DOI: 10.25728/mlsd.2023.1244

УПРАВЛЕНИЕ РИСКАМИ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ОХРАНЫ С ВЛОЖЕННЫМИ ЗОНАМИ БЕЗОПАСНОСТИ

Широкий А.А.
Институт проблем управления им. В. А. Трапезникова РАН, Москва, Россия
shiroky@ipu.ru

Аннотация. Работа посвящена решению задачи минимизации интегрального риска при проектировании систем охраны с несколькими вложенными зонами безопасности. Предложено общее правило размещения средств её обеспечения на границах зон в зависимости от их удалённости от периметра, а также алгоритм проектирования системы охраны с вложенными зонами безопасности.

Ключевые слова: системы охраны, проектирование систем охраны, управление рисками.

Введение

При решении задач обеспечения физической безопасности часто возникают системы охраны, имеющие структуру со вложенными зонами безопасности. В частности, такие системы получаются при организации помещений для совершения операций с ценностями [1], режимных помещений [2], охраны особо важных объектов [3].

Одним из стандартных [4] методов оценки рисков является сценарный анализ. Применительно к системам охраны он предполагает моделирование различных сценариев атаки, начиная с наиболее вероятных и заканчивая экстремальными, влекущими за собой наибольший ущерб. При этом модель атаки можно строить в виде графа, вершинами которого являются зоны безопасности (с присвоенными значениями вероятности успешного преодоления мер безопасности зоны и ущерба при наступлении такого события). Рёбра в таком графе отражают структуру исследуемой в данном сценарии атаки. Очевидно, что в наиболее простом невырожденном случае такой граф будет представлять собой простую цепь.

В настоящей работе обсуждаются принципы управления рисками систем охраны с учётом их структуры. Мы рассмотрим, как именно последняя влияет на интегральный риск системы охраны в целом, а также вопрос о том, каким образом следует проектировать такие системы для минимизации расходов на этапе эксплуатации.

1. Общая постановка задачи

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

Предположим, что существуют два субъекта (также пока произвольной природы), которых мы 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 объёмом *ресурса* $X \geq 0$, который он может произвольным образом распределять между элементами системы S: $x = (x_1, \dots, x_n)$, $x_i \geq 0$, $i \in N$, $\sum_{i=1}^{n} x_i \leq X$. Аналогично, будем считать, что игрок A также располагает некоторым объёмом *ресурса* $Y \geq 0$, который он может произвольным образом распределять между элементами системы S: $y = (y_1, \dots, y_n)$, $y_i \geq 0$, $i \in N$, $\sum_{i=1}^{n} y_i \leq Y$.

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, временные, производственные и иные ресурсы/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 $s_i \in S$, $i \in N$, системы 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:

$$\forall i \in N, x_i, y_i \geq 0: \rho_i(x_i, y_i) \geq 0. \quad (1)$$

Нестрогая монотонность риска:

$$\forall i \in N: \frac{\partial \rho_i(x_i,y_i)}{\partial x_i} \leq 0, \frac{\partial \rho_i(x_i,y_i)}{\partial y_i} \geq 0. \quad (2)$$

Ограниченность риска:

$$\forall i \in N, x_i, y_i \geq 0 \; \exists \; \rho_i^x = \text{const}, \rho_i^y = \text{const}: \rho_i^x \leq \rho_i(x_i, y_i) \leq \rho_i^y. \quad (3)$$

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 должно приводить к *снижению* локального риска для любого элемента системы S и, с другой стороны, *дополнительное* выделение ресурса Атакующим должно приводить к *повышению* локального риска для любого 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 на множестве элементов системы S задана структура $W = \langle G(S,E), T\rangle$, где $G(S,E)$ — 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.

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

$$\rho_i(x, y) = u_i(x, y) \cdot p_i(x, y) \quad (4)$$

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.

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

$$\langle S = \{s_i\}_{i\in N}, T, E, D, A, X, Y, \{\rho_i(\cdot,\cdot)\}_{i\in N}, \rho(\cdot,\cdot)\rangle. \quad (5)$$

Если структура $W = \langle G(S,E), T\rangle$ зафиксирована, то

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

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

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:

$$\mathcal{X}(X) = \{(x_1, \dots, x_n) \in \mathbb{R}_+^n: x_i \geq 0, i \in N, \textstyle\sum_{i=1}^n x_i \leq X\}, \quad (6)$$

$$\mathcal{Y}(Y) = \{(y_1, \dots, y_n) \in \mathbb{R}_+^n : y_i \geq 0, i \in N, \sum_{i=1}^n y_i \leq Y\}. \quad (7)$$

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

$$x^* = \underset{x \in \mathcal{X}}{\text{Argmin}}\, \rho(x, y) = \underset{x \in \mathcal{X}}{\text{argmin}} \sum_{i=1}^n \rho_i(x, y). \quad (8)$$

Аналогично, задача игрока *A* («задача Атакующего») заключается в нахождении распределения ресурса $y^* \in \mathcal{Y}$, максимизирующего интегральный риск, и может быть записана в виде:

$$y^* = \underset{y \in \mathcal{Y}}{\text{Argmax}}\, \rho(x, y) = \underset{y \in \mathcal{Y}}{\text{argmax}} \sum_{i=1}^n \rho_i(x, y). \quad (9)$$

Если же структуру $W = \langle G(S, E), T \rangle$ можно изменять (например, модифицируя множества *E* и/или *T*), то прежде, чем решать задачу (8), Защитник может дополнительно снизить риски, решив задачу построения структуры, оптимальной в смысле минимизации рисков.

