Семин Валерий Григорьевич
д-р техн. наук, профессор
ФГБОУ ВО «Российский государственный
социальный университет»
г. Москва

АЛГОРИТМЫ ФОРМИРОВАНИЯ ЭФФЕКТИВНЫХ МЕР ПРОТИВОДЕЙСТВИЯ РИСКАМ БЕЗОПАСНОСТИ

Аннотация: *в статье приведены алгоритмы решений задач оценки рисков с целью построения реестра рисков на этапе количественного анализа для формирования перечня наиболее эффективных контрмер противодействия угрозам безопасности.*

Ключевые слова: *интегральный риск, вероятность, угроза.*

Введение

Этап формирования перечня мер противодействия является заключительным шагом процесса управления рисками безопасности [2; 3; 7; 8; 12].

Задача оценки интегрального риска является ключевой в построении реестра рисков на этапе количественного анализа, на основе которого формируется алгоритм определения эффективных мер противодействия угрозам. безопасности [1; 4; 6; 9; 10]. При этом задача оптимального распределения мер противодействия по уязвимостям объекта безопасности является инвариантной по отношению к прикладной области [4; 5; 8; 11; 13].

Постановка задачи

В задаче управления рисками безопасности политику безопасности формулирует владелец ресурсов, в отношении которых должны быть разработаны меры противодействия возможным угрозам [7; 10].

Пусть дан: ресурс с номером i, для которого выделены опасные состояния S_{ij}, j = 1,…m, где m-число возможных состояний, а также вероятности инициирующих событий (угроз) x_k, k = 1,…h.

Требуется найти

Вероятности P_{ij} реализации опасных состояний i-го ресурса S_{ij}, j = 1,…m.

Значимости $Z(x_k)$ каждого инициирующего условия или события x_k с учетом его вклада в реализацию опасного состояния S_{ij}; k – номер инициирующего события или угрозы k = 1,…h.

Алгоритм решения

Шаг 1. Составление сценария опасного состояния S_{ij}.

Шаг 2. Построение функции алгебры логики (ФАЛ) с использованием операций конъюнкция и дизъюнкция на основе сценария опасного состояния S_{ij}.

Шаг 3. Построение вероятностной функции (ВФ) P_{ij} на основе функции алгебры логики.

Шаг 4. Расчет вероятности P_{ij} реализации опасного состояния с помощью вероятностной функции.

Шаг 5. Расчет значимости $Z(x_k)$ каждой угрозы с учетом ее вклада в реализацию опасного состояния. Значимость элемента (угрозы) определяется на вероятностной модели как частная производная ВФ. Результатом данного этапа является рейтинг угроз по степени влияния на реализацию опасного состояния. Для оценки вероятностей отказов ресурсов используются статистически достоверные, либо экспертные данные. Для подсчета ущерба используются известные подходы, такие как прямой счет и оценка пороговых значений риска [1; 4; 5; 7; 8].

Алгоритмы формирования перечня наиболее эффективных контрмер

Для дальнейшего исследования выделяются только те опасные состояния, для которых уровень риска $P_{ij} \geq P_0$, где P_0 – пороговое значение для уровня риска. Пороговое значение отражает критическую величину потерь от реализации опасного состояния. Пронумеруем угрозы, отобранные для дальнейшего рассмотрения опасных состояний, заново. Для этого введем новый индекс, учитывающий каждую из угроз для каждого опасного состояния каждого ресурса системы. При введении нового индекса учитывается тот факт, что одна и та же угроза может встречаться в нескольких опасных состояниях. В этом случае под значимостью

угрозы понимается сумма значимостей этой угрозы в различных опасных состояниях. Конечная цель – уменьшение уровня риска системы посредством реализации набора контрмер [2; 3; 8; 11; 12]. При этом полагаем, что для контрмеры известна стоимость ее реализации s_t, также задана величина s_0 – бюджет, выделенный на превентивные мероприятия.

Рассмотрим процедуру формирование перечня наиболее эффективных контрмер. Представим информацию о том, влияет или не влияет данная контрмера на угрозу, в виде матрицы:

$$a_{tv} = \begin{pmatrix} a_{11} & \dots & a_{1V} \\ \dots & \dots & \dots \\ a_{t1} & \dots & a_{TV} \end{pmatrix},$$

где $a_{tv} \in \{0,1\}$, $a_{tv} = 1$, если контрмера g_t влияет на угрозу x_v, и $a_{tv} = 0$, если контрмера g_t не влияет на угрозу x_v. Термин «влияет» означает «уменьшает вероятность реализации угрозы» или «устраняет угрозу».

Тогда задачу формирования перечня наиболее эффективных контрмер можно представить как задачу нахождения бинарного вектора (b_1, b_2, …, b_T), такого что:

$$\sum_{t=1}^{T}\left(\sum_{v=1}^{V} z_v a_{tv}\right) b_t \to \max$$

при ограничениях

$$\sum_{t=1}^{T} s_t b_t \le s_0, \quad a_{tv} \in \{0,1\}, \quad b_t \in \{0,1\}, \quad t = \overline{1,T}, \quad v = \overline{1,V}.$$

Алгоритм решения

Для решения задачи используется направленный перебор на множестве бинарных векторов длины T. Далее для простоты приведен алгоритм полного перебора. Задаем величину $max = 0$, текущий вектор $b = (0, 0, \dots, 0, 1)$, результирующий вектор $r=(0, 0, \dots, 0, 1)$. В цикле от 1 до 2^T выполняем шаги:

Шаг 1. Проверяем бюджетное ограничение для текущего вектора b.

Шаг 2. Если ограничение выполнено, то вычисляем величину

$$C = \sum_{t=1}^{T}\left(\sum_{v=1}^{V} z_v a_{tv}\right) b_t ,$$

иначе – переход к следующей итерации.

Шаг 3. Если $C > max$, то $max = C$, $r = b$.

Шаг 4. Формируем очередной вектор b.

Результатом работы алгоритма будет вектор r, на котором величина достигает максимума.

$$C = \sum_{t=1}^{T}\left(\sum_{v=1}^{V} z_v a_{tv}\right) b_t .$$

Вариант 2. Формирование перечня наиболее эффективных контрмер

Представим информацию о том, как влияет данная контрмера на угрозу в виде матрицы:

$$\Delta p_v^t = \begin{pmatrix} \Delta p_1^1 & \dots & \Delta p_V^1 \\ \dots & \dots & \dots \\ \Delta p_1^T & \dots & \Delta p_V^T \end{pmatrix},$$

где Δp_v^t - изменение вероятности реализации угрозы с номером v при попадании контрмеры с номером t в перечень контрмер для реализации или 0, если контрмера с номером t не оказывает влияния на угрозу с номером v. Тогда задачу формирования перечня наиболее эффективных контрмер можно представить как задачу нахождения бинарного вектора $(b_1, b_2, \dots, b_T)^T$, которому соответствует максимальное изменение интегрального риска системы $\Delta R \to \max$, такого что:

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} \Delta P_{ij} * C_{ij}\right) \to \max$$

при ограничениях

$$\sum_{t=1}^{T} s_t b_t \le s_0 , \quad b_t \in \{0,1\}, \quad t = \overline{1,T}, \quad v = \overline{1,V}$$

Заключение

Таким образом, полученные результаты представляют собой последовательное описание механизма формирования эффективных средств противодействия на основе общего логико-вероятностного метода моделирования структуры угроз в задаче управления рисками.

Список литературы

1. Семин В.Г. Оптимизация процесса управления рисками информационной и функциональной безопасности многофункциональных информационных систем при электромагнитных воздействия / В.Г. Семин, В.А. Михеев // Технологии электромагнитной совместимости. – 2013. – №4 (47). – С. 60–64.

2. Семин В.Г. Управление рисками автоматизированных систем на основе принципа гарантированного результата / В.Г. Семин, В.А. Михеев // Качество. Инновации. Образование. – 2015. – №1 (116). – С. 58–63.

3. Семин В.Г. Обобщенный алгоритм управления рисками автоматизированных систем / В.Г. Семин // Динамика сложных систем – XXI ВЕК. – 2012. – Т. 6. – №4. – С. 96–100.

4. Семин В.Г. Разработка концептуальной структуры системы управления рисками информационной и функциональной безопасности многофункциональных информационных систем при электромагнитных воздействиях / В.Г. Семин, В.А. Михеев // Технологии электромагнитной совместимости. – 2013. – №2 (45). – С. 70–73.

5. Семин В.Г. Разработка информационной модели управления рисками качества / В.Г. Домрачева, С.У. Увайсова // Инновации в условиях развития информационно-коммуникационных технологий: Материалы научно-практической конференции. под редакцией. – 2006. – С. 93–97.

6. Семин В.Г. Алгоритмизация процесса синтеза многопараметрических систем контроля // Измерительная техника. – 1995. – №2. – С. 19–20.

7. Семин В.Г. Разработка концепции политики безопасности инфокоммуникаций МИС ИС в условиях электромагнитных атак // Технологии электромагнитной совместимости. – 2014. – №4 (51). – С. 58–61.

8. Семин В.Г. Разработка формальной структуры системы управления рисками информационной и функциональной безопасности многофункциональных информационных систем при электромагнитных воздействиях // Технологии электромагнитной совместимости. – 2013. – №4 (47). – С. 65–68.

9. Semin V.G., Khakimullin E.R. The principle of the guaranteed result in the problem of factoring risk management» in15th International Scientific Conference on Economic and Social Development, 9–10 June 2016, Varazdin, Croatia, pp. 369–374.

10. Семин В. Г. Принципы и методы реализации политики безопасности системы обеспечения электромагнитной безопасности многофункциональных информационных сетей // Технологии электромагнитной совместимости. – 2014. – №4 (51). – С. 62–66.

11. Семин В.Г. Управление рисками факторинговой компании / В.Г. Семин, Е.В. Семина: редколлегия: В. Г. Домрачеев (ответственный редактор) // Инновации в условиях развития информационно-коммуникационных технологий: Материалы научно-практической конференции, 1–10 октября 2009 г., Россия, г. Сочи; Международная академия информатизации. – М., 2009. – С. 73–74.

12. Valeriy G. Semin, Alexei B. Los. The information security risk management. 2017 International Conference «Quality Management, Transport and Information Security, Information Technologies» (IT&QM&IS) Year: 2017. – P. 106–109 IEEE Conference Publications.

13. Valeriy Semin. Algorithmization of the context of management of risks of factoring. SGEM 2017 SOCIAL SCIENCE & ARTS. YEAR: 2017. – P. 331–339.