



**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.



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

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

ОРГАНІЗАТОРИ:

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

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

Відповідальна за випуск В. В. Трибулькевич

У–45

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

У збірнику подано матеріали Х Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

© Національний університет кораблебудування
імені адмірала Макарова, 2022

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ

УДК 004.056

ОСОБЛИВОСТІ УПРАВЛІННЯ ПРОЄКТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ МОРСЬКОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Автори: Блінцов В.С., д.т.н., професор; Буруніна Ж.Ю., к. т.н., доцент Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Згідно [1] до об'єктів критичної інфраструктури держави відносяться такі об'єкти, які є стратегічно важливими для економіки і національної безпеки, а порушення їх функціонування може завдати шкоди життєво важливим національним інтересам України. Очевидно, що водна транспортна система України (у першу чергу, морський транспорт, морські шляхи, портові інженерно-технічні споруди та будівлі) відноситься до об'єктів морської критичної інфраструктури (МКІ) і повинна мати відповідну систему безпеки. Захисту потребують також акваторії територіальних вод України і прилеглих зон. Під охороною і захистом МКІ розуміють комплекс режимних, інженерних, інженерно-технічних та інших заходів, які організовуються і проводяться суб'єктами державної системи захисту об'єктів МКІ з метою запобігання та/або недопущення чи припинення протиправних дій.

Завдяки процесу інформатизації та глобалізації інформаційно-телекомунікаційних систем (ІТС) з'являються нові можливості несанкціонованого втручання в процеси обробки та передачі даних, які можуть нанести об'єктам МКІ економічні, фінансові та інші збитки.

Сучасні загрози територіальній цілісності України вимагають створення єдиної системи моніторингу надводної, підводної та повітряної обстановки у територіальному морі України, існування якої неможливе без захищеної системи передачі даних.

На цей час питання управління проєктами захисту інформації, яка генерується, обробляється, передається та використовується на об'єктах МКІ, у науково-технічній літературі висвітлені неповно. Тому визначення загроз для інформації, що циркулює в ІТС об'єктів

МКІ, а також структуризація цих загроз як основа ефективного управління проектами їх захисту, на цей час є актуальними прикладними науковими задачами.

Базисом інформаційної безпеки в ІТС об'єкта МКІ є сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації, яка в ній циркулює. Захищена ІТС об'єкту морської інфраструктури являє собою розподілену мережу, до складу якої входять такі складові: кабельні мережі; система бездротових каналів зв'язку; автоматизовані робочі місця (АРМ) керування системою; АРМ баз даних (сервери); система охоронної сигналізації та відеспостереження; система контролю доступу; система інформаційного обміну робототехнічної складової системи захисту акваторій.

Характеристики інформації, що циркулює і обробляється у зазначених складових ІТС:

- дані та програмні коди у вигляді файлів різних форматів, що містять інформацію, яка підлягає захисту: інформація про результати моніторингу підводної, надводної та повітряної обстановки; відомості про стан системи сигналізації, відеоспостереження та системи контролю доступу; алгоритми та режими роботи безпілотних апаратів; команди керування технічними засобами та управління системою та апаратними засобами моніторингу та контролю;

- технологічна інформація, яка використовується для забезпечення функціонування ІТС;

- файли комплексу засобів захисту інформації: криптоалгоритми; ключові дані; параметри налагодження системи.

Під управління проектами захисту інформації в ІТС розуміють управління процесами розробки і впровадження комплексу організаційних, нормативно-правових та матеріально-технічних заходів, спрямованих на протидію загрозам інформації, яка циркулює в ІТС.

При цьому основну загрозу інформації становлять:

- витік інформації технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень;

- несанкціоновані дії та несанкціонований доступ до інформації, які можуть здійснюватися шляхом підключення до апаратури та ліній

зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін.;

- організація спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Загрози для інформації, яка обробляється в ІТС, залежать від характеристик ІТС, складності системи, типу застосованих технічних засобів збору та обробки інформації, фізичного середовища, персоналу та інших чинників, що можуть мати об'єктивну або суб'єктивну природу.

Основні джерела загроз для безпеки інформації в ІТС можуть бути: збої та відмови в роботі обладнання та технічних засобів ІТС; зміна умов фізичного середовища (стихійні лиха, аварії, пожежі тощо); помилки персоналу (користувачів) ІТС під час експлуатації; навмисні дії (спроби) потенційних порушників.

Очевидно, що створення системи протистояння вказаним та іншим загрозам є головною метою проектів інформаційної безпеки об'єктів МКІ.

За методами захисту такі проекти діляться на дві великі групи: проекти з технічного захисту інформації; проекти з криптографічного захисту інформації.

Перша група проектів охоплює, в основному, питання забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації, зокрема, управління процесами виявлення спроб та фактів несанкціонованого доступу до інформації, управління роботами щодо унеможливлення несанкціонованого фізичного доступу до інформації та її носіїв тощо [2].

Друга група проектів охоплює управління стандартизованими процесами спеціальних перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [3].

Класифікаційні ознаки проектів інформаційної безпеки об'єктів МКІ наведено на рис.

Класифікаційні ознаки проектів інформаційної безпеки приморського об'єкту МКІ

За складовими ІТС об'єкту МКІ, де циркулює інформація	За характерис- тиками інфор- мації, що обробляється	За видами загроз інформації	За методами захисту інформації
- кабельні мережі - системи бездротового зв'язку - АРМ керування об'єктом МКІ - АРМ керування базами даних - система охоронної сигналізації і відеоспостереження - система контролю доступу - система інформаційного обміну ЗМР	- результати моніторингу морської обстановки - стан системи сигналізації, відеоспостереження, контролю доступу - інформація з керування ЗМР - технологічна інформація системи захисту (ключі, криптоалгоритми тощо)	- витік по технічним каналам - несанкціонований доступ до інформації - помилки персоналу - закладні пристрої - спеціальний вплив на інформацію - зловмисні дії персоналу	- технічний захист інформації - криптографічний захист інформації

Рисунок – Класифікаційні ознаки проектів інформаційної безпеки об'єктів МКІ

Наведені вище класифікаційні ознаки проектів інформаційної безпеки об'єктів МКІ свідчать, що ефективно вирішувати завдання безпеки інформації, яка циркулює в інформаційних системах, можна лише шляхом створення в складі ІТС комплексної системи захисту інформації (КСЗІ), що поєднувала б організаційні, інженерно-технічні та криптографічні засоби захисту інформації від різного роду загроз.

Метою створення комплексної системи захисту інформації (КСЗІ) є забезпечення захисту інформації, що збирається, обробляється, передається та зберігається в ІТС об'єктів МКІ від несанкціонованого доступу.

До таких проектів відносяться проекти забезпечення захисту від загроз порушення цілісності, конфіденційності, несанкціонованої модифікації та знищення інформації, а також забезпечення доступності інформації для авторизованих користувачів.

