УДК 519

АНАЛИЗ МЕТОДОВ ОЦЕНКИ ИНТЕГРАЛЬНОГО РИСКА СЛОЖНЫХ СИСТЕМ

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: методы оценки риска, локальный риск, интегральный риск, сложная системы, неопределенность.

Аннотация: В работе проанализированы существующие подходы для оценки локальных рисков в сложных системах с точки зрения возможности их применения для оценки интегральных рисков таких систем. Особенностью задачи является необходимость учета различного рода неопределенностей, возникающих при рассмотрении системы в целом, а не ее элементов по отдельности. Характерными видами такой неопределенности являются: A) неопределенность значений параметров оценки состояния системы в целом; B) неопределенность, вызванная взаимным влиянием элементов системы друг на друга; C) неопределенность зависимости риска системы в целом от значений локальных рисков. Таким образом, перспективные методы оценки интегральных рисков сложных систем должны учитывать, как минимум, три этих вида неопределенности. Анализ используемых в настоящее время подходов к оценке рисков в сложных системах показал, что это требование не выполняется ни для одного из них. Из этого следует вывод, что для оценки интегрального риска сложных систем необходима модификации существующих методов оценки риска или разработка новых.

1. Введение

Решение задач управления безопасностью сложных систем требует применения подходов и методов оценки рисков, учитывающих неопределенность, вызванную как внутрисистемными, так и внешними факторами. Неопределенность является одной из основных причин отклонения системы от целевого режима функционирования, поэтому ее учет является обязательным для получения адекватных оценок интегрального риска сложной системы.

При рассмотрении сложной системы в целом наиболее часто приходится иметь дело со следующими видами неопределенности:

A. Неопределенность значений параметров оценки состояния системы в целом;
B. Неопределенность, вызванная взаимным влиянием элементов системы друг на друга;
C. Неопределенность зависимости риска системы в целом от значений локальных рисков.

Таким образом, метод оценки интегрального риска сложной системы должен позволять оценить риск системы в целом, с учетом неопределенности этих видов. Настоящая работа посвящена анализу существующих подходов и методов оценки рисков в сложных системах путем исследования источников за 2019-2023 гг. Целью анализа является определения наиболее адекватных методов оценки интегрального риска сложных информационных систем. Критериями анализа методов и подходов

является учет неопределенностей, возникающих при рассмотрении сложных систем в целом.

2. Анализ существующих методов оценки риска сложных информационных систем

Для оценки рисков в сложных системах используют количественные, качественные и комбинированные методы [1]. Более объективной оценкой является количественная, при этом из-за сложности их получения для реально существующих систем широко распространены оценки качественные. В данной работе были изучены подходы и методы, позволяющие работать как с количественными [2-17], так и с качественными [18-25] оценками. Отметим, что некоторые методы позволяют их комбинировать [26].

В результате анализа опубликованных с начала 2019 года исследований, посвященных управлению рисками в сложных системах, удалось выявить ряд методов, которые можно условно сгруппировать в следующие подходы.

Безмодельный подход. К данному подходу относятся методы машинного обучения [11, 13, 17], использующие большие массивы накопленных данных для мониторинга состояния системы (в первую очередь, идентификации аномалий) и классификации информационных активов. Алгоритмы машинного обучения способны предсказывать неизвестные для конкретной системы значения параметров, относя ее к тому или иному классу систем, для которых соответствующие значения были определены ранее. Это позволяет говорить о наличии механизма учета неопределенности вида А. Учесть влияние неопределенности видов В и С в рамках данного подхода невозможно.

Статистический подход. К статистическому подходу можно отнести такие методы, как стохастическое моделирование [12], статистический метод объективизации экспертных оценок [6]. В рамках подхода можно учесть неопределенность вида А, обычно с помощью введения в оценку рисков параметров вероятности или влияния в виде диапазона значений [12], а также путем генерации дискретного распределения на основе взвешенных мнений экспертов [6].

Теоретико-графовый подход. К теоретико-графовому подходу можно отнести методы теории графов [9], включая построение древовидных структур [8, 15, 16]. Матрица зависимости функционирования объектов системы позволяет строить оценки, учитывающие взаимное влияние элементов системы друг на друга [9], то есть учесть неопределенность вида В. При построении древовидных структур (структур атаки, защиты и др.) узлы представляют собой решения ЛПР или действия злоумышленника. Элементы системы в виде узлов в дерево обычно не включаются и рассматриваются как своего рода «вспомогательные активы» — соответственно, учет их взаимного влияния друг на друга не происходит. Тем не менее, поскольку их значения учитываются при оценке интегрального риска системы (см., например, [16]), можно говорить о наличии в рамках подхода механизма учета неопределенности вида С.

