потенційних загроз є невід'ємною частиною створення культури безпеки суб'єкта бізнесу.

Таким чином холократична модель управління бізнесом створює нові можливості для підприємств та організацій, але, одночасно, привносить й нові виклики у контексті кібербезпеки. Тому для її ефективного впровадження необхідно враховувати обидва аспекти і забезпечити паритет між ними. Щодо конкретних дій для забезпечення кібербезпеки в умовах холократії, мова може йти про створення спеціальних ролей, відповідальних за кібербезпеку, розробку процедур для оцінки кіберризиків, а також навчання співробітників основам кібербезпеки в умовах відкритості та прозорості.

Список використаних джерел:

1. Єршова О. О., Гончаренко І. М. Сучасні моделі управління розвитком бізнесу: сутність, види, інноваційні бізнес-моделі. Журнал стратегічних економічних досліджень. 2022. № 2(7). С. 75-85.
2. Чорній В. В., Приступа Т. В. Бірюзові організації: майбутнє чи модний тренд? URL: http://www.pev.kpu.zp.ua/journals/2019/5_16_uk/5_16_2019.pdf
3. Джур О. Є., Шепеленко Д. Ю. Застосування Teal-моделі в системі управління української компанії. Економіка та суспільство. 2021. № 32. URL: https://economyandsociety.in.ua/index.php/journal/article/download/849/816/

Ключові слова: управління, холократія, транспарентність, ризики, кібербезпека.
Keywords: governance, holocracy, transparency, risks, cybersecurity.

ІНТЕГРАЦІЯ КРИТИЧНИХ КОМПОНЕНТІВ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВОДНОГО ТРАНСПОРТУ

Пунченко Наталія

в.о. завідувача кафедри інформаційних технологій Одеського державного аграрного університету, кандидат технічних наук, доцент

В інноваційному суспільстві така галузь, як судноводіння під час зародження, визначила себе до інноваційної. Такому визначенню є доказ. Взято основний курс на збирання, інтеграцію, передачу та аналіз інформації про ситуацію на морі, на борту кораблів та на березі за допомогою електронних засобів з метою забезпечення навігації «від причалу до причалу», інновації суднобудування та технології освоєння світового океану [1]. Світ судноплавства зараз потребує управління безпекою сучасних інформаційних мереж водного транспорту – це комплекс заходів та технологій, спрямованих на забезпечення надійної та безпечної роботи мереж, що використовуються у сфері водного транспорту. Доктрина управління інформаційної безпекою показано рисунку 1. Комплекс є важливим аспектом у сучасній судноплавної

промисловості, оскільки водна промисловість включає пасажирські, вантажні перевезення і управління портової інфраструктурою. Ось деякі ключові аспекти управління безпекою в інформаційних мережах: захист від кіберзагроз, забезпечення надійності засобів зв'язку для координації дій, моніторингу погоди та інших аспектів роботи водного транспорту, запобігання аваріям, дотримання нормативів та стандартів. Особливістю сучасних інформаційних мереж, що вони інтерпретуються з наявністю штучного інтелекту. Сучасні інформаційні мережі належать до складних систем. Які розвиваються на користь систем управління роботою флоту, і що дає можливість формуванню віртуальних мультисервісних мереж з динамікою зміни структурних параметрів. Забезпечують вимогу інших систем управління генерацією інформаційних послуг. А ось інтенсифікація засобів і засобів захисту інформаційних ресурсів істотно ускладнює контроль низки параметрів, що викликає необхідність розробки засобів і засобів захисту у взаємозв'язку з процесом розробки методів і засобів контролю. Відмінна особливість сучасних інформаційних мереж управління в судноводженні полягає в наявності тісної взаємної залежності їх основних інтеграційних властивостей: готовності, мобільності, пропускної спроможності, скритності, доступності, керованості.

Рис. 1. Управління інформаційної безпекою.

