

А. В. Лаврентьев, В. П. Зязин (Москва, МГТУ МИРЭА). **Алгоритм управления рисками информационной безопасности на основе теоретико-игрового моделирования.**

Процесс противоборства между лицом, принимающим решения по управлению рисками информационной безопасности [1] (игрок 1), и нарушителем информационной безопасности (игрок 2) представлен в виде теоретико-игровой модели [5]. Полагаем, что есть непустые конечные множества $\mathcal{F} = \{f_1, f_2, \dots, f_N\}$ и $\mathcal{A} = \{a_1, a_2, \dots, a_m\}$, где $\mathcal{A}$ — множество путей нападения [3], а $\mathcal{F}$ — множество мер безопасности [4, 7]. Игрок 1 выбирает один из элементов $f \in \mathcal{F}$. Игрок 2 выбирает путь $a_i \in \mathcal{A}$ со стоимостью нападения $q(a_i) \in \mathbf{R}_+$. Очевидно, что множества $\mathcal{F}$ и $\mathcal{A}$ можно рассматривать как множества стратегий игроков 1 и 2 соответственно. Дополним это множество $\mathcal{A}$ стратегией «Не нападать», которую обозначим a_0 . Всякий раз, когда в игре используется путь нападения a , и игрок 1 выбирает меру безопасности f , он несет рисковую потерю $h_{f,a}$. Следовательно, потеря первого игрока — $h_{f,a} \in \mathbf{R}_+$, и чистая выгода второго равна $h_{f,a} - q(a)$. Для игрока 1 целью является минимизация «потери», а для игрока 2 — максимизация своей чистой выгоды [6].

Этот сценарий может быть смоделирован как биматричная игра с двумя игроками, где защитник и нарушитель выбирают свои чистые стратегии f и a в непустых и конечных множествах $\mathcal{F}$ и $\mathcal{A}$ соответственно, $|\mathcal{A}| = m$ и $|\mathcal{F}| = N$. Матрицами выплат для игроков будут

$$\tilde{H} = [H|0], \quad \tilde{Q} = [Q|0], \quad (1)$$

где H и Q — матрицы размера $N \times m$; $(H, [H]_{f,a} = h_{f,a})$ — неотрицательная матрица без нулевых строк (нулевая строка подразумевает отсутствие рисков для защитника и может быть исключена), и нет столбца в матрице $(Q, [Q]_{f,a} = h_{f,a} - q(a))$, который доминирует над всеми другими столбцами (наличие такого столбца означало бы однозначный выбор нападающего). «Последний» нулевой столбец в определении $\tilde{H}$ и $\tilde{Q}$ отражает нулевую потерю для защитника и нулевую выгоду для нападающего в случае, если последний выберет «не нападать».

Рассмотрим смешанные стратегии этой игры. Стратегией защитника будет вероятностное распределение $g = (g_f, f \in \mathcal{F})$ на $\mathcal{F}$, где все $g_f \geq 0$ и $\sum_{f \in \mathcal{F}} g_f = 1$, и для нападающего вероятностное распределение $(u(a), a \in \mathcal{A} \cup \{a_0\})$ на $\mathcal{A} \cup \{a_0\}$, где все $u(a) \geq 0$ и $\sum_{a \in \mathcal{A}} u(a) = 1$. Цель защитника состоит в том, чтобы минимизировать ожидаемую потерю

$$L(g, u) = \sum_{f \in \mathcal{F}} g_f \left(\sum_{a \in \mathcal{A}} u(a) h_{f,a} \right), \quad (2)$$

в то время как нападающий пытается максимизировать ожидаемую выгоду

$$R(g, u) = \sum_{a \in \mathcal{A}} u(a) \left(\sum_{f \in \mathcal{F}} g_f h_{f,a} - q(a) \right). \quad (3)$$

