МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«18» 06 2025 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

РОЗРОБКА БАЗИ ДАНИХ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ГАЛУЗІ ВОДНОГО ТРАНСПОРТУ

Ступінь вищої освіти: БАКАЛАВР
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 4 курсу групи 4381
Хван Юрій В'ячеславович

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Хван Ю.В.

Керівник: доцент кафедри комп'ютерних технологій та інформаційної безпеки к.т.н., доцент **Турти Марина Валентинівна** _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н., доцент, завідувач кафедри КТІБ
_____ С.М. Нужний
«18» 06 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Хван Юрій В'ячеславович

Курс:4

Група: 4381

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 «Кібербезпека та захист інформації»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: «Розробка бази даних нормативно-правового забезпечення кібербезпеки в галузі водного транспорту»
затверджена наказом НУК від «_23__» _квітня_____2025 р. № УЧ- 343

2. Вихідні дані до роботи: нормативно-правова кібербезпеки та захисту інформації в галузі водного транспорту, теоретичні основи управління інформаційною безпекою і побудови захищених баз даних

провести аналіз відкритих літературних джерел; визначити склад бібліотеки нормативно-правових актів, чинних у галузі водного транспорту, параметри документів, які мають бути віддзеркалені в базі даних, перелік типових запитів до розроблюваної бази даних; розробити і апробувати інформаційні моделі та систему запитів для типових процесів вирішення прикладних задач за допомогою розроблюваної бази даних відкритих нормативно-правових актів в галузі водного транспорту

4. Терміни виконання завдання:
термін видачі завдання: «_03_» _лютого_ 2025 р.
термін подання роботи: «18» _червня_ 2025 р.

5. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
1.	Організаційні збори.	23	03.02.2025	Вибір теми, визначення мети, завдань, об'єкта та предмета дослідження	
2.	Організаційні збори	25	20.02.2025	Попередній варіант оглядових розділів, підбір і опрацювання списку використаних джерел	
3.	Рубіжний контроль	31	03.04.2025	Попередній варіант повної КР.	
4.	Рубіжний контроль	33	20.04.2025	Попередній варіант презентації.	
5.	ЄДКІ на рівень «бакалавр»	34	29.04.2025	Здавання ЄДКІ зі спеціальності на ступінь бакалавра	
6.	Перевірка на плагіат	42	14.06.2025	1. Електронний варіант кваліфікаційної роботи; 2. Подання КР на перевірку на плагіат.	
7.	Кафедральний захист	43	18.06.2025	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії, висновок керівника). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	
8.	Подання документів на захист	44	24.06.2025	1. Подання щодо захисту КР 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Висновок кафедри про КР, допуск до захисту; 4. Електронний варіант та роздрукована презентація в кількості 5 примірників. 5. Електронний варіант КР на диску	
9.	Захист КР	44	25.06.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
Доцент кафедри комп'ютерних технологій
та інформаційної безпеки, к.т.н., доцент _____ М.В. Турти

Студент _____ Ю.В.Хван

АННОТАЦІЯ

Хван Ю.В. Розробка бази даних нормативно-правового забезпечення кібербезпеки в галузі водного транспорту. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти «бакалавр» за спеціальністю F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології», освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Пояснювальна записка: 47 с., 7 рис., 59 посилань.

Кваліфікаційна робота присвячена актуальній темі – розробці засобів автоматизації вирішення прикладних задач в галузі кібербезпеки та захисту інформації об'єктів критичної інфраструктури. Об'єктом дослідження в даній роботі є системи управління інформаційною безпекою (СУІБ) водного транспорту. Предметом дослідження є нормативно-правове забезпечення кібербезпеки та захисту інформації в галузі водного транспорту. Методами дослідження є аналіз відкритих літературних джерел, теоретичні основи управління інформаційною безпекою та побудови захищених баз даних. Метою роботи є розробка бази даних відкритих нормативно-правових актів з кібербезпеки в галузі водного транспорту.

В роботі проведено аналіз відкритих літературних джерел; визначено склад бібліотеки нормативно-правових актів, чинних у галузі водного транспорту, параметри документів, які віддзеркалені в базі даних для систематизації та ефективного пошуку інформації при вирішенні типових прикладних задач; розроблені інформаційні моделі для типових процесів вирішення прикладних задач за допомогою розроблюваної бази даних; визначені, розроблені і апробовані типові запити до розроблюваної бази даних; розроблена і апробована структура бази даних відкритих нормативно-правових актів в галузі водного транспорту.

Робота має практичне значення, оскільки її результати можуть бути використані в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації», при проектуванні КСЗІ та СУІБ в галузі водного транспорту і як складова для побудови повнофункціональної системи підтримки прийняття рішень щодо забезпечення кібербезпеки та захисту інформації в галузі водного транспорту.

Дана робота була апробована на XII Всеукраїнській науково-технічній конференції з міжнародною участю "Сучасні проблеми інформаційної безпеки на транспорті" 2024 р.

Ключові слова: кібербезпека, захист інформації, водний транспорт, база даних, нормативно-правове забезпечення.

ANNOTATION

Khvan Y.V. Development of a database of regulatory and legal support for cybersecurity in the water transport sector. – Qualification work in the form of a manuscript.

Qualification work on receiving a higher education degree "Bachelor" in the specialty F5 "Cybersecurity and Information Protection" of the field of knowledge F "Information Technologies", educational and professional program " Systems technical protection of information, automation of its processing" - Admiral Makarov National University of Shipbuilding, Mykolaiv, 2025.

Explanatory note: 47 pp., 7 figs., 59 references.

Qualification work is devoted to a topical issue – the development of automation tools for solving applied problems in the field of cybersecurity and information protection of critical infrastructure facilities. The object of research in this work is information security management systems (ISMS) of water transport. The subject of the research is the regulatory and legal support of cybersecurity and information protection in the field of water transport. The research methods are the analysis of open literary sources, theoretical foundations of information security management and the construction of protected databases. The purpose of the work is developing a database of open regulatory legal acts on cybersecurity in the field of water transport.

In thesis open literary sources have been analized; composition of the library of valid regulatory and legal acts in the field of water transport, the parameters of documents that are reflected in the database for systematization and effective search for information when solving typical applied problems have been determined; information models for typical processes of solving applied problems by using the developed database have been developed; typical queries for the developed database have been defined, developed and tested; structure of the database of open regulatory and legal acts in the field of water transport have been developed and tested.

The work has practical significance, since its results can be used in the educational process in the specialty F5 "Cybersecurity and Information Protection", in the design of CSIP and ISMS in the field of water transport and as a component for building a fully functional decision support system for ensuring cybersecurity and information protection in the field of water transport.

This work was tested at the XII All-Ukrainian Scientific and Technical Conference with International Participation "Modern Problems of Information Security in Transport" in 2024.

Keywords: cybersecurity, information protection, water transport, database, regulatory and legal support.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

BIMCO – Baltic and International Maritime Council (Балтійська і міжнародна морська рада);

CBS – Computer Based System (комп'ютеризовані системи);

CSA – Chamber of Shipping of America (Судноплавна палата Америки);

ENISA – European Union Agency for Network and Information Security (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки);

GDPR – General Data Protection Regulation (Загальний регламент захисту даних);

IACS – International Association of Classification Societies (Міжнародна асоціація класифікаційних співтовариств);

IAPH – International Association of Ports and Harbours (Міжнародна асоціація портів та гаваней);

ICS – International Chamber of Shipping (Міжнародна палата судноплавства);

IDS – Intrusion Detection Systems (системи виявлення вторгнень);

IMO – International Maritime Organization (Міжнародна морська організація);

INTERCARGO – International Association of Dry Cargo Shipowners (Міжнародна асоціація власників суховантажних суден);

IPS – Intrusion Prevention Systems (системи запобігання вторгненням);

ISAC – Information Sharing and Analysis Center (Центр обміну і аналізу інформації);

ISM code – International Safety Management code (Міжнародний кодекс з управління безпекою, МКУБ)

ISPS code – International Ship and Port Facility Security Code (Міжнародний кодекс охорони суден і портових засобів, Кодекс ОСПЗ)

IUMI – International Union of Marine Insurance (Міжнародний союз морського страхування);

MTS-ISAC – Maritime Transportation System Information Sharing and Analysis Center (Центр обміну та аналізу інформації та системи морського транспорту, США);

MSC – Maritime Safety Committee (Комітет з морської безпеки *IMO*);

NIST – United States National Institute of Standards and Technology's (Національний інститут стандартів і технологій США);

NORMA Cyber – Nordic Maritime Cyber Resilience Centre (Північний морський центр кіберстійкості);

OCIMF – Oil Companies International Marine Forum (Міжнародний морський форум нафтових компаній;

WSC – World Shipping Council (Всесвітня рада судноплавства);

АС – автоматизована система;

БС – безпека судноплавства;

ВВТ – внутрішній водний транспорт;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

ІТ – інформаційна технологія;

КЗЗ – комплекс засобів захисту;

КІ – критична інфраструктура;

КМІІ – критична морська інформаційна інфраструктура;

КСЗІ – комплексна система захисту інформації;

МКУБ – Міжнародний кодекс з управління безпечною експлуатацією суден і запобіганням забрудненню;

МРТ – морський і річковий транспорт;

ОІІ – об’єкт інформаційної інфраструктури;

ОКІ – об’єкт критичної інфраструктури;

ОКІІ – об'єкт критичної інформаційної інфраструктури;

ОМІ – об’єкт морської інфраструктури;

ОСПЗ – охорона суден і портових засобів;

ПЗ – програмне забезпечення;

СК – судноплавна компанія;

СУІБ – система управління інформаційною безпекою;

СУБ – система управління безпекою;

СУБС – система управління безпекою судноплавства.