Посилення взаємозалежності основних властивостей є наслідком конвергенції технологій. Крім того, новою інтегративною властивістю інформаційних мереж є наявність і характеристики розподіленої системної пам'яті, що дозволяє протягом певного періоду часу зберігати повідомлення, що передаються, що радикально впливає на інші властивості мережі. На додаток, системи мають агентів природного (професіоналізм) та штучного інтелекту. У таких системах агенти штучного інтелекту не обов'язково наділені самосвідомістю, але, на відміну від сучасних нейромереж, здатні справлятися з широким колом завдань у різних умовах. Вони вдаються до реалізації технологій вузько спеціалізованого штучного інтелекту, що вимагає налаштування та повторної перевірки з боку людини. Сукупність агентів за певних умов утворює суперсистему, поведінка якої може бути повною мірою формалізовано рамках класичної теорії управління. Труднощі формалізації пов'язані з високим ступенем невизначеності інфраструктури та впливом людського фактору (професіоналізму) у динаміці функціонування суперсистеми.

Суперсистема характеризується віртуальністю функціональної структури, в контексті інформаційної безпеки вказують на використання віртуальних систем або технологій для моделювання функцій та завдань у межах суперсистеми судноводіння. Віртуальні системи допомагають відтворювати та аналізувати різноманітні сценарії та ситуації без необхідності реального фізичного втручання. Такий підхід дозволяє удосконалювати та тестувати системи безпеки та управління судовими процесами. Також вказує на комплексну систему, яка включає у собі різноманітні підсистеми для управління судном та навігації. Віртуальність тут може використовуватись для створення віртуальних аналогів окремих компонентів суперсистеми для аналізу та тестування їх функціональності. У цьому можливі конфлікти управління системами управління безпекою сучасних інформаційних мереж.

Інформаційно-алгоритмічне забезпечення сучасної інформаційної мережі судноводіння в рамках кібербезпеки охоплює широкий спектр технологій та заходів для забезпечення безпеки та надійності інформаційних систем, що використовують у морському судноплавстві [2-4]. І є багаторівневими, включають фундаментальну та адаптаційну частину, заміна якої забезпечує нову спеціалізацію елементів. Технології Soft Definition Network (SDN), Network Function Virtualization (NFV), Soft Definition Radio (SDR) приклади такого забезпечення.

У зв'язку з цим інформаційна система загалом має пам'ять і гнучкість поведінки, для стійкого функціонування якої має виконуватися така умова: швидкість адаптації елементів до нових функціональних завдань має бути вищою за швидкість зміни зовнішніх факторів, що впливають [5]. У зв'язку з

цим актуальною є тематика досліджень, що існують та розробка нових підходів до забезпечення якісного зворотного зв'язку в системі управління безпекою сучасних інформаційних систем судноплавства, що й становить мету роботи. Існуюча методологія управління складними системами передбачає визначення необхідних умов організації управління. Роботи авторів Крючкової Л.П., Трофименка А.О., Майданевич С.Б., Лахно В.А. показують, що вимоги сучасних систем моніторингу інформаційних систем, які генерують нескінченний потік подій безпеки, які задля забезпечення повноти охоплення контролем і забезпечення режиму реального часу налаштовані фіксацію зміни параметрів кожного з елементів системи без деталізації його стану. Виникає надлишок повідомлень та нестача їхнього контексту, що ускладнює завдання ідентифікації стану безпеки та потребує додаткових перевірок, отже, знижується оперативність реагування на інциденти безпеки. Таким чином, виникає завдання обробки у режимі, близькому до реального часу, великого потоку повідомлень про події безпеки без втрати їхньої змістовності. Це і не дозволяє повною мірою забезпечувати взаємодію одночасно по вертикалі та горизонталі. Іншими словами, технологічні недоліки, не дають можливості вирішувати завдання взаємодії та контролю у сучасних інформаційних систем.

