \{\rho_i(\cdot,\cdot)\}_{i \in N}, \rho(\cdot,\cdot)\rangle. \tag{8}$$

Целью Защитника является распределение доступного ему ресурса X между элементами системы S с тем, чтобы добиться максимально возможного снижения значения функции интегрального риска $\rho(x,y)$.

Цель Атакующего противоположна: ему необходимо распределить доступный ему ресурс Y между элементами системы S таким образом, чтобы добиться максимально возможного увеличения значения функции интегрального риска $\rho(x,y)$.

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

$$\mathscr{X}(X) = \left\{ (x_1, ..., x_n) \in \mathbb{R}_n^+ : x_i \geqslant 0, i \in N, \sum_{i=1}^{n} x_i \leqslant X \right\}, \tag{9}$$

$$\mathscr{Y}(Y) = \left\{ (y_1, ..., y_n) \in \mathbb{R}_n^+ : y_i \geqslant 0, i \in N, \sum_{i=1}^{n} y_i \leqslant Y \right\}. \tag{10}$$

Тогда задача игрока D («задача Защитника») заключается в нахождении распределения ресурса $x^* \in \mathscr{X}$, минимизирующего интегральный риск, и формально может быть записана в виде:

$$x^* = \arg\min_{x \in \mathscr{X}} \rho(x,y) = \arg\min_{x \in \mathscr{X}} \sum_{i=1}^{n} \rho_i(x,y). \tag{11}$$

Аналогично задача игрока A («задача Атакующего») заключается в нахождении распределения ресурса $y^* \in \mathscr{Y}$, максимизи-

рующего интегральный риск, и может быть записана в виде:

$$y^* = \arg\min_{y \in \mathscr{Y}} \rho(x, y) = \arg\min_{y \in \mathscr{Y}} \sum_{i=1}^{n} \rho_i(x, y). \tag{12}$$

Далее рассмотрим модификацию задачи минимизации риска сложной системы, позволяющую исследовать влияние её структуры на значение интегрального риска.

4. Постановка задачи поиска оптимального размещения элементов защищаемой системы внутри заданной структуры

Пусть на множестве элементов системы S задана структура $W = \langle G(S, E), T \rangle$, где $G(S, E)$ – связный граф на множестве вершин-элементов S со множеством рёбер E, а $T \subseteq S$ – некоторое подмножество вершин, которое будем называть периметром системы S.

Будем считать, что игрок A атакует элементы рассматриваемой системы по выбранной им цепи $c = \langle u, v \rangle, u \in T, v \in S$, причём переход из некоторой вершины $s_i \in c$ по инцидентному ей ребру в смежную вершину $s_j \in c$ осуществляется только в случае успешной атаки элемента s_i.

Если структуру $W = \langle G(S, E), T \rangle$ можно изменять (например, модифицируя множества E или T), то прежде чем решать задачу (11), Защитник может дополнительно снизить риски, решив задачу построения структуры, оптимальной в смысле их минимизации.

Определение 2. Будем говорить, что элемент $s_i \in S$ расположен на расстоянии m от периметра и записывать $l(s_i) = m$, если все простые пути, оканчивающиеся в s_i и начинающиеся в любой из вершин $s_j \in T$, включают в себя не менее m рёбер.

Заметим, что $l(s_i) = 0 \; \forall i : s_i \in T$.

Предположим, что для каждого элемента $s_i \in S$ защищаемой системы нам известна зависящая от распределений ресурсов $x = (x_1, ..., x_n)$ и $y = (y_1, ..., y_n)$ вероятность $p_i(x_i, y_i)$ того, что он будет успешно атакован (в некотором смысле) злоумышленни-

ком. Также будем считать, что нам известны величины u_i ущерба защищаемой системе в случае успешной атаки соответствующего узла.

Определение 3. Функцию $\rho_i^0(x_i, y_i) = u_i \cdot p_i(x_i, y_i)$ будем называть удельным локальным риском элемента s_i.