Нечеткая математика. Аппарат нечеткой логики предполагает использование лингвистических переменных для формирования функции принадлежности на интервальном промежутке [4, 5], тем самым учитывая неопределенность вида А.

Энтропийный подход. В задачах оценки рисков энтропийный подход обычно используется для определения весовых значений экспертных оценок. А, например, в [7] авторы преобразуют нечеткие мнения в числовые значения, используя энтропию Шеннона и, соответственно, в некотором роде учитывают неопределенность вида А.

Использование открытых стандартов. Еще одним подходом для оценки рисков является определение факторов риска в рамках системы оценки уязвимостей, заданной

некоторым стандартом (открытый стандарт CVSS, стандарты семейств ISO 27005) [1, 2]. Наличие неопределенности значений этих факторов подразумевается, но в явном виде не учитывается. В то же время в некоторых стандартах (например, [2]) предлагается использовать иерархию рисков, что позволяет учесть неопределенность вида С в случае, если локальные риски полагаются независимыми.

Метод попарного сравнения. Обычно используется для объективизации экспертных оценок [14]. Параметры оценки рисков информационных систем основаны на точно-заданных весовых коэффициентах, определенных экспертами. Веса критериев и их подкритериев попарно сравниваются без учета взаимного влияния элементов системы друг на друга. Механизмов учета неопределенности рассматриваемых видов метод не содержит.

Сценарный подход. Применительно к задачам оценки рисков сценарные подходы чаще всего используются для ранжирования тяжести последствий. Например, в работах [20, 21] авторы рассматривают вероятные рисковые сценарии. Параметры оценки их рисков определяются экспертным методом в детерминированных шкалах. По задумке авторов, вероятность рассмотренных сценариев зависит от ключевых показателей эффективности, конфиденциальности, специальных возможностей, целостности, реальности, обслуживания, безопасности, гибкости. При этом возможное влияние этих критериев на риски других сценариев не учитывается. Расчет риска реализации сценария с последующим ранжированием исходов производится без учета структуры информационной системы. Таким образом, ни один из рассматриваемых в настоящей работе видов неопределенности в рамках подхода не учитывается.

Анализ иерархий. Метод анализа иерархий применяется для поддержки принятия решений на основе множества критериев. Например, в работах [18, 22] оценки отдельных факторов агрегируются в виде взвешенной суммы. Ни один из рассматриваемых видов неопределенности в рамках подхода не учитывается.

Ранжирование. Помимо методов, встречающихся в сценарном подходе, для ранжирования факторов риска используют такие методы, как например, FMEA (анализ режимов отказов и последствий) [24] или STRIDE (Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege — подмена, фальсификация, отказ от ответственности, раскрытие информации, отказ в обслуживании и повышение привилегий) [25]. Данные методы включают в себя параметры оценки локальных рисков информационных систем на основе точно-заданных весовых коэффициентов. Учет неопределенности в этих методах не производится.

Социотехнический подход. К данному качественному подходу относится, в первую очередь, метод профилирования [19, 22]. Несмотря на то, что авторы работают с неопределенным объектом, они рассматривают исключительно детерминированные случаи, не учитывая неопределенности.

Методы агрегирования. Для перехода от локальных рисков к интегральному можно воспользоваться одним из методов агрегирования. Основными методами в этой группе является метод порогового агрегирования [27] и механизм комплексного оценивания (КО) [26]. Последний проектировался для использования при управлении организационными системами и потому разработан так, чтобы быть устойчивым к небольшим изменениям значений отдельных критериев. Таким образом, манипулируя структурой дерева и матриц свертки критериев, учесть зависимость интегрального риска от значений локальных рисков и, таким образом учесть влияние неопределенности вида С.

«Когнитивная игра». Данный метод специально разработан для оценки и управления рисками сложной системы в условиях взаимного влияния элементов

сложной системы друг на друга [3, 10], что позволяет учитывать неопределенности вида B и C.

Результаты анализа представлены в таблице 1.

Таблица 1. Учет неопределенности в укрупненных группах методов и подходах оценки риска при оценивании интегрального риска сложных информационных систем.

