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

УДК 004.056.5;057.2

ІНФОРМАЦІЙНА МОДЕЛЬ РАНЖУВАННЯ ЗАГРОЗ ЗА BS ISO/IEC 27005:2011

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

Економіка і національна безпека держави безпосередньо залежать від наявності безпечних інформаційно-комунікаційних систем (ІКС), що функціонують в кіберпросторі держави, який повинен захищатися так само, як територія країни на суші, в морі і в повітрі.

Побудова ефективної системи захисту кіберпростору і об'єктів інформаційної діяльності (ОІД) можлива тільки на основі детального аналізу сукупності можливих загроз, аналізу пов'язаних з ними ризиків і визначення їх характеристик, механізмів і наслідків впливу. Функціонування організаційно-технічної моделі кіберзахисту, положення про яку затверджене постановою Кабінету Міністрів України від 29 грудня 2021 р. №1426 [1], здійснюється з урахуванням досвіду держав – членів ЄС та НАТО та забезпечується, зокрема, шляхом розвитку систем реагування на кіберзагрози і управління ризиками інформаційної безпеки.

Метою даної роботи є розробка інформаційної моделі ранжування загроз безпеці інформації згідно вимогам міжнародного стандарту BS ISO/IEC 27005:2011.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– провести аналіз нормативно-правової бази і відкритих літературних джерел та визначити критерії класифікації загроз безпеці інформації, доцільні для застосування у даній роботі;

– провести аналіз міжнародного стандарту BS ISO/IEC 27005:2011 і визначити вхідні і вихідні дані розроблюваної інформаційної моделі ранжування загроз;

– розробити основні алгоритми і побудувати інформаційну модель ранжування загроз безпеці інформації за вимогам міжнародного стандарту BS ISO/IEC 27005:2011.

Узагальнений механізм атаки враховує класифікацію загроз інформаційним ресурсам за різними критеріями. Із всієї множини способів класифікації загроз для аналізу згідно НД ТЗІ найбільш універсальною є класифікація загроз за результатом їх впливу на властивості захищеної інформації, згідно з якою розрізняють загрози порушення конфіденційності, цілісності, доступності і спостережуваності інформації.

При аналізі загроз ІКС певного функціонального призначення часто створюють спеціальну класифікацію загроз, що відображує особливості предметної галузі. Прикладами такої класифікації є класифікація загроз безпеці державних інформаційних ресурсів [2], критичної інфраструктури [3], соціально-економічних процесів [4], загроз соціального інжинірингу [5] тощо. При створенні систем захисту іфнормації в ідеалі повинен проводитися повний аналіз всіх можливих загроз, однак, загрози за своєю сутністю не можуть бути описані скінченною множиною. Тому до множини загроз, які враховуються при аналізі, відносять тільки ті загрози, що мають ймовірність виникнення більшу за деяке задане мінімальне значення, а при побудові систем захисту – враховують тільки ті загрози, що можуть бути реалізовані через певну наявну вразливість і пов'язані із ризиком, який є більшим за задане граничне значення. При цьому загрози мають бути докладно описані відповідно прийнятій класифікації за джерелами загроз, які в свою чергу класифікуються згідно рис.1, за природою виникнення (природні (об'єктивні) загрози, створювані техногенними і стихійними джерелами, і штучні (суб'єктивні) загрози, створювані антропогенними джерелами), за видом використовуваної уразливості, за порушуваними властивостями ІзОД, за технологіями атаки та їх наслідками тощо.

Згідно ISO/IEC 27005 [2] загрози класифікуються за такими критеріями як природа виникнення і тип загроз, причому одна загроза може мати різну природу виникнення.

За природою виникнення виокремлюють: навмисні антропогенні загрози, випадкові антропогенні загрози і природні (екологічні) загрози, які охоплюють всі негативні впливи зовнішнього середовища, що є випадковими процесами і не пов'язані з діями людини.

За типом загроз в ISO/IEC 27005 загрози об'єднуються в наступні групи: фізичні пошкодження; природні події; втрата необхідних сервісів; несправності внаслідок негативного впливу випромінювання; компрометація інформації; технічні відмови; несанкціоновані дії; компрометація функцій.

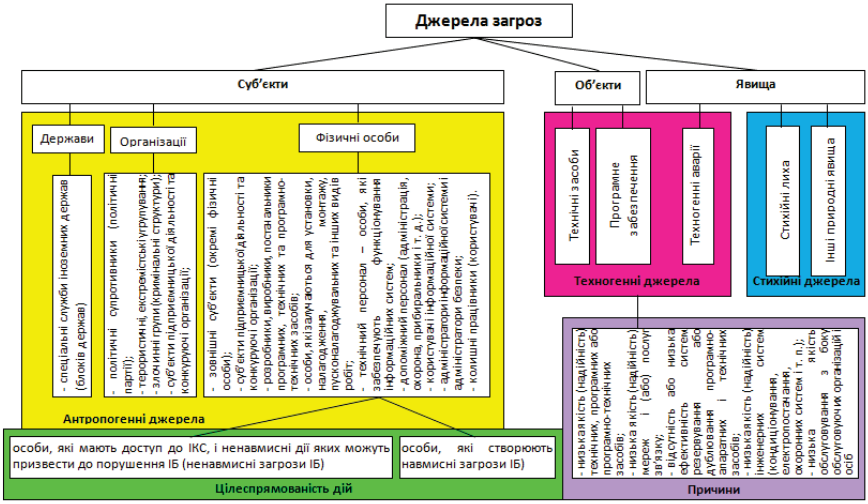

Рисунок 1 – Класифікація джерел загроз

Антропогенні загрози можут бути ініційовані зловмисниками різних типів, які мають різну мотивацію для злочинних дій, від чого залежать і наслідки успішної реалізації загроз.

Оцінювання і, відповідно, ранжування загроз за ISO/IEC 27005 здійснюється за рівнем асоційованих з ними ризиків, а оцінювання ризиків є окремим етапом менеджменту ризиків ІБ (рис.2). В процесі менеджменту ризиків після визначення контексту, ідентифікації ризиків (що включає ідентифікацію загроз) і кількісної оцінки ризику може здійснюватися оцінювання критичності загроз. Процеси обміну інформацією стосовно ризика, моніторингу та перегляду ризику супроводжуються процесами обміну інформацією стосовно загроз, моніторингу загроз та перегляду критичності загроз відповідно.

Процедура та інструменти оцінки ризиків і загроз є унікальними для кожної організації, однак, у будь-якому випадку мають бути виконані етапи, показані на рис.3.

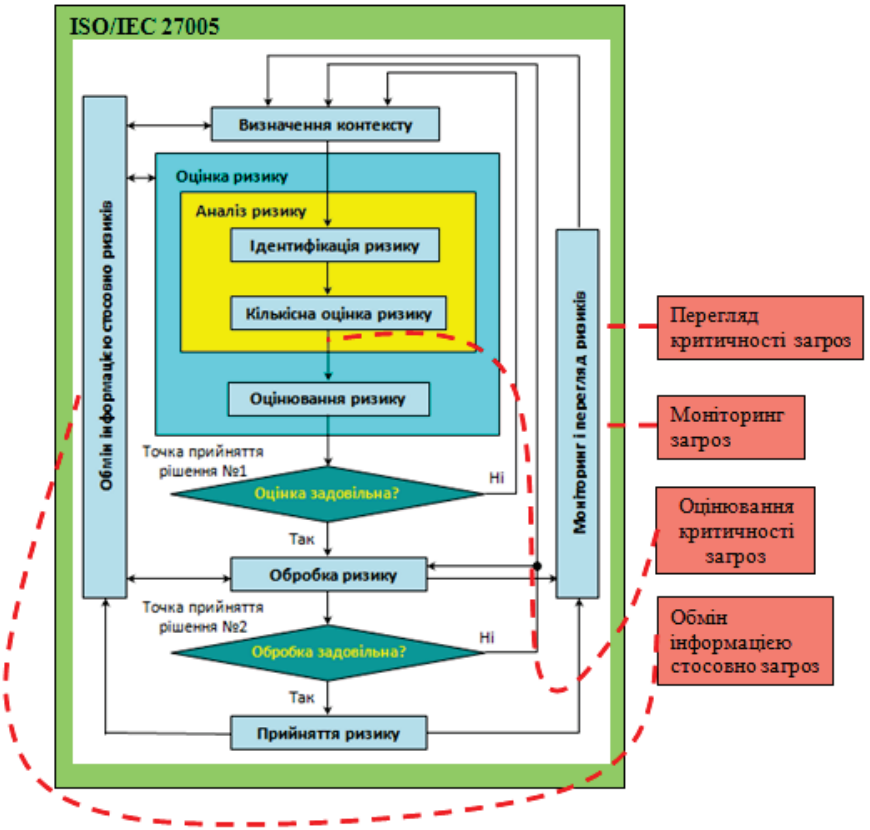

Рисунок 2 – Оцінювання загроз в ітераційному процесі менеджменту ризиків

Рисунок 3 – Етапи ранжування загроз

Ранжування загроз – це процес визначення і категоризації рівня критичності загроз. Критичність загрози визначається асоційованою з ним мірою ризику, яка може бути якісною або кількісною. Кількісні

міри можуть розраховуватися за різними формулами. В даній роботі ризик розраховується як добуток номерів рівнів цінності активу, ймовірності виникнення загрози, ймовірності реалізації загрози шляхом експлуатації певної вразливості активу, міри наслідків успішної реалізації загрози і ймовірності розвитку атаки за певним сценарієм. Інформаційні потоки в розробленій моделі наведені на рис.4.

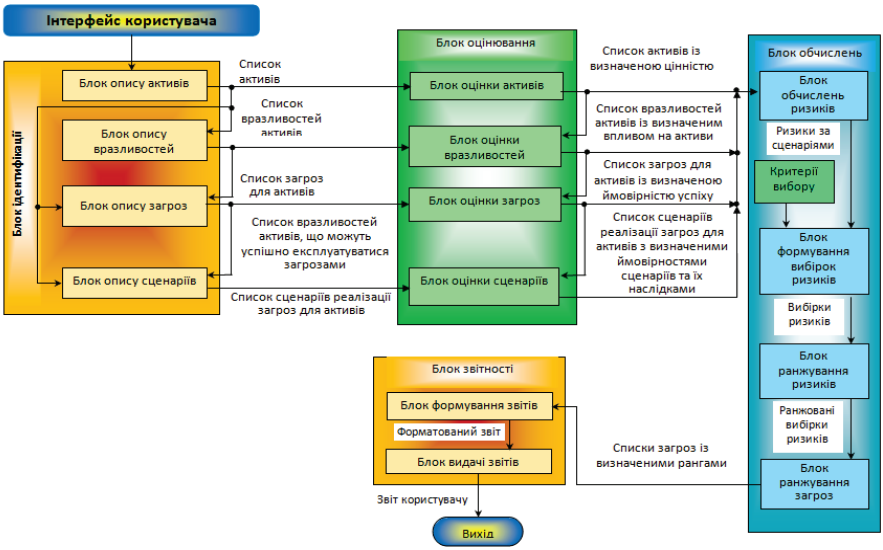

Рисунок 4. – Інформаційні потоки

Вибірка ризиків в блоці обчислень може здійснюватися за різними критеріями: спрямованістю загрози на певний актив організації чи на певну властивість ІзОД, використовуваною загрозою вразливістю, ймовірностями виникнення і успіху загрози, ступенем ймовірності сценарію тощо.

Дана інформаційна модель була апробована в якості бази даних MS Access, яка дозволяє користувачу описати об’єкт дослідження в термінах стандарту ISO/IEC 27005, визначити шкали для оцінювання вхідних і вихідних даних моделі і отримати ранги та категорії ризиків

і загроз. Форма з результатами розрахунків для одного із сценаріїв наведена на рис.5.

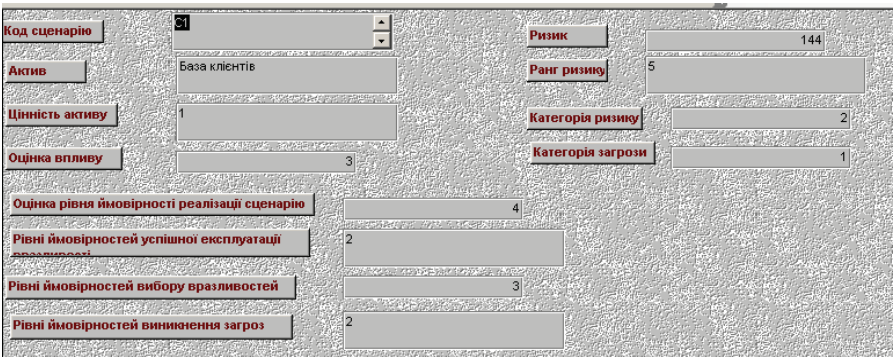

Рисунок 5. – Розрахункова форма

Висновки

В даній роботі проведено аналіз методів оптимізації інвестицій в інформаційну безпеку, визначені вхідні та вихідні дані для цих методів, особливості отримуваних результатів, критерії оптимізації інвестицій в інформаційну безпеку, а також розроблено структуру автоматизованої системи визначення оптимальних інвестицій в інформаційну безпеку за сукупністю критерієв, що обираються користувачем.

На основі проведеного аналізу нормативно-правової бази, зокрема міжнародного стандарту ISO/IEC 27005, і відкритих літературних джерел визначені критерії класифікації загроз безпеці інформації та вхідні і вихідні дані моделі, побудована і апробована інформаційна модель ранжування загроз безпеці інформації за вимогам ISO/IEC 27005:2011.

Список літератури:

1. Положення про організаційно-технічну модель кіберзахисту. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

2. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія. – К.: НАУ, 2015. – 214 с.

3. Салієва О.В., Яремчук Ю.Є. Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури

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.

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