неопределенности [Электронный ресурс]. – URL: https://railwayforum.ru/events/forum-1520/ Международный транспортно-логистический форум «PRO//Движение.1520» (дата обращения 22.10.2020).

3. Договор о Евразийском экономическом союзе, совершенный в Астане 29 мая 2014 года.

4. Закон Республики Беларусь от 06.01.1999 г. № 237-З «О железнодорожном транспорте».

5. Закон Республики Казахстан «О железнодорожном транспорте» от 8 декабря 2001 года № 266-II.

6. Федеральный закон Российской Федерации «О железнодорожном транспорте в Российской Федерации» от 10 января 2003 года № 17-ФЗ [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/19009 (дата обращения 22.10.2020).

7. *Ismailov Zh., Kononov D.* Integrated Management System for Rail Transport: Planning of Cargo Turnover in Conditions of Uncertainty /Proceedings of the 11th International Conference Management of Large-Scale System Development (MLSD), 2018 [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/document/8551807 (дата обращения 20.10.2020).

Аникина Е.В.

Управление рисками сложной сети на основе арбитражного решения

Аннотация: В работе рассматривается один из методов эффективного распределения ограниченного ресурса для управления информационными рисками на основе теоретико-игровых моделей (арбитражных схем).

Ключевые слова: управление информационными рисками, сложная сеть, менеджер риска, распределение ресурса, арбитражное решение

Современный этап развития России можно охарактеризовать одним словом – цифровизация, поскольку сфера и объемы использования цифровых, информационных технологий расширяются и возрастают с каждым днем. В рамках многих проектов создается большое количество крупномасштабных, распределенных систем, зачастую не имеющие аналогов как по

своей сложности, с одной стороны, так и по размерам потенциальных угроз, возникающих в случае их отказа или некорректной работы, с другой [1, 2].

Таким образом, проблема обеспечения безопасности и управления рисками сложных систем в настоящее время становится как никогда актуальной и злободневной. Причем, это касается не только активного внедрения существующих методов и средств информационной безопасности и управления рисками, но и их совершенствования, а также развития новых подходов для решения указанных проблем.

Для эффективного решения задач управления рисками и безопасностью сложных систем необходимо использование подходов, которые позволяют рассматривать риск-образующие события и связанные с ними риски не как «точки» в некотором фазовом пространстве, а как динамическую сеть, узлы которой оказывают на состояние друг друга существенное влияние.

Арбитражное решение

В рамках базовой модели, рассмотренной в [3], рассмотрим случай, когда элементы $s_i \in S$, $i \in N$, системы S являются *независимыми* и не оказывают друг на друга никакого влияния. Подход к решению указанной задачи, когда конкретный вид функций локального риска неизвестен, впервые был намечен, хотя и немного в другой постановке, в статье [5], а наиболее полно изложен в монографиях [1, 6].

В основе указанного подхода лежат следующие соображения (подробнее, см. [1, 6]).

Поскольку конкретный вид функций локального риска нам неизвестен, то представляется целесообразным перейти от «глобальной» задачи минимизации интегрального риска к «локальной» задаче *снижению максимума локальных рисков* $\rho_i(\cdot)$, $i \in N$:

$$\inf_{x \in X} \sup_{i \in N} \rho_i(x) \qquad (1)$$

Решением задачи (1) будут «хорошие» распределения ресурса $\hat{x}(X) \in \mathcal{X}(X)$ такие, что: $\hat{x}(X) = \arg\inf_{x \in X} \sup_{i \in N} \rho_i(x)$. Обозначим подмножество «хороших» распределений ресурса $\widehat{\mathcal{X}}(X) \subseteq \mathcal{X}(X)$.

Для задачи (1) верно следующее утверждение «о выравнивании локальных рисков» [1, 6], которое мы приведем в обозначениях рассматриваемой выше модели:

Утверждение 1. Пусть $\rho_i(\cdot)$, $i \in N$ удовлетворяют свойствам C1, C2 и C3 и существует распределение ресурса $(\tilde{x}_1, \dots, \tilde{x}_n) \in \mathcal{X}(X)$ такое, что: $\sum_{i=1}^{n} \tilde{x}_i = X$ и $\rho_1(\tilde{x}_1) = \dots = \rho_n(\tilde{x}_n) = c$, тогда $(\tilde{x}_1, \dots, \tilde{x}_n)$ – единственное решение задачи (1).