Будем рассматривать сценарии, при которых Атакующий последовательно выводит из строя узлы защищаемой сети, начиная с некоторого наперёд заданного узла-периметра и продвигаясь далее по соседям. Предполагаем, что каждый узел он посещает ровно один раз. Тогда функция локального риска примет следующий вид:

$$\rho_i(x, y) = \rho_i^0(x_i, y_i) \prod_{j=0}^{l(s_i)-1} \max_{k:l(s_k)=j} p_k(x_k, y_k). \tag{13}$$

Отметим, что функция интегрального риска, как и раньше, определяется в виде суммы локальных рисков (7). Важное отличие состоит в том, что значения функций локального риска теперь зависят не только от распределений ресурсов Атакующим и Защитником, но и от положения элементов внутри структуры W.

Справедливы следующие утверждения (доказательства приведены в работе [30]).

***Утверждение* 1.** *Если $\forall i \in N$ функции $\rho_i^0(x_i, y_i)$ монотонно убывают по первому аргументу и монотонно возрастают по второму, то функции $\rho_i(x, y)$ удовлетворяют свойствам* (3)–(5) *для всех $i \in N$.*

***Утверждение* 2.** *Добавление в систему структуры $W = \langle G(S, E), T\rangle$ не увеличивает риск, иными словами $\forall S = \{s_1, ..., s_n\}$, $i \in N$, $\forall E \neq \emptyset$, $T \subset S$ $\sum_{i=1}^n \rho_i(x_i, y_i) \leqslant \sum_{i=1}^n \rho_i^0(x, y)$.*

Теперь мы можем перейти к изучению влияния структуры сложной системы на её интегральный риск. С этой целью сформулируем задачу выбора оптимального размещения элементов S внутри заданной структуры. Чтобы исключить влияние выделяемого игроками ресурса, будем считать, что вероятности успешной атаки не зависят от x, y. Тогда функции локального риска при

фиксированном расположении элементов становятся константами.

Определение 4. *Пусть защищаемая система включает в себя множество элементов* $S = \{s_1, ..., s_i, ..., s_n\}$, $i \in N = \{1, ..., n\}$, $n \in \mathbb{N}$, *и задана некоторая структура* $W = \langle G(V, E),\ T\rangle, V = \{v_1, ..., v_n\}$. *Взаимно-однозначное отображение* $M^{-1} : S \to V$ *такое, что* $\forall i \leqslant n \quad \exists j \leqslant n : v_j = M^{-1}(s_i)$ *будем называть размещением узлов* S *в структуре* W. *Соответствующее обратное отображение* $M : V \to S$ *будем называть проекцией структуры* W *на множество элементов* S.

Для произвольного заданного размещения $M^{-1} : S \to V$ можно рассчитать значение интегрального риска

$$\rho\left(S, W, M^{-1}\right) = \sum_{i=1}^{n} \rho_{M(v_i)}, \tag{14}$$

где $\rho_{M(v_i)}$ – значение локального риска для узла $M(v_i)$, и записать задачу минимизации интегрального риска, заключающуюся в поиске такого множества размещений, для каждого из которых достигается минимальное значение интегрального риска ρ_{min}:

$$\mathbf{M}_{min} = \arg\min_{M} \rho\left(S, W, M^{-1}\right) : \tag{15}$$

$$\rho_{min} = \sum_{i=1}^{n} \rho_{M(v_i)} \forall M^{-1} \in \mathbf{M}_{min}.$$

В общем случае задача поиска оптимального размещения, по всей видимости, является NP-трудной. По этой причине поиск точного решения для систем сложной топологии с числом элементов более нескольких десятков уже является крайне трудоёмким. Вместе с тем автор считает возможным нахождение вычислительно простых эвристических алгоритмов, позволяющих решать эту задачу, например, с некоторой гарантированной максимальной погрешностью.

С этой целью планируется последовательно рассматривать структуры с одновершинным периметром в порядке возрастания их сложности, начиная с простой цепи и заканчивая структурами

произвольной топологии. Для простейших структур было найдено аналитическое решение, приведённое в следующем разделе.