Проекти розробки та експлуатації КСЗІ мають охоплювати стаціонарні та рухомі платформи (зокрема, засоби морської робототехніки). Реалізація функцій захисту досягається шляхом використання об'єднаних в єдину систему систем охорони, криптографічних засобів захисту, а також шляхом виконання спеціальних організаційних, інженерних та технологічних заходів із захисту інформації. Це робить актуальним проектний підхід до їх розробки та експлуатації.

Список літератури:

1. Проект Закону України «Про критичну інфраструктуру та її захист» // http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/681-20#Text>
3. Положення про порядок здійснення криптографічного захисту інформації в Україні. Затверджено Указом Президента України від 22 травня 1998 року N 505/98.

УДК 004.056.5: 623.82

ОСОБЛИВОСТІ ФОРМУВАННЯ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ІНІЦІАТИВИ «ФЛОТ МОРСЬКИХ ДРОНІВ УКРАЇНИ»

***Автор:** Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація.

Світова практика та й безпосередньо досвід України, особливо з врахуванням військових досягнень, показують, що значну частину задач, покладених на ВМФ ЗСУ можна вирішувати за рахунок використання морських дронів.

Однак, аналіз публікацій показує наявність загрози, пов'язаної з гіпертрофованим підходом в намірах по реорганізації структури та за-

дач Військово-Морського флоту України. В першу чергу це пов'язане з перебільшенням можливостей морських дронів та їх захищеності від засобів виявлення та протидії, розміщених на кораблях, в бухтах та ін. Аналогічна помилка вже була допущена при формуванні Морської Доктрини України, яка спиралась на ідею «москітного флоту». Так, прихильники ідеї «москітного флоту» намагаються її реанімувати за рахунок інтегрування до неї морських дронів. При цьому розглядається тільки варіант низькобортних надводних дронів.

Такий абсурдний, односторонній підхід призведе до результату, який дискредитує ідею дронів і може мати тяжкі наслідки для України.

В роботі проведено аналіз можливостей морських надводних та підводних дронів і запропоновано основні принципи формування структури флоту морських дронів та концепції інформаційної безпеки в рамках ініціативи «Флот морських дронів України»

Вступ.

Військова агресія Росії показала наявність значних недоліків в організації та структурі ВМФ України. Головними проявами такого стану стали:

- захоплення портів на Азовському морі;
- блокада портів Одеського та Миколаївського регіонів;
- захоплення острова Зміїний.

Одним із головних чинників цих подій стала відсутність відповідних бойових одиниць в складі флоту, спроможних протистояти бойовим кораблям Чорноморського флоту Росії (ЧФР).

Ця ситуація виникла давно, з моменту розділу Чорноморського флоту, що залишився після розпаду Радянського союзу. Її суттєво погіршила різниця в ставленні керівництв держав (України і Росії) до своїх флотів та захоплення значної кількості українських кораблів в Севастополі в 2014 році. – з 1992 року в Україні були добудовані та введені до складу флоту 2 корвети (малі протичовнові кораблі проєкту 1124) та один фрегат (прикордонний сторожовий корабель проєкту 11351) [1]. За вказаний період до складу ЧФР, крім захоплених в Україні в 2014 році, було введено 3 фрегати (великих протичовнових кораблів проєкту 11356Р), 6 підводних човнів (проєкту 877) та інші [2].

В Україні була спроба покращити ситуацію – розроблено та прийнятий до виконання проект «Український корвет». Розробка проекту була завершена у 2008 році, а будівництво першого корабля почалося у травні 2011 року. Однак, рад об'єктивних та суб'єктивних чинників (фінансова криза, зміни керівництва держави та інші, в тому числі й корупційні фактори) призвели до фактичного закриття проекту.

На його заміну Кабінетом міністрів України 7 жовтня 2009 року затверджено «Морську Доктрину України на період до 2035 р.» [3]. До головних, інституціональних змін в підході до забезпечення безпеки України на морі та морському узбережжю в документі необхідно віднести заміну проекту «Корвет України» на ідею створення «москітного флоту» – флоту, зібраного з патрульних катерів [6] (наприклад, типу «Айленд» [4], бойових патрульних катерів типу Mark VI [5] та ін.).

Як показав досвід війни, ця ідея стала провальною – російські фрегати та крейсер «Москва» заблокували український флот в портах Миколаєва, Одеси та Ізмаїла. Оборона прибережної зони повністю лягла на артилерію та мінні загородження. Як ексклюзивний фактор, необхідно вказати на високу ефективність використання РК-360МЦ «Нептун» [7], на рахунок якого крейсер «Москва», фрегат «Адмірал Ессен».

До того ж, при звільненні о. Зміїний для надання артилерійської підтримки, українські артилеристи ставили французькі самохідні установки CAESAR на баржі [8].

Однак ідея «москітного флоту» не вмерла – її намагаються відновити шляхом заміни катерів морськими дронами.

1. Мета та задачі дослідження

Метою дослідження є розробка пропозицій до Морської доктрини України по формуванню блоку інформаційної безпеки для флоту морських дронів.

Для досягнення мети в роботі були поставлені наступні завдання:

1. Аналіз задач, які виконуються з використанням морських дронів спеціального призначення.

2. Основні засади інформаційної безпеки для флоту морських дронів.

2. Аналіз задач, які виконуються з використанням морських дронів спеціального призначення

Захист морських акваторій та прибережних територій Азово-Чорноморського басейну є, згідно з [3], основним завданням із забезпе-

чення національної безпеки держави для Військово-Морського флоту Збройних Сил України.

Світова практика та й безпосередньо досвід України, особливо з врахуванням військових досягнень, показують, що значну частину задач, покладених на ВМФ ЗСУ можна вирішувати за рахунок використання морських дронів. До таких задач відносяться:

1. Висвітлення підводної та надводної обстановки.
2. Проведення диверсійно-розвідувальних операцій в акваторіях бухт, портів, гідро-технічних споруд та якірних стоянках кораблів в автономному, дистанційно-керованому варіанті, в тому числі повітряними дронами-камікадзе.
3. Доставка до місця проведення бойових операцій мін, торпед та повітряних дронів-камікадзе, забезпечення їх постановки та запуску.
4. Доставка та технічна підтримка диверсійно-розвідувальних груп, в тому числі повітряними дронами-камікадзе.

2.1. Висвітлення підводної та надводної обстановки

Задача відноситься до класичних, які вирішувались на протязі останніх 50...60 років стаціонарними, дрейфуючими, самохідними та такими, що буксируються пристроями/буями /виробами/снарядами/апаратами (в різних джерелах використовуються різні терміни для позначення однотипних пристроїв).

Для висвітлення підводної обстановки на пристроях використовують гідроакустичні станції (ГАС), що працюють в пасивному або активному режимі, та датчиків контролю параметрів середовища. Відповідно до цього, з точки інформаційної безпеки, їх розділяють на системи відкритого та прихованого спостереження. В залежності від вирішуваних задач та можливості і відстані переміщення такі пристрої використовуються як окремо, так і в складі груп.