Предположим, что тем или иным способом RM (менеджер риска) стали известны текущие значения локальных рисков для каждого элемента $s_i \in S$, $i \in N$, системы S, до распределения на них каких-либо ресурсов. Обозначим указанные значения $\rho_i(0)$, $i \in N$ и упорядочим их по убыванию: $\rho_{(1)}(0) \geq \dots \geq \rho_{(n)}(0)$. Откуда следует, что если целью RM является выравнивание локальных рисков, то для достижения указанной цели для разных элемента

$s_i \in S$, $i \in N$, системы S, вообще говоря, придется затратить различный объем ресурсов, причем: если $\rho_{(i)}(0) \geq \rho_{(j)}(0)$, то должно выполняться $x_{(i)} \geq x_{(j)}$. В этом случае, значения $\tilde{\rho}_i = \rho_i(0)$ можно рассматривать, как своеобразные «*заявки*» элементов $s_i \in S$, $i \in N$, системы S на предоставление ресурса со стороны RM. Обозначим $\tilde{\rho} = (\tilde{\rho}_1, \dots, \tilde{\rho}_n)$ – вектор «заявок» элементов $s_i \in S$, $i \in N$, системы S на предоставление ресурса со стороны RM.

Предположим теперь, что сам ресурс X, которым располагает RM, представляет собой функцию от «заявок» элементов системы S такую, что $X = X(\tilde{\rho}_1, \dots, \tilde{\rho}_n)$ – симметрична, непрерывна, строго монотонна и $X(0, \dots, 0) = 0$. Указанные свойства являются вполне естественными и отражают следующие особенности поведения защитника: 1) не выделять ресурс без необходимости; 2) в случае возрастания рисков увеличивать объем выделяемого ресурса; 3) в отсутствии дополнительной информации считать все элементы системы S однородными [1, 6].

В [1, 6] был сформулирован и обоснован ряд «разумных», с точки зрения управления рисками, требований, которым должно удовлетворять «хорошее» распределение ресурсов.

T1 (оптимальность по Парето): для любого $\hat{x}(X) \in \widehat{\mathcal{X}}(X)$: $\sum_{i=1}^{n} \hat{x}_i(X) = X$.

T2 (монотонность): для любых $X_1 > X_2 \geq 0$ и

$\hat{x}(X) \in \widehat{\mathcal{X}}(X)$: $\hat{x}(X_1) > \hat{x}(X_2)$, то есть $\hat{x}_i(X_1) \geq \hat{x}_i(X_2)$, $i \in N$ и существует $j \in N$ такое, что $\hat{x}_j(X_1) > \hat{x}_j(X_2)$.

Т3 (паритетность): для любого $\hat{x}(X) \in \widehat{\mathcal{X}}(X)$: если $\rho_{(1)}(0) \geq \cdots \geq \rho_{(n)}(0)$, то $\hat{x}_{(1)}(X) \geq \cdots \geq \hat{x}_{(n)}(X)$.

В [1, 6] было показано, что подмножество «хороших» распределений ресурса $\widehat{\mathcal{X}}(X) \subseteq \mathcal{X}(X)$, удовлетворяющих требованиям Т1, Т2 и Т3, не пусто, поскольку, в частности, указанным требованиям удовлетворяет равномерное распределение ресурса $\hat{e}(X) \in \widehat{\mathcal{X}}(X)$: $\hat{e}_i(X) = {}^{X}/_{n}$.

Приведенные предположения позволяют использовать для нахождения эффективного распределения ресурса теоретико-игровой подход на основе *арбитражной схемы, основанной на принципах стимуляции и неподавления* [7, 8]: будем рассматривать элементы $s_i \in S$, $i \in N$, системы S в качестве «игроков» некоторой игры $\Gamma(\tilde{\rho})$, где $\tilde{\rho} = (\tilde{\rho}_1, \dots, \tilde{\rho}_n)$ – вектор «заявок» элементов системы S на предоставление ресурса со стороны RM, который выступает в роли своеобразного «*арбитра*».

Определим, доступный для распределения RM ресурс $X(\tilde{\rho}) = X(\tilde{\rho}_1, \dots, \tilde{\rho}_n)$ и множество допустимых распределений ресурса X между элементами системы S:

$\mathcal{X}(\tilde{\rho}) = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_i \geq 0, i \in N, \sum_{i=1}^{n} x_i \leq X(\tilde{\rho})\}$.

Обозначим $\widehat{\mathcal{X}}(\tilde{\rho}) \subseteq \mathcal{X}(\tilde{\rho})$ – подмножество «хороших» распределений ресурса, удовлетворяющих требованиям Т1, Т2 и Т3.