5. Задача задачи поиска оптимального размещения элементов защищаемой системы в простой цепи

Определение 5. *Пусть задан граф* $G\left(V=\{v_1,...,v_n\},\right.$ $\left.E=\{(v_i,v_{i+1})\}_{i=1}^{m-1}\right.$, $n\in N$, *и периметр* $T=\{v_1\}$. *Тогда будем говорить, что кортеж* $W_n=\langle G(V,E),T\rangle$ *задаёт сценарий атаки длины* n.

Определение 6. *Будем говорить, что узлы* $s_i,s_j\in S$, $i,j\in N$, $i\neq j$, *нестрого упорядочены по возрастанию* (*убыванию*) *интегрального риска и записывать* $s_i\preceq s_j$ $(s_i\succeq s_j)$ *если при заданном сценарии атаки* W *для любых размещений* M^{-1},K^{-1} *и любых таких индексов* $p,q,k,l:\ p<q,\ k>l$, *что* $s_i=M(v_p)=K(v_k),s_j=M(v_q)=K(v_l)$ *и выполняется неравенство* $\rho\left(S,W,M^{-1}\right)\leqslant\rho\left(S,W,K^{-1}\right)$ $\left(\rho\left(S,W,M^{-1}\right)\geqslant\right.$ $\left.\geqslant\rho\left(S,W,K^{-1}\right)\right)$.

В работе [30] были доказаны следующие утверждения.

***Утверждение* 3.** *Пусть* $N=\{1,...,n\}$, $n\in\mathbb{N}$, $S=\{s_1,...,s_n\}$. *Тогда* $\forall i\in N\setminus\{n\}:\ s_i\preceq s_{i+1}\iff\frac{u_i}{u_{i+1}}\leqslant\frac{p_{i+1}(1-p_i)}{p_i(1-p_{i+1})}$; $s_i\succeq s_{i+1}\iff\frac{u_i}{u_{i+1}}\geqslant\frac{p_{i+1}(1-p_i)}{p_i(1-p_{i+1})}$.

***Утверждение* 4.** *Пусть* $N=\{1,...,n\}$, $n\in\mathbb{N}$, $S=\{s_1,...,s_n\}$. *Тогда* $\forall i,j,k\in N:i<j<k:\ s_i\preceq s_j\preceq s_k\implies s_i\preceq s_k$.

Эти утверждения задают транзитивный критерий упорядочивания узлов в простой цепи и позволяют решить задачу (15) для любого такого рассматриваемого сценария атаки в общем виде.

В большинстве реально существующих систем нет возможности изменять положение элементов в структуре. Тем не менее полученный принцип оптимального размещения элементов вполне применим, например, при проектировании компьютерных сетей или систем охраны со вложенными зонами безопасности.

Ниже приведён алгоритм проектирования системы безопасности сложной системы на основе описанного выше принципа.

Рассмотрим сложную систему с n элементами, задающими множество $S = \{s_1, ..., s_n\}$. Вначале будем предполагать, что все элементы доступны для Атакующего, т.е. структура системы на начальном этапе представляет собой полный граф $G(V, E)$, $V = S, E = \cup_{i \neq j}(s_i, s_j)$, $1 \leqslant i,\ j \leqslant n$, а возможные сценарии атаки – маршруты в нём. Будем рассматривать сценарии, являющиеся простыми путями.

Предположим, что Атакующий хочет нанести рассматриваемой системе максимальный ущерб. Тогда он должен вывести из строя все её элементы без исключения, решив при этом задачу, обратную задаче (15):

$$\mathbf{M}^{-1}_{max} = \underset{M^{-1}}{\operatorname{Arg\,max}}\, \rho\left(S, W, M^{-1}\right) : \tag{16}$$

$$\rho_{max} = \sum_{i=1}^{n} \rho_{M(v_i)}\ \forall M^{-1} \in M^{-1}_{max},$$

где M^{-1}_{max} – множество размещений, для каждого из элементов которого достигается максимальное значение интегрального риска ρ_{max}.

