

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

**СУЧАСНІ ПРОБЛЕМИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НА ТРАНСПОРТІ**

СПІБТ–2024

МАТЕРІАЛИ

**ХІІ 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

ОРГАНІЗАТОРИ:

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

**Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.**

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

© Національний університет кораблебудування
імені адмірала Макарова, 2024

УДК 004.056.5

НОРМАТИНО-ПРАВОВА БАЗА КІБЕРБЕЗПЕКИ ГАЛУЗІ ВОДНОГО ТРАНСПОРТУ

Автор: Хван Ю.В., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

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

Бурхливий розвиток цифровізації усіх галузей господарства, суспільного і політичного життя, військової справи зумовлює актуальність захисту інформації у всіх сферах людської діяльності. Водний транспорт є важливою складовою сучасних логістичних систем, належить до критичної інфраструктури і має велику кількість стейкхолдерів. Відповідно, кібербезпеки в цій галузі регламентується нормативно-правовими актами, що видаються законодавчими і виконавчими органами влади, міжнародними організаціями, галузевими відповідальними органами, місцевими органами влади, керівництвом окремих портів, судноплавних компаній тощо [1-12]. Кількість цих документів постійно зростає. Крім того, розвитком теоретичних основ кібербезпеки водного транспорту займаються займаються вітчизняні і зарубіжні науковці [13-17], які у своїх роботах визначають проблеми захисту інформації в галузі і пропонують методи для їх вирішення. Таким чином, актуальною задачею управління кібербезпекою в галузі водного транспорту є систематизація інформації щодо нормативно-правових актів, що є чинними для вирішення прикладних задач в галузі, і розробка засобів обробки цієї інформації.

Метою даної роботи є розробка структури бази даних відкритих нормативно-правових актів в галузі водного транспорту.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- провести аналіз відкритих літературних джерел і визначити типи інформаційних блоків, які мають бути включені в базу даних, і їх

параметри, що можуть використовуватися при вирішенні конкретних прикладних задач кібербезпеки у галузі водного транспорту;

- визначити перелік типових запитів до розроблюваної бази даних;
- розробити структуру бази даних відкритих нормативно-правових актів в галузі водного транспорту.

Інформацію, яка має бути представлена в базі даних можна умовно поділити на дві частини – нормативно-правові акти і публікації у відкритих джерелах. З метою нормалізації бази даних доцільно інформацію, яка може використовуватися для описів документів чи відповідати на деякі типові запити, винести в окремі допоміжні таблиці.

В базі даних має бути представлена інформація щодо нормативно-правових актів, які стосуються різних аспектів управління інформаційною безпекою на водному транспорті:

- опису загроз і вразливостей інформаційної безпеки для портів і суден, наприклад, на підставі [2-4, 6];
- вимог стейкхолдерів, країн, міжнародних і національних організацій до забезпечення кібербезпеки, наприклад, на підставі [1-12];
- вимог щодо обробки ризиків, наприклад, на підставі [2, 3, 8-12];
- рекомендацій щодо найкращих практик забезпечення кібербезпеки в галузі водного транспорту [2-4, 6, 7];
- опису процесів інформаційного обміну в галузі [5].

Наприклад, ISO 24060:2021 Ships and marine technology — Ship software logging system for operational technology (укр. Судна та морська технологія — Програмна система реєстрації суден для операційної технології) є міжнародним стандартом [5], виданим Міжнародною організацією із стандартизації, який визначає систему реєстрації і моніторингу стану програмного забезпечення (ПЗ) судна, зокрема:

- реєструє версії програмного забезпечення для судового обладнання;
- встановлює порядок реєстрації в журналі фактів встановлення обладнання або виявлення ПЗ, порядок автоматичної реєстрації звітів, надісланих обладнанням, і порядок розміщення у сховищі електронних звітів про послуги, пов'язаних із записами журналу.