ВСТУП

Захист інформації у період цифровізації є актуальним для усіх сфер людської діяльності. При цьому особливого значення набуває кібербезпека та захист інформації критичної інформаційної інфраструктури. Особливістю водного транспорту, який є складовою критичної інфраструктури, є велика кількість стейкхолдерів, що характерно для будь-якої транспортної системи. Морський та внутрішній водний транспорт задіяний у багатьох логістичних ланцюгах, які діють на територіях різних країн. Тому вимоги щодо кібербезпеки та інформаційної безпеки водного транспорту наявні у багатьох нормативно-правових актах, які видаються керівництвом окремих судноплавних компаній і портів; місцевими, законодавчими і виконавчими органами влади; галузевими відповідальними органами різних країн; міжнародними організаціями, які різняться за складом свої членів. На даний час в галузі водного транспорту спостерігається бурхливе зростання як кількості нормативно-правових актів, так і наукових досліджень, присвячених розвитку теоретичних основ кібербезпеки та інформаційної безпеки водного транспорту і розробці методів вирішення проблем захисту інформації в галузі. Таким чином, з міркувань побудови ефективних систем управління інформаційною безпекою (СУІБ) і оптимізації процесів створення комплексних систем захисту інформації (КСЗІ) в галузі водного транспорту актуальною є задача систематизації чинних для нормативно-правових актів і розробка засобів автоматизованої обробки інформації цих актів для вирішення прикладних задач.

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

Фактично для досягнення поставленої мети необхідно створити бібліотеку нормативно-правових актів і систему ефективних запитів до неї, що вимагає виконання наступних завдань:

− провести аналіз відкритих літературних джерел і визначити склад бібліотеки нормативно-правових актів, чинних у галузі водного транспорту;

− визначити параметри документів, які мають бути віддзеркалені в базі даних;

− розробити інформаційні моделі для типових процесів вирішення прикладних задач за допомогою розроблюваної бази даних;

− визначити перелік типових запитів до розроблюваної бази даних;

− розробити і апробувати структуру бази даних відкритих нормативно-правових актів в галузі водного транспорту та систему запитів до неї.

Об’єктом дослідження в даній роботі є СУІБ водного транспорту.

Предметом дослідження в даній роботі є нормативно-правове забезпечення кібербезпеки та захисту інформації в галузі водного транспорту.

Методами дослідження є аналіз відкритих літературних джерел, теоретичні основи управління інформаційною безпекою та побудови захищених баз даних.

1 ЗАГАЛЬНИЙ АНАЛІЗ НОРМАТИВНО–ПРАВОВИХ ДОКУМЕНТІВ ТА СТРУКТУРА РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В ГАЛУЗІ ВОДНОГО ТРАНСПОРТУ

1.1 Роль нормативно–правового забезпечення в сфері кібербезпеки водного транспорту

У сучасному світі кібербезпека перестала бути виключно технічною проблемою — вона перетворилася на питання національної безпеки, міжнародної співпраці та сталої діяльності критичних галузей. Водний транспорт, що включає морське та річкове судноплавство, функціонування портів, логістичних та інформаційних систем, офіційно визнаний об’єктом критичної інфраструктури України відповідно до Закону України «Про критичну інфраструктуру».

Із розвитком цифрових технологій, автоматизованих систем керування суднами, портовими комплексами та логістичними ланцюгами, рівень їх підключення до глобальної мережі зростає. Це, у свою чергу, підвищує ризик виникнення кіберзагроз, зокрема: несанкціонованого доступу до навігаційних систем, шифрування або викрадення конфіденційної інформації, порушення функціонування SCADA-систем, атак на логістичні сервери, інфраструктуру морських портів, тощо.

У цьому контексті нормативно-правове забезпечення виконує ключову роль. Воно формує правові рамки для захисту інформаційних систем, визначає обов’язки і відповідальність суб’єктів, регламентує технічні, організаційні та процедурні заходи кібербезпеки.

Основні функції нормативно-правового забезпечення:

– Регуляторна — встановлення обов’язкових правил і вимог до безпеки ІТ-систем;

– Координаційна — уніфікація підходів на різних рівнях (державному, галузевому, локальному);

– Захисна — правова основа для реагування на інциденти;

– Превентивна — стимулювання впровадження системного підходу до управління ризиками;

− Освітня — регламентація кваліфікаційних вимог, стандарти навчання персоналу у сфері ІБ.

Правове регулювання охоплює широкий спектр аспектів — від класифікації інформаційних активів до обов'язкових процедур звітування про кіберінциденти, від регламенту дій у кризових ситуаціях до міждержавного обміну інформацією щодо загроз. Це особливо важливо в умовах міжнародної діяльності морських портів і судноплавних компаній, які працюють у межах загальносвітових стандартів.

Разом з тим, через швидкий розвиток технологій та змінність законодавства постає потреба не лише в прийнятті нових документів, але й у забезпеченні оперативного доступу до чинних, актуальних та систематизованих нормативно-правових актів, що й обґрунтовує необхідність створення автоматизованої бази даних таких документів.

1.2 Класифікація джерел нормативно–правового забезпечення

Нормативно-правове забезпечення в сфері кібербезпеки водного транспорту є багаторівневою та багатоджерельною системою, яка складається з документів різного правового статусу, походження, сфери дії та функціонального призначення. Для ефективної обробки таких документів необхідна їх чітка класифікація (табл. 1.1 – табл. 1.4).

Таблиця 1.1 – Розподіл документів за рівнем дії

Рівень дії	Характеристика	Приклад
Міжнародний	Встановлює базові стандарти, обов'язкові або рекомендовані для держав-учасниць	IMO MSC.428(98), ISO/IEC 27001:2022
Національний	Обов'язкові для всіх суб'єктів на території України	Закон України «Про кібербезпеку», Постанова КМУ №518
Галузевий	Документи органів галузевого управління або відомчих структур	Накази Мінінфраструктур, накази Держспецзв'язку
Локальний (організаційний)	Політики безпеки, внутрішні регламенти суб'єктів транспортної інфраструктури	Політика кібербезпеки порту «Південний», інструкції судноплавних компаній

Таблиця 1.2 – Розподіл документів за джерелом формування (органом-ініціатором)

Орган	Сфера відповідальності	Приклад документів
Міжнародна морська організація (IMO)	Встановлення міжнародних стандартів безпеки судноплавства	MSC-FAL.1/Circ.3
Міжнародна організація за стандартизації (ISO)	Розробка технічних стандартів в т.ч. щодо ІБ	ISO/IEC 27000-серія
Європейський Союз (для інтеграції та адаптації)	Глобальні рамкові директиви з кібербезпеки	Директива NIS2
Верховна Рада України	Законодавче регулювання	Закон України «Про інформацію»
Кабінет Міністрів України (КМУ)	Регламентуючі постанови	Постанова КМУ №518 від 2019 р.
Міністерство інфраструктури України	Визначення вимог до об'єктів транспорту	Накази МІУ про безпеку портів
Держспецзв'язку, СБУ, НКЦК	Технічне регулювання в сфері захисту ІКС	НД ТЗІ, методичні рекомендації
Компанії, оператори портів	Практична реалізація СУІБ	Внутрішні регламенти політики, інструкції

Таблиця 1.3 – Розподіл за правовим статусом документу

Статус	Опис	Значення
Закон	Прийнятий парламентом, обов’язковий для виконання	Найвища юридична сила
Постанова	Рішення уряду щодо реалізації положень законів	Виконавчий рівень
Наказ / Інструкція	Регуляторний документ галузевого рівня	Стандартизація на підприємствах
Стандарт (ISO, ДСТУ)	Технічні вимоги, методики	Переважно добровільні, але часто обов’язкові у контрактах
Рекомендації / Політика	Внутрішній документ, що регламентує правила в компанії	Адаптація нормативів до практики

Таблиця 1.4 – Розподіл документів за галузевою спрямованістю

Галузь	Опис
Загальні документи	Охоплюють усю критичну інфраструктуру, у т.ч. водний транспорт
Морський транспорт	Стосується океанських/морських суден, портів, тощо
Річковий транспорт	Нормативи щодо судноплавства на внутрішніх водних шляхах
Портова інфраструктура	Охоплює захист інформації в логістичних системах портів, автоматизованих системах керування
Телекомунікаційні системи	Документи щодо захисту каналів зв’язку, SCADA-систем тощо

1.3 Структура нормативного забезпечення кібербезпеки у водному транспорті

Структура нормативного забезпечення є системою взаємопов’язаних рівнів правових актів, яка дозволяє формувати, реалізовувати та контролювати заходи кібербезпеки. Для ефективної побудови системи управління інформаційною безпекою (СУІБ) у галузі водного транспорту необхідно розуміти, як саме нормативні документи взаємодіють між собою та які функції вони виконують на різних рівнях (табл. 1.5).

Таблиця 1.5 – Ієрархічна структура рівнів

Рівень	Суть	Роль	Функції та приклад
Стратегічний (державний)	Визначає загальні принципи, політики та цілі у сфері кібербезпеки	Формує рамки національної безпеки, в тому числі в контексті інтеграції до європейських та міжнародних структур.	Національна стратегія кібербезпеки України, Закон України «Про основи національної безпеки»
Нормативно-правовий (законодавчий)	Закони, постанови, які регулюють правовідносини у сфері ІБ	Регламентує відповідальність, повноваження органів, порядок обміну інформацією, реагування на інциденти.	Закон України «Про кібербезпеку», Постанова КМУ №518
Технічний/галузевий (прикладний)	Визначає технічні вимоги до систем захисту	Деталізує вимоги до конкретних сфер — морські порти, судна, логістика.	НД ТЗІ, накази МІУ, стандарти ISO
Операційний (організаційний)	Впроваджує механізми реалізації вимог у конкретних організаціях	забезпечує реалізацію вимог через інструкції, регламенти, навчання персоналу.	Політики ІБ, інструкції з доступу, процедури реагування

1.4 Проблематика і потреба у систематизації нормативно-правових документах

Сучасний стан нормативно-правового забезпечення кібербезпеки в галузі водного транспорту характеризується динамічністю, складністю структури та високим ступенем фрагментарності. Попри значну кількість наявних документів, які регулюють кібербезпеку на різних рівнях — від міжнародного до організаційного, їх практичне використання залишається ускладненим. Це

зумовлено низкою системних проблем, які впливають на ефективність реалізації заходів з інформаційної безпеки на водному транспорті.

Однією з ключових проблем є *відсутність централізованого джерела або інтегрованого інформаційного ресурсу*, який би містив повний і актуальний перелік нормативно-правових актів, що регулюють кібербезпеку в транспортній галузі. Документи публікуються на вебресурсах різних органів влади — Верховної Ради, Кабінету Міністрів, міністерств, міжнародних організацій, що ускладнює пошук, перевірку актуальності та логічне поєднання нормативів у єдину систему.

Наступною значною проблемою є *фрагментарність нормативної бази*. Багато нормативно-правових актів дублюють або навіть суперечать одне одному. Частина з них регулює загальні питання інформаційної безпеки, не враховуючи особливостей водного транспорту, зокрема складну багаторівневу інфраструктуру, використання спеціалізованих інформаційно-телекомунікаційних систем, впровадження SCADA-комплексів та інші специфічні технічні та операційні особливості.

Також слід зазначити проблему *різноманітності форматів документів*, які часто представлені у вигляді скан-копій, недоступних для автоматизованого аналізу. Відсутність структурованості та єдиної логіки представлення інформації призводить до труднощів у впровадженні систем електронного обліку, пошуку за критеріями та генерації звітів.

Важливою є і *проблема актуальності нормативних актів*. Багато організацій використовують застарілі документи через відсутність чітких механізмів відстеження змін у нормативній базі. Це не лише знижує ефективність впроваджених систем кібербезпеки, але й створює ризики порушення законодавства або невідповідності міжнародним стандартам.

Крім того, *недостатня деталізація вимог з урахуванням специфіки водного транспорту* є суттєвим бар’єром для практичного впровадження кіберзахисту. Загальні положення законів і постанов не завжди відповідають реальним умовам роботи суден, портів чи транспортно-логістичних хабів.

Враховуючи вищезазначене, виникає необхідність у створенні спеціалізованої, автоматизованої бази даних, яка б виконувала функції:

- сховища актуальних нормативно-правових актів;
- інструмента фільтрації та пошуку документів за типом, датою, органом прийняття, сферою дії тощо;
- аналітичного засобу, що дозволяє формувати звіти, здійснювати аудит відповідності, будувати інформаційні моделі взаємозв’язків між документами;
- системи підтримки прийняття рішень для спеціалістів з кібербезпеки та керівників транспортних підприємств.

Такий підхід дозволить впорядкувати інформацію, зменшити дублювання, уникнути використання застарілих даних та забезпечити простий доступ до нормативної бази для фахівців галузі. Це особливо важливо в умовах інтенсивної цифрової трансформації транспорту, де безпечне управління інформацією є критично важливим фактором.

У результаті, створення централізованої та структурованої бази нормативно-правових документів із можливістю гнучкого пошуку та оновлення стане важливим кроком до підвищення ефективності управління інформаційною безпекою у галузі водного транспорту.

2 АНАЛІЗ ХАРАКТЕРИСТИК НОРМАТИВНО–ПРАВОВИХ ДОКУМЕНТІВ ТА ПРИКЛАДИ ЇХ СТРУКТУРУВАННЯ

2.1 Необхідність структурованого представлення нормативних документів

У процесі створення ефективної системи управління інформаційною безпекою у галузі водного транспорту особливе значення має доступ до актуальних, точних і систематизованих нормативно-правових документів. Враховуючи, що водний транспорт є частиною критичної інфраструктури, а його функціонування тісно пов’язане з використанням складних інформаційно-телекомунікаційних систем, вимоги до нормативного забезпечення мають бути не лише суворими, а й оперативно доступними для фахівців. Однак, на практиці більшість нормативних актів подані у вигляді документів різних форматів — PDF-файлів, сканованих копій, веб-сторінок — без уніфікованої структури. Це ускладнює їх пошук, аналіз, перевірку актуальності та практичне використання.

Нормативні акти, що стосуються кібербезпеки, часто дублюються, змінюються, замінюють одне одного або мають різний ступінь обов’язковості (наприклад, рекомендації міжнародних організацій, постанови уряду, внутрішні політики підприємств). В умовах такого нормативного розмаїття виникає потреба у структурованому представленні інформації про документи, що дозволить систематизувати нормативну базу, зробити її доступною для обробки, пошуку, фільтрації та оновлення.

Під структурованим представленням розуміють опис кожного нормативно-правового документа за чітко визначеним набором атрибутів: назва, тип документа, дата прийняття, орган-розробник, галузь застосування, рівень дії, статус чинності, ключові слова, посилання на джерело тощо. Такий підхід дозволяє уніфікувати подання різнорідної нормативної інформації та

забезпечити технічну можливість її інтеграції в електронні системи — наприклад, у базу даних або інформаційний портал.

Переваги структурованого представлення полягають у можливості автоматизованого пошуку документів за різними критеріями, фільтрації за тематикою, генерації звітів для аудиту чи перевірки відповідності, а також у забезпеченні актуальності інформації завдяки відстеженню дати останнього оновлення або втрати чинності документа. Для галузі водного транспорту це особливо важливо, оскільки тут діють як національні, так і міжнародні вимоги, стандарти і процедури, що потребують гармонізації та узгодженості.

Крім того, структуризація дозволяє формалізувати взаємозв'язки між документами: наприклад, вказати, який наказ реалізує норми певного закону, або який стандарт замінює попередній. Це значно полегшує орієнтацію у нормативній базі як для фахівців служби інформаційної безпеки, так і для керівництва підприємств, державних регуляторів або зовнішніх аудиторів.

Таким чином, структуроване представлення нормативно-правових документів є не просто зручним інструментом, а необхідною умовою для створення ефективної, живої та динамічної бази знань, що забезпечує повноцінне функціонування системи кібербезпеки у водному транспорті. Саме тому на наступному етапі дослідження визначаються конкретні характеристики, які будуть включені до бази даних для кожного документа, з метою побудови її логічної структури та забезпечення зручного інтерфейсу взаємодії з користувачем.

2.2 Основні характеристики нормативно–правових документів

Для створення ефективної бази даних нормативно-правових документів, що стосуються кібербезпеки у сфері водного транспорту, необхідно визначити перелік ключових характеристик, які мають описувати кожен документ. Ці характеристики становлять основу структури бази даних і формують

уніфікований підхід до зберігання, обробки та аналізу інформації. Вони дозволяють не лише здійснювати пошук документів, але й підтримувати систему у актуальному стані, виявляти взаємозв’язки між документами, класифікувати їх за призначенням, сферою дії, джерелом походження тощо.

Основні характеристики нормативного документа мають відображати як його формальні (адміністративні), так і змістовні (тематичні, прикладні) параметри. До таких характеристик відносяться:

− Назва документа — повна офіційна назва відповідно до первинного джерела або реєстраційного запису. Це дозволяє точно ідентифікувати документ та уникнути плутанини з подібними за змістом актами.

− Тип документа — вказує на юридичний або організаційний формат документа: закон, постанова, наказ, стандарт, інструкція, рекомендація, циркуляр тощо. Це дозволяє автоматично визначати його місце у нормативній ієрархії.

− Дата прийняття — офіційна дата затвердження чи публікації документа. Поле є важливим для аналізу актуальності та хронології нормативного розвитку.

− Номер документа — реєстраційний або внутрішній номер, який часто використовується в посиланнях та судовій або адміністративній практиці.

− Орган-розробник або видавець — юридична особа чи орган влади, який створив або затвердив документ (наприклад, Верховна Рада України, Кабінет Міністрів, ISO, IMO, Мінінфраструктури). Ця інформація дозволяє розподілити документи за джерелами авторитетності.

− Рівень дії — визначає масштаб застосування документа: міжнародний (наприклад, IMO), національний (закон України), галузевий (наказ МІУ), локальний (внутрішня політика компанії).

− Сфера застосування — галузевий або функціональний контекст, до якого належить документ (морський транспорт, портові комплекси, логістика, SCADA-системи тощо).

− Актуальність документа — вказує, чи є документ чинним, втратив чинність, чи перебуває на стадії проєкту або замінений новим. Це дозволяє уникнути використання застарілої інформації.

− Ключові слова — короткий перелік тем, понять або термінів, що характеризують зміст документа. Це забезпечує тематичну індексацію та зручність пошуку.

− Посилання на джерело — URL-адреса офіційної публікації документа, або інше джерело (наприклад, завантаження PDF). Це необхідно для швидкого доступу до повного тексту документа.

− Мова документа — вказує мовну версію: українська, англійська чи інша. У багатьох випадках важливо мати обидва варіанти (наприклад, для міжнародних актів).

− Короткий опис (анотація) — стисла характеристика змісту документа, яка дозволяє ознайомитися з його призначенням без повного читання.

Окрім основних полів, для підвищення інформативності бази даних можуть бути введені також додаткові мета-характеристики. Серед них особливу цінність мають:

− Підпорядкування (група документів) — дає змогу відстежити, чи належить документ до певної нормативної групи або стандарту (наприклад, входить до серії ISO/IEC 27000).

− Пов’язані документи — дозволяє фіксувати відношення між актами: наприклад, реалізація, скасування, заміна, дублювання.

− Стан документа — уточнює етап життєвого циклу: чинний, застарілий, розробляється, очікує набуття чинності.