Определение 1. Пусть $\tilde{\rho}_{(1)} \geq \cdots \geq \tilde{\rho}_{(n)}$, тогда назовем распределение ресурса $\hat{\pi}(\tilde{\rho}) = \left(\hat{\pi}_{(1)}(\tilde{\rho}), \dots, \hat{\pi}_{(n)}(\tilde{\rho})\right)$ «максимально стимулирующим» (МС-решением) если:

1) $\hat{\pi}(\tilde{\rho}) \in \widehat{\mathcal{X}}(\tilde{\rho})$;
2) $\hat{\pi}_{(1)}(\tilde{\rho}) = \sup_{\hat{x}(\tilde{\rho}) \in \widehat{\mathcal{X}}(\tilde{\rho})} \hat{x}_{(1)}(\tilde{\rho})$;
   $\hat{\pi}_{(2)}(\tilde{\rho}) = \sup_{\hat{x}(\tilde{\rho}) \in \widehat{\mathcal{X}}^{(1)}(\tilde{\rho})} \hat{x}_{(2)}(\tilde{\rho})$;
   …
   $\hat{\pi}_{(n-1)}(\tilde{\rho})(\tilde{\rho}) = \sup_{\hat{x}(\tilde{\rho}) \in \widehat{\mathcal{X}}^{(1)(2)\dots(n-2)}(\tilde{\rho})} \hat{x}_{(n-1)}(\tilde{\rho})$,

где $\widehat{\mathcal{X}}^{(1)(2)\dots(k)}(\tilde{\rho}) = \left\{\hat{x}(\tilde{\rho}) \in \widehat{\mathcal{X}}(\tilde{\rho}) : \hat{x}_{(1)}(\tilde{\rho}) = \hat{\pi}_{(1)}(\tilde{\rho}), \hat{x}_{(2)}(\tilde{\rho}) = \pi(2)\rho, \dots, x(k)\rho = \pi(k)\rho\right.$ и

$k = 1,2, \dots, n-2$.

Таким образом, под МС-решением будем понимать такое распределение ресурса X между элементами системы S, при

котором: во-первых, для него выполнены требования Т1, Т2 и Т3, а, во-вторых, на элемент с номером (1), с максимальной «заявкой», выделяется максимально возможное для номера (1), среди всех таких распределений, количество ресурса; на элемент с номером (2), со второй по значимости «заявкой», выделяется максимально возможное для номера (2), среди распределений у которых, количество ресурса для номера (1) уже зафиксировано и равно $\hat{\pi}_{(1)}(\tilde{\rho})$ и так далее.

Как следует из приведенного выше определения МС-решения, его существование отнюдь не является очевидным. Тем не менее, оказывается верным следующее утверждение [1, 5-8]:

Утверждение 2. Пусть $\tilde{\rho}_{(1)} \geq \cdots \geq \tilde{\rho}_{(n)}$, тогда МС-решение $\hat{\pi}(\tilde{\rho}) = \left(\hat{\pi}_{(1)}(\tilde{\rho}), \ldots, \hat{\pi}_{(n)}(\tilde{\rho})\right)$ существует и единственно.

Приведенное утверждение дает возможность в рамках решения задачи (1) организовать эффективное управление рисками сложной системы при котором сначала снижается максимальный риск, затем следующий по значимости и так далее. К сожалению, доказательство утверждения 2 не является конструктивным и не определяет МС-решение в аналитической форме. Тем не менее, для ряда частых случаев это может быть сделано, что и позволяет применить МС-решение на практике.

Предположим, что функция $X(\tilde{\rho})$ имеет вид:

$X(\tilde{\rho}) = X(\tilde{\rho}_1 + \cdots + \tilde{\rho}_n)$, то есть, зависит только от суммы «заявок» всех элементов $s_i \in S$, $i \in N$, системы S, что довольно часто встречается на практике, причем $\frac{\partial X(\tilde{\rho}_1 + \cdots + \tilde{\rho}_n)}{\partial \tilde{\rho}_i} > 0$, для $i \in N$. Тогда для случаев, когда $X(\tilde{\rho})$ выпукла, вогнута или линейна оказываются верным следующие утверждения [1, 6]:

Утверждение 3. Пусть $\tilde{\rho}_{(1)} \geq \cdots \geq \tilde{\rho}_{(n)}$ (для простоты, будем считать, что $\tilde{\rho}_1 \geq \cdots \geq \tilde{\rho}_n$ и $X(\tilde{\rho})$ выпукла, то есть:

$\frac{\partial^2 X(\tilde{\rho}_1 + \cdots + \tilde{\rho}_n)}{\partial \tilde{\rho}_i^{\,2}} \geq 0$, для $i \in N$. Тогда МС-решение имеет вид:

$\mu_n^+(\tilde{\rho}) = \frac{1}{n} X(n\tilde{\rho}_n)$;

$\mu_k^+(\tilde{\rho}) = \frac{1}{k}\left(X\left(k\tilde{\rho}_k + \sum_{i=k+1}^{n} \tilde{\rho}_i\right) - \sum_{i=k+1}^{n} \mu_i^+(\tilde{\rho})\right)$,

$k = 1,2, \ldots, n-1$.