Головними недоліками таких систем є:

- простота виявлення зловмисником, особливо при використанні ГАС в активному режимі;
- вразливість (пошкодження, знищення, захоплення) до дій зловмисника;
- обмеженість автономного джерела живлення.

Також необхідно відмітити, що в Україні, в наслідок ряду об'єктивних та суб'єктивних причин, таких систем майже не залишилось (як виняток – декілька радіогідроакустичних систем на базі пасивних ненаправлених буїв РГБ-16В, шифр «Ятрань»).

На даний час для України є необхідність розробки нових систем, основаних на використанні морських дронів, які спроможні долати значні відстані (до 600 миль) та, за необхідності «відірватись» від переслідування, занурюватись на глибини до 150 метрів.

Встановлена на дроні ГАС повинна мати пристрій опускання антени, що буде імітувати роботу вертолітного буя. Також можливо встановлення спеціалізованої системи що буде підробляти шуми гвинтокрила. Такий підхід дозволить створювати інформаційний потік, що буде дезінформувати противника.

Такі дрони зможуть стати очима та вухами України в морі.

2.2. Проведення диверсійних та розвідувальних операцій

Одним з варіантів морських дронів для проведення диверсійних та розвідувальних представлено в [9]. Їх використання в бухті Севастополя показав виняткові можливості таких систем, особливо з погляду на політичні та суспільні результати.

Одночасно з цим, аналіз відеозвітів атаки (див. [10]) показує, що технологія застосування та наслідки атаки мають досить сумнівний військовий результат. Знаковим є запис атаки морського дрону з гвинтокрила – прорив дрону через зону враження в більшій мірі є випадковістю та не готовністю сил захисту акваторії до таких атак. Гарантії повторення такого збігу обставин не має.

Отже, для отримання сталих результатів, необхідно змінювати можливості такого дрону:

- максимально зменшити демаскуючі характеристики (кільватерний слід, гучність двигуна та ін.);
- надати можливість пірнати;
- збільшити масу вибухового заряду

Одночасно з цим необхідно терміново запускати інші типи дронів:

- мінні загороджувачі;
- носії торпед;
- носії повітряних дронів-камікадзе
- носії засобів РЕБ;

– носії ГАС та засобів цілевказання.

Головною особливістю таких дронів буде можливість скритно проникати в місця дислокації флоту противника та проведення значної частини дій в підводному стані.

2.3. Доставка до місця проведення бойових операцій мін, торпед та повітряних дронів-камікадзе, забезпечення їх постановки та запуску

Відмінність від попередніх дронів буде полягати в можливості провадити бойові операції, в тому числі, й з переходом з підводного руху на надводний на високих глісуючих швидкостях, і навпаки. Це дозволить використовувати ефект несподіванки.

2.4. Доставка та технічна підтримка диверсійно-розвідувальних груп, в тому числі повітряними дронами-камікадзе.

В даному випадку морський дрон виконує функції вантажної платформи та транспортувальника водолазів.

Основним завдання таких дронів є максимально приховано доставити/евакуувати ДРГ та забезпечити її інформаційну (зв'язок, навігація та ін.) та бойове прикриття (повітряні дрони-камікадзе).

3. Основні засади інформаційної безпеки для флоту морських дронів

Інформаційна підтримка морських дронів повинна включити в себе:

1. Забезпечення конфіденційності, достовірності (цілісності) та своєчасності отримання інформації всіма ланками комплексу морського дрона (навігаційна інформація, зв'язок, інформація про надводну і підводну обстановку та ін.).

2. Розробка методів і засобів зменшення демаскуючих ознак морських дронів та унеможливлення їх ідентифікації засобам виявляти противника.

3. Розробка імітаційних методів і засобів приховування діяльності морських дронів.

3.1. Забезпечення конфіденційності, достовірності (цілісності) та своєчасності отримання інформації

Цей блок задач пов'язаний з впровадження існуючих новітніх технологій супутникової навігації та зв'язку, а також розробкою спеціа-

лізованих засобів. Необхідними вимогами до них є здатних забезпечити стійкий обмін в умовах застосування противником засобів РЕБ; стійкість робота при значній хитавиці (до 6...7 балів) та можливість підтримувати радіозв'язок на малих глибинах занурення (до 5 м).

Виконання вказаних вимог суттєво вплине на можливість виконання 2 та 3 пунктів.

Важливим елементом успішного виконання задач даного пункту є розробка активних ГАС, робота яких основана на шумоподібних сигналах.

3.2. Розробка методів і засобів зменшення демаскуючих ознак морських дронів

Основними демаскуючими ознаками морських дронів є:

1. Ознаки переміщення (кільватерний та кавітаційний сліди; акустичні/гідроакустичні поля працюючих механізмів та ін.).

2. Електромагнітне випромінювання засобів зв'язку та обміну інформацією в радіочастотному каналі.

3. Робота ГАС в активному режимі.

4. Магнітне (електромагнітне) поле морського дрона.

5. Створення гідроакустичної тіні на екрані активної ГАС супротивника.

Вирішення вказаних та інших задач дозволить суттєво знизити вірогідність виявлення морських дронів засобами спостереження супротивника.

3.3. Розробка імітаційних методів і засобів приховування діяльності морських дронів.

Вказаний пункт тісно пов'язаний з попереднім, однак має ряд суттєвих відмінностей:

1. Використовуються за умови неможливості приховати роботу підводної/надводної системи:

– використання активних ГАС (пропонується маскуванню їх під акустичні буї гвинтокрилів – створюється гідроакустичне поле гвинтокрила в точці спуску буя);

– подолання великих відстаней в надводному положенні та великій швидкості (пропонується маскуванню гідроакустичним полем швидкісного катера супротивника).

2. Робота засобів радіозв'язку:

– використання імпульсних та шумоподібних сигналів в каналах зв'язку, в тому числі супутникового;

– використання магнітних антен та антен з розподіленими параметрами (маскуються під поплашкову систему рибацьких сіток).

Висновки

В роботі запропоновано основні положення, які необхідно враховувати при формуванні блоку інформаційної безпеки для флоту морських дронів.

Розглянуто та обґрунтовано:

1. На основі відкритих джерел інформації та досвіду автора проведено аналіз сучасного стану робіт по створенню «флоту морських дронів» України:

– показано основні загрози, що можуть призвести до негативних наслідків;

– визначені основні задачі ВМФ ЗСУ, що можуть виконуватись з використанням морських дронів спеціального призначення;

– запропоновано склад, за призначенням, «флоту морських дронів»;

– вказано, що з метою уніфікації та зменшення вартості виготовлення, є доцільним створення багатофункціональної платформи, як основи для декількох типів морських дронів.