Таке розширене поле характеристик дозволяє створити не просто електронний реєстр нормативної документації, а повноцінну інформаційну модель нормативно-правового середовища у сфері кібербезпеки водного транспорту.

З практичної точки зору, саме ці характеристики будуть покладені в основу структури таблиць реляційної бази даних у наступному етапі розробки.

Вони також формуватимуть шаблон для введення нових документів, забезпечать гнучкий пошук, фільтрацію, формування звітів і інтеграцію з іншими системами.

2.3 Аналіз документів за характеристиками

Щоб продемонструвати застосування запропонованої структури опису нормативно-правових документів, доцільно навести приклади конкретних актів, що регулюють кібербезпеку у сфері водного транспорту, із заповненням усіх ключових характеристик. Такі приклади дозволяють оцінити ефективність моделі метаданих та підтверджують її практичну придатність для впровадження в базі даних.

Першим прикладом буде Закон України «Про кібербезпеку», який є основоположним національним документом у сфері захисту інформації та критичної інфраструктури. Його характеристика за запропонованою моделлю наведена в таблицях 2.1.

Таблиця 2.1 Перший приклад характеристики для документа

Характеристика	Документ
Назва документа	Закон України «Про кібербезпеку»
Тип	Закон
Дата прийняття	02 жовтня 1992 року
Номер документа	№2657-XII
Орган-розробник/ видавець	Верховна Рада України
Рівень дії	Національний
Сфера застосування	Уся територія України, усі сфери діяльності, пов’язані з обробкою, захистом, поширенням інформації
Актуальність документа	Чинний; з останніми змінами від 19.04.2024
Ключові слова	Інформація, доступ до інформації, публічна інформація, конфіденційна інформація, право на інформацію
Посилання на джерело	https://zakon.rada.gov.ua/laws/main/2657-12#Text

Продовження таблиці 2.1

Характеристика	Документ
Мова документа	Українська
Короткий опис	Закон визначає загальні правові основи інформаційних відносин в Україні, встановлює права і обов'язки суб'єктів інформаційної діяльності, принципи доступу до інформації, механізми захисту інформації, а також порядок класифікації даних за режимами доступу.

Другий приклад — міжнародний стандарт ISO/IEC 27001:2022, який регламентує вимоги до системи управління інформаційною безпекою (табл. 2.2).

Таблиця 2.2 Другий приклад характеристики для документа

Характеристика	Документ
Назва документа	ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements
Тип	Міжнародний стандарт
Дата прийняття	25 жовтня 2022 року
Номер документа	ISO/IEC 27001:2022
Орган-розробник/ видавець	ISO/IEC JTC 1/SC 27
Рівень дії	Міжнародний
Сфера застосування	Інформаційна безпека організацій будь-якої галузі, включно з водним транспортом
Актуальність документа	Чинний; організації повинні завершити перехід з версії 2013 до 2022 до 31 жовтня 2025 року
Ключові слова	ISMS, кібербезпека, захист даних, аудит, сертифікація; нова редакція включає оновлену структуру, зменшену кількість контролів (93 замість 114), нові атрибути та розширену класифікацію
Посилання на джерело	https://www.iso.org/standard/27001
Мова документа	Англійська (доступні переклади, наприклад EN ISO/IEC 27001:2023)
Короткий опис	Встановлює вимоги до створення, впровадження та підтримування СУІБ з акцентом на кібербезпеку та захист приватності. У новій версії оптимізовано структуру на основі «Annex SL», зроблено акцент на

Продовження таблиці 2.2

Характеристика	Документ
	процесному підході та додано нові засоби контролю для сучасних загроз.

Ще одним важливим прикладом є циркуляр MSC-FAL.1/Circ.3, виданий Міжнародною морською організацією (IMO), який регламентує управління кіберризиками на суднах (табл. 2.3).

Таблиця 2.3 – Третій приклад характеристики для документа

Характеристика	Документ
Назва документа	MSC-FAL.1/Circ.3 — Guidelines on Maritime Cyber Risk Management
Тип	Рекомендаційний циркуляр
Дата прийняття	4 квітня 2025 року
Номер документа	MSC-FAL.1/Circ.3/Rev.3
Орган-розробник/ видавець	IMO (Facilitation and Maritime Safety Committees)
Рівень дії	Міжнародний
Сфера застосування	Морський транспорт — судна, порти, оператори морських систем
Актуальність документа	Чинний; це третя редакція циркуляру, що оновлює попередні версії (включно з Rev.2 2023 року)
Ключові слова	Кіберризики, судна, ISM-кодекс, кібербезпека, нормативна гармонізація; містить функціональні вимоги та рекомендації, адаптовані під сучасні загрози та технології
Посилання на джерело	(PDF на сайті IMO: MSC-FAL.1/Circ.3/Rev.3)
Мова документа	Англійська
Короткий опис	Представляє оновлені вимоги щодо управління кіберризиками у судновому секторі — включно з рекомендаціями щодо інтеграції кібербезпеки у ISM-системи управління безпекою суден, засновані на кращих практиках і сучасних технологічних викликах. Rev. 3 оновлено з урахуванням нових підходів, NIST-2.0 та посилань на IACS UR E26/E27.

3 РОЗРОБКА БАЗИ ДАНИХ НОРМАТИВНО–ПРАВОВИХ АКТІВ І СТРУКТУР ЗАПИТІВ

3.1 Аналіз функціоналу пошукової системи як приклад для моделювання бази даних

На першому етапі проектування бази даних доцільно вивчити існуючі приклади систем, що вже реалізують подібну функціональність — зокрема пошук, фільтрацію та перегляд нормативно-правових документів. Однією з найпоказовіших у цьому контексті є офіційна пошукова система порталу Верховної Ради України (*https://zakon.rada.gov.ua*), яка дозволяє користувачам здійснювати розширений пошук документів за реквізитами.

На рис. 3.1 зображено інтерфейс цієї пошукової системи. Він включає низку ключових фільтрів, які реалізують логіку доступу до документів на основі структурованих атрибутів. Зокрема, система дозволяє користувачу:

− здійснювати повнотекстовий пошук за словами або фразами (в назві, тексті чи абзаці). При цьому після виконання пошуку користувачу повідомляється загальна кількість виявлених фрагментів тексту, і на кожний фрагмент утворюється гіперпосилання, що дозволяє переходити послідовно від одного знайденого фрагмента до іншого;

− фільтрувати документи за видавником (органом влади, який прийняв цей акт);

− обирати тип документа (закон, кодекс, постанова, наказ тощо);

− задавати дату прийняття або період дії документа;

− фільтрувати за станом документа (чинний, втратив чинність, скасований тощо);

− уточнювати пошук за реєстраційними номерами;

− активувати опцію сортування або пошуку лише з термінологічною складовою.

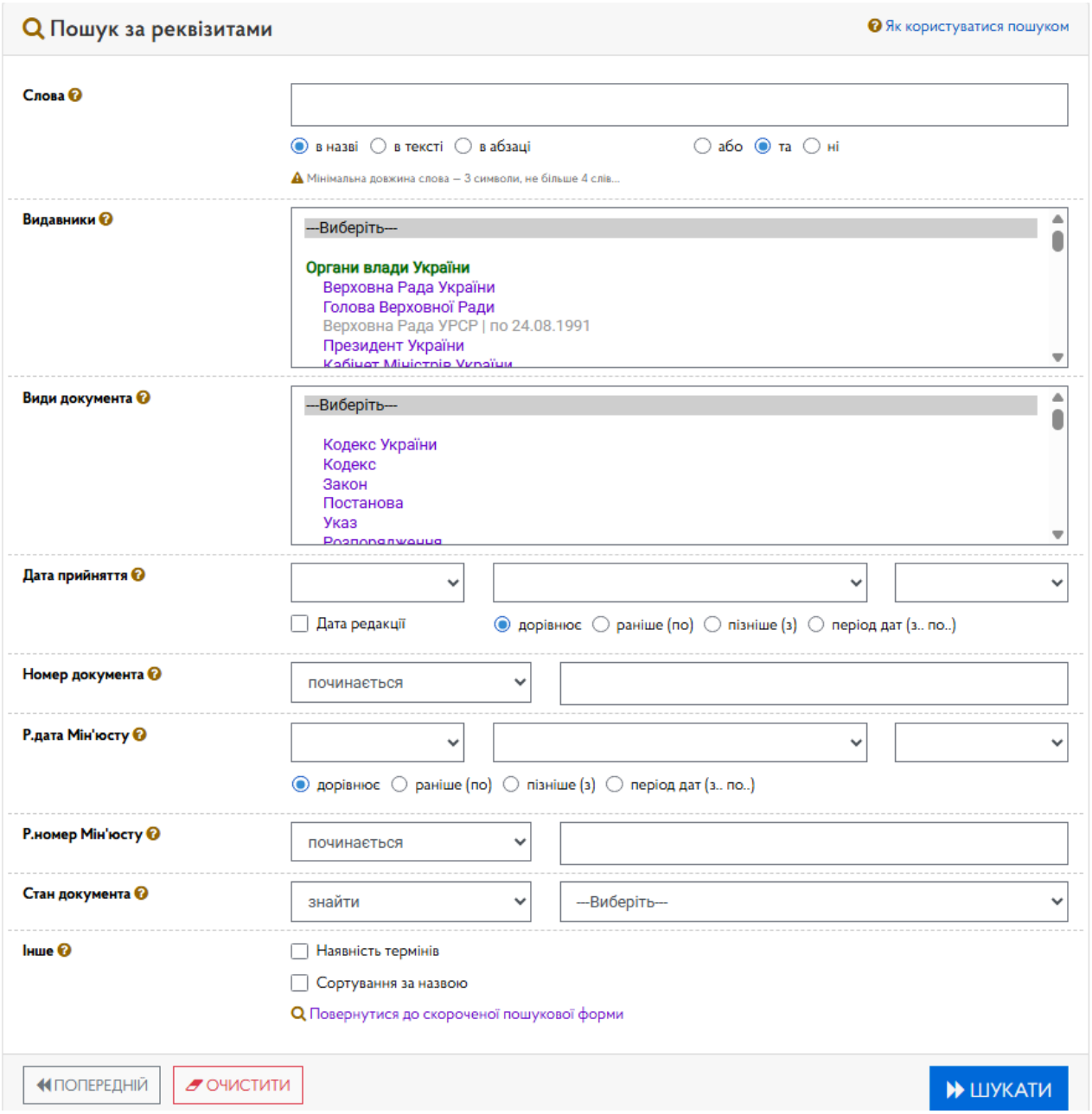


Рисунок 3.1 – Пошукова система порталу Верховної Ради України

3.2 Аналіз інтерфейсу документа та функціональних елементів перегляду

Наступним прикладом, що демонструє можливості ефективного доступу до нормативної інформації, є функціональний інтерфейс перегляду тексту документа на порталі Верховної Ради України. Цей інтерфейс з'являється після вибору конкретного документа з результатів пошуку (рис. 3.2) та реалізує набір зручних інструментів взаємодії з нормативним текстом.