Многогранник $S_{\tilde{H}}$, соответствующий матрице $\tilde{H}$, в [2] определен как векторная сумма выпуклой оболочки ее строк $\text{conv}(h_1, h_2, \dots, h_N)$ и неотрицательного ортанта $\mathbf{R}_+^m$:

$$S_H = \text{conv}(h_1, h_2, \dots, h_N) + \mathbf{R}_+^m. \quad (4)$$

Там же введено понятие несущественной строки, т. е. такой строки, добавление которой в $\tilde{H}$ не изменит многогранника S_H , и показано существование такого класса матриц $\mathcal{P}$, что для любой матрицы $P \in \mathcal{P}$ выполняется

$$S_H = \{x \in \mathbf{R}_+^m | Px \geq (1)_N\}. \quad (5)$$

Более того, из любой матрицы класса $\mathcal{P}$ можно получить любую другую матрицу данного класса с помощью перестановки строк и добавления или удаления несущественных. Для дальнейших рассуждений все матрицы $P \in \mathcal{P}$ равносильны относительно формулы (5).

В работе [2] также показано, что строка e матрицы P представима в виде $e = (e(a), a \in \mathcal{A})$. Пусть $e(\mathcal{A}) = \sum_{a \in \mathcal{A}} e(a)$. Так как $e(a) \geq 0$ для всех $a \in \mathcal{A}$ и $e(\mathcal{A}) > 0$, то $(e(a)/e(\mathcal{A}), a \in \mathcal{A})$, где $\sum_{a \in \mathcal{A}} [e(a)/e(\mathcal{A})] = 1$, можно рассматривать как вероятностное распределение на $\mathcal{A}$, которое будем называть *распределением e* .

Для простоты запись $e \in P$, где P — матрица, будет означать, что e принадлежит множеству строк матрицы P .

Для каждой строки $e \in P$ определим

$$h(e) = \min_{f \in \mathcal{F}} \left\{ \sum_{a \in \mathcal{A}} \frac{e(a)}{e(\mathcal{A})} h_{f,a} \right\}, \quad (6)$$

$$v(e) = h(e) - \sum_{a \in \mathcal{A}} \frac{e(a)}{e(\mathcal{A})} q(a), \quad (7)$$

где $h(e)$ — минимальная потеря защитника, если нападающий выбрал путь согласно распределению $e = (\frac{e(a)}{e(\mathcal{A})}, a \in \mathcal{A})$; $v(e)$ может рассматриваться как ожидаемая выгода нападения в соответствии с распределением e .

Будем называть строку e *критической*, если

$$v(e) = \max_{\tilde{e} \in P} v(\tilde{e}). \quad (8)$$

Соответствующее критической строке распределение вероятности дает максимум выгоды нападающему при оптимальном выборе стратегии защитника.

Определим $v = v(e)$, где e — критическая строка, и пусть $P_{\max}$ — матрица, состоящая из критических строк матрицы P . Пусть $(z_e, e \in P_{\max})$ — дискретное вероятностное распределение на $P_{\max}$, где все $z_e \geq 0$ и $\sum_{e \in P_{\max}} z_e = 1$.

Теорема. Для рассматриваемой игры всегда выполняется следующее.

А. Если $v \leq 0$, то стратегия «Не нападать» (т. е. $u(a_0) = 1$) является оптимальной стратегией нападающего и находится в равновесии Нэша со стратегией защитника $(g_f, f \in \mathcal{F})$, удовлетворяющей неравенствам

$$\bar{h}_g(a) = \sum_{f \in \mathcal{F}} g_f h_{f,a} \leq q(a), \quad \forall a \in \mathcal{A}. \quad (9)$$

Соответствующие выплаты (2), (3) нулевые.