Группы методов	Основной метод	Учет неопределенности вида:			Ссылки
		A	B	C	
Безмодельный подход	Методы машинного обучения	Да	Нет	Нет	[11, 13, 17]
Статистический подход	Стохастическое моделирование	Да	Нет	Нет	[12]
	Объективизация экспертных оценок	Да	Нет	Нет	[6]
Теоретико-графовый подход	Методы теории графов и матричной записи	Нет	Да	Нет	[9]
	Построение деревьев отказов, атак, защиты	Нет	Нет	Да	[8, 15, 16]
Нечеткая математика	Методы нечеткой логики	Да	Нет	Нет	[4, 5]
Энтропийный подход	Энтропия Шеннона	Да	Нет	Нет	[7]
Использование открытых стандартов	Методы оценки рисков в соответствии со стандартами CVSS, ISO27005	Нет	Нет	Да	[1, 2]
Попарное сравнение	Метод попарного сравнения	Нет	Нет	Нет	[14]
Сценарный подход	Сценарный анализ	Нет	Нет	Нет	[20, 21]
Анализ иерархий	Метод анализа иерархий	Нет	Нет	Нет	[18, 23]
Ранжирование	FMEA, STRIDE	Нет	Нет	Нет	[24, 25]
Социотехнический подход	Профилирование	Нет	Нет	Нет	[19, 22]
Методы агрегирования	Пороговое агрегирование	Нет	Нет	Да	[27]
	Комплексная оценка	Нет	Да	Да	[26]
«Когнитивная игра»	Динамические взвешенные графы	Нет	Да	Да	[3, 10]

Как следует из проведенного анализа, существующие подходы и методы оценки рисков в сложных системах, в подавляющим большинстве, направлены на оценку локальных рисков и для оценивания интегральных рисков сложных систем в чистом виде непригодны. Тем не менее, представляется возможным разработать комбинированный метод, позволяющий учесть все три вида неопределенности. В частности, если метод КО дополнить механизмом учета неопределенности вида A, то полученный инструмент будет в полной мере удовлетворять предъявляемым требованиям. Тоже можно сказать и о методе оценки риска с помощью «когнитивной игры».

В силу того, что механизм комплексного оценивания изначально предназначен для оценки состояния организационных систем с активными агентами, он, возможно, требует некоторой адаптации и, возможно, доработки для применения в задачах оценки интегральных рисков сложных систем. Применительно к конкретным классам систем (в частности, информационным) потребуется создание обоснованных алгоритмов отбора критериев, являющихся локальными рисками. Однако в настоящее время приведенный анализ свидетельствует о том, что этот механизм, как и метод

«когнитивной игры» позволяет решать задачи оценки интегрального риска сложной системы с минимальными модификациями.

3. Заключение

При решении задач управления рисками сложных систем, в частности, информационных, возникает необходимость получения оценок текущих значений как локальных рисков защищаемой системы, так и интегрального, характеризующего систему в целом. Большинство исследований, доступных в настоящий момент в открытом доступе, сфокусировано на построении оценок локальных рисков. В то же время, при переходе к оценке интегрального риска сложных систем, возникают неопределенности, которые необходимо учесть при построении оценки. В данной работе из общесистемных соображений были выделены три вида неопределенности, которые, по мнению автора, должны быть учтены при разработке метода оценивания интегрального рисков и проведен анализ наиболее распространенных подходов к оценке рисков в сложных системах. Анализ показал, что в настоящее время ни один из рассмотренных методов не учитывает одновременно все три вида неопределенности.

Тем не менее, среди основных методов оценки рисков можно выделить методы комплексного оценивания и «когнитивной игры», которые, каждый по-своему позволяет учесть два вида характерных для сложных информационных систем неопределенности из трех. Причем, первый из них делает упор на качественную оценку локальных рисков, а второй, - на количественную. В связи с этим, видится разумным, для учета всех видов неопределенности, адаптировать один из этих методов для дальнейшего применения при оценивании интегрального риска сложных систем.