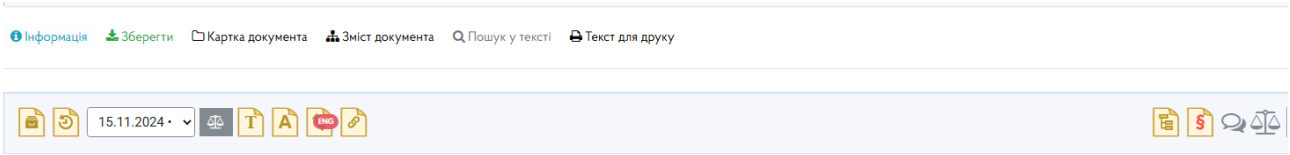


Рисунок 3.2 – Функціональні кнопки навігації документа

На зображенні видно, що система пропонує ряд іконок та опцій, кожна з яких виконує специфічну функцію для роботи з документом. Їхній опис наведено нижче:

– Картка документа – відкриває зведену інформаційну сторінку, яка містить ключові атрибути документа: його тип, видавника, дату прийняття, реєстраційний номер та інші метадані. Це відповідає блоку основних характеристик у структурі бази даних.

– Редакція документа – дає доступ до історії змін: можна побачити всі редакції документа з позначенням дат та змістовних змін. Такий функціонал особливо важливий для дотримання актуальності.

– Поточна редакція – дозволяє переглянути текст документа в редакції, чинній на певну дату. Це ключова можливість для юридичного аналізу та перевірки відповідності.

– Порівняння – автоматично порівнює різні редакції документа (наприклад, чинну і попередню), виділяючи змінені фрагменти. Це дозволяє точно відстежувати правові зміни.

– Терміни – відкриває список усіх термінів, що вживаються у документі, з поясненнями та посиланнями. Такий підхід є дуже корисним для створення вбудованого глосарію в інформаційній системі.

– Анотації – подає стисле резюме документа. Це відповідає полю "Короткий опис" у запропонованій структурі бази даних.

– Переклад – відкриває англомовну версію документа (якщо вона доступна). Це важливо для документів міжнародного значення або у сфері співпраці з іноземними партнерами.

− Пов’язані документи – надає гіперпосилання на всі акти, які мають правовий або функціональний зв’язок із даним документом (наприклад, акти, які були змінені ним, або на які він посилається). Це аналог таблиці зв’язків у реляційній базі даних.

− Структура документа – відкриває зміст або заголовки розділів для швидкої навігації. Така функція корисна для роботи з великими актами (наприклад, кодексами або технічними стандартами).

− Відображення тексту на всю ширину – розширює текст документа для зручного читання.

− Коментарі – вмикає або вимикає правовий коментар до тексту (де доступно).

3.3 Розробка структури бази даних

База даних нормативно-правового забезпечення кібербезпеки у сфері водного транспорту створена на основі функціональної моделі, яка враховує особливості галузі, потреби користувачів щодо швидкого доступу до актуальної інформації та вимоги до можливості аналітичної обробки нормативних документів. Структура бази даних реалізована як інтегрована система з чітким поділом на логічні модулі, які забезпечують ефективне зберігання, пошук і аналіз документів.

У розробленій структурі бази даних (рис. 3.3) виділено чотири основні блоки: інтерфейс користувача та адміністратора, засоби обробки інформації, описи документів та допоміжна інформація. Інтерфейс користувача забезпечує доступ до основних функцій системи, включаючи формування типових запитів, перегляд документів і генерацію звітів.

Інтерфейс адміністратора надає можливість модифікації вмісту бази даних, включаючи додавання нових документів, оновлення довідників і підтримку структури записів.

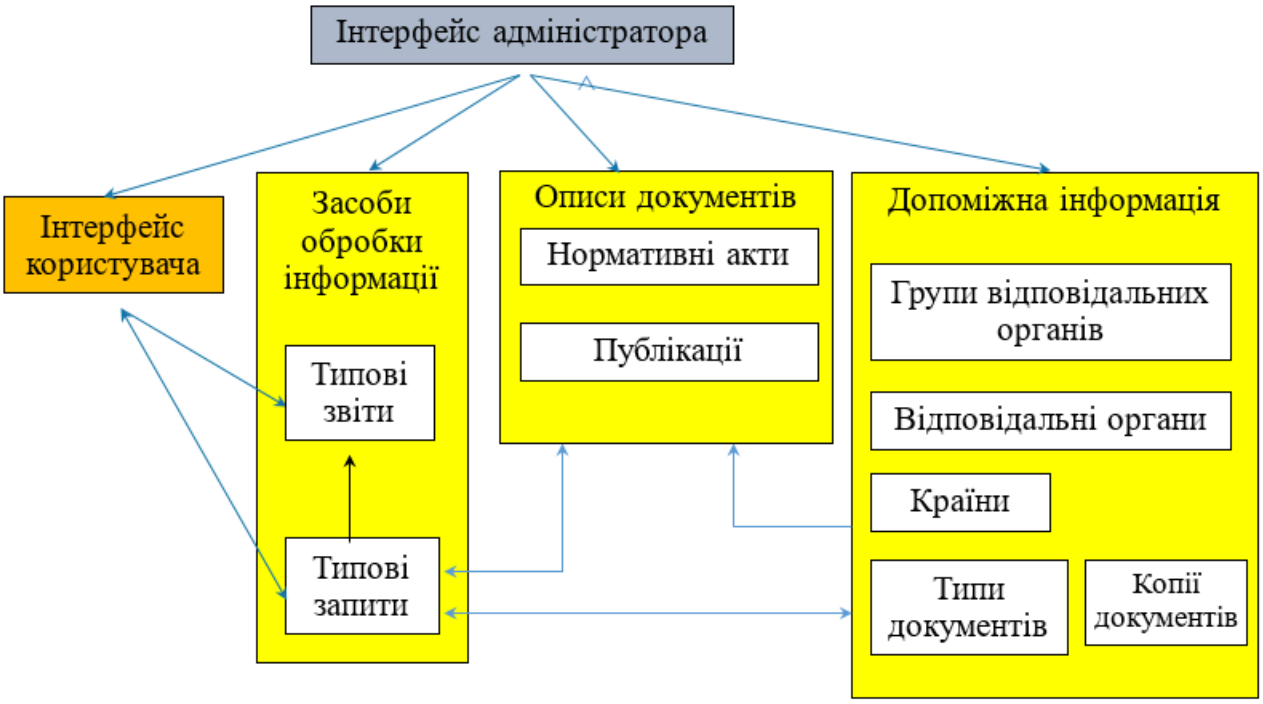


Рисунок 3.3 – Структура розроблюваної бази даних

Засоби обробки інформації включають механізми формування типових звітів на основі структурованих запитів.

Центральне місце в структурі бази займає блок описів документів. Тут зберігається інформація про нормативно-правові акти, включаючи такі параметри, як назва документа, його тип, дата прийняття, орган-розробник, рівень дії, сфера застосування, ключові слова, гіперпосилання на джерело та статус чинності. Передбачено також поле для стислої анотації змісту документа.

Допоміжна інформація представлена у вигляді окремих довідкових таблиць, таких як "Країни", "Типи документів", "Групи відповідальних органів", "Відповідальні органи", "Копії документів" тощо. Ці таблиці пов’язані з основною таблицею через зовнішні ключі, що забезпечує цілісність даних і дозволяє уникнути дублювання інформації.

Модель бази даних реалізована на основі реляційного підходу. Основна таблиця має унікальний ідентифікатор кожного запису, а всі взаємозв’язки між

таблицями побудовані відповідно до принципів нормалізації. Це дозволяє забезпечити ефективне функціонування бази, її масштабованість і зручність оновлення.

Технічно база даних реалізована у середовищі Microsoft Access, що забезпечує доступність та простоту розробки. Це середовище дозволяє створювати інтерактивні форми для введення, редагування і перегляду інформації, а також налаштувати багаторівневий доступ для адміністратора і користувачів.

4 АПРОБАЦІЯ РОЗРОБЛЕНОЇ БАЗИ ДАНИХ

4.1 Логічна структура бази даних та її реалізація

Проектування бази даних для нормативно-правового забезпечення кібербезпеки у сфері водного транспорту розпочалося з аналізу інформаційних потреб майбутньої системи. На основі цих потреб було розроблено реляційну модель, яка забезпечує зручний доступ до всіх документів, їхню уніфіковану класифікацію та простоту подальшого розширення (рис. 4.1).