В. Если $v \geq 0$, то для распределения вероятности $(z_e, e \in P_{\max})$ стратегия нападающего $(u(a), a \in \mathcal{A})$ определенная как

$$u(a) = \sum_{e \in P_{\max}} z_e \frac{e(a)}{e(\mathcal{A})}, \quad (10)$$

находится в равновесии Нэша с любой стратегией $(g_f, f \in \mathcal{F})$ защитника, которая удовлетворяет следующим условиям:

$$\begin{aligned} \bar{h}_g(a) - q(a) &= v \text{ для всех таких } a \in \mathcal{A}, \text{ что } u(a) > 0, \\ \bar{h}_g(a) - q(a) &\leq v \text{ для всех } a \in \mathcal{A}. \end{aligned} \quad (11)$$

По крайней мере, одна такая стратегия $(g_f, f \in \mathcal{F})$ существует.

Соответствующие выплаты: v — для нападавшего и $r(z)$ — для защитника, где

$$r(z) = \sum_{e \in P_{\max}} z_e h(e). \quad (12)$$

Если все $q(a) = 0$, то каждая пара равновесий Нэша удовлетворяет выражениям (10), (11).

На основании рассматриваемой теоретико-игровой модели можно предложить следующий **алгоритм принятия решений по управлению рисками ИБ**.

1. Формируем множества $\mathcal{F}$ и $\mathcal{A}$.
2. Находим $h_{f,a} \in \mathbf{R}_+$ для всех $a \in \mathcal{A}$ и всех $f \in \mathcal{F}$, а также $q(a) \in \mathbf{R}_+$ для всех $a \in \mathcal{A}$.
3. Для многогранника S_H (формула (4)) строим одну из возможных матриц P по формуле (5).
4. Для всех $e \in P$ считаем значения $h(e)$ и $v(e)$ по формулам (6) и (7).
5. По формуле (8) определяем критические строки матрицы P и вычисляем v как максимально достижимое значение в этой формуле. Формируем $P_{\max}$ как матрицу, состоящую из критических строк матрицы P .

6а. Если $v \leq 0$, то стратегия «Не нападать» (т.е. $u(a_0) = 1$) — оптимальная стратегия нападающего. Ищем стратегию защитника $(g_f, f \in \mathcal{F})$, находящуюся в равновесии Нэша с указанной стратегией нападающего, в соответствии с неравенствами (9). В этом случае потеря защитника и выигрыш нападающего равны нулю.

6б. Если $v \geq 0$, то для стратегии нападающего $(u(a), a \in \mathcal{A})$, соответствующей выражению (10), ищем стратегию $(g_f, f \in \mathcal{F})$ защитника, которая удовлетворяет условиям (11). При этом потеря защитника равна значению выражения (12), а выигрыш нападающего равен v .

П р и м е ч а н и я. 1. Если для $q(a) = 0$ всех $a \in \mathcal{A}$, то всегда выполняется шаг 6б. 2. Распределение $(z_e, e \in P_{\max})$ позволяет описать множество равновесий Нэша игры. Оно может использоваться, например, для моделирования предпочтений нападающего при атаке. В простейшем случае это распределение является распределением равновероятных событий.

7. Смешанная стратегия $(g_f, f \in \mathcal{F})$ позволяет осуществлять распределение ресурсов при управлении рисками ИБ: каждая вероятность события g_f отражает пропорцию ресурсов, приходящихся на соответствующий элемент $f \in \mathcal{F}$. Смешанная стратегия $(u(a), a \in \mathcal{A})$ отражает наиболее вероятные пути нападения на систему защиты игрока 1.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 27005:2011, Information technology—Security techniques—Information security risk management. Geneva: 2011.
2. Fulkerson D. R. Blocking and Anti-Blocking Pairs of Polyhedra. — Math. Progr., 1971, № 1, p. 168–194.
3. BSI: Attack Pattern Glossary. Cigital Inc., 2006.
4. NIST IR 7298 Revision 1, Glossary of Key Information Security Terms, 2011.
5. Данилов В. И. Лекции по теории игр. М.: Российская экономическая школа, 2002.

6. Гальперин В. М., Игнатьев С. М., Моргунов В. И. Микроэкономика. В 2-х томах. СПб.: Экономическая школа, 2004.
7. Национальный стандарт Российской Федерации ГОСТ Р 53114-2008. «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».