Математические структуры и моделирование
2023. № 3 (67). С. 104–110

УДК 004.056
DOI 10.24147/2222-8772.2023.3.104-110

ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ К ЗАДАЧЕ ОЦЕНКИ АКТУАЛЬНОСТИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.Ф. Богаченко[1]
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru
Д.Н. Лавров[1, 2]
к.т.н., доцент, e-mail: dmitry.lavrov72@gamil.com

[1]Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

[2]Нижневартовский государственный университет, Нижневартовск, Россия

Аннотация. Для оценки актуальности угроз информационной безопасности предлагается использовать подход, основанный на методе анализа иерархий. Особенностью подхода является автоматическое вычисление весов уровня альтернатив (соответствующих угрозам) за счёт использования оценок близости текстовых описаний объектов защиты, связанных с угрозами, и уязвимостей, а также на основе оценок уровней опасности уязвимостей и значимости объектов защиты.

Ключевые слова: угрозы, уязвимости, анализ текстов, метод анализа иерархий.

1. Введение

Для построения модели угроз информационной безопасности предприятия в соответствии с методическими рекомендациями Федеральной службы по техническому и экспортному контролю (ФСТЭК) [1] необходимо оценить актуальность угроз. Сделать это можно, связав существующие уязвимости, размещённые в различных базах данных, с угрозами [2]. Обычно для этого используется экспертный подход: специалисты различных ИТ-отделов и подразделений входят в экспертную группу по определению актуальности тех или иных угроз. В группу рекомендуется включать: специалиста по ИТ-трансформации, опытного технического специалиста из отдела информационной безопасности, ответственного за поддержку основных автоматизированных бизнес-процессов, специалиста по АСУ и АСУТП предприятия, ответственного за эксплуатацию сетей связи. К сожалению, экспертный подход достаточно трудоёмкий и обладает долей субъективизма.

Одной из сложных задач в работе экспертной группы является процедура сопоставления уязвимостей и угроз. В существующих базах данных угроз и уязвимостей нет прямых связей между конкретными представителями этих понятий.

Ранее была предложена методика сопоставления угроз и уязвимостей, основанная на экспертных количественных оценках угроз [3].

Позднее в работах [4–7] был предложен подход на основе интеллектуального анализа текстов с использованием технологий word2vec, doc2vec, fasttext, lsa и других алгоритмов. Основная суть сводится к векторизации текстовых описаний угроз и уязвимостей с последующим построением матриц парных сравнений расстояний между описаниями угроз и уязвимостей (1).

$$\begin{array}{c|ccc} & V_1 & \dots & V_m \\ \hline T_1 & r_{1,1} & \dots & r_{1,m} \\ \vdots & \vdots & \ddots & \vdots \\ T_n & r_{n,1} & \dots & r_{n,m} \end{array} \tag{1}$$

Здесь T_i – i-я угроза; V_j – j-я уязвимость; $r_{i,j}$ – мера близости между текстовыми описаниями ($r_{i,j} \in [0, 1]$; 0 – текстовые описания не схожи, 1 – тексты совпадают).

Далее автоматизированное связывание угроз и уязвимостей, тактик и техник реализации угроз по их текстовым описаниям уточняется экспертами.

В работе [7] показана эффективность разработанного на таком подходе средства автоматизации. Скорость сопоставления по сравнению с работой экспертной группы в «ручном» режиме увеличилась более чем в 4 раза, но, к сожалению, согласованность экспертной и автоматизированной оценок составила всего лишь 59 %. Учитывая сложность задачи, результат достаточно приемлемый.

Представляется возможным повысить качество сопоставления за счёт добавления в модель подробных текстовых описаний объектов защиты конкретного предприятия и их компонентов. При таком расширении общих терминов, имён и понятий в описаниях объектов защиты и уязвимостей будет больше, что позволит более точно оценить меру близости указанных текстовых описаний. Каждый объект защиты, в свою очередь, в соответствии с методическими рекомендациями ФСТЭК связан с угрозами, что и позволит оценить актуальность угроз по связанным с ними уязвимостям (построить оценку матрицы (1)).

