MODERN MILITARY THREATS IN THE BALTIC-BLACK SEA REGION AND COUNTERMEASURES

DOI https://doi.org/10.30525/978-9934-26-527-3-6

CYBERATTACKS ON SHIPS IN THE BLACK SEA: A GROWING THREAT

КІБЕРАТАКИ НА СУДНА В ЧОРНОМУ МОРІ: ЗРОСТАЮЧА ЗАГРОЗА

Dryzhakova Dina Yuriivna
Postgraduate Student at the Department of Criminal Policy and Criminal Law, Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

Дрижакова Діна Юріївна
аспірантка кафедри кримінально-правової політики та кримінального права
Київський національний університет імені Тараса Шевченка
м. Київ, Україна
https://orcid.org/0009-0004-7585-5860

Чорне море, як стратегічно важливий водний шлях та центр торгівлі, стає все більш вразливим до кібератак. Сучасні судна оснащені складними системами управління, які, з одного боку, підвищують ефективність судноплавства, а з іншого – стають мішенню для кіберзлочинців.

Сьогодні природно, що кібербезпека портових терміналів, морської логістики має бути у фокусі особливої уваги не лише портових операторів чи судновласників, а і відповідних державних структур України.

Як зазначив ЦТС керівник одного з українських портів, робота над підсиленням кібербезпеки почалася задовго до повномасштабного вторгнення росії. Власне, після початку війни у 2014 році СБУ активно взялася за порти. Щоб позбутися усіх можливих загроз з боку росії у програмному забезпеченні і запобігти можливому впливу. “Ми тільки за, і якісь нові перевірки і рекомендації у цьому випадку лише на краще”, – сказав він [1].

Кібератаки на судна можуть мати різні форми та наслідки. Найпоширенішими є:

Викрадення даних: Зловмисники можуть отримати доступ до конфіденційної інформації про вантаж, маршрути, фінансові дані компанії-власника судна.

Блокування систем: Кібератаки можуть призвести до блокування систем управління судном, що може призвести до аварій та матеріальних збитків.

Маніпуляція з навігаційними системами: Зловмисники можуть змінювати дані GPS, що призводить до збою в навігації та зіткнення судна.

Вимога викупу: Кіберзлочинці можуть зашифрувати дані судна і вимагати викуп за їх розшифровку.

Дистанційне управління судном: У найскладніших випадках зловмисники можуть отримати повний контроль над судном і використовувати його в своїх цілях [2].

Специфічними для кібербезпеки судноплавства є інформаційні системи – автоматична ідентифікаційна система (AIS); електронно-картографічна навігаційно-інформаційна система (ECDIS); реєстратор даних рейсу (VDR), бортовий самописець; IT-інфраструктура автоматизації процесів із вантажами в порту (TOS); система відстежує рух контейнерів за допомогою GPS (CTS); аварійний радіобуй (EPIRB).

Дослідження, присвячені безпеці AIS, показали два напрями атаки: перший – на AIS-провайдерів, що збирають дані з AIS-шлюзів, встановлених на узбережжях для збору інформації AIS і далі для надання комерційних та безкоштовних сервісів у реальному часі; друге – лише на рівні радіопередачі, тобто самого протоколу AIS. Атаку на протокол було проведено з використанням SDR (software-defined radio). Можливий розвиток наступних сценаріїв:

– зміна даних про судно – імені, місця розташування, курсу, швидкості, інформації про вантаж;

– створення «кораблів-примар», які розпізнаються іншими судами як справжнє судно;

– надсилання неправдивої погодної інформації для зміни курсу;

– активація хибних попереджень про зіткнення;

– можливість зробити існуюче судно «невидимим»;

– створення неіснуючих пошуково-рятувальних вертольотів;

– фальсифікація сигналів EPIRB, що активують тривогу на судах, що знаходяться поблизу;

– можливість проведення кібератаки збільшенням частоти передачі AIS-повідомлень.

Відзначається особливість AIS дозволяти судам ставати «невидимкою», а також вручну змінювати інформацію, що транслюється. Зміна AIS-карток у територіальних водах чужої країни може спровокувати дипломатичний конфлікт. Зловмисні атаки призводять до відхилення судна з курсу за рахунок підміни повідомлень про можливе зіткнення з ним або до заманювання в певну точку акваторії

помилковим сигналом аварійного радіобую. У більшості ECDIS-систем, що являють собою встановлену на містку судна робочу станцію [3], за допомогою бортової мережі організований доступ в інтернет; AIS; радари та GPS-обладнання, датчики та сенсори. Застосовувані суднові Windows-системи далеко не завжди встигають отримувати навіть критично важливі оновлення безпеки в розумні терміни. Вразливості переважно зв'язуються з сервером, встановленому у комплексі системи. Використання шкідливого коду може виконати як зовнішній порушник через інтернет, так і член команди через фізичний носій, який використовується для оновлення або доповнення навігаційних карт. Виявлені вразливості дозволяють зчитувати, завантажувати, переміщати, замінювати та видаляти будь-які файли, що знаходяться на робочій станції. При цьому атакуючий отримує доступ до читання та зміни даних з усіх сервісних пристроїв, підключених до бортової мережі судна. Враховуючи важливість коректності роботи ECDIS, порушення чіткості її роботи призводять до травм і навіть смертей людей, перекриття морських каналів, посадок на мілину, забруднення навколишнього середовища та великих економічних збитків. При розслідуванні інцидентів, аварій та катастроф вкрай важливими є дані суднового VDR. У різноманітних зібраних і збережених навігаційних та статистичних даних судна, звукозаписах розмов на містку судна, радіопереговорах та радарних знімках, трапляються випадки зникнення сенсорних параметрів та голосових записів під час інциденту [4]. Результатом кібератак є: перезапис даних самим VDR та умисне знищення доказів, за допомогою підключення USB-носія до VDR, що призводило до стирання з нього всіх файлів та голосових записів. Існуюча можливість редагування даних на бортовому самописці та/або їх заміни становить велику ймовірність організації підробки та напрямок розслідування у хибне русло. Зазначені можливості зміни та видалення даних, а також можливість віддаленого виконання команд повністю компрометує VDR [5].

