МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

МАТЕРІАЛИ

XII Всеукраїнської науково-технічної конференції з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2024

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю [Електронний ресурс]. – Миколаїв : НУК, 2024. – 234 с.

У збірнику подано матеріали XII Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

обслуговування та мінімізує ризики, пов'язані з людським фактором. Подальший розвиток технологій комп'ютерного зору та ШІ дозволить вдосконалити методи моніторингу, забезпечуючи підвищену безпеку та надійність глобальної інфраструктури.

Список літератури:

1. Han, J., et al. "Anomaly Detection in Underwater Environments Using Deep Learning Approaches." IEEE Journal of Oceanic Engineering, 2020.

2. Torres, J., et al. "Real-Time Event Processing Architecture for Underwater Networks." Oceanography Systems Journal, 2021.

3. Parker, D., et al. "DLP and Cryptographic Solutions for Underwater Data Transmission." Information Security in Maritime Engineering, 2019.

4. Kim, H., et al. "Deep Learning-Based IDS and IPS for Underwater Networks." Journal of Marine Technology, 2020.

5. Smith, M. A., and Johnson, K. "Advances in Autonomous Underwater Surveillance Systems." Journal of Autonomous Systems in Marine Science, 2019.

6. Yamamoto, N., et al. "Environmental Monitoring with Autonomous Underwater Vehicles." Sensors and Actuators in Marine Science, 2018.

7. Williams, T., and Brown, A. "Network Traffic Analysis in Underwater Wireless Sensor Networks." IEEE Transactions on Wireless Communications, 2019.

УДК 004.056.5

КРИТЕРІЇ ВИБОРУ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ВОДНОГО ТРАНСПОРТУ

Автор: *Тотх М., магістрантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Зростаюча інтеграція комп'ютерних систем та автоматизації в морському транспорті, хоча й підвищує ефективність та маневреність суден, ненавмисно створила складне середовище, чутливе до кібератак. Поширення взаємопов'язаних систем на суднах та в портах сильно збільшило площу

атаки, зробивши ці об'єкти першочерговими цілями для зловмисників, і змусило приділяти їм особливу увагу. Зокрема за даними [1]:

– 2022 рік: внаслідок кібератаки програм-вимагачів під назвою LockBit на web-сайт порту web-сайт порту був закритий на кілька днів, викрадені фінансові звіти, контракти, суднові журнали та іншу інформація. Атака на дві німецькі нафтові компанії з метоюі викрадання інтелектуальної власності призвела до значних проблем у галузі доставки та розподілу нафти, компанія Shell змушена була змінити маршрут поставок нафти, що вплинуло на системи завантаження та розвантаження компаній. Міністр внутрішньої безпеки США Алехандро Майоркас заявив, що кібератаки є найбільшою загрозою для портів США;

– 2023 рік: внаслідок атаки програм-вимагачів на програмну компанію, яка постачає кораблі, її сервери для власної системи ShipManager були вимушено вимкнені, що мало негативний вплив на більше ніж 1000 суден;

– 2024 рік: адміністрація Байдена видала розпорядження про внесення змін, спрямованих на посилення безпеки, зокрема кібербезпеки, у портах США.

Сучасні системи навігації сильно залежать від супутникових технологій, які можуть бути скомпрометовані, що призводить до неточностей навігації та загрожує безпеці мореплавства. Крім того, широке впровадження електронних систем для управління вантажами, контролю руху суден та інших портових операцій піддає ці критично важливі інфраструктури кіберзагрозам, що може призвести до порушення роботи та компрометації безпеки.

Системи виявлення вторгнень (СВВ) є одним із сучасних засобів забезпечення кібербезпеки сучасних інформаційно-комунікаційних систем і можуть застосовуватися в різних галузях діяльності, зокрема у сфері водного транспорту. Дослідженню специфіки і перспектив їх застосування на водному транспорті присвячено роботи багатьох фахівців [2-6], однак, на даний час методики вибору СВВ для критичної морської інформаційної інфраструктури відсутні.