2. Задача минимизации риска при проектировании системы охраны

Будем проектировать систему охраны с m вложенными зонами безопасности. Предположим, что мы располагаем множеством $S = \{s_1, \dots, s_n\}$, $i \in N = \{1, \dots, n\}$ наборов средств её обеспечения. Для каждого такого набора средств s_i нам известна вероятность p_i его успешного преодоления злоумышленником, а также величина u_i ущерба системе безопасности в случае успешной атаки. Напомним, что целью настоящей работы является изучение принципов построения структур систем охраны, в связи с чем стоимость защищаемых материальных ценностей игнорируется.

Определение 1. Пусть задан граф $G\big(V = \{v_1, \dots, v_m\}, E = \{(v_i, v_{i+1})\}_{i=1}^{m-1}\big), m \in \mathbb{N}$ и периметр $T = \{v_1\}$. Тогда будем говорить, что кортеж $W_m = \langle G(V, E), T \rangle$ задаёт простую цепную структуру длины m.

В общем случае число вершин графа G может не совпадать с числом элементов множества S. Содержательно случай $m > n$ соответствует ситуации нехватки средств обеспечения безопасности для построения системы охраны с требуемым уровнем вложенности. Случай $m < n$ соответствует ситуации, когда Защитник располагает большим количеством средств безопасности, чем необходимо для организации системы охраны с требуемым числом зон безопасности. Вначале решим задачу для случая $m = n$, а затем покажем способ распространения решения на ситуации, в которых $m \neq n$. Для удобства будем опускать нижний индекс у обозначения структуры.

Определение 2. Взаимно-однозначное отображение $M^{-1}: S \to V, S = \{s_1, \dots, s_n\}, n \in N: \forall i \leq n\ \exists! j \leq n: v_j = M^{-1}(s_i)$ будем называть размещением элементов 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

$$\rho(S, W, M^{-1}) = \sum_{i=1}^n \rho_{M(v_i)}, \quad (10)$$

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

$$\mathbf{M}_{min} = \underset{M^{-1}}{\text{Argmin}}\, \rho(S, W, M^{-1}): \rho_{min} = \sum_{i=1}^n \rho_{M(v_i)}\ \forall M^{-1} \in \mathbf{M}_{min}. \quad (11)$$

Определение 3. Будем говорить, что элементы $s_i, s_j \in S, i, j \in N, i \neq j$ нестрого упорядочены по возрастанию (убыванию) локального риска и записывать $s_i \preccurlyeq s_j$ ($s_i \succcurlyeq s_j$) если при заданной простой цепной структуре W для любых размещений M^{-1}, K^{-1} и любых таких индексов $p, q, k, l, p < q, k > l$, что $s_i = M\big(v_p\big) = K(v_k), s_j = M\big(v_q\big) = K(v_l)$ выполняется неравенство $\rho(S, W, M^{-1}) \leq \rho(S, W, K^{-1})$ ($\rho(S, W, M^{-1}) \geq \rho(S, W, K^{-1})$).

В работе [5] были доказаны следующие утверждения.

Утверждение 1 (критерий упорядоченности). Пусть $N = \{1, .., n\}$, $S = \{s_1, \dots, s_n\}$. Тогда $\forall i \in N \backslash \{n\}\ s_i \preccurlyeq s_{i+1} \Leftrightarrow \frac{u_i}{u_{i+1}} \leq \frac{p_{i+1}(1-p_i)}{p_i(1-p_{i+1})}$; $s_i \succcurlyeq s_{i+1} \Leftrightarrow \frac{u_i}{u_{i+1}} \geq \frac{p_{i+1}(1-p_i)}{p_i(1-p_{i+1})}$.

Утверждение 2 (транзитивность критерия упорядоченности). Пусть $N = \{1, .., n\}$, $S = \{s_1, \dots, s_n\}$. Тогда $\forall i, j, k \in N: i < j < k\ s_i \preccurlyeq s_j \preccurlyeq s_k \Longrightarrow s_i \preccurlyeq s_k$.

Приведённые утверждения позволяют решить задачу (11) для любой цепной структуры с одновершинным периметром в общем виде, в том числе для случаев, когда $m \neq n$. Если $m > n$, то множество наборов средств обеспечения безопасности достаточно дополнить $n - m$ нулевыми элементами, соответствующими отсутствию средств безопасности, после чего задача сведётся к случаю $m = n$. Если же $m < n$, то достаточно перенумеровать элементы множества S так, чтобы выполнялось условие $s_i \preccurlyeq s_{i+1}\ \forall i < n$, а затем исключить из него все элементы с номерами, большими m. Отметим, что стоимость реализации того или иного набора средств обеспечения безопасности мы в данном решении не учитываем.