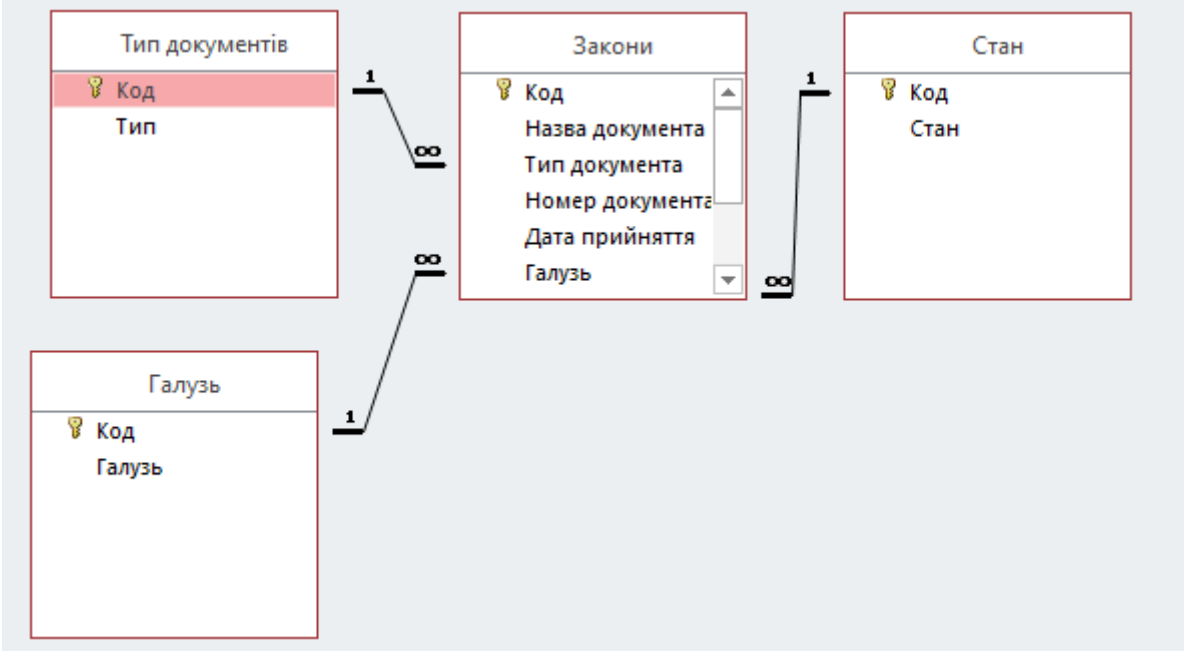


Рисунок 4.1 – Реляційна схема структури БД

Логічна структура бази даних реалізована за допомогою чотирьох таблиць: «Закони», «Галузь», «Тип документів» та «Стан», між якими встановлено зв’язки типу «один-до-багатьох». Така структура унеможливлює дублювання інформації та забезпечує цілісність збережених даних.

Головна таблиця — **«Закони»** — містить повний набір атрибутів для кожного нормативного акта: унікальний код запису, офіційну назву документа,

тип акта, його номер, дату прийняття, галузь застосування та поточний стан. Поля «Тип документа», «Галузь» і «Стан документа» реалізовані як зовнішні ключі, що посилаються на однойменні довідкові таблиці. Такий підхід дозволяє уніфікувати значення кожного поля, спрощує оновлення бази та гарантує логічність зв'язків: у кожному записі використовується лише один із попередньо заданих типів, галузей або станів.

Довідкова таблиця **«Галузь»** використовується для групування документів за сферами застосування — наприклад, «Транспорт», «Кібербезпека», «Інформаційна сфера», «Критична інфраструктура» — і містить унікальний код та текстове значення для кожного запису. Таблиця **«Тип документів»** виконує аналогічну функцію для класифікації документів за видом (Закон, Наказ, Постанова, Указ, Інструкція), а таблиця **«Стан»** — для визначення статусу кожного акта (Чинний, Втратив чинність, Розробляється, Тимчасовий). Завдяки цьому в таблиці «Закони» містяться тільки посилання на ці довідники, а всі текстові значення зберігаються централізовано й стандартизовано.

Така структура бази даних має кілька важливих переваг. По-перше, використання зовнішніх ключів гарантує цілісність посилань і виключає можливість внесення некоректного або неузгодженого значення типу, галузі чи статусу. По-друге, оновлення довідкових таблиць (наприклад, при додаванні нового типу документа або при зміні статусу чинності) одразу відображається у всій базі без необхідності редагувати кожний окремий запис. По-третє, нормалізована структура спрощує побудову вибірок, звітів і аналітичних запитів — наприклад, можна легко отримати перелік усіх чинних законів у сфері кібербезпеки або всі акти, що стосуються водного транспорту.

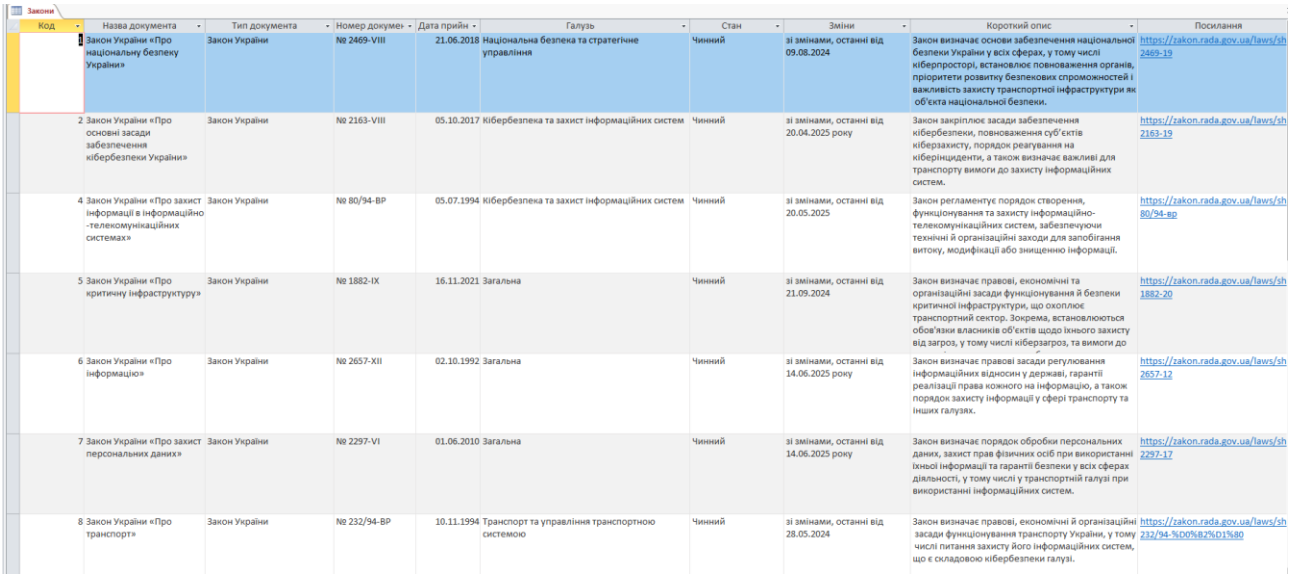
Практична реалізація цієї схеми у MS Access передбачає створення чотирьох таблиць із зазначеними полями, встановлення цілісних зв'язків у конструкторі схеми даних, а також розробку зручних форм для введення й редагування інформації. Форми забезпечують користувачу можливість обирати тип документа, галузь і стан із випадаючих списків, що значно спрощує роботу

та запобігає появі помилок. Створення запитів на вибірку дозволяє формувати аналітичні вибірки — наприклад, переглядати лише чинні акти або аналізувати розподіл документів за сферами. Таким чином, розроблена логічна структура бази даних не лише відповідає потребам системи нормативно-правового забезпечення кібербезпеки у сфері водного транспорту, а й створює міцний фундамент для подальшого масштабування й інтеграції системи з іншими модулями управління безпекою.

4.2 Заповнення бази даних текстовими документами

Після розробки логічної структури бази даних важливим етапом є її практичне наповнення тестовими записами. Цей процес дозволяє перевірити правильність реалізації зв’язків, зручність роботи користувачів при введенні даних, а також готовність системи до експлуатації. Заповнення бази даних розпочиналося зі створення й оновлення довідкових таблиць «Галузь», «Тип документів» і «Стан», які містять перелік можливих значень для кожного з цих атрибутів, що гарантувало коректність подальшого пошуку й класифікації.

Після цього було наповнено головну таблицю «Закони» (рис. 4.2) тестовими прикладами документів, обраними для демонстрації можливостей системи. Серед них — чинні закони України, що безпосередньо стосуються кібербезпеки, критичної інфраструктури, інформації та її захисту, транспорту. Кожний запис містить повний набір характеристик: унікальний код, повна назва документа, його тип, номер, дату ухвалення, сферу застосування й поточний статус. Зокрема, було додано такі акти, як Закон України «Про кібербезпеку», Закон України «Про транспорт», Закон України «Про критичну інфраструктуру» та низку галузевих постанов і наказів, що регулюють безпеку водного транспорту й інформаційних систем управління.