Метою даної роботи є визначення критеріїв вибору систем виявлення вторгненнь для водного транспорту.

Для досягнення даної мети необхідно вирішити наступні задачі:

– провести комплексний аналіз сучасних проблем застосування СВВ у морському середовищі;

– визначити унікальні компоненти СВВ, адаптовані для морського транспорту;

– визначити критерії і оцінити за ними продуктивність та придатність сучасних СВВ для морських застосувань.

При виборі СВВ для застосування у галузі водного транспорту необхідно враховувати їх здатність виявляти кібератаки на морі, здійснювані найчастіше застосовуваними зловмисниками способами, такими як [1]:

– фішинг, що спрямовується на велику кількість людей з метою отримання хоча б однієї відповіді, яка дозволить отримати доступ до атакованої системи або інформаційних ресурсів;

– шкідливе програмне забезпечення, яке часто надсилається через посилання в електронних листах і застосовується зловмисниками для порушення функціонування системи, що є об'єктом атаки, до того, як власники чи оператори ідентифікують загрозу, або для отримання інформації про об'єкт атаки, яка може бути використана для для атак в майбутньому чи сама по собі становить цінність для зловмисників;

– маніпуляція паролем, що здійснюється зловмисником за допомогою програмного забезпечення для систематичного вгадування паролів, щоб отримати несанкціонований доступ;

– соціальна інженерія, яка не є високотехнологічним способом організації кібератак і передбачає проведення прямих чи віртуальних розмов з особами, що володіють необхідною зловмиснику інформацією, при чому зловмисник може видавати себе за іншу особу або хибно посилатися на відому об'єкту атаки особу для отримання інформації.

При виборі СВВ витрати на їх придбання чи розробку, встановлення і експлуатацію не повинні перевищувати очікувані потенційні втрати внаслідок відсутності СВВ. Як наслідки кібератак у морській галузі можуть розглядатися збитки в короткостроковій і довгостроковій перспективі внаслідок збоїв у роботі суднового і портового обладнання:

– порушення судноплавства та роботи портів;

– порушення логістичних ланцюгів, пов'язаних із пасажирськими і грузовими перевезеннями, портами, річковим і морським транспортом;

– порушення інтересів стейкхолдерів;
– порушення безпеки судноплавства;
– порушення екологічної безпеки;
– порушення функціонування систем зв'язку та навігації на суднах;
– викрадання і втрати вантажу;
– ускладнення геополітичних відносин;
– репутаційні збитки тощо.

Ці атаки можуть завдати шкоди окремим працівникам на суднах і в портах, які можуть втратити дохід та роботу, тобто кібератаки здійснюватимуть негативний вплив на соціум. Збої в роботі систем безпеки, навігації та зв'язку можуть призвести до аварій на суднах і в портах, які можуть спричинити травмування чи загибель персоналу та пасажирів.

Захист морської інформаційної інфраструктури, що включає бази даних, системи відстеження вантажів та електронні системи безпеки, є надзвичайно важливим. Охорона баз даних, які містять критично важливі дані про судна, вантажі, екіпаж та операції, є необхідною. Впровадження надійних заходів автентифікації, авторизації та шифрування є вирішальним. Системи відстеження вантажів повинні бути захищені від несанкціонованого доступу та маніпуляцій, щоб забезпечити цілісність та точність даних. Крім того, системи безпеки, такі як контроль доступу та відеоспостереження, повинні бути захищені від кібератак.