У судноплавстві портові IT-структури є функціонально складними системами. Виникнення інциденту портової кіберзлочинності пов'язане з роботою IT-департаментів злочинних банд, які перехоплюють 9-знакові PIN-коди для використання у проведенні операцій з контейнерами. По портовим бездротовим мережам віддавалися команди вантажних систем переміщати «певний» контейнер на свою вантажівку до приїзду власника Контрабандний підхід до підкупу робітників для заміни записів про контейнери з наркотиками досі досконало не вивчений транспортними компаніями.

Чорне море є вразливим до кібератак з кількох причин:

Географічне розташування: Чорне море є важливим торговим шляхом, що з'єднує Європу з Азією. Це робить його привабливою мішенню для кіберзлочинців.

Конфлікти в регіоні: Політична нестабільність в регіоні створює додаткові ризики для кібербезпеки.

Недостатня кібербезпека суден: Багато суден не обладнані сучасними системами кібербезпеки.

Слабка координація між країнами регіону: Відсутність єдиної стратегії кібербезпеки ускладнює боротьбу з кіберзагрозами.

Для захисту суден від кібератак необхідно вживати комплекс заходів:

Регулярне оновлення програмного забезпечення: Всі програмні продукти на судні повинні бути регулярно оновлюватися для усунення вразливостей.

Сильні паролі: Співробітники судна повинні використовувати сильні і унікальні паролі для доступу до систем.

Обмеження доступу: Доступ до критичних систем повинен бути обмежений тільки авторизованим користувачам.

Резервне копіювання даних: Регулярне резервне копіювання даних дозволить відновити роботу системи після кібератаки.

Співпраця з кібербезпекою: Компанії-власники суден повинні співпрацювати з фахівцями з кібербезпеки для оцінки ризиків та розробки планів реагування на інциденти.

Міжнародне співробітництво: Країни регіону повинні обмінюватися інформацією про кіберзагрози та розробляти спільні стратегії захисту [6].

З технологічної точки зору українським транспортним компаніям слід якомога швидше відмовлятися від софту з російським корінням. А перехід на нові перспективні платформи відкриває шлях і для широкого впровадження нових технологій безпеки: блокчейн; верифікація даних на основі ШІ; методи обчислення для підвищення конфіденційності даних (PEC); хмарні платформи з високим рівнем захисту та ін. Транспортним компаніям сьогодні як ніколи важливо приділяти особливу увагу локалізації своєї діджитал-інфраструктури та залученню фахівців з кібербезпеки. Важливим трендом стає впровадження концепції zero trust (нульової довіри), в якій усі пристрої, користувачі та софт, що взаємодіє з мережею, розглядаються як потенційні загрози [1].

Висновок

Кібератаки на судна в Чорному морі є серйозною загрозою для морської безпеки та економіки регіону. Для боротьби з цією проблемою необхідно вживати комплексних заходів, спрямованих на підвищення рівня кібербезпеки суден та портів.

Література:

1. Порти під кібератаками: Зростаюча загроза для морської галузі // https://cfts.org.ua/articles/porti_pid_kiberatakami_zrostayucha_zagroza_dlya_morsko_galuzi_2021/140318
2. Cybersecurity Challenges in the Maritime Sector // https://www.mdpi.com/2673-8732/2/1/9
3. Analysis of cyber security aspects in the maritime sector, ENISA, 10.2011.
4. Maritime Security: Hacking into a Voyage Data Recorder (VDR), R. Samanta, IOActive Labs, 09.01.2015.
5. Spread Spectrum Satcom Hacking: Attacking the Globalstar Simplex Data Service, C. Moore, Black Hat USA 2015.
6. Guidelines on Cyber Security Onboard Ships, Version Four // https://www.ics-shipping.org/resource/guidelines-on-cyber-security-onboard-ships-version-four/

DOI https://doi.org/10.30525/978-9934-26-527-3-7

MARITIME SECURITY AND COUNTERING AGGRESSOR'S PROVOCATIONS IN AREA OF «SCIENTIFIC COOPERATION»

МОРСЬКА БЕЗПЕКА ТА ПРОТИДІЯ ПРОВОКАЦІЯМ АГРЕСОРА У СФЕРІ «НАУКОВОЇ СПІВПРАЦІ»

Tytska Yana Olexandrivna
Ph.D., Associate Professor, Dean of the Faculty of Law and Economics International Humanitarian University Odesa, Ukraine

Тицька Яна Олександрівна
кандидат юридичних наук, доцент, декан факультету права та економіки Міжнародний гуманітарний університет м. Одеса Україна

Потреба удосконалення форм та методів реагування органів влади, академічного середовища та громадянського суспільства України на виклики російської агресії у контексті імітації «наукової співпраці» для просування антиукраїнських провокацій та для підриву морської безпеки у регіональному та глобальному вимірі, потребує на системне дослідження.На прикладах наведених в публікаціях правозахисників та експертів, зокрема Асоціації Реінтеграції Криму (далі – Асоціація) можна проаналізувати відповідні тенденції та розробити тенденції