В данной работе обсуждается возможность дальнейшего использования матрицы (1) для автоматизации процесса оценки актуальности угроз.

2. Выбор критериев в методе анализа иерархий

Согласно методике [1] «при оценке угроз безопасности информации могут использоваться программные средства, позволяющие автоматизировать данную деятельность». Основой такой разработки может послужить количественная оценка актуальности угроз.

Используем хорошо известный из теории поддержки принятия решений метод анализа иерархий (МАИ) [8]. В качестве выбираемых альтернатив МАИ будут выступать угрозы: $T_1, \dots, T_n$. Ожидаемый результат – ранжирование угроз по уровню актуальности. В этом случае вершина иерархии (цель или решение) – выбор наиболее актуальной угрозы.

Особенностью МАИ является то, что получаемые веса альтернатив (в нашем случае угроз) неотрицательны и в сумме дают единицу. Это позволяет с некоторой

степенью вольности ассоциировать их с вероятностями реализаций угроз для конкретных объектов защиты. Подбор критериев МАИ может усилить эту ассоциацию.

Перейдём к выбору критериев. Выдвинем ряд следующих эвристических предположений:

1. Чем больше уязвимостей реализует угрозу, тем выше вероятность её реализации.
2. Чем выше уровень опасности уязвимости (количественная оценка уязвимости, вычисленная по стандарту Common Vulnerability Scoring System (CVSS) [2]), реализующей угрозу, тем выше вероятность её реализации. Исходим из того, что стратегия злоумышленника нанести максимальный урон объекту защиты, а следовательно, вероятность использования более опасной уязвимости выше.
3. Чем выше уровень значимости объекта воздействия, на который направлена угроза, тем выше актуальность его защиты. Значимость может быть оценена на основе методики ФСТЭК для объектов критической информационной инфраструктуры [9] с применением МАИ [10].

Согласно этим предположениям, можно предложить три критерия для построения иерархии МАИ для оценки актуальности угроз:

1. K_A – число уязвимостей, реализующих угрозу.
2. K_B – максимальный уровень опасности уязвимостей, реализующих угрозу.
3. K_C – уровень значимости объекта воздействия, на который направлена угроза.

Пусть $w_{A,1}, \ldots, w_{A,n}, w_{B,1}, \ldots, w_{B,n}, w_{C,1}, \ldots, w_{C,n}$ – относительные весовые коэффициенты уровня альтернатив для критериев K_A, K_B, K_C соответственно. Относительные весовые коэффициенты уровня критериев обозначим w_A, w_B, w_C (см. рис. 1).

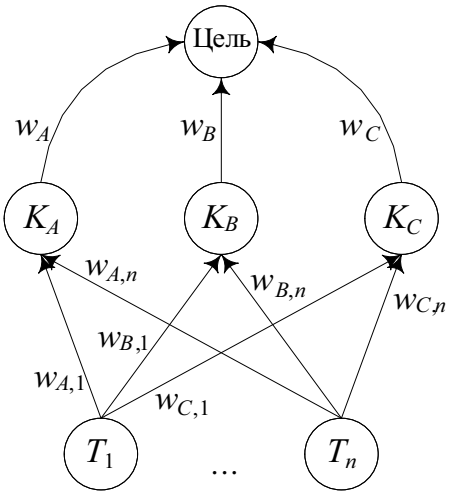

Рис. 1. Иерархия задачи оценки актуальности угроз

Тогда, согласно МАИ, актуальность угрозы T_i равна i-му комбинированному ве-

совому коэффициенту:

$$P(T_i) = w_A \cdot w_{A,i} + w_B \cdot w_{B,i} + w_C \cdot w_{C,i}. \tag{2}$$

Далее определим формулы для вычисления величин, участвующих в равенстве (2).

3. Относительные весовые коэффициенты уровня альтернатив

Пусть $\varepsilon \in [0, 1]$ – некоторое пороговое значение, определяющее значимую близость текстовых описаний угрозы T_i и уязвимости V_j: если $r_{i,j} > \varepsilon$, то будем считать, что уязвимость V_j реализует угрозу T_i. Преобразуем матрицу (1) в бинарную матрицу (3)

$$\begin{pmatrix} \tilde{r}_{1,1} & \dots & \tilde{r}_{1,m} \\ \vdots & \ddots & \vdots \\ \tilde{r}_{n,1} & \dots & \tilde{r}_{n,m} \end{pmatrix} \tag{3}$$

по следующему правилу:

$$\tilde{r}_{i,j} = \begin{cases} 1, & \text{если } r_{i,j} > \varepsilon; \\ 0, & \text{если } r_{i,j} \leqslant \varepsilon. \end{cases}$$

Далее предлагается относительные весовые коэффициенты уровня альтернатив вычислять по формулам (4), (6), (8).

$$w_{A,i} = \frac{N_i}{N_1 + \ldots + N_n}, \tag{4}$$

$$N_i = \sum_{j=1}^{m} \tilde{r}_{i,j}. \tag{5}$$

Очевидно, что N_i – это число единичных элементов в i-й строке матрицы (3), т. е. число уязвимостей, реализующих угрозу T_i.

$$w_{B,i} = \frac{M_i}{M_1 + \ldots + M_n}, \tag{6}$$

$$M_i = \max\{c_1 \cdot \tilde{r}_{i,1}, \ldots, c_m \cdot \tilde{r}_{i,m}\}, \tag{7}$$

где c_j ($j \in [1, m]$) – уровень опасности уязвимости V_j, который указан в базах данных уязвимостей, например [2].

$$w_{C,i} = \frac{O_i}{O_1 + \ldots + O_n}, \tag{8}$$

где O_i – уровень значимости объекта защиты, на который направлена угроза T_i.

Замечание 1. В предложенной иерархии МАИ удалось подобрать такие критерии, что относительные весовые коэффициенты уровня альтернатив вычисляются без заполнения матриц парных сравнений, т. е. без привлечения механизма экспертных оценок. Такой подход, во-первых, существенно снижает время работы алгоритма, а во-вторых, избавляет МАИ от постоянного источника критики – несогласованности матриц парных сравнений вследствие субъективизма суждений экспертов.

Замечание 2. В формулах (5) и (7) бинарные значения $\tilde{r}_{i,j}$ можно заменить на произведения $\tilde{r}_{i,j} \cdot r_{i,j}$. В этом случае в формуле (5) каждая уязвимость, реализующая угрозу, будет вносить не единичный вклад, а некоторую долю, определяемую мерой близости $r_{i,j}$ между текстовыми описаниями угрозы T_i и уязвимости V_j. В свою очередь, в формуле (7) при нахождении максимума будут рассматриваться «взвешенные» значения уровней опасности, где под весом понимается всё та же мера близости $r_{i,j}$.

4. Построение матрицы парных сравнений критериев

Сравнивая попарно критерии K_A, K_B, K_C по степени влияния на актуальность угроз, заключаем, что:

- K_B умеренно превосходит K_A. Действительно, количество уязвимостей менее важно, чем максимальная степень опасности одной из них.
- K_C существенно превосходит K_A: значимость объекта защиты намного важнее числа уязвимостей.
- K_C незначительно превосходит K_B: значимость объекта защиты всё же важнее максимальной степени опасности уязвимости.

Таким образом, используя шкалу относительной важности [8], получаем хорошо согласованную матрицу парных сравнений уровня критериев (Индекс согласованности равен 0,001847; относительная согласованность — 0,003185)

$$\begin{pmatrix} 1 & 1/3 & 1/5 \\ 3 & 1 & 1/2 \\ 5 & 2 & 1 \end{pmatrix} \tag{9}$$

Матрица может быть модифицирована другой группой экспертов в случае других подходов к оценкам значимости объектов защиты и актуальности угроз.

5. Заключение

Одним из недостатков метода анализа иерархий является то, что при его применении экспертам приходится заполнять большое количество матриц парных сравнений. Для снижения трудоёмкости этих рутинных процедур необходимо использовать уже полученные оценки из других процессов. Так, значимость объектов защиты предлагаем брать из процедуры категорирования объектов критической информационной инфраструктуры (если таковые имеются на предприятии) или отдельного процесса определения значимости объекта защиты. Оценку уровня опасности

уязвимости будем брать из открытых и доступных баз данных уязвимостей (например ФСТЭК [2]), а привязку уязвимостей к угрозам автоматизируем посредством интеллектуального анализа текстовых описаний уязвимостей и объектов защиты (последние напрямую связаны с угрозами) с помощью хорошо известных алгоритмов word2vec, doc2vec, fasttext, lsa. Предварительную оценку важности выбранных критериев оценивания сделаем по построенной в предыдущем пункте матрице парных сравнений. Таким образом, матрицы парных сравнений всех уровней иерархии МАИ будут заполнены, и эксперту останется лишь удостовериться в корректности такого заполнения и при необходимости внести изменения. Также можно отказаться от заполнения матриц парных сравнений уровня альтернатив, так как основная цель в МАИ – получить веса дуг (см. рис. 1), а они уже посчитаны по формулам (4), (6), (8). На выходе алгоритма МАИ получим уровни актуальности угроз, по которым легко определить, какие первоочередные меры должны быть приняты по защите информации на предприятии.

Литература

1. Методика оценки угроз безопасности информации. М., 2021. 83 с. URL: `https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf` (дата обращения: 11.08.2023).
2. Банк данных угроз безопасности информации. URL: `https://bdu.fstec.ru` (дата обращения: 11.08.2023).
3. Селифанов В.В., Юракова Я.В., Карманов И.Н. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах // Интерэкспо Гео-Сибирь. 2018. № 7. С. 271–276.
4. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии text mining // Вопросы кибербезопасности. 2020. № 4 (38). С. 22–31.
5. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134.
6. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров // Вопросы кибербезопасности. 2022. № 2 (48). С. 27–38.
7. Кучкарова Н.В. Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов: дис. ... канд. техн. наук. Уфа, 2023. 183 с.
8. Saaty T.L. The Analytic Hierarchy Process. New York : McGraw Hill, 1980.
9. Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации. Методический документ (Проект). URL: `https://fstec.ru/dokumenty/vse-dokumenty/proekty/proekt-metodicheskogo-dokumenta-2` (дата обращения: 17.08.2023).
10. Бочков А.В. Использование метода анализа иерархий для целей категорирования критически важных объектов по степени совокупного ущерба и риску противоправных действий // Проблемы анализа риска. 2008. Т. 5, № 4. С. 6–13.

APPLICATION OF THE ANALYTIC HIERARCHY PROCESS TO THE PROBLEM OF ASSESSING THE RELEVANCE OF INFORMATION SECURITY THREATS

N.F. Bogachenko[1]
Ph.D. (Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru
D.N. Lavrov[1, 2]
Ph.D. (Techn.), Associate Professor, e-mail: dmitry.lavrov72@gamil.com

[1]Dostoevsky Omsk State University, Omsk, Russia
[2]Nizhnevartovsk State University, Nizhnevartovsk, Russia

Abstract. To assess the relevance of information security threats, it is proposed to use an approach based on the analytic hierarchy process. A feature of the approach is the automatic calculation of the weights of the level of alternatives (corresponding to threats), by using estimates of the proximity of text descriptions of protected objects associated with threats and vulnerabilities, as well as based on estimates of the severity levels of vulnerabilities and the importance of protected objects.

Keywords: threats, vulnerabilities, text analysis, AHP.

Дата поступления в редакцию: 17.08.2023