С учётом изложенного выше результата решение строится тривиальным образом и заключается в выборе простого пути $\left(v^A_1, v^A_2, ..., v^A_n\right)$, включающего все вершины графа G, причём $v^A_i \succeq v^A_{i+1}\ \forall i < n$.

Задача Защитника, в свою очередь, заключается в том, чтобы направить Атакующего по наименее «выгодной» для последнего траектории. Эта траектория также легко вычисляется и, как и в предыдущем случае, представляет собой простой путь $\left(v^D_1, v^D_2, ..., v^D_n\right)$, включающий в себя все вершины графа G, причём $v^D_i \preceq v^D_{i+1}\ \forall i < n$. Отметим, что в случае, когда выполнено условие

$$\frac{1 - p_i}{u_i p_i} = \frac{1 - p_j}{u_j p_j} \iff i = j,\ i, j \in \{1, ..., n\}, \tag{17}$$

обе задачи имеют единственное решение, причём $v^D_i = v^A_{n-i+1}$. Иными словами, Атакующий и Защитник стремятся к реализации

противоположных траекторий.

Тогда алгоритм решения задачи Защитника при выполнении условия (17) выглядит следующим образом:

1. Обеспечить единственную точку входа в систему (задать периметр) в узле v_1^D (он же v_n^A).

2. Назначить узел v_1^D текущим (положить i равным 1).

3. Последовательно удалять рёбра, соединяющие текущий узел v_i^D с узлами $v_{i+2}^D, ..., v_n^D$.

4. Если $i < n$, то назначить текущим узел v_{i+1}^D (положить i равным $i + 1$). В противном случае завершить алгоритм.

5. Перейти к пункту 3.

Отметим, что при выполнении условия

$$\frac{1 - p_i}{u_i p_i} = \frac{1 - p_j}{u_j p_j} \; \forall i, j \in \{1, ..., n\}, \tag{18}$$

узлы становятся нейтральными к перестановкам в смысле утверждения 3. В то же время, если Защитник знает о том, что в дальнейшем будет располагать неким ограниченным ресурсом, с помощью которого он сможет снижать удельные вероятности успешной атаки узлов, то у него появляется дополнительный критерий упорядоченности. А именно, Защитник будет заинтересован в том, чтобы вынести ближе к периметру узлы, наиболее отзывчивые к выделению ресурса в смысле повышения их стойкости к действиям Атакующего. В рамках настоящей работы эта задача не рассматривается, но представляется интересной для будущих исследований.

6. Заключение

В настоящей работе описан ранее не применявшийся подход к исследованию влияния структуры сложной системы на её интегральный риск. Идея заключается в модификации постановки классической задачи минимизации риска с заменой управляемого параметра на размещение элементов защищаемой системы внутри заданной структуры, тогда как в классической постановке управление риском осуществляется путём назначения ресурсов элементам системы.

Предложенная модификация позволяет не рассматривать зависимости локальных рисков от выделенных игроками ресурсов и сосредоточиться на изучении структурных эффектов. В данной статье автор рассматривает наиболее простую структуру сложной системы – простую цепь с одновершинным периметром. Результатом является принцип упорядочения элементов системы внутри простой цепи.

Хотя возможность прямого практического применения полученного результата ограничена тем, что большинство реально функционирующих систем не предполагают возможности перестановки элементов при сохранении структуры связей, полученный принцип будет использован для построения алгоритмов (возможно, не точных) минимизации риска в более сложных структурах, в частности, древовидных.

Литература

1. *ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство. – Официальное издание*. – М.: Стандартинформ, 2021.
2. КАЛАШНИКОВ А.О., АНИКИНА Е.В. *Модели управления информационными рисками сложных систем* // Информация и безопасность. – 2020. – Т. 23, №2. – С. 191–202.
3. КАЛАШНИКОВ А.О. *Модели и методы организационного управления информационными рисками корпораций*. – М.: ИПУ РАН, 2011. – 312 с.
4. КОНОНОВ Д.А. *Исследование безопасности систем управления на основе анализа их системных параметров* // В сб.: Проблемы управления безопасностью сложных систем. Материалы XXVIII международной конференции / Под общ. ред. А.О. Калашникова, В.В. Кульбы. – М: ИПУ РАН, 2020. – С. 102-108.
5. НОВИКОВ А.М., НОВИКОВ Д.А. *Методология научного исследования*. – М.: CRC Press, 2017. – 280 с.
6. НОВИКОВ Д.А. *«Когнитивные игры»: линейная импульсная модель* // Проблемы управления. – 2008. – №3. – С. 14–22.