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 31.10.2023).
2. Зима В.М., Крюков Р.О., Кравчук А.В. Методика оценивания информационных рисков на основе анализа уязвимостей // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 11-12. С. 36-46.
3. Калашников А.О., Аникина Е.В. Управление информационными рисками сложной системы с использованием механизма «когнитивной игры» // Вопросы кибербезопасности. 2020. № 4 (38). С. 2-10.
4. Киселева Т.В., Маслова Е.В. Классификация рисков ИТ-сервисов и способы оценивания вероятностей их возникновения // ИТНОУ: информационные технологии в науке, образовании и управлении. 2020. № 1 (15). С. 67-71.
5. Колосок И. Н., Гурина Л.А. Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств // Методические вопросы исследования надежности больших систем энергетики. Ташкент, 23-27 сентября 2019 года: Институт систем энергетики им. Л.А. Мелентьева Сибирского отделения Российской академии наук, 2019. Книга 1. Выпуск 70. С. 238-247.
6. Akinrolabu O., et al. Cyber risk assessment in cloud provider environments: Current models and future needs // Computers & Security. 2019. Vol. 87. P. 101600.
7. Ershadi M. J., Forouzandeh M. Information Security Risk Management of Research Information Systems: A hybrid approach of Fuzzy FMEA, AHP, TOPSIS and Shannon Entropy // J. Digit. Inf. Manag. 2019. Vol. 17, No. 6. P. 321.
8. Grishunin S. et al. Development of the mechanism of assessing cyber risks in the internet of things projects // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 12th Conference, ruSMART 2019. St. Petersburg: Springer, 2019. P. 481-494.
9. Häckel B. Assessing IT availability risks in smart factory networks // Business Research. 2019. Vol. 12, No. 2. P. 523-558.

10. Kalashnikov A.O., Anikina E.V. Management of Risks for Complex Computer Network // Proceedings of the 23rd International Conference on Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN-2020, Moscow): Springer, 2020. Vol 1337. C. 144-157.
11. Korneev N.V., et al. An Approach to Risk Assessment and Threat Prediction for Complex Object Security Based on a Predicative Self-Configuring Neural System // Symmetry. 2022. Vol. 14, No. 1. P. 102.
12. Krisper M., et al. RISKEE: a risk-tree based method for assessing risk in cyber security // European conference on software process improvement. 2019. P. 45-56.
13. Palko D., et al. Cyber Security Risk Modeling in Distributed Information Systems // Applied Sciences. 2023. Vol. 13, No. 4. P. 2393.
14. Tusher H.M., et al. Cyber security risk assessment in autonomous shipping // Maritime economics & logistics. 2022. Vol. 24, No. 2. P. 208-227.
15. Rios E., Rego A., Iturbe E., Higuero M., Larrucea X. Continuous quantitative risk management in smart grids using attack defense trees // Sensors. 2020. Vol. 20. P. 4404.
16. Schmitz C., Pape S. LiSRA: Lightweight security risk assessment for decision support in information security // Computers & Security. 2020. Vol. 90. P. 101656.
17. Wang Y., Xue W., Zhang A. Application of Big Data Technology in Enterprise Information Security Management and Risk Assessment // Journal of Global Information Management (JGIM). 2023. Vol. 31, No. 3. P. 1-16.
18. Бакеев Д.Ш., Тишина Н.А. Программная реализация оценки рисков безопасности информации на основе гибридного метода // Приоритетные направления инновационной деятельности в промышленности. Сборник научных статей по итогам пятой международной научной конференции. Казань, 30–31 мая 2020 года. Часть 2. Казань: Общество с ограниченной ответственностью «КОНВЕРТ», 2020. С. 6-12.
19. Беззатеев С. В. и др. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, №. 4. С. 553-561.
20. Bolbot V., Theotokatos G., Boulougouris E., Vassalos D. A novel cyber-risk assessment method for ship systems // Safety science. 2020. P.104908.
21. Gunes B., Kayisoglu G., Bolat P. Cyber security risk assessment for seaports: A case study of a container port // Computers & Security. 2021. Vol. 103. P. 102196.
22. Kioskli K., Polemi N. A Socio-Technical Approach to Cyber-Risk Assessment // World Academy of Science, Engineering and Technology International Journal of Electrical and Computer Engineering. 2020. Vol. 14, No. 10. P. 305-309.
23. Ntafloukas K., McCrum D.P., Pasquale L. A cyber-physical risk assessment approach for Internet of Things enabled transportation infrastructure // Applied Sciences. 2022. Vol. 12, No. 18. P. 9241.
24. Subriadi A.P., Najwa N.F. The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment // Heliyon. 2020. Vol. 6, No. 1.
25. Wang Y., et al. A systematic risk assessment framework of automotive cybersecurity // Automotive Innovation. 2021. Vol. 4. P. 253-261.
26. Баркалов С.А., Новиков Д.А., Новосельцев В.И. и др. Модели управления конфликтами и рисками / Под ред. Д.А. Новиков. Воронеж: Научная книга, 2008. 495 с.
27. Алескеров Ф.Т., Якуба В.И. Метод порогового агрегирования трехградационных ранжировок // Доклады академии наук. 2007. Т. 413, №2. С. 181-183.