2. Розглянуто та формалізовано підходи та вимоги до забезпечення інформаційної безпеки при виконанні бойових морськими дронами що дало змогу визначити основні засади інформаційної безпеки для флоту морських дронів:

– методи та засоби забезпечення конфіденційності, достовірності (цілісності) та своєчасності отримання інформації всіма ланками комплексу морського дрона;

– методи і засоби зменшення демаскуючих ознак морських дронів та унеможливлення їх ідентифікації засобам виявляти противника

– методи і засоби імітаційного приховування діяльності морських дронів.

Список літератури:

1. Список кораблів і суден Військово-Морських Сил України. Вікіпедія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Список_кораблів_і_суден_Військово-Морських_Сил_України

2. Чорноморський флот ВМФ Росії. Вікіпедія. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Чорноморський_флот_ВМФ_Росії

3. Про затвердження Морської доктрини України на період до 2035 року. Постанова Кабінету Міністрів України; Доктрина від 07.10.2009 № 1307. [Електронний ресурс] – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1307-2009-п/ed20091007#Text>

4. Патрульні катери типу «Айленд». Вікіпедія. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Патрульні_катери_типу_«Айленд»

5. Mk VI (малий бойовий катер). Вікіпедія. [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/Mk_VI_\(малий_бойовий_катер\)](https://uk.wikipedia.org/wiki/Mk_VI_(малий_бойовий_катер))

6. Чому турецькі корвети у ВМСУ не на часі. Ukrainian Military Pages (інтерв'ю з експертом Центру оборонних стратегій Андрієм Риженко). [Електронний ресурс]. – Режим доступу: <https://www.ukrmilitary.com/2021/07/vmsu.html>

7. Нептун (береговий ракетний комплекс). Вікіпедія. [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/Нептун_\(береговий_ракетний_комплекс\)](https://uk.wikipedia.org/wiki/Нептун_(береговий_ракетний_комплекс))

8. Steven Erlanger, Lara Jakes (2022). U.S. and NATO Scramble to Arm Ukraine and Refill Their Own Arsenals. The New York Times (Published Nov. 26, 2022 Updated Nov. 29, 2022). [Електронний ресурс] – Режим доступу: <https://www.nytimes.com/2022/11/26/world/europe/nato-weapons-shortage-ukraine.html?smid=nytcore-ios-share&referringSource=articleShare>

9. Україна запустить флот морських дронів. [Електронний ресурс] – Режим доступу: <https://mil.in.ua/uk/news/ukrayina-zapustyt-flot-morskyh-droniv/>

10. Відео атаки підводних дронів на російські кораблі у Севастополі. Youtube. [Електронний ресурс] – Режим доступу: https://www.youtube.com/watch?v=O0glD242Znw&ab_channel=Телеканал_Київ

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

УДК 681.391

**ДОСЛІДЖЕННЯ АДАПТИВНОЇ СИСТЕМИ АКТИВНОГО
ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ У ВИДІЛЕНОМУ
ПРИМІЩЕННІ**

***Автор:** Демідов І.А., студент, Національний університет
кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет
кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Мовна інформація є одним з головних джерел отримання інформації з обмеженим доступом про різні сфери життєдіяльності людини – особисте життя, фінансову, адміністративну або виробничу діяльність організації тощо. Дуже часто ця інформація має оперативний характер. Тому природньо, що мовна інформація з обмеженим доступом є предметом особливої уваги воєнних і комерційних розвідок та інших злоумисників.

Носієм мовної інформації є акустичний сигнал, який представляє собою коливання частинок пружного середовища, що поширюються від джерела мовлення в навколишній простір і можуть потрапляти у технічні канали витоку акустичної інформації. Несанкціонований доступ до конфіденційної мовної інформації може здійснюватися шляхом безпосереднього прослуховування або за допомогою технічних засобів.

Безпосереднє прослуховування переговорів злоумисником може здійснюватися через двері, відкрите вікно, стіни, перегородки або вентиляційні канали. В якості технічних засобів, для доступу до змісту переговорів можуть використовуватись спрямовані, провідні або радіо- мікрофони, контактні або безконтактні стетоскопи тощо.

Захист мовної інформації від витоку прямими (повітряними) акустичними каналами реалізується пасивними та активними засобами. Основним пасивним засобом є звукоізоляція, основними активними

засобами є акустичні генератори завад (шуму). Найбільш ефективними є активні засоби, оскільки дають можливість регулювати рівень завад в процесі експлуатації та навіть в процесі переговорів.

Актуальність даної роботи визначається широким використання активних засобів зашумлення в захисті мовної інформації від витоку акустичним каналом та проблемами оперативного контролю захищеності і забезпечення комфортності ведення переговорів у виділених приміщеннях.

Об'єкт дослідження – процес захисту мовної інформації у виділеному приміщенні від витоку прямим акустичним каналом.

Методи дослідження. Для визначення рівнів сигнал/шум використовуються методи статистичної теорії акустики приміщень. Для визначення ефективності адаптивної системи використовується оцінка захищеності мовної інформації шляхом аналізу ефективності зашумлення мовного сигналу перешкодою типу «білий» шум.

В залежності від важливості мовної інформації та поставленої задачі захисту пропонуються два критерії:

- в прийнятому (перехопленому) повідомленні неможливо виявити наявність інформації та предмет оповіщення;
- в прийнятому (перехопленому) повідомленні неможливо виявити інформаційних мовних сигналів.

Інформативність мови характеризується її розбірливістю, яка означає відносну або процентну кількість спеціально тренованими слухачами елементів мови від загальної кількості переданих по тракту.

Для дослідження системи адаптивної генерації шуму зручніше оперувати не розбірливістю інформації, а відношенням напруги сигналу до завади (шуму). Використаємо залежність словесної розбірливості мови W (рис. 1).

З рис 1 визначаємо, що значенню $W = 18\%$, відповідає $E = -11\text{дБ}$, значенню $W = 8\%$ відповідає $E = -14\text{дБ}$. Результати наведені в табл. 1.

Для дослідження ефективності адаптивної системи активного захисту мовної інформації пропонується наступний порядок дій:

1. скориставшись генератором мово подібного сигналу, створити сигнал певного рівня;
2. визначити рівень завади, яку створює адаптивна система;
3. обчислити відношення сигнал/завада;

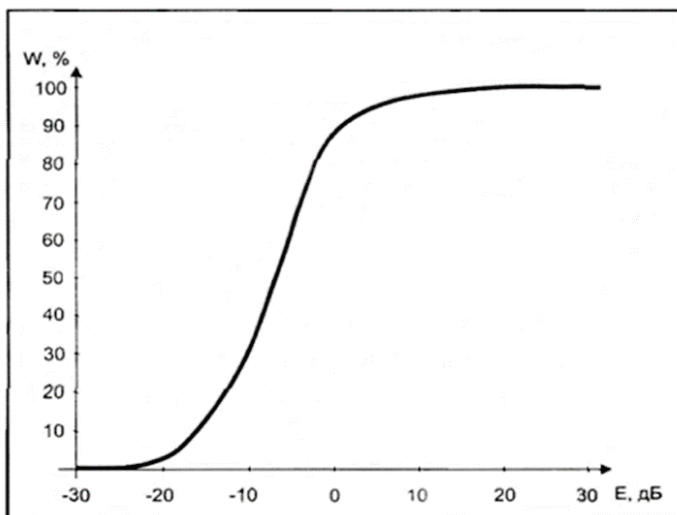


Рисунок 1 – Залежність словесної розбірливості мови W від інтегрального співвідношення сигнал / «білий» шум

Таблиця 1 – Параметри захищеності мовної інформації.

