УДК 519

МЕТОДЫ ОЦЕНКИ ЛОКАЛЬНЫХ И ИНТЕГРАЛЬНЫХ РИСКОВ СЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

А.А. Широкий
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: shiroky@ipu.ru

А.С. Рей
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: a.rey@ipu.ru

Ключевые слова: локальный риск, интегральный риск, оценка рисков, информационные системы, комплексное оценивание.

Аннотация: Актуальными направлениями развития фундаментальных исследований в области управления рисками сложных информационных систем является разработка методов идентификации и оценки рисков в условиях неопределенности, а также инструментов быстрой оценки интегрального риска сложных систем, учитывающих структуру последних. В настоящей работе описан вариант адаптации механизма комплексного оценивания для оценки информационных рисков, а также алгоритм быстрой оценки интегральных рисков информационной системы в условиях неопределенности.

1. Введение

Активное развитие информационных систем вызывает необходимость совершенствовать методы по управлению информационными рисками. В частности, существует потребность в разработке и внедрении инструментов, учитывающих неопределенность, вызванную как природой элементов информационной системы, так и ее операционным окружением. Стандарты семейств ISO 27005 и 31000 классифицируют методы оценки информационных рисков на качественные, количественные и комбинированные [1,2]. При этом назначение таких документов не предполагает регламентации применения конкретных способов и алгоритмов для оценки локальных и интегральных рисков информационных систем. Все, что может найти специалист в области информационной безопасности — это обобщенное описание процедуры оценивания отдельно взятых информационных активов с дальнейшим их ранжированием для приоритезации осуществления защитных мер.

Таким образом, при решении задачи оценки риска на практике специалисту по безопасности требуется решать следующие задачи.

i) подобрать адекватные методы и инструменты оценки отдельных аспектов (или элементов) рисков информационной системы (иными словами — локальных рисков), учитывающих эффекты, привносимые неопределенностью и структурой защищаемой системы;

ii) выбрать процедуру агрегирования, позволяющую получить достоверную оценку интегрального риска информационной системы.

Отметим, что, несмотря на многообразие способов, методов и инструментов оценки информационных рисков, учет неопределенности в них чаще всего предлагается вероятностного типа. Для этого необходимо знать функцию распределения риска, идентифицировать которую требуется на основе накопленных статистических данных о функционировании системы. В то же время информационные системы характеризуются высокой степенью изменчивости, что ставит под вопрос возможность использования таких данных, полученных в предшествующие периоды времени. Кроме того, остается открытым вопрос о минимизации рисков на этапе проектирования системы, когда исторических данных о ее функционировании просто нет.

Одним из возможных решений является применение качественных методов оценки рисков, например, мнения экспертов. В этом случае определенную сложность представляет выбор подходящей процедуры агрегирования, позволяющей компоновать как экспертные (т. е. качественные) оценки, так и количественные.

Далее предложен способ оценки интегрального риска информационных систем в условиях ограниченных данных на основе метода комплексного оценивания (МКО) [3]. Кроме того, предложен метод экспресс-оценки интегрального риска с учетом структуры информационной системы (подробно проблема учета структуры сложной системы при оценке ее интегрального риска обсуждается в [4]).

2. Способ комплексного оценивания интегрального риска информационной системы

Построим способ комплексного оценивания интегрального риска информационных систем на основе оценок локальных рисков: конфиденциальности (C), целостности (I), доступности (A). Каждый из них принимает в некоторой наперед заданной порядковой шкале одно из возможных значений $k_C \in K_C$, $k_I \in K_I$, $k_A \in K_A$ соответственно, причем k_C, k_I, $k_A \subset \mathbb{N}$. Тогда возможное состояние системы описывается вектором $k = (k_C, k_I, k_A)^T$, и задача построения комплексной оценки заключается в нахождении следующего отображения:

(1) $$w(\cdot): K_C \times K_I \times K_A \to K_S.$$

Здесь $K_S \subset \mathbb{N}$ — множество возможных значений (или, иначе, рангов) интегрального риска.

В случае, когда значения k_C, k_I, k_A уже известны, решение задачи (1) можно найти, например, в [5]. Авторы предлагаю для определения значений локальных рисков следующий алгоритм, включающий шесть шагов.