ISO 24060:2021 вимагає, щоб ПЗ було зареєстроване, і можна було б отримати інформацію про його поточний робочий стан, що з точки

зору кібербезпеки є корисним для виявлення причин кіберінцидентів, пов'язаних із використанням певного ПЗ, певного судового операційного технологічного обладнання та інтегрованих систем, включаючи, системи електрогенерації, контролю і сигналізації, навігації та зв'язку, рульового керування тощо.

Розроблювана база даних повинна формувати звіти за результатами типових запитів, зокрема, надавати користувачу відповіді на наступні питання:

- які нормативні документи і/або публікації пов'язані із вирішуваною користувачем задачею (за ключовими словами, що задаються користувачем);
- які документи є обов'язковими/рекомендованими для виконання в заданій сфері;
- чи є певний документ чинним і в якій сфері, і з якого часу;
- ким і коли був затверджений/відмінений документ;
- чи були наявні попередні версії документів і коли вони були чинними або на заміну якому документу був прийнятий даний документ; чи планується і коли видання нової версії.

База даних повинна дозволяти користувачу отримувати переліки нормативно-правових актів, рекомендацій і публікацій, що є і/або були чинними у певній сфері; визначати органи, які випускали нормативні акти у заданій сфері, науковців і практиків, що займаються розробкою теорії і засобів кібербезпеки у заданій сфері; ознайомлюватися з оригіналами нормативно-правових актів і рекомендацій, їх перекладами, науковими публікаціями і практичними рекомендаціями, а у разі відсутності оригіналів у вільному доступі – з описами і умовами отримання; планувати власну діяльність на підставі інформації про заплановані зміни нормативно-правових актів.

Для вирішення цих завдань опис документу має містити наступну інформацію:

- назва документу;
- посилання на документ: посилання на документ мовою оригіналу, посилання на переклад/переклади документу;

- стан документу: чинний/ не чинний;
 - сфера дії: опис;
 - обов’язковість: обов’язковий для сфери дії, рекомендації;
 - ключові слова: перелік;
 - зміст: опис;
 - відповідальний орган: група [18] (Верховна Рада, Президент України, Кабінет міністрів України, Адміністрація Держспецзв’язку, Національний банк України, міністерство, служба, агентство, інспекція, ЦОВВ зі спеціальним статусом, колегіальні органи, інші центральні органи виконавчої влади, місцеві органи влади, міжнародна організація, зарубіжна організація, група організацій тощо), орган, країна/країни;
 - затверджуючий документ: тип (Закон України, міжнародний стандарт, ДСТУ, НД ТЗІ, Постанова кабінету міністрів України, Розпорядження Кабінету міністрів України, Указ Президента України, Наказ Адміністрації Держспецзв’язку, Наказ Міністерства (назва)), дата прийняття документу (день, місяць, рік), номер документу, введення в дію (день, місяць, рік);
 - втрата чинності: дата (день, місяць, рік), підстава (опис документу);
 - пов’язані документи: перелік і посилання;
 - пов’язані публікації: перелік і посилання (підручники, наукові статті, тези доповідей на наукових конференціях, web-публікації тощо);
 - версії документа: попередні версії (назва, часові рамки чинності, посилання), заплановане оновлення (дата, джерело інформації).
- Опис публікацій повинен мати реквізити згідно з [19], наприклад для книги – автори, назва, місце публікації, видання, рік, кількість сторінок, гіперпосилання.

Структура бази даних наведена на рис.1.

Висновки

В даній роботі проведено аналіз відкритих літературних джерел і визначені типи інформаційних блоків в базі даних і їх параметри, типові запити до розроблюваної бази даних; розроблена структура бази даних відкритих нормативно-правових актів в галузі водного транспорту.

