Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: mathmod.esrae.ru/45-180
Ссылка для цитирования этой статьи:
Володин Д.Н., Кондратов Д.В. Математические модели анализа рисков информационной безопасности и их практическое применение // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2024. №1

УДК 51-7 DOI:10.24412/2541-9269-2024-1-12-17

МАТЕМАТИЧЕСКИЕ МОДЕЛИ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Д.Н. Володин[1], Д.В. Кондратов[2]
[1]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов. danil3000200@mail.ru
[2]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, Институт проблем точной механики и управления Российской академии наук (ИПТМУ РАН), г. Саратов, Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского kondratovdv@yandex.ru.

MATHEMATICAL MODELS OF INFORMATION SECURITY RISK ANALYSIS AND THEIR PRACTICAL APPLICATION

D.N. Volodin[1], D.V. Kondratov[2]
[1]Saratov State Technical University named after Yuri A. Gagarin, Russia, Saratov. danil3000200@mail.ru
[2]Yuri Gagarin State Technical University of Saratov, Russia, Saratov, Institute of Precision Mechanics and Control of the Russian Academy of Sciences, Saratov, Russia; Saratov State University, Saratov, Russia, kondratovdv@yandex.ru

Аннотация: В статье рассматриваются современные методы и подходы к математическому моделированию рисков в области информационной безопасности. Представлен обзор основных теоретических концепций, связанных с анализом рисков, и предлагают их практическое применение в контексте обеспечения безопасности информационных систем. Рассмотрены математические модели, используемые для выявления угроз, оценки вероятности и влияния возможных инцидентов, а также определения стратегий управления рисками. Особое внимание уделяется применению этих моделей в реальных сценариях, что делает статью ценным ресурсом для специалистов по информационной безопасности, исследователей и практикующих профессионалов.

Ключевые слова: математические модели, риски информационной безопасности, анализ рисков, метод, модель.

Abstract: The article discusses modern methods and approaches to mathematical modeling of risks in the field of information security. An overview of key theoretical concepts

related to risk analysis is presented, along with their practical application in the context of ensuring the security of information systems. Mathematical models used for threat detection, probability assessment, impact analysis of potential incidents, and the determination of risk management strategies are examined. Special attention is given to the application of these models in real-life scenarios, making the article a valuable resource for information security specialists, researchers, and practicing professionals.

Keywords: mathematical models, information security risks, risk analysis, method, model.

В современном цифровом мире, где информационные технологии становятся неотъемлемой частью бизнеса и повседневной жизни, вопросы информационной безопасности становятся все более критическими. С огромным объемом ценных данных, хранящихся и обрабатываемых в сети, организации сталкиваются с разнообразными угрозами и рисками, которые могут нанести серьезный ущерб как финансовым, так и репутационным аспектам.

Эффективное управление рисками в области информационной безопасности требует системного подхода, способного оценивать и предсказывать потенциальные угрозы. В этом контексте математические модели становятся неотъемлемым инструментом для анализа и количественной оценки рисков. Эти модели позволяют не только выявлять слабые места в системах безопасности, но и принимать обоснованные решения по распределению ресурсов для их смягчения. Нынешняя ситуация требует построения новых математических методов, но для того чтобы понять какие методы нужны необходимо провести обзор существующих методов.

Целью данной статьи является разбор существующих математических моделей анализа рисков в области информационной безопасности, а также их преимущества и недостатки при использовании. Таким образом для того чтобы построить новые математические модели мы рассмотрим уже существующие с их достоинствами и недостатками.

Анализ рисков с применением математических методов в информационной безопасности - это процесс оценки и управления возможными угрозами и уязвимостями в информационных системах с использованием математических методов. Основные этапы включают в себя определение рисков, оценку вероятности и возможных последствий инцидентов, а также разработку стратегий по их управлению. Для построения математических моделей анализа рисков информационной безопасности необходимо пройти несколько основных этапов [1]:

- Идентификация рисков:
  - Определение ценных активов информационной системы (например, данные, программное обеспечение, оборудование);
  - Идентификация потенциальных угроз, которые могут повлиять на активы (например, вредоносные программы, несанкционированный доступ);
  - Анализ уязвимостей системы, которые могут быть использованы угрозами для атак.
- Оценка рисков:
  - Оценка вероятности возникновения угроз и эксплуатации уязвимостей;
  - Оценка потенциального ущерба или воздействия на активы в случае реализации угрозы.
- Математические модели:
  - Использование статистических методов для оценки вероятности различных сценариев инцидентов (Вероятностные модели);
  - Анализ возможных последствий инцидентов с использованием математических моделей.
- Контроль и управление рисками:

  - Разработка стратегий для снижения вероятности возникновения рисков и минимизации их последствий;
  - Регулярное обновление и анализ политик безопасности для соответствия современным угрозам.
- Мониторинг и обновление:
  - Постоянное отслеживание изменений в информационной среде и оценка их влияния на риски;
  - Регулярное обновление математических моделей и стратегий управления рисками в соответствии с изменяющимися условиями.
- Бизнес-процессы:
  - Интеграция процессов математического анализа рисков в общие бизнес-процессы организации;
  - Обучение персонала управлению рисками и соблюдению политик безопасности.