Необхідно домагатися стійкості у частині передбачуваності поведінки та повної функції управління системою. Це можливо за рахунок синтезу інтелектуальної системи контролю на основі теорії функціональних систем та формалізації процесу зіставлення, відбору та об'єднання (синтезу) різноманітних за значенням аферентних потоків збуджень, що становить основу початкового етапу розгортання функціональної системи поведінки. Скорочення циклу контролю ІБ можливе на основі нового підходу до забезпечення самоорганізації системи контролю ІБ за заданими критеріями якості результатів контролю шляхом автоматичної генерації профілів контролю та самосинхронізації мультиагентної мережі контролю.

Список використаних джерел:

1. N. Punchenko, V. Strelbitskyi, O. Tsyra. Shaping the future of the marine industry as a condition for adaptation in an innovative society. Short Paper Proceedings of the 2nd International Conference on Intellectual Systems and Information Technologies (ISIT 2021). CEUR Workshop Proceedingsthis link is disabled, 2021, 3126 CEUR-WS.org, ISSN 1613-0073. P. 103–107.
2. Analysis of cyber security aspects in the maritime sector. ENISA (10.2011). P. 31.
3. AIS Exposed: Understanding Vulnerabilities & Attacks 2.0 (4. video), Dr. M. Balduzzi, Black Hat Asia. (2014).
4. Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, Yevgen Dyryavyy, NCC Group. (03.03.2014).

5. Слюсаренко А. Впровадження та вплив кібер-безпеки на сучасне технічне обслуговування обладнання суден і судноплавних компаній. Λ΄ΟΓΟΣ. ОНЛАЙН. 2020. № 10. Водний транспорт № 1 (37) 2023 187 DOI: 10.36074/2663-4139.10.09.
6. Лахно В.А. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту. Безпека інформації. 2016. Том 22. No 1. С. 44-50.

Ключові слова: інформаційні системи судноводіння, морський транспорт, кіберзахист.
Keywords: navigation information systems, maritime transport, cyber defense, threat.

СТРАТЕГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ТА ІННОВАЦІЙНОГО УПРАВЛІННЯ ДЛЯ СТАЛОГО РОЗВИТКУ СУСПІЛЬСТВА

Котлубай Вячеслав

доцент кафедри національної економіки Національного університету «Одеська юридична академія», кандидат економічних наук, доцент

Сучасний світ характеризується швидким розвитком інформаційних технологій та комунікацій, що відкриває нові можливості для соціального, економічного та культурного прогресу. Однак, разом з цим, зростає й обсяг кіберзагроз, які ставлять під загрозу безпеку, стабільність та благополуччя суспільства. Кіберзлочинність, кібершпигунство, кібертероризм, кібервійна, кібератаки на критичну інфраструктуру, порушення конфіденційності, цілісності та доступності інформації - це лише деякі з викликів, з якими стикаються держави, організації та окремі особи в кіберпросторі.[1, 2]

У цьому контексті, кібербезпека стає одним з ключових факторів сталого розвитку суспільства, який вимагає стратегічного підходу та інноваційного управління. Стратегічний підхід передбачає визначення цілей, пріоритетів, принципів та механізмів забезпечення кібербезпеки на національному та міжнародному рівнях, а також врахування глобальних тенденцій, ризиків та можливостей в кіберсередовищі. [3]

Стратегічний підхід до кібербезпеки має бути застосований на національному та міжнародному рівнях, що означає, що держава має враховувати свої внутрішні та зовнішні інтереси, можливості та обмеження, а також співвідносити свої цілі, пріоритети, принципи та механізми з тими, що мають інші держави, міжнародні організації та інші зацікавлені сторони. В якості цілей повинно бути встановлено: захист суверенітету, прав та інтересів громадян, інтеграція до європейських та євроатлантичних структур, розвиток інформаційного суспільства. При цьому головними пріоритетами є: посилення національної системи кібербезпеки, протидія кіберзагрозам, співпраця з міжнародними партнерами, інноваційний розвиток. Все це повинно бути реалізо-