Критерій	Розбірливість слів, $W\%$	Відношення мовного сигналу/завада, E , дБ
У разі неможливості записати інформацію на носій – відсутність змістовної інформації	36	-6,5
Відсутність змістовної інформації	18	-11
Відсутність ознак мови	8	-14

4. повторити пункт 1-3 декілька разів, змінюючи рівень мовного сигналу;
5. провести дослідження 1-4 для кожної октавної полоси;
6. подувати графік досліджень;

Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах

7. за графіком визначити реальну словесну розбірливість для кожної октавної частоти та полосі частот 180-5600 Гц.

Згідно з розробленою методикою по черзі визначено рівні мовних сигналів та відповідно рівні створених завад типу «білий» шум адаптивною системою для всіх октавних полос. Результати вимірювань представлено в таблиці 2.

Таблиця 2 – Результати вимірювань рівнів сигнал/шум та словесної розбірливості

Октавна полоса, Гц	Відношення сигнал/ завада, дБ					Середнє значення, дБ	Розбір- ливість, W%
	1	2	3	4	5		
250	+3,2	+2,4	+1,1	+3,2	+4,5	+2,88	27
500	+1,2	-0,7	+0,4	+0,9	+0,4	+0,44	29
1000	-3,1	-2,5	-4,6	-6,2	-5,1	-4,3	50
2000	-11,7	-13,2	-14,9	-15	-10,2	-13	42
4000	-9,6	-13,2	-15,6	-15,1	-14	-13,5	68
180- 5600	-4	-5,44	-6,72	-6,44	-4,88	-5,496	43,2

З таблиці видно, що для діапазону частот 180 – 2000 Гц відношення рівнів сигнал/шум відповідає приблизно рівню словесної розбірливості 40% (27-50). Такий показник в цілому означає, що без можливості запису мовного сигналу, зрозуміти його зміст буде майже неможливо.

Для частот 2000 Гц та вище рівень словесної розбірливості зростає, та складає 60-70%.

При збільшенні рівня основного мовного сигналу. При рівнях мовного сигналу 28-49 дБ словесна розбірливість становить 40% та нижче. А для сигналів низької та великої гучності, при використанні адаптивної системи, рівень словесної розбірливості становить вище 40%, тобто можна зрозуміти зміст мовного сигналу.

Висновок. Під час дослідження системи адаптивної системи активного захисту мовної інформації у виділеному приміщенні було визначено її ефективність від прослуховування без можливості запису мовного сигналу в діапазоні частот 180 – 2000 Гц та при частотах бі-

льше 2000 Гц словесна розбірливість зростає до 60-70%, при цьому не перевищує гранично допустимий рівень словесної розбірливості 75%.

Список літератури:

1. Юрх Н.Г. Оцінка ефективності захисту мовної інформації, Сучасна спеціальна техніка, 2016.

КОМБІНОВАНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Автор:** Кобзєв В.Г., к.т.н., с.н.с., доцент кафедри Програмної інженерії та доцент кафедри Прикладної математики (за сумісництвом), Харківський національний університет радіоелектроніки, м. Харків, Україна*

Безпека на усіх видах транспорту, у тому числі інформаційна безпека, завжди відіграє важливу роль у його результативному і ефективному функціонуванні. Особливу гостроту інформаційна безпека приймає у періоди соціальних потрясінь природнього і, тим паче, воєнного характеру.

Серед величезної кількості напрямів і відповідних їм засобів і методів забезпечення бажаного рівня інформаційної безпеки зупинимося лише на контрольованому доступі до об'єктів інформаційної діяльності та збереження конфіденційності інформації при обміні через засоби загального доступу. Контроль фізичного доступу (аутентифікація) осіб може здійснюватися з використанням спеціальних носіїв (перепусток, магнітних ключів, чіпованих карток і т.п.) або базуватися на особистих ознаках персоналу (райдужна оболонка ока, голос, папілярні візерунки кінцівок пальців) [1].

Не припиняючи важливість інших методів, зупинимося на використанні папілярних візерунків, які не змінюються з віком. На цей час існує багато різних за фізичною природою засобів отримання цифрових зображень «відбитків» фаланг пальців. Для відокремлення зображень папілярних візерунків конкретної особи з множини інших осіб з різним рівнем надійності використовуються групи методів (алгоритмів) [2], що розглядаються далі.

Кореляційне порівняння базується на почерговому накладанні вхідного зображення на зразок з бази даних (БД), і обчислюється ступінь співпадіння двох зображень. Потрібно не забувати що палець може бути прикладений до сканера не так, як при попередній реєстрації, тому необхідно враховувати поворот зображення, зсув і розмитість за рахунок різного притиснення (при контактному способі фіксації «відбитка»).

У алгоритмі порівняння за локальними ознаками [2] знаходяться реперні точки зображення, складається карта – двомірна поверхня з виділеними на ній цими ключовими точками (точки розгалуження ліній папілярного візерунка і точки закінчення ліній). Такий образ співвідноситься з образами, існуючими у БД, і виноситься вердикт. Перевага цього алгоритму полягає в швидкості його роботи, але при цьому виявляється головний недолік – високі вимоги до якості зображення.

Метод порівняння зображень за візерунком спирається безпосередньо на особливості будови папілярного візерунка на поверхні пальців. Отримане зображення розбивається на зони і більш дрібні комірки, розмір яких залежить від необхідної точності. У кожній зоні проводиться опис параметрів синусоїдальної хвилі (напрямок поширення хвилі, довжина хвилі та початковий зсув фази). Особливість цього методу [3] полягає у складній реалізації та вимоги використання глибокої математичної бази – фільтра Габора, при цьому вимоги до якості зображення незначні та швидкість роботи залишається на прийнятному рівні.

