Шаханова М.В., Киселева С.Д., Шаханова Э.С. Оценка рисков информационной безопасности объектов морской транспортной инфраструктуры // Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 1(39) с. 49–52

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ МОРСКОЙ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ

[1]Шаханова М.В., Киселева С.Д., Шаханова Э.С.
ФГБОУ ВО «ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

В данной статье рассматривается проблема оценки рисков информационной безопасности объектов морской транспортной инфраструктуры, которая становится все более критичной в свете увеличивающихся кибератак. Защита информационной безопасности этих объектов считается стратегически важной для обеспечения стабильности и безопасности мировой торговли. Автор исследует методы и подходы для анализа и управления рисками. Основное внимание уделяется использованию современных технологий и инструментов для обеспечения безопасности данных, а также обучению персонала для повышения осведомленности в области информационной безопасности.

Ключевые слова: Информационная безопасность морского транспорта, информационная безопасность объектов морской транспортной инфраструктуры, оценка рисков информационной безопасности объектов морской транспортной инфраструктуры, морская транспортная инфраструктура, объекты морской инфраструктуры, угрозы информационной безопасности, защита информации, анализ рисков.

ASSESSMENT OF INFORMATION SECURITY RISKS OF MARINE TRANSPORT INFRASTRUCTURE FACILITIES

[1]Shakhanova M. V., Kiseleva S.D., Shakhanova E.S.
MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

This article considers the problem of information security risk assessment of maritime transportation infrastructure facilities, which is becoming increasingly critical in light of increasing cyberattacks. Protecting the information security of these facilities is considered strategically important for ensuring the stability and security of global trade. The author explores methods and approaches for analyzing and managing risk. The focus is on the use of modern technologies and tools to ensure data security, as well as staff training to increase information security awareness.

Keywords: Information security of maritime transportation, information security of maritime transportation infrastructure objects, risk assessment of information security of maritime transportation infrastructure objects, maritime transportation infrastructure, maritime infrastructure objects, information security threats, information protection, risk analysis.

В современном мире, где уникальная информация является ключевым фактором успеха, информационная безопасность играет критическую роль в функционировании многих отраслей промышленности. Актуальность же оценки рисков информационной безопасности объектов морской транспортной инфраструктуры обусловлена ростом угроз

кибербезопасности в мире. Морская транспортная инфраструктура включает в себя порты, суда, морские терминалы и другие объекты, которые играют далеко не второстепенную роль в международной торговле и перевозках. Поэтому защита информационной безопасности этих объектов имеет стратегическое значение для обеспечения стабильности и безопасности мировой торговли [1].

Оценка рисков информационной безопасности в сфере морской транспортной инфраструктуры становится все более критической в свете увеличивающегося количества кибератак на судовые системы, включая блокирование управления судами, кибершпионаж и акты кибервандализма. Эти угрозы могут повлечь серьезные последствия, такие как ущерб для морских операторов, нарушение транспортных потоков и риски для человеческой безопасности.

Таким образом, оценка рисков в области информационной безопасности морской транспортной инфраструктуры является важной составляющей обеспечения безопасности данных и защиты в данной отрасли. Она позволяет выявить потенциальные угрозы и уязвимости, разработать эффективные стратегии управления ими и обеспечить надежную защиту информационных систем в морской транспортной сфере.

Оценка рисков информационной безопасности в сфере морской транспортной инфраструктуры стремится к следующим целям и задачам [2]:

1) Идентификация потенциальных угроз: Анализ возможных угроз информационным системам, связанным с морской транспортной инфраструктурой, таким как кибератаки, хакерские атаки, вирусы, программные ошибки и другие.

2) Оценка уязвимостей: Определение слабых мест в системах защиты, которые могут быть использованы злоумышленниками для нарушения информационной безопасности.

3) Анализ и количественная оценка рисков: Измерение уровня рисков, связанных с различными угрозами и уязвимостями, с целью установления приоритетов для принятия мер по снижению рисков.

4) Разработка и внедрение мер по снижению рисков: Формирование и внедрение стратегий для минимизации рисков, таких как улучшение систем безопасности, обучение персонала, обновление программного обеспечения и т. д.