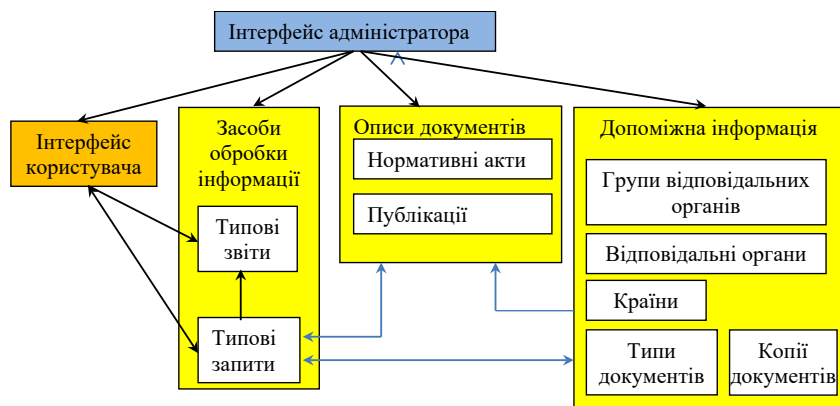


Рисунок 1 – Структура бази даних

Список літератури:

1. IACS 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
2. 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
3. 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>
4. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf
5. ISO 24060:2021 Ships and marine technology — Ship software logging system for operational technology. URL: <https://www.iso.org/ru/standard/77678.html>
6. Recommendation on Cyber Resilience No.166. URL: <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/24150438/rec-166-corr2-apr-2022-ul.pdf>
7. Rules for the survey and construction of steel ships. Part X. Computer-based systems. URL: https://www.classnk.or.jp/hp/pdf/rules/465_part_x_e_202406.pdf

8. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

9. Наказ № 23 Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів КІ». URL: <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text>

10. Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг Постанова № 4 Правління Національного банку України від 16.01.2021 URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>

11. Про критичну інфраструктуру. Закон України URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

12. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука безпечного розвитку країни. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n7>.

13. Juan Ignacio Alcaide, Ruth Garcia Llave. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. 2020. Volume 45. Pages 547–554. URL: <https://www.sciencedirect.com/science/article/pii/S2352146520302209>

14. Баронова О., Турти М., Ганчо С. Визначення рівня впливу кіберзагроз на розвиток морської галузі. *Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ICT-2020»*. Харків: ХНУРЕ, 2020. С.275-278.

15. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. *Вісник Одеського Національного ун-ту. Серія: Правознавство*. 2024. Т.26. Випуск 1(38). С.112-117. URL: <https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462>

16. Грищенко С.Л. Принципи інтелектуального управління інформаційною безпекою корпоративної мережі порту. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК,

2023. С.168-175. URL: <https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf>

17. Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. *Водний транспорт*. №.1(37). 2023. С.179–188. URL: <https://vt.duit.in.ua/index.php/home/article/view/267/224>

18. Інші органи виконавчої влади <https://www.kmu.gov.ua/catalog>

19. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення. URL: https://dnaop.com/html/61984/doc-ДСТУ_3008_2015

ЗМІСТ

Секція 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ..... 3

Загрози об'єктам морської критичної інфраструктури України та напрямки досліджень щодо їх нейтралізації <i>Блінцов В.С.; Буруніна Ж.Ю.</i>	3
Аналіз загроз системі інформаційного обміну між постом керування та дроном <i>Гололобов О.В.</i>	5
Оцінка безпеки баз даних NOSQL у системах відстеження та моніторингу транспорту <i>Євдокимов С.О.</i>	8
Перспективи комп'ютерного зору в задачах підводного моніторингу <i>Іванов В.А.</i>	13
Критерії вибору системи виявлення вторгнень для водного транспорту <i>Тотх М.</i>	15
Зважене оцінювання критичності об'єктів морського та річкового транспорту <i>Турти М.В.</i>	22
Критерії прийняття рішень щодо забезпечення кіберстійкості в морській галузі <i>Турти М.Ю.</i>	29

Секція 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ..... 35

Система аналізу методів забезпечення безпеки у бездротових мережах <i>Бердніков В.В.</i>	35
Автоматизована система реєстрації відвідувачів на основі wi-fi підключення <i>Білець О.О.</i>	38
Модель прогнозування кібератак на основі аналізу поведінки <i>Божаткін С.М.; Гусєва-Божаткіна В.А.; Пасюк Б.Б.</i>	42
Дослідження використання прихованих каналів сучасних месенджерів <i>Восков К.П.</i>	46
Аналіз та виявлення мережових атак грубої сили на інтернет-сервіси <i>Десятов А.М.</i>	49

Дослідження функціонування системи захищеного електронного документообігу в підрозділах національної поліції України <i>Дзюбас Д.С.</i>	51
Розробка пакету документів для атестації АС-1 «Гермес-2» на IV категорію обмеження доступу кафедри КТІБ <i>Дибченко М.Є.</i>	59
Дослідження вразливостей протоколу керування безпілотним апаратом спеціального призначення <i>Душенко О.В.</i>	66
Система підтримки прийняття рішень щодо оцінювання ризиків глобальної маршрутизації <i>Єсипенко А.О.</i>	77
Система підтримки прийняття рішень щодо категоризації об'єктів критичної інфраструктури <i>Злочевська О.В.</i>	85
Аналіз системи захисту платформи BLYNK <i>Зобова Е.В.</i>	91
Розробка рекомендацій з покращення захисту інформації в АС-2 та АС-3 класів 4 категорії для об'єкту критичної інфраструктури <i>Мацibuра Д.О.; Мельничук О.Ю.; Шевченко В.В.</i>	94
Розробка системи моніторингу та інформування про відмови в роботі інтернет-сервісів <i>Ніколаєв В.Д.</i>	99
Систем захисту мовної інформації для об'єктів інформаційної діяльності <i>Нужний С.М.</i>	101
Організація захисту бази знань при роботі з хмарним сховищем <i>Письменюк В.А.</i>	108
Система підтримки прийняття рішень щодо вибору засобів захисту від DDoS-атак <i>Садалюк Є.О.</i>	113
Аналіз захищеної системи віддаленого контролю кліматичних параметрів серверних приміщень та можливі шляхи їх модернізації <i>Стефанюк Ю.О.</i>	120
Оцінка та адаптація стійкості інформаційно комунікаційної системи критичного об'єкту <i>Стефанюк Ю.О.</i>	124
Програмне моделювання кольорових фракталів з поліноміальною функцією перетворення та дослідження їх параметричної чутливості <i>Сулiма М.М.; Корчевський Д.О.; Данилець Є.В.; Новак С.М.; Самойленко Д.М.</i>	129
Системи безперебійного живлення комп'ютерних мереж <i>Трибулькевич С.Л.; Трибулькевич В.В.; Трешнюк А.І.</i>	133

Оцінка залежності консолідації інформаційного WEB ресурсу від впливу інформаційної та кібернетичної безпеки *Хавело Д.С.* ..140

Секція 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 147

Система підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022 *Іванюк А.О.*147
Нормативно-правова база кібербезпеки галузі водного транспорту *Хван Ю.В.*..... 156

Секція 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ..... 163

Оцінювання звукоізоляції акустичних сигналів огорожувальними конструкціями режимних приміщень *Касьянов Ю.І.; Нужний С.М.* 163
Узагальнення спектрів довготривалих мовленнєвих сигналів з використанням можливостей MatLab *Касьянов Ю.І.; Щербаков М.С.* 169
Врахування характеристик слуху в системах цифрового звуку *Лях О.Д.,*..... 174

Секція 5. СТВОРЕННЯ ПІДВОДНО-ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ЗАХИСТУ МОРСЬКИХ ОБ'ЄКТІВ ТА АКВАТОРІЙ..... 178

Стенд для випробувань установок гребних електроприводів *Большаков Є.Д.*..... 178
Система керування просторовим рухом дистанційно керованого апарату *Верещака О.І.* 180
Розробка альтернативного джерела електроенергії на основі сонячних елементів та вітрогенераторної установки *Малишев Б.Г.* 182
Розробка алгоритмів керування системи рухом мобільної робототехнічної установки *Назаров В.Ю.* 184
Інтелектуальна система керування дистанційно керованим роботом *Новиков А.Ю.* 186

Наукове видання

**СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ НА ТРАНСПОРТІ**

СПІБТ–2024

**ХІІ 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