Метод зіставлення за шаблоном включає загальну характеристику, що визначається товщиною ліній, їх кривизною або щільністю, та ключовими точками, як у попередніх методах. У процесі реєстрації даний метод знаходить різні додаткові характеристики образу пальця. Найбільш значущі з них – ділянки навколо ключових точок та ділянки з невеликим радіусом вигину. При визначенні ступеня відповідності відбитка наявному шаблону використовується поріг, що відповідає найменшому припустимому відхиленню. Його головною перевагою є сумісність з будь-якими типами сканерів відбитків пальців, незалежно від роздільної здатності сканера. Суттєвими недоліками є несумісність з базою даних AFIS (автоматизована дактилоскопічна система ідентифікації) і слабка пристосованість до розпізнавання (при безлічі пошуків в базі даних).

У алгоритмі порівняння на основі графів вихідне зображення відбитка пальця перетворюється на зображення поля орієнтації папілярних ліній, на якому помітні області з однаковою орієнтацією ліній. Потім визначаються центри цих областей (вершини), сусідні на зображенні області з'єднуються ребрами графа. Вигляд такого графа (розташування його вершин і їх з'єднання ребрами) є характерною ознакою зображення відбитка конкретної особи.

Найбільш ефективними та надійними є комбіновані методи розпізнавання відбитків пальців. В них використовується розбиття відбитків пальців на підкласи, ґрунтуючись на характерних ознаках, властивих тому чи іншому класу, а потім у знайденому підкласі здійснюють пошук конкретного відбитка за допомогою будь-якого з наведених вище методів. Побудовані на такому принципі сучасні системи з високою достовірністю (до 0,999) зіставляють зображення папілярного візерунка, що перевіряється, з зареєстрованим раніше його зразком з бази даних.

Список літератури:

1. С.І. Болобан, О.М. Перегуда, В.В. Умінський. Методи аутентифікації користувачів інформаційно-комунікаційних систем / Військово-технічний збірник Розроблення та модернізація ОБТ. – 2009, №2. – С. 47–52.
2. Bykh A., Visotska E., Kobzev V. et al. Analysis of Dermatoglyphic Signs for Definition Psychic Functional State of Human's Organism // Information Science and Computing, Book 7 Artificial Intelligence and Decision Making, 2008. – P. 49–52.
3. Кобзев В.Г. Дослідження методів аналізу особливостей папілярних візерунків / Н. Кононенко, В.Г. Кобзев // Матеріали 8-ї міжнародної науково-технічної конференції «Інформаційні системи та технології-2019», 9-14 вересня 2019 р. Коблеве-Харків, Україна. – Х.: ТОВ «Друкарня Мадрид». – 2019. – С. 291–292.

УДК 004.056.53

РОЗРОБКА КСЗІ ДЛЯ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВОДНОТРАНСПОРТНОГО КОМПЛЕКСУ

Автор: Крюк А.С., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Анотація.

В роботі проведено аналіз нормативно-правового забезпечення захисту інформації в ІТС об'єкту критичної інфраструктури воднотранспортного комплексу; виокремлено класифікаційні ознаки та особливості функціонування ІТС спеціального призначення; проведено аналіз існуючих методів та засобів захисту інформації в ІТС об'єкту критичної інфраструктури воднотранспортного комплексу; виявлено проблемні питання забезпечення інформаційної безпеки в ІТС об'єкту критичної інфраструктури воднотранспортного комплексу; проведено аналіз зарубіжного досвіду забезпечення інформаційної безпеки в ІТС; запропоновано вдосконалені методи та засоби захисту інформації в ІТС спеціального призначення; розроблено модель захищеної інформаційної системи об'єкту критичної інфраструктури воднотранспортного комплексу

Вступ.

Різке зростання великої кількості різноманітних інформаційних та інформаційно-телекомунікаційних систем в Україні обумовлено інтенсивним впровадженням сучасних інформаційних технологій. Разом з тим зростає і небезпека несанкціонованого втручання в роботу цих автоматизованих систем. Особливо це проявилось на передодні та на протязі вторгнення збройних сил Російської федерації в Україну. Важливість постановки та вирішення проблеми забезпечення безпеки сучасних інформаційних технологій обумовлюється необхідністю уточнення та обґрунтування достатності застосовуваних заходів захисту інформації, оптимізації систем захисту, підвищення ефективності контролю безпеки інформації.

Неконтрольоване поширення і використання віртуального та реального просторів, перш за все як сфери ведення воєнних конфліктів сучасності і найближчого майбутнього, зростання впливу засобів масової

інформації, а також впливу ІКТ та ІТС на постіндустріальне суспільство, поява небезпеки розриву між інформаційною елітою та споживачами призвело, у свою чергу, до того, що поряд з отриманням значних переваг від застосування інформаційного та кіберпросторів світове співтовариство набуло й усі пов'язані з ними проблеми.

Це фактично дає можливість стверджувати, що проблеми інформаційної та кібернетичної безпеки за сучасних умов і для України, і для переважної більшості інших держав світу стають нині особливо актуальними.

1. Мета та задачі дослідження

Метою дослідження є вдосконалення теоретико-методичних підходів до створення інформаційної платформи захисту інформації в ІТС спеціального призначення.

Для досягнення поставленої мети вирішувались такі завдання:

1. Проведення аналізу нормативно-правового забезпечення захисту інформації в інформаційно-телекомунікаційних системах;
2. Проведення аналізу існуючих методів та засобів захисту інформації в ІТС спеціального призначення;
3. Запропоновано моделі захищеної інформаційно-телекомунікаційної системи спеціального призначення.

2. Аналіз нормативно-правового забезпечення захисту інформації в інформаційно-телекомунікаційних системах

Основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності містяться у Законі України "Про основи національної безпеки України" [1].

За місцем в ієрархічній (вертикальній) структурі законодавства всі нормативно правові акти у сфері захисту інформації поділяються на [2]:

1. Документи вищої юридичної дії (Конституція України, Закони України, укази Президента України, постанови КМ України);
2. Загальнодержавні (міжгалузеві) документи у сфері ЗІ (нормативно-правові акти та організаційно-розпорядчі документи міжвідомчого значення, що реєструються у Міністерстві юстиції України, нормативні документи міжвідомчого значення технічного характеру, що

реєструються уповноваженим органом в сфері ЗІ (НД ТЗІ), а також державні стандарти і норми (ДСТУ, ДБН));

3. Галузеві документи у сфері ЗІ (відомчі положення, інструкції, рекомендації, нормативно-технічні та методологічні документи).

Актуальність вирішення проблеми захисту ІР обумовлюється зростанням доступу до мереж загального користування окремих категорій протиправно налаштованих громадян, певною вразливістю окремих мереж, зростанням попиту з боку злочинних елементів на здобування або руйнування інформації, що циркулює в спеціальних мережах зв'язку, системах управління військами та озброєнням, на блокування публічних державних інформаційних ресурсів (ДІР) в мережі Інтернет, ІР об'єктів критичної інфраструктури, а також вразливістю загальних ефірних телеканалів, радіостанцій громадського віщання.