Утверждение 4. Пусть $\tilde{\rho}_{(1)} \geq \cdots \geq \tilde{\rho}_{(n)}$ (для простоты, будем считать, что $\tilde{\rho}_1 \geq \cdots \geq \tilde{\rho}_n$) и $X(\tilde{\rho})$ вогнута, то есть:

$\frac{\partial^2 X(\tilde{\rho}_1+\cdots+\tilde{\rho}_n)}{\partial \tilde{\rho}_i{}^2} \leq 0$, для $i \in N$. Тогда МС-решение имеет вид:

$\mu_1^-(\tilde{\rho}) = \frac{1}{n} X(n\tilde{\rho}_1)$;

$\mu_k^-(\tilde{\rho}) = \frac{1}{n-(k-1)} X\left(\sum_{i=1}^{k-1} \tilde{\rho}_i + (n-(k-1))\tilde{\rho}_k\right) - \frac{1}{n-(k-1)} \sum_{i=1}^{k-1} \mu_i^-(\tilde{\rho}), \quad k = 2, \dots, n.$

Утверждение 5. Пусть $\tilde{\rho}_{(1)} \geq \cdots \geq \tilde{\rho}_{(n)}$ (для простоты, будем считать, что $\tilde{\rho}_1 \geq \cdots \geq \tilde{\rho}_n$) и

$X(\tilde{\rho}) = \alpha(\sum_{i=1}^{n} \tilde{\rho}_i) + \beta$ (линейная функция), то есть: $\frac{\partial^2 X(\tilde{\rho}_1+\cdots+\tilde{\rho}_n)}{\partial \tilde{\rho}_i{}^2} \equiv 0$, для $i \in N$. Тогда МС-решение имеет вид:

$\mu_k(\tilde{\rho}) = \alpha\tilde{\rho}_k, k = 1, \dots, n.$

Анализ приведенного МС-решения позволяет сделать вывод о том, что достоверная информация о значениях «заявок» элементов $s_i \in S$, $i \in N$, системы S на предоставление ресурса со стороны игрока RM: $\tilde{\rho}_i = \rho_i(0)$ является ключевой, для реализации указанного подхода.

Заключение

В работе рассмотрена задача управления рисками в условиях неопределенности, когда информация о конкретном виде функций локального риска элементов системы отсутствует.

Показано, что в случае независимости (отсутствия взаимного влияния друг на друга) элементов системы для нахождения эффективного распределения ресурса может быть использован теоретико-игровой подход на базе арбитражной схемы, основанной на принципах стимуляции и неподавления (МС-решение).

Литература:

1. *Калашников А.О.* Модели и методы организационного управления информационными рисками корпораций. – М.: «Эгвес», 2011. – 312 с.

2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/42128 (дата обращения 20.10.2020).

3. *Калашников А.О., Аникина Е.В.* Модели управления

информационными рисками сложных систем//Информация и безопасность. – 2020. – Т. 23. №2(4). – С. 191-202.

4. *Калашников А.О.* Управление информационными рисками с использованием арбитражных схем//Системы управления и информационные технологии. – 2004. – № 4 (16). – С. 57-61.

5. *Калашников А.О.* Организационные механизмы управления информационными рисками корпораций. – М.: «ПМСОФТ», 2008. – 175 с.

6. *Ротарь В.И.* О принципе стимуляции в арбитражной схеме//Экономика и математические методы. – 1984. – Т. XVII. В. 4. – С. 751-764.

Асратян Р.Э.

Разграничение прав доступа к сервисным функциям в Службе защищенных сообщений на основе электронной подписи

Аннотация: Рассмотрены принципы авторизации и разграничения прав доступа в сетевой Службе защищенных сообщений, предназначенной для безопасной обработки информационных запросов в распределенных информационных системах. Отличительная особенность службы заключается в использовании реквизитов подписантов информационного запроса для определения возможности доступа к обрабатывающим сервисным функциям.

Ключевые слова: распределенные системы, Интернет-технологии, информационное взаимодействие, информационная безопасность, разграничение прав доступа

Современные Интернет-технологии являются важнейшей составной частью распределенных информационных систем, в значительной степени, определяющей эффективность и безопасность сетевых обменов. Сегодня в распоряжении разработчиков таких систем имеется целый ряд сетевых информационных технологий высокой степени универсальности и гибкости [1-3]. Достаточно упомянуть Web-технологии [3], покрывающие широчайший спектр применений от электронной