Морські СВВ значно відрізняються від тих, що використовуються в традиційних офісних середовищах. Морська СВВ є складною системою, розробленою для виявлення та моніторингу потенційних вторгнень або загроз морській безпеці. Ці системи можуть застосовуватися на суднах та в портах [7-10] і включати:

– радари та системи відеоспостереження для моніторингу оточення судна в реальному часі;

– автоматизовані системи ідентифікації для відстеження руху суден та їх ідентичності;

– біометричні системи ідентифікації для систем контролю доступу на основі розпізнавання облич та інших біометричних даних для підвищення безпеки за рахунок використання багатофакторної ідентифікації;

– системи виявлення аномалій для ідентифікації відхилень від шаблонів нормальної поведінки мереж, суден, суднового та портового обладнання і виявлення потенційних загроз.

– системи глобального позиціонування для відстеження суден та вантажів в реальному часі і перевірки їх місцезнаходження.

– системи виявлення надзвичайних ситуацій та реагування для оперативного реагування на інциденти різного типу, в тому числі – на інциденти інформаційної безпеки.

Інтегровані морські СВВ поєднують різні технічні та програмні рішення для забезпечення комплексної безпеки суден, вантажів, екіпажів та пасажирів. Ці системи дозволяють обробляти ризики, асоційовані із широким спектром загроз, включаючи вторгнення, тероризм, піратство, аварії та інші небезпеки.

Вибір СВВ можна здійснити за множиною критеріїв, які для різних середовищ функціонування СВВ можуть мати різну вагу і поділяються за сутністю на функціональні, експлуатаційні, ресурсні та якісні критерії. До функціональних критеріїв, наприклад, можна віднести:

– здатність СВВ розпізнавати певні класи кібератак, зокрема атаки «0-day», і кількість цих класів;

– доступні методи виявлення атак;

– наявність шаблонів «нормальної» поведінки системи;

– задтність СВВ реагувати на кібератаку певним чином;

– задтність СВВ працювати в режимі реального часу (і параметри, що характеризують цю здатність) та у багатопоточному режимі;

– рівні застосовуваності СВВ (і їх кількість) за моделлю OSI та за мережевою архітектурою, область захисту;

– підтримувані СВВ операційні системи та протоколи (типи і кількість);

– здатність СВВ взаємодіяти з іншим програмним забезпеченням (типи і кількість);

– тип управління СВВ;

– відкритість коду.

Експлуатаційні критерії вибору СВВ характеризують її захищеність, масштабованість, адаптовність, здатність обробляти певний обсяг інформації.

До підмножини ресурсних критеріїв вибору СВВ відносяться:

– умови розповсюдження СВВ і її вартість;

– наявність документації і підтримки розробника при налаштуванні та експлуатації СВВ;

– наявність персоналу з достатнім рівнем кваліфікації;

– витрати часу і коштів на навчання персоналу;

– вирати часу і коштів на встановлення, налаштування та експлуатацію СВВ;

– необхідний обсяг пам'яті і вимоги до середовища функціонування СВВ.

Якісні критерії вибору СВВ включають кількість використовуваних сигнатур і шаблонів; показники ефективності виявлення атак та ефективності протидії атакам певного типу; оцінки зручності оновлення сигнатур і шаблонів нормального стану, зручності інтерфейсу і використання СВВ; здатність адаптувати налаштування під вимоги користувача.

За наведеними вище критеріями можна оцінювати продуктивність та придатність сучасних СВВ для морських застосувань. Загалом, СВВ для водного транспорту суттєво відрізняються від аналогічних систем, застосовуваних в офісних умовах. Оскільки водний транспорт має специфічні загрози, такі як піратство, тероризм, аварії та природні лиха, системи безпеки тут повинні бути адаптовані до відповідних ризиків. Відповідні ключові компоненти морської інформаційної інфраструктури мають захищатися СВВ. Наприклад, проведений в [6] аналіз показав, що система Naval Dome [11], пропонує цілісний підхід до кібербезпеки у сфері морського транспорту, захищаючи окремі компоненти та створюючи кібербезпечне середовище. Ця багаторівнева стратегія захисту ускладнює зловмисникам компрометацію системи, оскільки їм потрібно проникнути через кілька рівнів захисту. Основні компоненти, які Naval Dome може контролювати та захищати, включають системи управління судном, системи зв'язку, захист від піратства, системи управління кризовими ситуаціями та багато інших.