1) Составить следующие списки:

   U — список типичных для защищаемой системы уязвимостей.

   A_C — список известных уязвимостей, влияющих на конфиденциальность.

   A_I — список известных уязвимостей, влияющих на целостность.

   A_A — список известных уязвимостей, влияющих на доступность.

2) Построить бинарные матрицы соответствия уязвимостей атакам E_C, E_I, E_A, имеющие размерности $A_C \times U$, $A_I \times U$, $A_A \times U$ соответственно. Если атака $a \in A_C$ может быть

проведена с эксплуатацией уязвимости $u \in U$, то в соответствующей клетке матрицы должна стоять единица, в противном случае — ноль.

3) Проранжировать классы атак в каждом из множеств A_C, A_I, A_A в соответствии с числом возможных эксплуатируемых уязвимостей. Атаке (атакам), задействующим наибольшее число уязвимостей, присвоить ранг 1. Атаке (атакам), задействующим число уязвимостей меньшее, чем атаки ранга 1, но большее остальных атак, присвоить ранг 2. Продолжать ранжирование до тех пор, пока ранги не будут присвоены всем атакам без исключения.
4) Построить поддеревья комплексного оценивания для локальных рисков конфиденциальности, целостности и доступности, руководствуясь следующими правилами:

i) ближе к корням располагать критерии, соответствующие атакам с наибольшим рангом;

ii) сворачивать пары критериев с близкими или равными рангами.

Более подробно правила построения деревьев комплексного оценивания обсуждаются в работе [6].

5) Определить шкалу оценивания для каждого из критериев. Стандартом является шкала из трех значений, соответствующих низкому, среднему и высокому уровню риска [1].
6) Для каждого критерия, полученного на шаге 4, построить монотонные матрицы свертки критериев.

В заключение отметим, что вышеприведенный алгоритм позволяет корректно учитывать экспертные оценки, к которым зачастую приходится прибегать при определении значений показателей уязвимостей. Получаемые с его помощью оценки локальных рисков являются устойчивыми к изменениям отдельных сворачиваемых критериев (подробнее см., например, [7]).

3. Методика быстрой оценки рисков информационных систем с учетом их структуры

Рассмотрим информационную систему, состоящую из конечного множества элементов $S = \{s_1, \ldots, s_n\}$, $i \in N = \{1, \ldots, n\}$, $n \in \mathbb{N}$. Каждому элементу s_i сопоставлены *удельная вероятность* p_i его успешной атаки злоумышленником, а также величина u_i ущерба системе в этом случае. Будем считать, что нам неизвестны точные значения этих величин, но известен интервал, в котором они находятся. Иначе говоря, мы осведомлены о значениях величин p_{min} и p_{max}, $0 < p_{min}, p_{max} < 1$:

$$p_{min} \le p_i^0 \le p_{max} \ \forall i = 1, 2, \ldots, n, n \in \mathbb{N}.$$

Обозначим структуру информационной системы $W = \langle G(V, E), T \rangle$, $T \subseteq V$, где $G(V, E)$ — граф со множеством вершин V и множеством ребер E, а T — подмножество V, называемое периметром. В данной работе мы будем рассматривать структуры с типа «звезда с m лучами», периметр которых включает в себя ровно одну вершину, то есть

$$V = \left\{ \{v_0\} \cup \bigcup_{b=1}^{m} \bigcup_{l=1}^{l_b} \{v_{bl}\} \right\}, E = \left\{ \bigcup_{b=1}^{m} \left\{ (v_0, v_{b1}) \cup \bigcup_{l=2}^{l_b} (v_{b(l-1)}, v_{bl}) \right\} \right\}, T = \{v_0\}.$$

Тогда при $m = 1$ оценка интегрального риска ρ_1 данной информационной системы будет иметь следующий вид:

$$\rho_1^- = u\sum_{l=1}^{n}\left(p_{min}\right)^l \le \rho_1 \le u\sum_{l=1}^{n}\left(p_{max}\right)^l = \rho_1^+,$$

где u – некоторая оценка «среднего» ущерба в случае успешной атаки элемента злоумышленником. Заметим, что эти суммы будут конечны даже если множество элементов системы счетно при условии, что $p_{max} \le \frac{1}{2}$.