5) Мониторинг и управление рисками: Регулярное изучение и пересмотр рисков для отслеживания изменений в угрозах и уязвимостях, а также оценки эффективности принятых мер по снижению рисков.

Существует разнообразие инструментов и стратегий, используемых для оценки рисков информационной безопасности в морской транспортной инфраструктуре. Среди них [3]:

- Анализ угроз и уязвимостей (например, OWASP Top 10) - данный подход нацелен на оценку рисков, связанных с ключевыми угрозами информационной безопасности, включая несанкционированный доступ, межсетевые атаки и уязвимости веб-приложений.
- Моделирование рисков с применением количественных методов (например, анализ дерева отказов или анализ влияния на стоимость) - эти подходы помогают определить вероятность возникновения инцидентов и их последствий с использованием математических моделей.

- Экспертная оценка - это стратегия, опирающаяся на мнение экспертов в области информационной безопасности, которые проводят оценку рисков и предоставляют рекомендации по их снижению.
- Использование специализированных инструментов для оценки рисков, таких как CRAMM, COBRA или Microsoft Security Assessment Tool, которые автоматизируют процесс оценки рисков и предоставляют рекомендации по их минимизации.
- Моделирование угроз и уязвимостей: данный метод вовлекает математические модели для оценки вероятности появления угроз и уязвимостей.

Каждый из этих подходов выбирается в зависимости от специфики объекта и требований оценки рисков информационной безопасности.Выбор конкретного метода зависит от конкретных потребностей и характеристик организации [4-5].

Оценка рисков информационной безопасности является неотъемлемой и значимой составляющей для объектов морской транспортной инфраструктуры, обеспечивая защиту систем и информации от потенциальных угроз. Ее цели и задачи включают выявление угроз, оценку уязвимостей, количественный анализ рисков, внедрение мер по их снижению и постоянный контроль. Методы оценки рисков охватывают анализ сценариев угроз, изучение уязвимостей, математическое моделирование рисков, а также качественные методы оценки [6-7]. Применение инструментов и подходов, таких как анализ угроз и уязвимостей, количественное моделирование, экспертная оценка и специализированные инструменты, помогает в проведении всесторонней оценки рисков информационной безопасности.

Список литературы

1. Information Security Management: From Risk to Control - by Andrew Paton and Jonathan Muffett "Управление информационной безопасностью. От рисков к мерам"
2. Risk Assessment and Management in Cyber Security - by Thomas Kragh "Оценка риска и управление в области кибербезопасности"
3. Maritime Security: Protection of Marinas, Ports, Small Watercraft, Yachts, and Ships - by Daniel J. Benny "Информационная безопасность в морской индустрии"
4. Security Threats in Maritime and Port Operations - by Khalid Bichou "Угрозы информационной безопасности в морских и портовых операциях"
5. Maritime Cyber Security: Principles and Practice - by L. Rayner "Информационная безопасность в судоходстве: принципы и практика"
6. Cyber Security in the Maritime Domain: Threats, Challenges, and Opportunities - by S. Ghosh. "Кибербезопасность в морской отрасли: руководство по управлению угрозами"
7. Managing Cybersecurity Risk in the Maritime Industry - by N. Dimopoulos "Управление кибербезопасностью в морской индустрии"

References

1. Information Security Management: From Risk to Control - by Andrew Paton and Jonathan Muffett "Information Security Management. From risks to measures"
2. Risk Assessment and Management in Cyber Security - by Thomas Kragh "Risk assessment and management in the field of cybersecurity"

3. Maritime Security: Protection of Marinas, Ports, Small Watercraft, Yachts, and Ships - by Daniel J. Benny "Information security in the marine industry"
4. Security Threats in Maritime and Port Operations - by Khalid Bichou "Threats to information security in maritime and port operations"
5. Maritime Cyber Security: Principles and Practice - by L. Rayner "Information Security in Shipping: principles and practice"
6. Cyber Security in the Maritime Domain: Threats, Challenges, and Opportunities - by S. Ghosh. "Cybersecurity in the maritime industry: Threat Management Guide"
7. Managing Cybersecurity Risk in the Maritime Industry - by N. Dimopoulos "Cybersecurity Management in the Maritime Industry"