7. ALBERT R., JEONG H., BARABASI A.-L. *Error and Attack Tolerance of Complex Networks* // Nature. – 2000. – No. 406. – P. 378–382.
8. ANNIBALE A., COOLEN A.C.C, BIANCONI G. *Network resilience against intelligent attacks constrained by the degree-dependent node removal cost* // J. Phys. A. – 2010. – Vol. 43, No. 39. – e395001.
9. AZIMI-TAFRESHI N., GOMEZ-GARDENES J., DOROGOVTSEV S.N. *k-Core percolation on multiplex networks* // Phys. Rev. E. – 2014. – Vol. 90, No. 3. – e032816.
10. BAK P., CHEN K., TANG C. *A forest-fire model and some thoughts on turbulence* // Phys. Lett. A. – 1990. – Vol. 147, No. 5–6. – P. 297–300.
11. BAXTER G.J., DOROGOVTSEV S.N., GOLTSEV A.V., MENDES J.F.F. *Heterogeneous k-core versus bootstrap percolation on complex networks* // Phys. Rev. E. – 2011. – Vol. 83, No. 5. – e051134.
12. BROWN G., CARLYLE M., SALMERON J., WOOD R. *Defending Critical Infrastructure* // Interfaces. – 2006. – Vol. 36. – P. 530–544.
13. BRUMMITT C.D., D'SOUZA R.M., LEICHT E. *Suppressing cascades of load in interdependent networks* // Proc. Natl. Acad. Sci. – 2012. – Vol. 109, No. 12. – e680–689.
14. COHEN R., HAVLIN S., BEN-AVRAHAM D. *Efficient immunization strategies for computer networks and populations* – Phys. Rev. Lett. – 2003. – Vol. 91, No. 24. – e247901.
15. COTRONEO D., DE SIMONE L., LIGUORI P., NATELLA R. et al. *Enhancing Failure Propagation Analysis in Cloud Computing Systems* // Proc. of IEEE 30th Int. Symposium on Software Reliability Engineering (ISSRE). – 2019. – P. 139–150.
16. CUI P., ZHU P., WANG K., XUN P., XIA Z. *Enhancing robustness of interdependent network by adding connectivity and dependence links* // Physica A. – 2018. No. 497. –

P. 185–197.

17. DONG G., GAO J., DU R., TIAN L. et al. *Robustness of network of networks under targeted attack* // Phys. Rev. E. – 2013. – Vol. 87, No. 5. – e052804.
18. DOROGOVTSEV S.N., GOLTSEV A.V., MENDES J.F.F. *k-Core organization of complex networks* // Phys. Rev. Lett. – 2006. – Vol. 96, No. 4. – e040601.
19. GALLOS L.K., COHEN R., ARGYRAKIS P., BUNDE A. et al. *Network robustness and fragility: Percolation on random graphs* // Phys. Rev. Lett. – 2000. – Vol. 85, No. 25. – e5468.
20. GALLOS L.K., COHEN R., ARGYRAKIS P., BUNDE A. et al. *Stability and topology of scale-free networks under attack and defense strategies* // Phys. Rev. Lett. – 2005. – Vol. 94, No. 18. – e188701.
21. GAO C., LI X., ZHANG X., LI K. *Network immunization for interdependent networks* // J. Comput. Inf. Syst. – 2013. – Vol. 9, No. 16. – P. 6661–6668.
22. GOLTSEV A.V., DOROGOVTSEV S.N., MENDES J.F.F. *k-Core (bootstrap) percolation on complex networks: Critical phenomena and nonlocal effects* // Phys. Rev. E. – 2006. – Vol. 73, No. 5. – e056101.
23. GUO H., YU S.S., IU H.H., FERNANDO T. et al. *Complex network theory analytical approach to power system cascading failure – From a cyber-physical perspective* // Chaos. – 2019. – Vol. 29, No. 5. – e053111.
24. HAJIZADEH M., VISHKAIE F.R., BAKOUIE F., GHARIBZADEH S. *Modeling the Outbreak of an Infectious Disease on a Heterogeneous Network* // Adv. Syst. Sci. Appl. – 2016. – Vol. 16, No. 4. – P. 89–99.
25. HOLME P., KIM B.J., YOON C.N., HAN S.K. *Attack vulnerability of complex networks* // Phys. Rev. E. – 2002. – Vol. 65. No. 5. – e056109.
26. *ISO 31000:2018 Risk management – Guidelines*, [Электронный ресурс]. – Режим доступа: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en.