За критеріями адаптовності, швидкості реагування, здатністю виявляти атаки невідомих типів слід визнати перспективними інтелектуальні СВВ, що використовують машинне навчання [12, 13].

Висновки. В даній роботі на основі інформації з відкритих джерел проведено комплексний аналіз сучасних проблем застосування СВВ у морському середовищі; визначені унікальні компоненти СВВ, адаптовані для морського транспорту, критерії оцінювання СВВ та оцінки сучасних СВВ за критеріями продуктивності та придатності для застосування в морській галузі.

Список літератури:

1. Maritime Cybersecurity. URL: https://www.maritimeinjurycenter.com/accidents-and-injuries/cybersecurity/

2. Ibokette A. I., Ogundare T. O., Anyebe A. P., Odeh I. I., Okafor, F. C. Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions. International Journal of Scientific Research and Modern Technology, 3(10). URL: https://doi.org/10.38124/ijsrmt.v3i10.73

3. Farah M.-A.-B., Ukwandu E., Hindy H., Brosset D., Bures M., Andonovic I., Bellekens X. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information. 2022. No.13(1). URL: https:// doi.org/10.3390/info13010022. URL: https://www.researchgate.net/publication/357654089_Cyber_Security_in_the_Maritime_Industry_A_Systematic_Survey_of_Recent_Advances_and_Future_Trends

4. Li M., Zhou J., Chattopadhyay S., Goh M. Maritime Cybersecurity: A Comprehensive Review. IEEE Transactions on intelligent transportation systems. 2024 URL: https://arxiv.org/pdf/2409.11417

5. Smith, J. Cybersecurity in Maritime Transportation: Challenges and Solutions. Journal of Maritime Security. 2018. №10(2). P.145-162. URL: https://www.mdpi.com/2673-8732/2/1/9

6. Тотх М. Системи виявлення вторгнень для водного транспорту як основний метод захисту. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.43-46. URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf

7. IACS UR E22 Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e22_rev.3_june_2023_ul.pdf

8. IACS UR E26 Cyber resilience of ships URL: https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf

9. IACS UR E27 Cyber resilience of on-board systems and equipment. URL: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103854/UR-E27-Rev.1-Sep-2023-UL.pdf

10. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

11. Naval Dome. URL: https://navaldome.com/index.html

12. Anomaly-Based Intrusion Detection Systems Using Machine Learning. Journal of Cybersecurity and Information Managemen. 2024. Vol. 14. No. 01. PP. 20-33. URL: https://americaspg.com/article/pdf/2836

13. Стефанюк Ю.В. Інтелектуальні засоби в системах виявлення та запобігання вторгнень. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.129-133. URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf

УДК 004.056.5

ЗВАЖЕНЕ ОЦІНЮВАННЯ КРИТИЧНОСТІ ОБ'ЄКТІВ МОРСЬКОГО ТА РІЧКОВОГО ТРАНСПОРТУ

Автор: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Морський та річковий транспорт є підсектором сектору «Транспорт і пошта», критичної інфраструктури (КІ) України, що підпорядковується Мінінфраструктури. Кібербезпеці об'єктів КІ (ОКІ) і об'єктів критичної інформаційної інфраструктури (ОКІІ) приділяється особлива увага як на міжнародному, так і на національному рівнях, оскільки ці об'єкти надають послуги, що є життєво важливими для населення та держави, а часто – і для інших держав.

Наприклад, у червні 2024 року Норвегія, Фінляндія та Швеція прийняли рішення про створення військово-транспортного коридору крізь північні території цих країн, який сприятиме швидкому переміщенню персоналу та матеріалів із портів Норвегії через Швецію до Фінляндії [1].

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

XII Всеукраїнська науково-технічна конференція
з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич