Инженерный вестник Дона, №8 (2024)
ivdon.ru/ru/magazine/archive/n8y2024/9428

Алгоритм ранжирования угроз информационной безопасности на основе метода анализа иерархий

Д.А. Рыленков

Московский финансово-юридический университет

Аннотация: Одними из наиболее актуальных задач при обеспечении защиты данных в информационных системах являются классификация и ранжирование источников угроз. Все источники угроз имеют различную степень опасности для активов информационной системы. Ранжирование позволяет расставить приоритеты при проектировании системы информационной безопасности и выделить большие ресурсы на предотвращение наиболее актуальных и значимых угроз. В данной статье рассматривается алгоритм ранжирования угроз информационной безопасности, проведено пилотажное исследование на основе метода анализа иерархий.
Ключевые слова: защита данных, информационные технологии, метод анализа иерархий, системный анализ, информационные системы, информационная безопасность.

Классификация и ранжирование источников угроз является достаточно важным этапом при анализе уровня защищённости информационной системы и проектировании системы информационной безопасности. Данная исследовательская задача является многокритериальной, и одним из методов, предназначенных для решения проблем такого класса, является Метод анализа иерархий [1-3].

Выделены следующие шаги для метода анализа иерархий:

1) Формулировка цели.
2) Определение набора критериев и альтернатив.
3) Создание иерархии.
4) Построение матрицы парных сравнений.
5) Анализ матриц, полученных на прошлом этапе.
6) Расчет весов каждой из исследуемых альтернатив.

Рассматриваемая задача – выделить наиболее значимые угрозы для защищаемой информационной системы.

В качестве альтернатив рассматривается набор угроз сетевой инфраструктуры предприятия. Наименования угроз выделены из банка данных угроз безопасности ФСТЭК России.

Перечень альтернатив:

1) Угроза использования слабостей протоколов сетевого/локального обмена данными (УБИ. 034);
2) Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб (УБИ. 098);
3) Угроза приведения системы в состояние «отказ в обслуживании» (УБИ. 140).

Для каждой из перечисленных альтернатив выделены ключевые критерии значимости с целью выполнения исследования на основе метода анализа иерархий:

1) Реализация угрозы требует физического доступа к системе для атакующего;
2) Угроза влияет на конфиденциальность данных в системе;
3) Реализация данной угрозы не требует аутентификации в системе.

В качестве баллов оценок используются значения в диапазоне от 1 до 9 [4-6]. В таблице 1 указан смысл каждого из значений.

Таблица № 1

Шкала оценок

Значение оценки	Пояснение
1	2
1	Одинаковая значимость двух сравниваемых элементов.
3	Незначительное превосходство первого сравниваемого элемента над вторым
5	Достаточно сильное превосходство первого элемента над вторым

1	2
7	Значительное превосходство первого элемента
9	Явное значительное превосходство 1 элемента. Речь идет о максимально возможном различии между двумя рассматриваемыми элементами
2, 4, 6, 8	Промежуточные значения оценок

С данной шкалой оценок было проведено пилотажное исследование, для выполнения анализа сформирована группа из 3 экспертов, специалистов в области информационных технологий.

Каждый из экспертов заполнил таблицу парного сравнения значимости критериев и таблицы значимости по каждой из альтернатив.

Далее перечислены сведения о каждом из экспертов сформированной группы.

Сведения о 1-м эксперте:

- Направление работ - системы защиты информации;
- Научная подготовка - кандидат наук;
- Стаж работы по приоритетному направлению – 24 года;

Сведения о 2-м эксперте:

- Направление работ - системы защиты информации;
- Научная подготовка - кандидат наук;
- Стаж работы по приоритетному направлению – 20 лет;

Сведения о 3-м эксперте:

- Направление работ - телекоммуникационные технологии;
- Научная подготовка - кандидат наук;
- Стаж работы по приоритетному направлению – 21 год;

Итоговые значения вектора глобальных приоритетов получены путем усреднения оценок экспертов.

Далее показаны этапы расчета оценок, выполненные первым экспертом. Выполнено парное сравнение каждого из критериев методом парных оценок.

Сравнение критериев и полученный вектор локальных приоритетов указаны в таблице 2.

Таблица № 2

Парное сравнение критериев

	1	2	3	Ср. геометрическое	Нормализованная оценка критерия
1	1	0,1	0,2	0,27	0,06
2	10	1	1	2,15	0,52
3	5	1	1	1,7	0,41
Итого	16	2,1	2,2		

Для оценки качества полученных данных произведен расчет индекса согласованности (ИС) и отношения согласованности (ОС).

$$\text{ИС} = \frac{|\lambda_{max} - n|}{n - 1}$$

В данном выражении n является размерностью матрицы, а λ_{max} рассчитывается следующим образом:

$$\lambda_{max} = (16*0,06)+(2,1*0,52)+(2,2*0,41) = 2,95$$

Индекс согласованности равен:

$$\text{ИС} = \frac{|2,95 - 3|}{3 - 1} = 0,025$$

Далее необходимо определить величину значения случайной согласованности. Она зависит только от размерности анализируемой матрицы (Таблица 3) [7].

Таблица № 3

Значения случайной согласованности

Размерность матрицы	1	2	3	4	5	6	7	8	9	10
Случайная согласованность	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Из таблицы 3 получаем, для матрицы размерности 3 значение случайной согласованности равно 0,58.

Отношение согласованности равно:

$$\text{ОС} = \frac{\text{ИС}}{\text{СС}} = \frac{0{,}025}{0{,}58} = 0{,}04$$

Уровень ОС не должен быть выше 0,1. В иных случаях, значения выше могут говорить о рассогласованности оценок в матрице [8-10]. В данном случае, значение ОС равное 0,04 означает, что оценки эксперта согласованы.

Аналогично по каждому из перечисленных критериев произведено сравнение рассматриваемых альтернатив.

В таблице 4 показано сравнение угроз по критерию требования физического доступа к защищаемой системе.

Таблица № 4

Сравнение альтернатив по первому критерию

	1	2	3	Ср. геометрическое	Нормализованная оценка критерия
1	1	1	2	1,25	0,36
2	1	1	5	1,7	0,49
3	0,5	0,2	1	0,46	0,13
Итого	2,5	2,2	8		

Для полученной таблицы рассчитана оценка согласованности:

$$\lambda_{max}= (2,5*0,36)+(2,2*0,49)+(8*0,13) = 3,02$$

$$\text{ИС} = \frac{|3,02 - 3|}{3 - 1} = 0,01$$

$$\text{ОС} = \frac{\text{ИС}}{\text{СС}} = \frac{0,01}{0,58} = 0,02 < 0,1$$

В таблице 5 показано сравнение рассматриваемых угроз по критерию влияния на конфиденциальность в системе.

Таблица № 5

Сравнение альтернатив по второму критерию

	1	2	3	Ср. геометрическое	Нормализованная оценка критерия
1	1	2	1	1,25	0,41
2	0,5	1	1	0,79	0,25
3	1	1	1	1	0,32
Итого	2,5	4	3		

Для полученной таблицы рассчитана оценка согласованности:

$$\lambda_{max}= (2,5*0,41)+(4*0,25)+(3*0,32) = 2,99$$

$$\text{ИС} = \frac{|2,99 - 3|}{3 - 1} = 0,005$$

$$\text{ОС} = \frac{\text{ИС}}{\text{СС}} = \frac{0,005}{0,58} = 0,01 < 0,1$$

На следующем шаге выполнено сравнение угроз по критерию требования аутентификации в защищаемой информационной системе (Таблица 6).

Таблица № 6

Сравнение альтернатив по третьему критерию

	1	2	3	Ср. геометрическое	Нормализованная оценка критерия
1	1	9	9	4,32	0,81
2	0,1	1	1	0,48	0,09
3	0,1	1	1	0,48	0,09
Итого	1,2	11	11		

Для полученной таблицы рассчитана оценка согласованности:

$$\lambda_{max}= (1,2*0,81)+(11*0,09)+(11*0,09) = 2,95$$

$$\text{ИС} = \frac{|2,95 - 3|}{3 - 1} = 0,025 \qquad \text{ОС} = \frac{\text{ИС}}{\text{СС}} = \frac{0,025}{0,58} = 0,04 < 0,1$$

Аналогично расчет матриц оценок был выполнен для второго и третьего экспертов.

Для каждого из наборов экспертных оценок составлен вектор глобальных приоритетов (Таблица 7).

Итоговый вектор глобальных приоритетов альтернатив получен путем усреднения значений.

Таблица № 7

Значения векторов глобальных приоритетов

№ Альтернативы	Оценка 1 эксперта	Оценка 2 эксперта	Оценка 3 эксперта	Среднее значение
1	0,57	0,48	0,44	0,46
2	0,21	0,29	0,26	0,25
3	0,22	0,23	0,28	0,24

На основании проведенного анализа угроз по каждому из рассматриваемых критериев и парного сравнения критериев получен вектор глобальных приоритетов для угроз информационной безопасности системы (Таблица 8).

Таблица № 8

Итоговое значение глобального приоритета

Наименование угрозы	Глобальный приоритет
Угроза использования слабостей протоколов сетевого/локального обмена данными	0,46
Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	0,25
Угроза приведения системы в состояние «отказ в обслуживании»	0,24

Таким образом, проведенное пилотажное исследование показало, что наибольшее значение глобального приоритета имеет угроза использования слабостей протоколов сетевого/локального обмена данными. На ее предотвращение следует выделять большее число ресурсов. Рассматриваемый метод применим для информационных систем различного масштаба, и позволяет указывать большее число специфических критериев.