Закони

Код	Назва документа	Тип документа	Номер докуме	Дата прийн	Галузь	Стан	Зміни	Короткий опис	Посилання
1	Закон України «Про національну безпеку України»	Закон України	№ 2469-VIII	21.06.2018	Національна безпека та стратегічне управління	Чинний	зі змінами, останні від 09.08.2024	Закон визначає основи забезпечення національної безпеки України у всіх сферах, у тому числі кіберпросторі, встановлює повноваження органів, пріоритети розвитку безпекових спроможностей і важливість захисту транспортної інфраструктури як об'єкта національної безпеки.	https://zakon.rada.gov.ua/laws/sh2469-19
2	Закон України «Про основні засади забезпечення кібербезпеки України»	Закон України	№ 2163-VIII	05.10.2017	Кібербезпека та захист інформаційних систем	Чинний	зі змінами, останні від 20.04.2025 року	Закон закріплює засади забезпечення кібербезпеки, повноваження суб'єктів кіберзахисту, порядок реагування на кіберінциденти, а також визначає важливі для транспорту вимоги до захисту інформаційних систем.	https://zakon.rada.gov.ua/laws/sh2163-19
4	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»	Закон України	№ 80/94-ВР	05.07.1994	Кібербезпека та захист інформаційних систем	Чинний	зі змінами, останні від 20.05.2025	Закон регламентує порядок створення, функціонування та захисту інформаційно-телекомунікаційних систем, забезпечуючи технічні й організаційні заходи для запобігання витоку, модифікації або знищенню інформації.	https://zakon.rada.gov.ua/laws/sh80/94-вр
5	Закон України «Про критичну інфраструктуру»	Закон України	№ 1882-IX	16.11.2021	Загальна	Чинний	зі змінами, останні від 21.09.2024	Закон визначає правові, економічні та організаційні засади функціонування й безпеки критичної інфраструктури, що охоплює транспортний сектор. Зокрема, встановлюються обов'язки власників об'єктів щодо їхнього захисту від загроз, у тому числі кіберзагроз, та вимоги до	https://zakon.rada.gov.ua/laws/sh1882-20
6	Закон України «Про інформацію»	Закон України	№ 2657-XII	02.10.1992	Загальна	Чинний	зі змінами, останні від 14.06.2025 року	Закон визначає правові засади регулювання інформаційних відносин у державі, гарантії реалізації права кожного на інформацію, а також порядок захисту інформації у сфері транспорту та інших галузях.	https://zakon.rada.gov.ua/laws/sh2657-12
7	Закон України «Про захист персональних даних»	Закон України	№ 2297-VI	01.06.2010	Загальна	Чинний	зі змінами, останні від 14.06.2025 року	Закон визначає порядок обробки персональних даних, захист прав фізичних осіб при використанні їхньої інформації та гарантії безпеки у всіх сферах діяльності, у тому числі у транспортній галузі при використанні інформаційних систем.	https://zakon.rada.gov.ua/laws/sh2297-17
8	Закон України «Про транспорт»	Закон України	№ 232/94-ВР	10.11.1994	Транспорт та управління транспортною системою	Чинний	зі змінами, останні від 28.05.2024	Закон визначає правові, економічні й організаційні засади функціонування транспорту України, у тому числі питання захисту його інформаційних систем, що є складовою кібербезпеки галузі.	https://zakon.rada.gov.ua/laws/sh232/94-%D0%B2%D1%80

Рисунок 4.2 – Заповнена головна таблиця «Закони»

Для зручного управління даними у середовищі MS Access було розроблено спеціальні форми для введення й редагування записів. Користувачеві при додаванні нового документа достатньо заповнити текстові поля для назви, номера й дати прийняття документа, а для решти параметрів — вибрати готові значення зі спадних списків. Такий підхід суттєво скорочує ймовірність помилок і забезпечує повну узгодженість усіх пов’язаних таблиць. При цьому розроблені форми дозволяють швидко переглянути й оновлювати наявні записи, додаючи або змінюючи дані без необхідності безпосереднього доступу до таблиць, що підвищує зручність і безпеку експлуатації системи.

У результаті тестового наповнення було перевірено цілісність зв’язків між таблицями й правильність реалізації зовнішніх ключів: при спробі видалення значення з довідкової таблиці система попереджала користувача про наявність пов’язаних документів, а при виборі некоректного типу або статусу форма не дозволяла зберегти запис. Отримані результати апробації показали, що розроблена модель бази даних і механізми введення інформації повністю відповідають вимогам завдання, забезпечуючи логічний і безпомилковий облік нормативно-правових актів для потреб кібербезпеки у сфері водного транспорту.

У подальшому така структура легко масштабуватиметься для розширення списку документів або впровадження додаткових довідників без порушення логіки роботи системи.

4.3 Інтерфейс користувача та реалізація запитів

Одним із ключових етапів апробації розробленої бази даних стало створення інтерфейсу користувача, який забезпечує зручну взаємодію з інформаційною системою. Інтерфейс реалізовано у середовищі Microsoft Access у вигляді стартової форми з графічним оформленням та кнопками навігації, що значно полегшує роботу з базою навіть для користувачів без досвіду програмування або знань структури баз даних.

На головній формі (рис. 4.3) розміщено логотип кафедри комп'ютерних технологій та інформаційної безпеки Національного університету кораблебудування імені адмірала Макарова, а також повна назва інформаційної системи: «База даних нормативно-правового забезпечення кібербезпеки в галузі водного транспорту». Інтерфейс побудовано за принципом інтуїтивної навігації, що включає три основні кнопки:

− «Про систему» — відкриває додаткову форму з інформацією про призначення та функціональну структуру бази, що дозволяє новим користувачам швидко ознайомитися з її можливостями.

− «Про розробників» — містить анкетні відомості про авторів проєкту (прізвище, ім'я, навчальна група, керівник роботи), що важливо у контексті освітнього використання бази.

− «Вихід» — завершує роботу з базою даних, забезпечуючи стандартну функцію безпечного виходу.

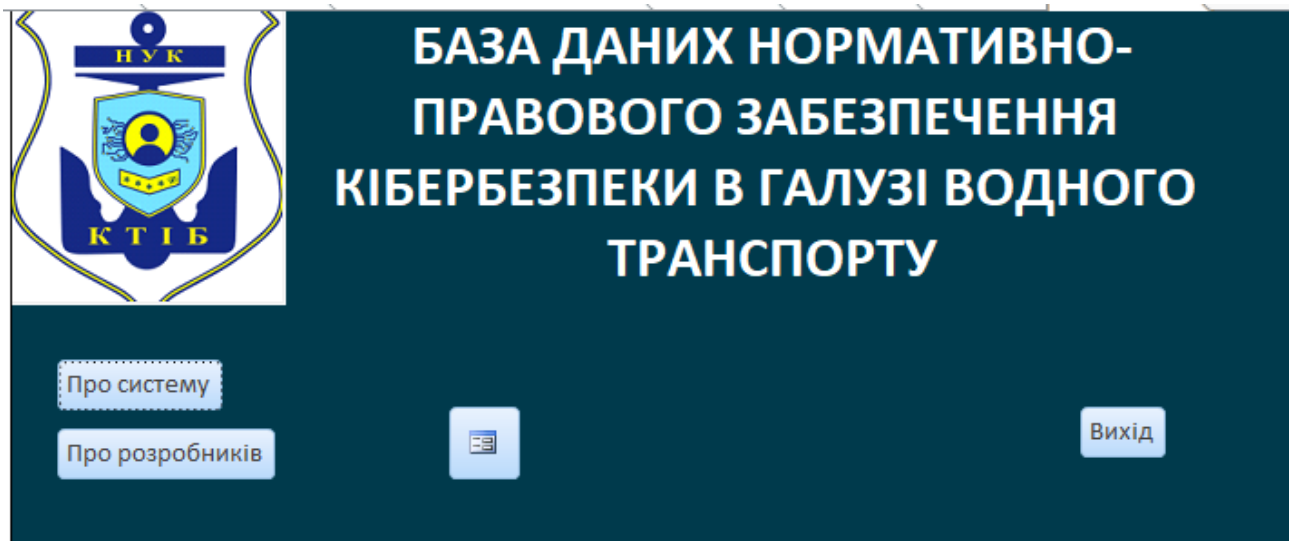


Рисунок 4.3 – Головна форма БД із кнопками доступу до основних функцій системи

Для підтримки автоматичного запуску головного меню при відкритті бази використано спеціальну форму avtoexec, яка автоматично викликає стартову форму без необхідності втручання користувача. Це підвищує зручність експлуатації та дозволяє використовувати БД у навчальному або демонстраційному режимі.

Крім навігаційної частини, у базі реалізовано приклад типового запиту, що демонструє функціонал фільтрації даних — зокрема, запит «Закони_вибірка за датою», представлений у навігаційній панелі Access (рис. 4.4).

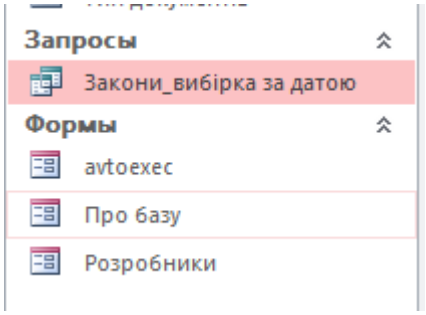


Рисунок 4.4 – Реалізований запит на вибірку документів за датою прийняття

Цей запит дозволяє здійснювати вибірку нормативно-правових актів, що були прийняті у певному році або в межах заданого діапазону дат. Такий

функціонал особливо актуальний для аналітиків, що відстежують зміни у законодавстві або планують аудит чинних актів.

Результати запиту відображаються у вигляді таблиці з фільтрованими записами з головної таблиці «Закони», включаючи назву, тип, галузь і статус документа. Це дає змогу швидко і зручно сформувати звіти за обраними критеріями, наприклад, усі чинні закони за останні 3 роки, або усі накази у сфері критичної інфраструктури.

З метою забезпечення зручності наповнення бази та її масштабування передбачено також можливість перегляду записів через табличний інтерфейс (режим «таблиці»), який дає змогу адміністраторам бази здійснювати масове оновлення або аналіз записів вручну. За потреби база може бути доповнена модулями звітів, що формуються автоматично відповідно до фільтрованих запитів (наприклад, щомісячний звіт по актуальних документах або статистика змін нормативної бази).

Таким чином, розроблений інтерфейс бази даних у Microsoft Access повністю відповідає вимогам до системи зручного, структурованого та аналітичного доступу до нормативно-правових документів у сфері кібербезпеки водного транспорту. Його архітектура дозволяє масштабування, імпорт нових даних, а також подальшу інтеграцію з зовнішніми джерелами — наприклад, порталами нормативної інформації (zakon.rada.gov.ua, imo.org) або системами електронного документообігу в транспортній галузі.