27. MOORE S., ROGERS T. *Predicting the speed of epidemics spreading in networks* // Phys. Rev. Lett. – 2020. – Vol. 124, No. 6. – P. e068301.
28. NEWMAN D.E., NKEI B., CARRERAS B.A., DOBSON I. et al. *Risk assessment in complex interacting infrastructure systems* // Proc. of 40th Annual Hawaii Int. Conf. on System Sciences (HICSS'07). – 2007.
29. SHAO S., HUANG X., STANLEY H.E., HAVLIN S. *Percolation of localized attack on complex networks* // New J. Phys. – 2015. – Vol. 17, No. 2. – e023049.
30. SHIROKY A.A., KALASHNIKOV A.O.: *Mathematical Problems of Managing the Risks of Complex Systems under Targeted Attacks with Known Structures* // Mathematics. – 2021. – Vol. 9, No. 19. – e2468.
31. STURARO A., SILVESTRI S., CONTI M., DAS S.K. *A realistic model for failure propagation in interdependent cyber-physical systems* // IEEE Trans. Netw. Sci. Eng. – 2018. – Vol. 7, No. 2. – P. 817–831.
32. TAN F., XIA Y., ZHANG W., JIN X. *Cascading failures of loads in interconnected networks under intentional attack* // EPL. – 2013. – Vol. 102, No. 2. – e28009.
33. WANG L., YAO C., YANG Y., YU X. *Research on a Dynamic Virus Propagation Model to Improve Smart Campus Security* // IEEE Access. – 2018. – No. 6. – P. 20663–20672.

THE INFLUENCE OF THE STRUCTURE OF A COMPLEX SYSTEM IN RISK MANAGEMENT

Alexander Shiroky, V.A. Trapeznikov Institute of Control Sciences of RAS, Moscow, Cand.Sc., Senior researcher (shiroky@ipu.ru).

Abstract: Risk management problems are often addressed using game-theoretic models such as the «Defender – Attacker» and «Defender – Attacker – Defender». Players employ sets of acceptable distributions of limited resources as strategies. In the classical problem settings, the Defender is unable to reduce risk by changing the composition or structure of the system to be protected, as most real systems cannot be altered in such ways or cannot be altered at all. However, the question of the influence of the system structure on its overall risk is still relevant when designing one. Therefore, there is a need for methods to compare structures with each other. This article proposes a modification of the classical formulation of the problem of minimizing the integral risk of a complex system. This modification allows one to quantify the influence of the placement of system elements within a given structure on the value of risk. The study provides a solution to the problem for a simple chain, which is the simplest specific case, as well as an algorithm to build a structure minimizing the risk of a complex system. The result obtained can be used in the future to find solutions to this problem in the case of structures of more complex topologies, such as tree-like ones.

Keywords: complex systems, complex system structure, risk management.

УДК 519
ББК 22.18
DOI: 10.25728/ubs.2024.107.05

Статья представлена к публикации
членом редакционной коллегии Г.А. Угольницким.

Поступила в редакцию 31.10.2023.
Дата опубликования 31.01.2024.