Оценка и управление рисками в информационной безопасности - это непрерывный процесс, который требует внимания к деталям, адаптации к изменяющимся условиям и сотрудничества между различными уровнями организации. Анализ рисков с применением математических методов играет важную роль в обеспечении точности и объективности в этом процессе.

Математические модели анализа рисков информационной безопасности широко используются для оценки уровня угроз и разработки стратегий по их смягчению. В настоящее время существуют следующие модели анализа рисков информационной безопасности:

- Модель OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
- Модель FAIR (Factor Analysis of Information Risk).
- Модель NIST SP 800-30 (Risk Management Guide for Information Technology Systems).
- Модель ISO 27001/27005.
- Модель Monte Carlo.

Модель OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). OCTAVE - это методология разработки стратегии управления рисками, фокусирующаяся на определении критически важных активов, угроз и уязвимостей. Оценка рисков основывается на матрице, где пересекаются активы, угрозы и уязвимости. Риски вычисляются как произведение вероятности угрозы, степени уязвимости и важности актива.

Говоря про практическое применением данной модели можно сказать, что она помогает выявить свои ключевые активы, которые нуждаются в наибольшей защите, а также она помогает проанализировать угрозы и уязвимости, которые могут быть использованы для атак

У модели OCTAVE есть несколько преимуществ: она учитывает операционные потребности организации и включает в себя оценку как угроз, так и уязвимостей. Но также у данной модели есть свои недостатки: она требует значительных усилий и ресурсов для реализации и может быть менее эффективена для крупных организаций

Модель OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) сосредотачивается на определении критически важных активов, угроз и уязвимостей. Она обеспечивает структурированный процесс для оценки рисков и разработки стратегий управления ими. [3] Основная ее преимущества включают в себя фокус на ключевых активах и простоту в использовании. Однако, она может потребовать адаптации под конкретные потребности организации.

Модель FAIR (Factor Analysis of Information Risk). FAIR предлагает формализованный подход к количественной оценке рисков, основанный на факторном

анализе. [2] Включает в себя расчет вероятности инцидента, степени воздействия, степени уязвимости и контрольных мер. Итоговый расчет дает количественное выражение риска.

В практике модель FAIR может применяться для проведения количественной оценки влияния рисков на бизнес, а также она помогает определить наиболее эффективные меры по управлению рисками.

Плюсами данной модели являются: предоставление количественных показателей рисков, что облегчает принятие решений, а также способность к адаптации к различным сценариям и контекстам. Но у каждой модели есть и ряд недостатков, модель FAIR не исключение, из недостатков можно выделить: требование высокой квалификации для правильной оценки параметров модели и зависимость точности оценок от доступности актуальных данных.

FAIR предоставляет количественные оценки рисков, позволяя более точно измерять и сравнивать их между собой. Однако, данная модель может быть более сложной в использовании и требовать высокого уровня экспертизы.

Модель NIST SP 800-30 (Risk Management Guide for Information Technology Systems). Разработана Национальным институтом стандартов и технологий (NIST) США. Это руководство предоставляет методику для оценки и управления рисками в информационных технологиях. [4] Оценка рисков включает в себя вычисление вероятности угрозы, воздействия на активы и степени уязвимости. Используется формула риска: Risk=Threat×Vulnerability×Impact.

На практике модель может использоваться для предоставления стандартного подхода к оценке и управлению рисками для ИТ-систем, а также она соблюдает требования многих регулирующих органов.

Плюсами данной модели являются: широкое применение в сообществе информационной безопасности, а также предоставление четких инструкций для проведения оценок рисков. Из минусов можно выделить, что модель NIST SP 800-30 может не обеспечить достаточной гибкости для специфических бизнес-контекстов и некоторые организации могут считать её слишком формальным и тяжеловесным.

Модель NIST SP 800-30 (Risk Management Guide for Information Technology Systems) предоставляет методологию для оценки и управления рисками в информационных технологиях. Она акцентирует внимание на стандартизированном подходе к анализу рисков, с учетом требований Национального института стандартов и технологий (NIST). Преимущества включают в себя широкую признаваемость и интеграцию с другими стандартами. Однако, ее обширность и ориентированность на стандарты могут потребовать дополнительных усилий при внедрении.