Теперь предположим, что структура системы представляет собой два луча с примерно одинаковыми длинами l_1 и l_2, то есть $|l_1 - l_2| \le 1$, $l_1 + l_2 + 1 = n$. Тогда величину интегрального риска ρ_2 такой информационной системы можно оценить снизу и сверху через p_{min} и p_{max} соответственно. Запишем вначале выражение для нижней оценки:

$$\rho_1^- = u\left(p_{min} + 2\sum_{l=2}^{\lfloor\frac{n}{2}\rfloor}\left(p_{min}\right)^l + \left(n - 1 - 2\left\lfloor\frac{n-1}{2}\right\rfloor\right)\left(p_{min}\right)^{\lfloor\frac{n}{2}\rfloor+1}\right).$$

Запись $\lfloor n \rfloor$ здесь и далее внутри текущего подпункта означает выделение целой части числа n. Величина $n - 1 - 2\left\lfloor\frac{n-1}{2}\right\rfloor$ будет равна нулю для нечетных n и 1 — для четных. При этом в первом случае мы получим два луча одинаковой длины, а во втором их длины будут отличаться на единицу. Для верхней оценки выражение будет таким же с точностью до замены p_{min} на p_{max}.

Теперь запишем выражение для нижней оценки интегрального риска системы со структурой, включающей в себя произвольное конечное число лучей m:

$$\rho_m^- = u\left(p_{min} + m\sum_{l=2}^{\lfloor\frac{n-1}{m}\rfloor+1}\left(p_{min}\right)^l + \left(\mathrm{n} - 1 - \mathrm{m}\left\lfloor\frac{\mathrm{n}-1}{\mathrm{m}}\right\rfloor\right)\left(\mathrm{p_{min}}\right)^{\lfloor\frac{\mathrm{n}-1}{\mathrm{m}}\rfloor+2}\right).$$

Нетрудно заметить (доказательство приведено в работе [4]), что величина $\rho_m^+ - \rho_m^-$ при $p_{min} < p_{max}$ также монотонно возрастает с ростом m. При $p_{min} = p_{max}$ достигается равенство верхней и нижней оценок.

4. Заключение

В настоящей работе описан вариант адаптации механизма комплексного оценивания для оценки информационных рисков, а также алгоритм экспресс-оценки интегрального риска информационной системы в условиях неопределенности. Предложенные алгоритмы могут найти применение при управлении рисками сложных систем в условиях неопределенных значений локальных рисков. Алгоритм экспресс-оценки интегрального риска, учитывающий структуру информационной системы, приведен в варианте для систем с топологией «звезда с m лучами». Предположительно, в будущих исследованиях удастся доказать, что получаемая с его помощью оценка остается справедливой и для систем произвольной топологии.

Список литературы

1. ISO/IEC 27005:2022(en) Information security, cybersecurity and privacy protection — Guidance on managing information security risks. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en. (дата обращения 9.10.2023).
2. ISO 31000:2018 Risk management — Guidelines. https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en (дата обращения 9.10.2023).
3. Баркалов С.А., Новиков Д.А., Новосельцев В.И., и др. Модели управления конфликтами и рисками: монография. Под ред. Д.А. Новикова. Воронеж: Научная книга, 2008. 495 с.
4. Shiroky A.A., Kalashnikov A. O. 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. e998. – URL: https://www.mdpi.com/2227-7390/11/4/998 (date accessed: 29.11.2023).
5. Калашников А.О. Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информационная безопасность. 2016. Т. 3, № 1. С. 315-322.
6. Власова Е.А., Карпов Ю. А., Тарасов Б. В. Построение дерева сверток для комплексной оценки на основе матрицы парных сравнений критериев // ВЕСТНИК Воронежского государственного технического университета. 2009. Т. 5, № 10. С. 187-191.
7. Алексеев А.О. Исследование устойчивости механизмов комплексного оценивания к стратегическому поведению агентов (на примере согласования политики организации в области риск-менеджмента) // Прикладная математика и вопросы управления. 2019. № 4. С. 136-154.