ВИСНОВКИ

В даній кваліфікаційній роботі:

− проведено аналіз відкритих літературних джерел і визначено склад бібліотеки нормативно-правових актів, чинних у галузі водного транспорту;

− визначені параметри документів, які віддзеркалені в базі даних для систематизації та ефективного пошуку інформації при вирішенні типових прикладних задач;

− розроблені інформаційні моделі для типових процесів вирішення прикладних задач за допомогою розроблюваної бази даних;

− визначені, розроблені і апробовані типові запити до розроблюваної бази даних;

− розроблена і апробована структура бази даних відкритих нормативно-правових актів в галузі водного транспорту.

Розроблена база даних нормативно-правового забезпечення кібербезпеки в галузі водного транспорту має практичне значення, оскільки результати роботи можуть бути використані:

− в навчальному процесі зі спеціальності F5 «Кібербезпека та захист інформації»;

− при проектуванні КСЗІ та СУІБ в галузі водного транспорту;

− як складова для побудови повнофункціональної системи підтримки прийняття рішень щодо забезпечення кібербезпеки та захисту інформації в галузі водного транспорту.

Дана робота була апробована на XII Всеукраїнській науково-технічній конференції з міжнародною участю “Сучасні проблеми інформаційної безпеки на транспорті” 2024 р.

ПЕРЕЛІК ПОСИЛАНЬ

1. *Cyber-attack on ShipManager servers – update. DNV. URL*: *https://www.dnv.com/news/cyber-at-tack-on-shipmanager-servers-update-237931.*

2. *Cyberattack Threatens Release of Port of Lisbon Data. The Maritime Executive. URL: https://maritime-ex-ecutive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data.*

3. *Definition of cybersecurity. International Telecommunication Union (ITU). URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.*

4. *Dimitrios D. Exploring the Issue of Technology Trends in the «Era of Digitalisation». World Maritime Day Parallel Event. At: Szczecin-Poland, 2018. URL:https://www.researchgate.net/publication/325877588_Exploring_the_Issue_of_Technology_Trends_in_the_Era_of_Digitalisation.*

5. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). O.J. L 333, 27.12.2022, p. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj*

6. *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*

7. *IACS UR E26 and E27 Press Release. URL: https://iacs.org.uk/news /iacs-ur-e26-and-e27-press-release*

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. *ISO 24060:2021 Ships and marine technology — Ship software logging system for operational technology. URL: https://www.iso.org/ru/standard/77678.html*

12. *Juan Ignacio Alcaide, Ruth Garcia Llave. Critical infrastructures cybersecurity and the maritime sector. Trans-portation Research Procedia. 2020. Vol.45. PP.547–554. URL: https://www.sciencedirect.com/science/article/pii/S2352146520302209.*

13. *Maritime Cyber Risk Report: Shipping industry remains «Easy target», pays average US $ 3.2. M in cyber-attacks. HFW. URL: https://www.hfw.com /Maritime-Cyber-Risk-Report-Shipping-Industry-Remains-Easy-Target.*

14. *MSC.*428(98). *Maritime cyber risk management in safety management systems: resolution IMO*, прийнята 16.06.2017. *URL: https://www.dohle-yachts.com/wp-content/uploads/2021/05/MSC.42898-2.pdf*

15. *MSC-FAL.1/Circ.3/Rev.2 Guidelines on maritime cyber risk management*. *URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf*

16. *NIS2 Directive | Prepare Your Organization Now. The NIS2 Directive. URL: https://nis2directive.eu*

17. *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*

18. *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*

19. *Shipping industry vulnerable to cyber attacks and GPS jamming. CNBS. URL: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html.*

20. *The Guidelines on Cyber Security Onboard Ships. Version 5 (2024). URL: https://www.maritimeglobalsecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_ cyber_security-v5-final.pdf*

21. *Xue Chenglei Design of integrated navigation for underwater vehicle with multiple sensor information fusion***.** Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2021. - С.142-147. *URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf*

22. Баронова О., Турти М., Мавроді В. Аналіз впливу загроз інформаційній безпеці на проблеми портової галузі**.** Матеріали 9-ої Міжнародної науково-технічної конференції «Інформаційні системи та технології ІСТ-2020». Харків: ХНУРЕ, 2020.

23. Божаткін С.М., Сірівчук А.С., Турти М.Ю. Аналіз ринку програмних інструментів для оцінювання ризиків інформаційної безпеки**.** Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». Миколаїв: НУК, 2022. С.79 – 90.

24. 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*

25. 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*

26. Держспецзв'язку, Київська політехніка та *USAID* посилюють кіберстійкість України у спільному проекті**.** *URL: https://www.kmu.gov.ua /news/derzhspetszviazku-kyivska-politekhnika-ta-usaid-posyliuiut-kiberstiikist-ukrainy-u-spilnomu-proekti*

27. Дзюбас Д.С. Кибербезопасность на флоте**.** Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2021. С.164-173. *URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf*

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

29. Загальні вимоги до кіберзахисту об'єктів КІ, затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. №518. *URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text*

30. Зубков А.П. Критерії прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури**.** Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2023. С.175-181. *URL: https://nuos.edu.ua /wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf*

31. Європейський Союз посилює кіберстійкість України *URL: https://eufordigital.eu/uk/european-union-strengthens-ukraines-cyber-resilience/*

32. Кібербезпека**.** *URL: https://www.usaid.gov/uk/ukraine/fact-sheets/aug-05-2022-cybersecurity*

33. Кодекс №2 від 12.12.2002 Міжнародний кодекс з охорони суден та портових засобів (Кодекс ОСПЗ) (*ISPS*). *URL: https://zakononline.com.ua /documents/show/235300___235365*

34. Кравцова О.С. Розробка системи підтримки прийняття рішень щодо методів і засобів аудиту ІТ-інфраструктури підприємства**.** Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2021. С.72-77. *URL: https://nuos. edu.ua/wp-content/ uploads / 2022 / 06 /SPIBT-2021_ materiali. pdf*

35. Методика категоризації об'єктів КІ, затверджена Постановою Кабінету міністрів України «Деякі питання об'єктів критичної інформаційної

інфраструктури» від 9 жовтня 2020 р. №1109. *URL: https://zakon.rada.gov.ua/rada/show/1109-2020-%D0%BF#*

36. Нікулін О.С. Розробка шаблону комплексної системи захисту інформації для підприємства припортової галузі**.** Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2021. С.78-83. *URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf*

37. Нормативно-правова база. Сайт Державної служби морського і внутрішнього водного транспорту та судноплавства України. *URL: https://marad.gov.ua/ua/diyalnist/normativno-pravova-baza*

38. Основні завдання. Сайт Державної служби морського і внутрішнього водного транспорту та судноплавства України. *URL:* https://marad.gov.ua/ua/pro-sluzhbu/misiya-ta-strategiya

39. 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*

40. Положення про систему управління безпекою судноплавства на морському і річковому транспорті, затверджене Наказом Міністерства транспорту України №904 від 20.11.2003. *URL: https://zakon.rada.gov.ua/laws/show/z1193-03#n16*

41. Порядок формування переліку об’єктів критичної інформаційної інфраструктури, затверджений Постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 943. *URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n16*

42. Про внесення змін до Постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. Постанова Кабінету міністрів України №48 від 16 січня 2024 р. *URL: https://zakon.rada.gov.ua/laws/show/48-2024-%D0%BF#Text*

43. Про внутрішній водний транспорт. Закон України *URL: https://zakon.rada.gov.ua/laws/show/1054-20#n125*

44. Про затвердження переліку внутрішніх морських вод і внутрішніх водних шляхів, віднесених до категорії судноплавних. Постанова Кабінету Міністрів України від 9 лютого 2022 р. № 136. *URL: https://zakon.rada.gov.ua/laws/show/136-2022-%D0%BF#Text*

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

46. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України. Розпорядження № 1163-р Кабінету міністрів України від 19 грудня 2023 р. *URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text*

47. Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року. *URL: https://zakon.rada.gov.ua /rada/show/984_013-16#*

48. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. Директива Ради 2008/114/ЄС від 08 грудня 2008 року. *URL: https://zakon.rada.gov.ua/ rada/ show/984_002-08#n4*

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

50. Про ліцензування видів господарської діяльності: Закон України. *URL: https://zakon.rada.gov.ua/laws/show/222-19?find=1&text=%D1%82%D1% 80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82#w1_22*

51. Про основні засади забезпечення кібербезпеки України: Закон України. *URL: https://zakon.rada.gov.ua/laws/show/2163-19*

52. Про схвалення Національної транспортної стратегії України на період до 2030 року. Розпорядження Кабінету Міністрів України від 30 травня 2018 р.

№ 430-р. *URL: https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80?find=1&text=%D0%BA%D1%96%D0%B1%D0%B5%D1%80#w1_1*

53. Про транспорт: Закон України. *URL*: *https://zakon.rada.gov.ua /laws/show/232/94-%D0%B2%D1%80#Text*

54. Садалюк Є.О. Наслідки *DDoS*-атак на водний транспорт**.** Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2023. С.215-217. *URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf*

55. Система управління якістю. Сайт Державної служби морського і внутрішнього водного транспорту та судноплавства України. *URL: https://marad.gov.ua/ua/pro-sluzhbu/sistema-upravlinnya-yakistyu*

56. Стратегія кібербезпеки України. *URL: https://zakon.rada.gov. ua/ laws/show/447/2021#n98*

57. Структура служби. Сайт Державної служби морського і внутрішнього водного транспорту та судноплавства України. *URL: https://marad.gov.ua /ua/pro-sluzhbu/struktura-sluzhbi.*

58. 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*

59. 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.*