У національному законодавстві закріплено кілька термінів, пов'язаних з ДІР та ІР. Найбільш показовим у цьому контексті є визначення, закріплене в Законі України "Про Державну службу спеціального зв'язку та захисту інформації України", а саме, ДІР – "інформація, яка є власністю держави та необхідність захисту якої визначено законодавством" [3].

Аналіз стану захисту інформації в інформаційних системах міністерств, інших центральних і місцевих органів державної влади, установ України свідчить, що в цілому рішення цієї проблеми в державі далеко від досконалості.

Реалізації існуючих загроз для інформації, що обробляється в ІТС, сприяють наступні обставини [4]:

- широке застосування іноземних засобів обчислювальної й комутаційної техніки, що на сьогодні викликане об'єктивною нездатністю вітчизняної промисловості задовольнити потреби в сучасному комп'ютерному й телекомунікаційному встаткуванні;
- прагнення ряду комерційних, а також деяких державних структур безконтрольно, не скоординовано створювати виділені або корпоративні телекомунікаційні системи;
- здійснення інвестиційної політики в галузі інформатизації й телекомунікацій у ряді випадків без ретельного аналізу її наслідків, а також без врахування інтересів державної безпеки;
- використання в інформаційних системах не сертифікованого встаткування й програмного забезпечення;

– недооцінка значимості захисту інформації й недостатньо розвинена система підготовки й перепідготовки кадрів в області ІБ.

3. Модель захищеної інформаційно-телекомунікаційної системи спеціального призначення

Успішні практики розробки інформаційних моделей виробничих процесів ІТС дають змогу представити інформаційну платформу управління базовим проектом у складі наступних модулів:

- інформаційного модуля типових характеристик ІТС;
- інформаційного модуля характеристик типових загроз основним складовим ІТС;
- інформаційного модуля характеристик існуючих типових методів та організаційно-технічних засобів протистояння інформаційним загрозам;
- інформаційного модуля характеристик типових технологій практичної побудови систем захисту ІТС.

В загальному розумінні успішні практики розробки інформаційних моделей виробничих процесів ІТС дають змогу представити інформаційну платформу управління базовим проектом у складі наступних модулів:

- інформаційного модуля типових характеристик ІТС;
- інформаційного модуля характеристик типових загроз основним складовим ІТС;
- інформаційного модуля характеристик існуючих типових методів та організаційно-технічних засобів протистояння інформаційним загрозам;
- інформаційного модуля характеристик типових технологій практичної побудови систем захисту ІТС.

В результатуючому вигляді запропонована модель захищеної ІТК спеціального призначення:

а) Моделі MV_V визначення властивостей об'єктів захисту:

$$MV_V = \{MV_{V-F}; MV_{V-P}; MV_{V-S}; MV_{V-I}\}.$$

б) Моделі MV_Z визначення загроз безпеки інформації

$$MV_Z = \{MV_{Z-U}; MV_{Z-F}; MV_{Z-P}; MV_{Z-D}\}.$$

в) Моделі MV_U визначення типових вразливостей ІТС

$$MV_U = \{MV_{U-O}; MV_{U-E}; MV_{U-I}; MV_{U-P}\}.$$

г) Моделі MS_O організаційного забезпечення системи захисту в ІТС

$$MS_O = \{MS_{O-P}; MS_{O-C}; MS_{O-E}\}.$$

д) Моделі MS_T технічного забезпечення системи захисту в ІТС

$$MS_{TS} = \{MS_{TS-O}; MS_{TS-E}; MS_{TS-I}; MS_{TS-P}\}.$$

е) Моделі MZ_S управління заходами впровадження систем захисту інформації в ІТС

$$MZ_S = \{MZ_{SA}; PT_{NT}; PT_{CS}; PT_{PM}; PT_{AP}; PT_{BIM}\},$$

Узагальнюючи опис моделей MZ_S :

$$MZ_{SA} = \{MZ_{SA-A}; MZ_{SA-R}\};$$

$$MZ_{ST} = \{MZ_{ST-A}; MZ_{ST-N}\};$$

$$MZ_{SS} = \{MZ_{SS-U}; MZ_{SS-M}\};$$

$$MZ_{SM} = \{MZ_{SM-M}; MZ_{SS-M}\}.$$

ж) Моделі P_Z перевірки відповідності впроваджених заходів нормативним документам із захисту інформації

$$P_Z = \{P_{Z-K}; P_{Z-D}\};$$

Множина моделей MF_F управління процесами з відновлення функціонування ІТС

$$M_{FF} = \{MF_{F-D}; MF_{F-P}; MF_{F-F}\}.$$

з) Інформаційна платформа робіт із захисту ІТС спеціального призначення

$$IM_{XI} = \{IX_{Ob}, IX_{Eb}, IX_{Ib}, IX_{KI}\};$$

$$IM_{BI} = \{IB_{Ob}, IB_{Eb}, IB_{Ib}, IB_{KI}\};$$

$$IM_{T3I} = \{IT_{3Ob}, IT_{3Eb}, IT_{3Ib}, IT_{3KI}\};$$

$$IM_{PI} = \{IP_{Ob}, IP_{Eb}, IP_{Ib}, IP_{KI}\}.$$

Висновки

В дослідження отримані результати, які дозволили запропонувати вдосконалення теоретико-методичних підходів створення інформаційної платформи захисту інформації в ІТС спеціального призначення.

Отримані наступні результати:

1. Проведено аналіз нормативно-правового забезпечення захисту інформації в інформаційно-телекомунікаційних системах, що дозволило визначити методи та засоби, які застосовуються до захисту інформації в інформаційно-телекомунікаційних системах спеціального призначення.

2. Проведено аналіз існуючих методів та засобів захисту інформації, які використовуються в ІТС спеціального призначення, що до-

зволило визначити проблемні питання забезпечення інформаційної безпеки в таких системах.

3. Розглянуто основні загрози та проблеми забезпечення інформаційної безпеки в інформаційно-телекомунікаційній системі спеціального призначення та запропоновано пропозиції щодо удосконалення методів та засобів захисту інформації в інформаційно-телекомунікаційній системі спеціального призначення.

4. На основі розроблених пропозицій щодо удосконалення методів та засобів захисту інформації проведено вдосконалення моделі захищеної інформаційно-телекомунікаційної системи спеціального призначення.

Список літератури:

1. Про основи національної безпеки України: Закон України від 07 серпня 2015 р. № 944 – IV // Відомості Верховної Ради. – 2015. – [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/964-15>.

2. Біла книга Держспецзв'язку. [Електронний ресурс]. – Режим доступу: <http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=49948/>.

3. Закон України "Про інформацію". [Електронний ресурс]. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/2657-12>.

4. Національна безпека України: Навчальний посібник для слухачів і студентів денної, вечірньої, заочно-дистанційної та заочної форм навчання / [І.Ф. Усатюк, О.А. Остапенко О.М. Овчар, П.С. Кривоцюк]; за редакцією к.е.н. доцента М.М. Іжі та к.і.н. доцента В.М. Кривцової. – Одеса: ОРІДУ НАДУ, 2010. – 272с.