Модель ISO 27001/27005. Стандарт ISO 27001 определяет требования к системе управления информационной безопасностью, а стандарт ISO 27005 - методику управления рисками в ИБ. Использует матрицы рисков, вероятности и воздействия для определения уровней риска. [5]

Данные модели в практике используются для предоставления структурированного подхода к созданию и управлению системой управления информационной безопасностью (СУИБ) и обеспечению методологии оценки рисков, соответствующую требованиям ISO.

Говоря про преимущества данных моделей нельзя не сказать про то, что они являются международными стандартами, что обеспечивает их широкую признаваемость и применимость в различных отраслях и странах. Так же они легко интегрируется с другими стандартами управления, такими как ISO 9001 (качество) и ISO 22301 (управление бизнес-контингентностью). Из недостатков можно выделить, что реализация стандартов может потребовать существенных затрат на подготовку и обучение персонала, а также новым пользователям может потребоваться время для освоения обширных требований и концепций стандартов.

ISO 27001/27005 являются международными стандартами и обеспечивают структурированный подход к управлению рисками в информационной безопасности.

Однако, их внедрение может потребовать значительных затрат на подготовку и обучение персонала.

Модель Monte Carlo. Включает в себя использование метода Монте-Карло для моделирования случайных событий и оценки рисков. Генерация случайных входных данных (например, вероятности угроз) для определения вероятности различных исходов событий. [6]

На практике метод Monte Carlo применяется для моделирования случайных событий, позволяя оценивать вероятности и воздействия различных сценариев, а также позволяет проводить анализ рисков, учитывая неопределенность входных данных и параметров.

Из плюсов данного метода можно выделить то, что Monte Carlo может быть применен к различным видам задач, включая финансовый анализ, инженерное моделирование, и, в данном случае, оценку рисков информационной безопасности. Моделирование случайных событий позволяет учесть неопределенность и разнообразие сценариев. Минусами данного метода являются: зависимость точности результатов от качества и количества входных данных, сбор и обработка которых могут потребовать значительных ресурсов, также для неподготовленных пользователей результаты моделирования могут быть сложными для интерпретации.

Метод Monte Carlo предоставляет гибкий инструмент для анализа рисков, учитывая случайные события. Он подходит для моделирования разнообразных сценариев, но требует тщательной подготовки данных.

Эти модели могут быть применены в зависимости от конкретных потребностей и характера бизнес-процессов организации. Однако, при использовании любой модели важно учесть, что анализ рисков в ИБ - это динамический процесс, и модели должны регулярно обновляться в соответствии с изменениями в бизнесе и технологической среде.

Таким образом были рассмотрены следующие математические модели анализа рисков информационной безопасности, был проведен их анализ: OCTAVE, FAIR, NIST SP 800-30, ISO 27001/27005, а также метод Monte Carlo. Каждая из этих моделей предоставляет свой уникальный подход к оценке и управлению рисками, а также обладает своими преимуществами и недостатками.

Выбор подходящей модели должен основываться на особенностях организации, ее целях, и уровне зрелости в области управления рисками. Использование всех моделей подряд может привести к избыточности и потере эффективности. Таким образом, для достижения наилучших результатов в управлении рисками информационной безопасности необходимо тщательно выбирать модель в зависимости от конкретной задачи и контекста. Разработка новых моделей остается весьма актуальным направлением, поскольку каждый случай требует индивидуального подхода.

Литература

1. Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума «Информационная безопасность – 2021»), 29 ноября – 3 декабря 2021 г : материалы конференции / под редакцией А. В. Ефимова [и др.] ; RU. — Новосибирск : СибГУТИ, 2021. — 153 с. — ISBN 978-5-91434-067-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/257288 (дата обращения: 08.12.2023). — Режим доступа: для авториз. пользователей.

2. FAIR Model Risk Management – Pros and Cons / [Электронный ресурс] // Centraleyes : [сайт]. — URL: https://www.centraleyes.com/fair-model-risk-management-pros-and-cons/ (дата обращения: 09.12.2023).

3. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) / [Электронный ресурс] // CIO wiki : [сайт]. — URL: https://cio-

wiki.org/wiki/OCTAVE_(Operationally_Critical_Threat,_Asset_and_Vulnerability_Evaluation) (дата обращения: 06.12.2023).
4. NIST SP 800-30 / [Электронный ресурс] // NIST : [сайт]. — URL: https://csrc.nist.gov/pubs/sp/800/30/final (дата обращения: 10.12.2023).
5. Официальное издание М.: Стандартинформ, 2011 год ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности / Официальное издание М.: Стандартинформ, 2011 год [Электронный ресурс] // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» : [сайт]. — URL: https://docs.cntd.ru/document/1200084141 (дата обращения: 09.12.2023).
6. Мусаев, Л. А. Менеджмент риска на предприятии : учебное пособие / Л. А. Мусаев. — Грозный : ГГНТУ, 2019. — 190 с. — ISBN 978-5-6041021-3-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156894 (дата обращения: 10.12.2023). — Режим доступа: для авториз. пользователей.