Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

X ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

13-14 грудня 2022 р.

Миколаїв ■ НУК ■ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2022

МАТЕРІАЛИ

X Всеукраїнської науково-технічної конференції з міжнародною участю

13–14 грудня 2022 року

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

МИКОЛАЇВ • НУК • 2022

УДК 004
У 45

ОРГАНІЗАТОРИ:

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

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2022. – 209 с.

У збірнику подано матеріали X 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

ранжуванням загроз //Реєстрація, зберігання і обробка даних. – 2020. – Т. 22. – № 2. – С.63-76. URL: http://drsp.ipri.kiev.ua/article/view/211279

4. Шандрівська О. Є., Шинкаренко Н. В. Прикладна оцінка ризиків у системі забезпечення безпеки соціально-економічних процесів у кіберпросторі //Вісник Національного університету "Львівська політехніка". Серія "Проблеми економіки та управління". – 2020. – №2(8). – С.94-104.

5. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. – К.: ДУТ, 2015. – 288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

УДК 004.056.5;057.2

ІНФОРМАЦІЙНА МОДЕЛЬ КАТЕГОРИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Автори: *Турти М.В., к.т.н., доцент; Злочевська О.В., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Наявність у будь-якій країні критичної інфраструктури, що забезпечує життєво важливі для населення та держави послуги, без яких неможливі їх добробут і безпечне існування загалом, зумовлює актуальність питання їх захисту та стійкості до всього спектру ризиків. Забезпечення безпеки критичної інфраструктури (КІ) є складовою національної безпеки особливо в умовах загальносвітових тенденцій посилення екстремізму та тероризму, в тому числі на державному рівні, зростання організованої злочинності тощо.

Захист КІ є комплексною науковою проблемою, яка передбачає вирішення питань нормативно-правового, організаційного, технологічного та ін. забезпечення. Розвязку цієї проблеми присвячені роботи багатьох науковців [1-6], однак на даний час залишається невирішеним питання автоматизації типових процедур аналізу стану інформаційної безпеки (ІБ) на об'єктах КІ.

Метою даної роботи є розробка інформаційної моделі категоризації об'єктів критичної інфраструктури.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– провести аналіз нормативно-правової бази і визначити принципи і процедури категоризації об'єктів критичної інфраструктури (ОКІ);

– визначити вхідні та вихідні дані інформаційної моделі категоризації ОКІ;

– розробити основні алгоритми і побудувати інформаційну модель категоризації ОКІ.

Нормативно-правову базу категоризації ОКІ складають:

1. Директива Ради 2008/114/ЄС від 08 грудня 2008 року "Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту".

2. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року "Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу".

3. Закон України «Про критичну інфраструктуру».

4. Закон України «Про основні засади забезпечення кібербезпеки України».

5. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни.

6. План реалізації Стратегії кібербезпеки України.

7. Постанови КМУ

– №518 (19.06.2019): Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури;

– № 943 (9.10.2020), якою затверджені:

а) Порядок формування переліку об'єктів критичної інфраструктури;

б) Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування;

– №1109, якою затверджені:

а) Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави;

б) Порядок віднесення об'єктів до об'єктів критичної інфраструктури;

в) Методика категоризації об'єктів критичної інфраструктури;

– №821 (22.07.2022), якою затверджено: Порядок здійснення моніторингу оцінки рівня безпеки об'єктів критичної інфраструктури.

8. Наказ № 23 Адміністрації ДССЗЗІ від 15.01.2021: Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури.

Категоризація ОКІ є важливою процедурою процесу управління КІ і здійснюється поетапно. Початком категоризації можна вважати утворення робочої групи.

Робоча група утворюється в певному секторі або підсекторі, діє на постійній основі і має певні нормативні вимоги до складу групи. Завданнями для робочої групи є:

– ідентифікація ОКІ у відповідному секторі КІ;
– проведення категоризації ОКІ;
– підготовка секторального переліку ОКІ;
– подання відомостей щодо категорованих ОКІ галузі до Національного переліку ОКІ.

Згідно Директив ЄС [7, 8] кожна держава-член для своєї території створює список операторів основних послуг, що є суттєвими для підтримки критичної соціальної та/або економічної діяльності. Оцінювання послуг, що надаються суб'єктом, як критичних зводиться до перевірки наявності такої послуги в цьому списку.

Оцінювання мережевих та інформаційних систем як критичних полягає у доведенні факту залежності основної послуги, що надається суб'єктом від мережевих та інформаційних систем.

Оцінювання ступеня негативного впливу інциденту на надання послуги здійснюється з врахуванням певних міжсекторальних і секторальних чинників. Оцінка ОКІ за кожним критерієм виражається в балах (від 0 до 4). Загальна отримана сума балів нормується сумою балів, що максимально можлива для підсектора, якому належить ОКІ, і за нормованою оцінкою критичності ОКІ присвоюється одна з чотирьох категорій (I – особливо важливі об'єкти, II – життєво важливі об'єкти, III – важливі об'єкти, IV – необхідні об'єкти, або ОКІ визнається некритичним.

Узагальнений алгоритм категоризації наведено на рис.1, а, який містить процедури оцінювання за секторальними і міжсекторальними кри-

теріями. Ці процедури виконуються функціонують за однаковими алгоритмами рис.1, б, що різняться тільки кількістю критеріїв I_{max} (для міжсекторальних критеріїв I_{max} =16, а для секторальних критеріїв I_{max} =1 або I_{max} =2 в залежності від сектору).

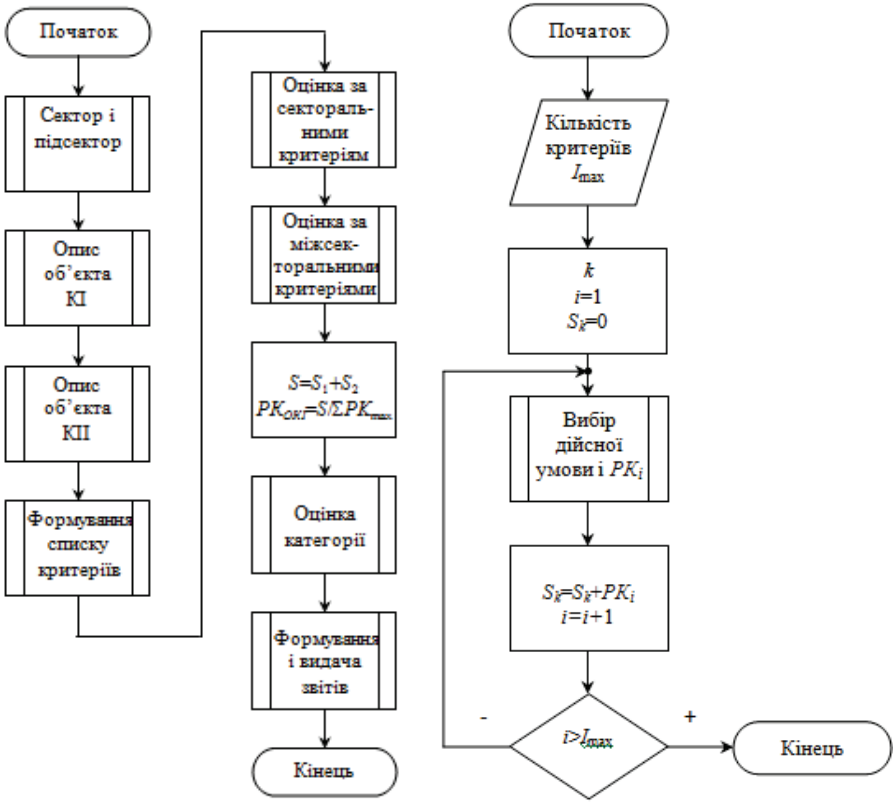

Рисунок 1 – Основні алгоритми

Структура розробленої інформаційної моделі складається з чотирьох взаємопов'язаних блоків – блоку інтерфейсу, блоку даних, блоку оцінювання і блоку формування звітності (рис.2). Блок даних представлено на рис.2 в узагальненому вигляді. Більш детальне представлен-

ня змісту вбудованих даних і даних користувача має вигляд наведений на рис.3. Вхідні дані включають не тільки інформацію, що необхідна для категоризації, а й дані для заповнення акту категоризації і форми відомостей про об'єкт категоризації для секторального переліку об'єктів критичної інфраструктури.

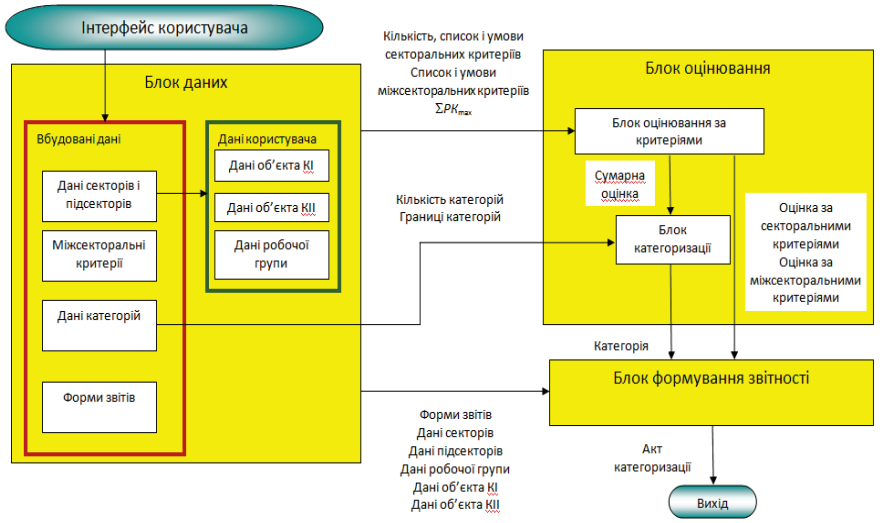

Рисунок 2 – Інформаційна модель

Апробація розробленої інформаційної моделі була здійснена шляхом реалізації основних алгоритмів в MS Access. Після визначення параметрів категоризації та оцінювання об'єкта за списком критеріїв в наведеній на рис.4 формі відображаються оцінки за секторальними критеріями, оцінки за міжсекторальними критеріями і максимальна сума балів для сектора, до якого відноситься об'єкт. Далі у формі розраховуються суми балів, що характеризують об'єкт за категоріями міжсекторальних критеріїв і загальна сума балів за всіма критеріями, і нормована оцінка критичності PK_{OKI}. Категорія визначається діапазоном значень, в який потрапляє нормована оцінка:

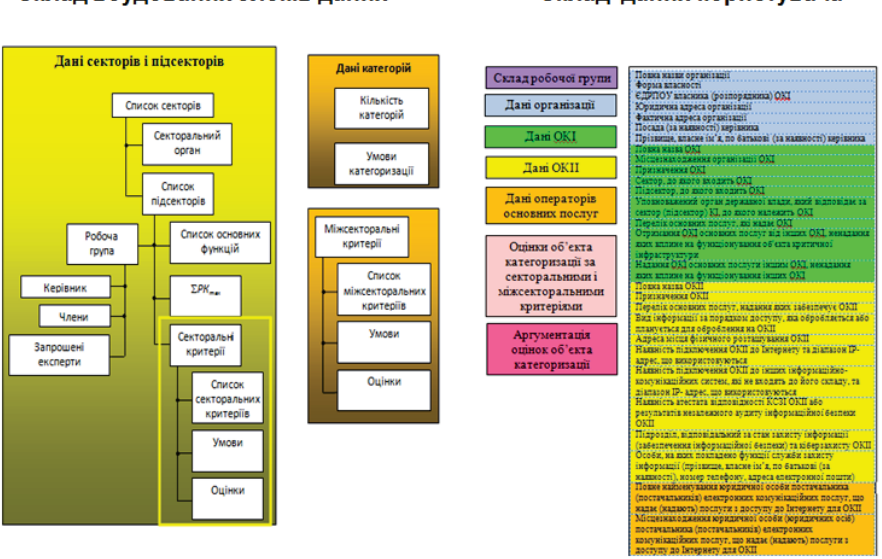

Рисунок 3 – Деталізація вхідних даних

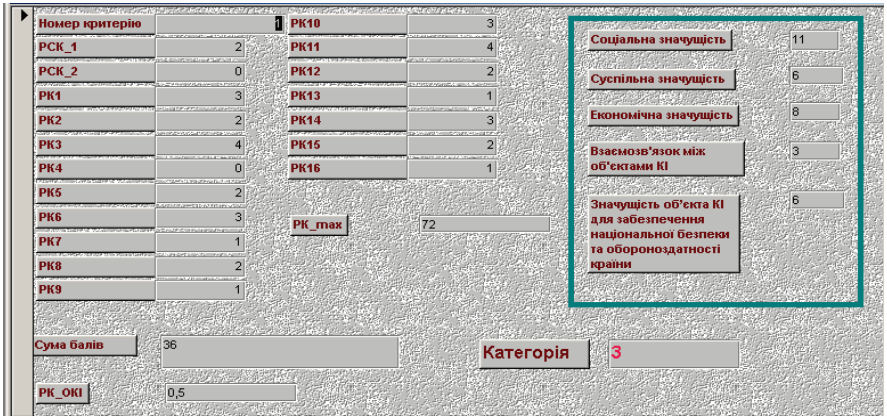

Рисунок 4 – Вихідні дані моделі

I категорія критичності: $0,8 < РК_{ОКІ} \leq 1$;
II категорія критичності: $0,63 < РК_{ОКІ} \leq 0,8$;
III категорія критичності: $0,37 < РК_{ОКІ} \leq 0,63$;
IV категорія критичності: $0,2 < РК_{ОКІ} \leq 0,37$;
об'єкт не є критичним: якщо $РК_{ОКІ} \leq 0,2$.

Висновки

В даній роботі проведено аналіз нормативно-правової бази і визначені принципи і процедури категоризації об'єктів критичної інфраструктури, вхідні та вихідні дані інформаційної моделі; арозробилені основні алгоритми і побудована та апробована інформаційна модель категоризації об'єктів критичної інфраструктури.

Список літератури:

1. Limba, Tadas, et al. "Cyber security management model for critical infrastructure." (2019). The International Journal Entrepreneurship and Sustainability Issues ISSN 2345-0282 (online) http://jssidoi.org/jesi/ 2017 Volume 4 Number 4 (June) http://doi.org/10.9770/jesi.2017.4.4(12)

2. Osei-Kyei, Robert, et al. "Critical review of the threats affecting the building of critical infrastructure resilience." International Journal of Disaster Risk Reduction 60 (2021): 102316.

3. Бірюков Д. С. Захист КІ в Україні: від наукового осмислення до розробки засад політики / Д. С. Бірюков // Науково-інформаційний вісник Академії національної безпеки. – 2015. – № 3-4. – С. 155-170. – URL: http://nbuv.gov.ua /UJRN/nivanb_2015_3-4_14.

4. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. – К.ДУТ, 2015.— 288 с. URL: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

5. Рогов П.Д., Воровичб Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: зб. наук. праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського. – 2017. – № 1. – С. 64-72. URL: http://znp-cvsd.nuou.org.ua/article/view/125525

6. Зелена книга з питань захисту КІ в Україні (друга версія проекту документа). URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf

7. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 06 липня 2019 року "Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу". URL: https://zakon.rada.gov.ua /rada/show/984_013-16#n3

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

УДК 004.056.5;057.2

ІНФОРМАЦІЙНА МОДЕЛЬ СИСТЕМИ ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ІНВЕСТИЦІЙ В ІНФОРМАЦІЙНУ БЕЗПЕКУ

Автори: *Турти М.В., к.т.н., доцент; Осипчук А.В., магістр, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Задача економічно ефективного менеджменту інформаційної безпеки (МІБ) в сучасному інформаційному суспільстві є актуальною як для великих компаній, так і для представників малого і середнього бізнесу. Порушення інформаційної безпеки великих компаній може спричинити значні матеріальні збитки, як через прямі матеріальні втрати, так і внаслідок погіршення репутації компанії.

Існує багато методик економічного обґрунтування витрат на інформаційну безпеку, розроблених вітчизняними і зарубіжними науковцями [1-8], з використанням різноманітних сукупних показників доцільності інвестицій, але на даний час рекомендації із вибору певної методики для вирішення прикладних задач і засоби підтримки прийняття рішень щодо обсягу інвестицій відсутні.

Метою даної роботи є розробка структури автоматизованої системи визначення оптимальних інвестицій в інформаційну безпеку за сукупністю критеріїв, що обираються користувачем.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2022

X Всеукраїнська науково-технічна конференція
з міжнародною участю

13–14 грудня 2022 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