Литература

1. Мироненко А. Н. Обработка данных методом анализа иерархий // Математическое и компьютерное моделирование: сборник материалов IV Международной научной конференции, Омск, 11 ноября 2016 года / отв. за

вып. И. П. Бесценный. Омск: Омский государственный университет им. Ф.М. Достоевского, 2016. С. 107-109.

2. Глущенко И. С., Баранова Е. М., Баранов А. Н., Борзенкова С. Ю. Современные информационные системы анализа и управления рисками в сфере информационной безопасности // Известия Тульского государственного университета. Технические науки. 2021. № 2. С. 311-316.

3. Галлямова Е. Р., Сайфуллина Л. Д. Применение метода анализа иерархий в социально-экономических системах // Инновации в науке и практике: сборник статей по материалам XIII международной научно-практической конференции, Барнаул, 26 декабря 2018 года. Том Часть 2(5), 2018. С. 86-92.

4. Рыленков Д. А. Анализ средств мониторинга системы информационной безопасности предприятия // Эффективное управление и программное обеспечение для образовательных, финансовых, транспортных, логистических и маркетинговых систем: Сборник научных статей аспирантов. Москва: Московский финансово-юридический университет МФЮА, 2023. С. 40-42.

5. Никитина, Я. С., Кужелева С. А., Соколова Ю. В. Программные средства реализации метода анализа иерархий при принятии управленческих решений // Информационные системы и технологии: сборник материалов V всероссийской очной научно-технической конференции «ИСТ-2019», Курск, 20 мая 2019 года. Юго-Западный государственный университет. Курск: Юго-Западный государственный университет, 2019. С. 138-142.

6. Футерман М. Ю., Лаган Е. А., Амплиев А. Е. Практики по управлению инцидентами ИБ // Новая наука: Теоретический и практический взгляд. 2016. № 3-1(69). С. 41-44.

7. Кравченко Т. К., Середенко Н. Н., Щербинин О. П., Коряковцева Н. А. Адаптация метода анализа иерархий к экспертной системе поддержки

принятия решений (ЭСППР) // Актуальные вопросы современной науки. – 2010. № 11. С. 217-222.

8. Бильтаев И. С. Разработка центра управления безопасностью для информационно-аналитической системы предприятия // Студенческие научные исследования: сборник статей XV Международной научно-практической конференции, Пенза, 20 декабря 2022 года. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 35-41.

9. Saaty T.L. Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process // RACSAM - Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas. 2008. V. 102 (2). P. 251–318.

10. Kafi M. A., Akter N. Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection //American Journal of Trade and Policy. 2023. Vol. 10. No. 1. pp. 15-26.

References

1. Mironenko, A. N. Matematicheskoye i komp'yuternoye modelirovaniye: sbornik materialov IV Mezhdunarodnoy nauchnoy konferentsii, Omskiy gosudarstvennyj universitet im. F.M. Dostoyevskogo, 2016. pp. 107-109.

2. Glushchenko I. S, Baranova E. M., Baranov A. N., Borzenkova S. Y. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskiye nauki. 2021. № 2. pp. 311-316.

3. Gallyamova Y. R. Innovatsii v nauke i praktike: sbornik statey po materialam XIII mezhdunarodnoy nauchno-prakticheskoy konferentsii, Barnaul,

26 dekabrya 2018 goda. 2(5). Barnaul. Obshchestvo s ogranichennoy otvetstvennost'yu Dendra, 2018. pp. 86-92.

4. Rylenkov D. A. Sbornik nauchnykh statey aspirantov. Moskva: Moskovskiy finansovo-yuridicheskiy universitet MFYUA, 2023. p. 40-42.

5. Nikitina Y. S. Informatsionye sistemy i tekhnologii: sbornik materialov V vserossiyskoy ochnoy nauchno-tekhnicheskoy konferentsii «IST-2019», Kursk, 20 maya 2019 goda. Yugo Zapadnyy gosudarstvennyj universitet, 2019. pp. 138-142.

6. Futerman M. Y. Novaya nauka: Teoreticheskiy i prakticheskiy vzglyad. 2016. № 3-1(69). pp. 41-44.

7. Kravchenko T. K., Seredenko N. N., Shcherbinin O. P., Koryakovtseva N. A. Aktual'nyye voprosy sovremennoy nauki. 2010. № 11. pp. 217-222.

8. Bil'tayev I. S. Sbornik statey XV Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Penza, 20 dekabrya 2022 goda. Penza: Nauka i Prosveshcheniye. 2022. pp. 35-41.

9. Saaty T.L. American Journal of Trade and Policy. 2023. Vol. 10. No. 1. pp. 15-26.

10. Kafi M. A., Akter N. American Journal of Trade and Policy. 2023. Vol. 10. No. 1. pp. 15-26.

Дата поступления: 23.06.2024

Дата публикации: 27.07.2024