3. Алгоритм проектирования системы охраны с вложенными зонами безопасности

Рассмотрим систему безопасности с n элементами, задающими множество $S = \{s_1, \dots s_n\}$. Вначале будем предполагать, что все элементы доступны для Атакующего. Будем считать, что последний может проводить сложные атаки, включающие в себя несколько последовательно выводимых из строя элементов системы. Таким образом, модель системы на начальном этапе представляет собой полный граф $G(V, E), V = S, E = \bigcup_{i \neq j}(s_i, s_j), 1 \leq i, j \leq n$, а возможные сценарии атаки — маршруты в нём.

Предположим, что Атакующий хочет нанести защищаемой системе максимальный ущерб. Тогда он должен вывести из строя все элементы системы без исключений. Тогда он должен успешно атаковать все узлы без исключения, решив при этом задачу, обратную задаче (11):

$$\mathbf{M}_{max} = \underset{M^{-1}}{\operatorname{Argmax}}\, \rho(S, W, M^{-1}) \colon \rho_{max} = \sum_{i=1}^{n} \rho_{M(v_i)}\ \forall M^{-1} \in \mathbf{M}_{max}. \quad (12)$$

С учётом изложенного в предыдущем параграфе результата решение строится тривиальным образом и заключается в выборе простого пути $\left(v_1^A, v_2^A, \dots, v_n^A\right)$, включающего все вершины модельного графа G, причём $v_i \succcurlyeq v_{i+1}\ \forall i < n$.

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 $(v_1^D, v_2^D, \dots, v_n^D)$, включающий в себя все вершины графа G. Отметим, что в случае, когда выполнено соотношение

$$\frac{1-p_i}{u_i p_i} = \frac{1-p_j}{u_j p_j} \Leftrightarrow i = j, i, j \in \{1, \dots, n\}, \quad (12)$$

обе задачи имеют единственное решение, причём $v_i^D = v_{n-i+1}^A$. Иными словами, Атакующий и Защитник стремятся к реализации противоположных траекторий.

Тогда алгоритм решения задачи Защитника при выполнении условия (12) выглядит следующим образом:

1. Обеспечить единственную «точку входа» в системе (задать периметр) в вершине v_1^D (она же v_n^A).
2. Назначить вершину v_1^D текущей (положить i равным 1).
3. Последовательно удалять рёбра, соединяющие текущую вершину v_i^D с вершинами $v_n^D, v_{n-1}^D, \dots, v_{i+1}^D$.
4. Если $i < n$, то назначить текущей вершину v_{i+1}^D (положить i равным $i + 1$).
5. Перейти к пункту 3.

Отметим, что при выполнении условия

$$\frac{1-p_i}{u_i p_i} = \frac{1-p_j}{u_j p_j}\ \forall i, j \in \{1, \dots, n\}, \quad (13)$$

элементы становятся нейтральными к перестановкам в смысле утверждения 1. 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 элементов, то у него появляется дополнительный критерий упорядоченности. Конкретно, Защитник будет заинтересован в том, чтобы вынести вперёд (ближе к периметру) вершины, наиболее отзывчивые к выделению ресурса в смысле повышения её стойкости к действиям Атакующего. Эту задачу автор в рамках настоящей работы не рассматривает.

4. Заключение

В настоящей работе рассматривается задача минимизации интегрального риска при проектировании систем охраны с несколькими вложенными зонами безопасности. Содержательно

полученный результат представляет собой правило размещения средств её обеспечения на границах зон в зависимости от их удалённости от периметра. Предложен алгоритм проектирования системы охраны с вложенными зонами безопасности.

Отметим, что порождаемая при решении задачи оптимального размещения средств обеспечения безопасности модель является линейной относительно ожидаемых ущербов. Это позволяет использовать её и на этапе эксплуатации системы для управления рисками за счёт перераспределения материальных ценностей между зонами безопасности, а также для решения задач оптимального распределения ресурсов между ними.

Дальнейшим развитием работы видится изучение более сложных структур охраны, включающих в себя непересекающиеся зоны с различным уровнем безопасности внутри контролируемого периметра.

Литература

1. Положение о порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации N 630-П : принято ЦБ РФ 29 янв. 2018 г. // Вестник Банка России. – 2018. – N 51. – С. 2–65.
2. Приказ «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации» N 152 : принято ФАПСИ 13 июн. 2001 // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2001. № 34. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102095483&rdk=.
3. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности Р 089-2022 : утв. Росгвардией 1 мар. 2022 г. // Информационно-правовая система «Гарант». – 2022. – URL: https://www.garant.ru/products/ipo/prime/doc/404396762/?ysclid=lh60xgbkzj683998058.
4. Национальный стандарт Российской Федерации «Менеджмент риска. Технологии оценки риска» ГОСТ Р 58771-2019 : утв. Росстандартом 17 дек. 2019 // Информационно-правовая система «Гарант». – 2020. – URL: https://base.garant.ru/73747568/?ysclid=lh61et4sda564727091.
5. *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, N 19. – URL: https://www.mdpi.com/2227-7390/9/19/2468.