УДК 004.021

ІДЕНТИФІКАЦІЯ СТАНУ ПРИСТРОЇВ ІоТ ДЛЯ ЗАДАЧ ЗАХИСТУ ІНФОРМАЦІЇ

Автор: Лисинчук В.В., студент, Державний університет телекомунікацій, м. Київ, Україна

Науковий керівник: Крючкова Л.П., д.т.н., професор, Державний університет телекомунікацій, м. Київ, Україна

Вступ. Сучасний інтернет речей представляє собою обчислювальну мережу предметів. Кожен із цих предметів взаємодіє як один з одним, так і з зовнішнім середовищем. Різноманітність технологій, що використовуються в такій системі для ідентифікації, вимірювання, передачі, зберігання та оброблення інформації, потребує створення все нових і нових систем захисту інформації (СЗІ) та моніторингу стану інформаційної безпеки (ІБ), для нейтралізації загроз інтернету речей (Internet of Things, IoT).

Безпека даних – пріоритетне завдання при проектуванні всіх мереж IoT. Деякі виробники не мають жодних стандартів безпеки своєї продукції; деякі пристрої використовують власний фактичний стандарт безпеки, який не сумісний з іншими виробниками; деякі старі версії пристроїв взагалі не мають заходів безпеки. Пристрої, що керуються комп'ютерами в автомобілях, такі як вимикачі, двигуни, замки та панелі приладів, виявилися вразливими для зловмисників, які мають доступ до мережі. Оскільки IoT є об'ємним джерелом даних, він завжди буде вразливим до складних атак.

Важливим є комплексний підхід до організації захисту подібних систем. Реалізація СЗІ та моніторингу стану ІБ інформаційно-телекомунікаційних систем і мереж будуються на забезпеченні безпеки зв'язку, контролю взаємодії в мережі, захисту пристроїв [1-2]. Однак подібні системи припускають динамічний розвиток і виникнення ситуацій, що вимагають аналізу, коли відбувається одночасне підключення і старих і нових пристроїв, використовуються різні версії прошивок, апаратних та програмних рішень, застосовується безліч протоколів сполучення, технологій обробки, аналізу та передачі даних.

Пристрої, що реалізують функції IoT, в окремих випадках, знаходяться поза контрольованою зоною, вимагають контролю, оновлення

програмного забезпечення, оптимізації ряду процесів функціонування протягом життєвого циклу. Вбудовані системи захисту в подібних пристроях не завжди ефективні. Це зумовлено тим, що такі системи мають широковідомі зловмисникам типові вразливості, і не виникає труднощів з отриманням доступу до системи та використанням даних вразливостей.

Зазвичай у процесі реалізації та протягом життєвого циклу інформаційних систем і мереж виникає необхідність вдосконалення систем захисту, контролю та моніторингу ІБ пристроїв IoT [3-5]. При цьому основною задачею є розробка універсальних моделей і методів ідентифікації стану інформаційної безпеки малопотужних з обчислювальної точки зору пристроїв, які використовують комплексні підходи аналізу даних, що надходять від внутрішніх та зовнішніх (сторонніх) інформаційних каналів.

Основу подібних рішень складає те, що елементи IoT мають невеликі програмно-апаратні можливості, заздалегідь зумовлені діями і реакціями, і, протягом життєвого циклу, в основному, не змінюють свій обмежений функціонал. Багато пристроїв, сегменти IoT, мають граничні допустимі значення параметрів функціонування, виконують запрограмовану послідовність на керуючі команди та зовнішні події, що відбуваються в інформаційній системі.

Нами пропонується застосування часових рядів для математичного опису стану захищеності пристроїв в мережі IoT. В якості ідентифікаційних ознак для класифікації стану інформаційної безпеки пристроїв IoT використовуються ознаки: загрузка мережі, загрузка процесора, загрузка пам'яті.

Основна частина.

В більшості випадків системи та пристрої являються закритими (представляють собою “чорну скриньку”). Це означає, що при розробці різні виробники використовують різні апаратні та програмні платформи, стандартні бібліотеки, де не завжди є можливість аналізувати вихідний код та апаратні прошивки. В більшості випадків пристрої IoT реалізуються виробниками як закриті системи, де можливість вносити зміни апаратної або модифікації програмної частини відсутні.

Механізми захисту є внутрішніми. При перевірці цілісності у разі колізії запускаються механізми захисту (аж до припинення роботи пристрою). Проте, у процесі роботи, виникають необхідності конфігурації, налаштування, покращення характеристик функціонування системи. Так як більшість елементів системи використовують однакові алгоритми функціонування, стає можливим використання реверс-інжинірингу (англ. Reverse-engineering, укр. Зворотне проектування), для пошуку вразливостей, спроби передачі широкомовних керуючих команд, здійснення різноманітних деструктивних впливів. Це в свою чергу веде до переведення пристрою в режим роботи, що супроводжується відхиленням параметрів від гранично допустимих значень, що суттєво впливає на робочий функціонал пристрою (включаючи вбудовані захисні механізми). У зв'язку з цим необхідно використовувати одночасно кілька інформаційних каналів, які можуть бути як сторонніми, так і внутрішніми.

З метою виявлення аномалій в роботі пристроїв IoT необхідно переглядати декілька дискретних станів. Це зумовлено тим, що, як і в будь-якій системі, процеси пристроїв IoT протікають в динаміці, одночасно змінюється множина параметрів, тому для відображення актуальної ситуації одного стану не достатньо.

Запропонований підхід пов'язаний з використанням шаблонів поведінки. Під шаблоном поведінки розуміються синхронізовані за часом множини послідовностей із визначеною частотою знімання значень з внутрішніх і зовнішніх датчиків, що реєструють параметри процесів, що відбуваються в пристрої.

Шаблон поведінки формується на основі інформації про функціонування пристрою IoT і його компонентів: завантаження і потреба ресурсів, дані про електромагнітні і звукові спектри, частоти і амплітуди, вібрації, температури тощо [6].

Запропонований підхід ідентифікації стану відрізняється використанням шаблонних послідовностей. Шаблонні послідовності описують сформовані умови функціонування пристрою на базі синхронізованих часових рядів, які відображають отримані від різних датчиків числові значення під час виконання процесів. Це дозволяє визначати стан ІБ без збільшення обсягу бази даних, що важливо через технічні обмеження пристроїв IoT.

Використання запропонованого підходу на початковому етапі передбачає “налаштування” пристрою в заздалегідь заданих режимах роботи, де відбувається перед обробка, пов'язана з обчисленням кластерних областей та порогових значень, що може відбуватися на основі вибірки. На етапі функціонування на основі функції розбиття простору здійснюється співвідношення поточного стану до визначених на початковому етапі.

Подальший аналіз відхилень відбувається з урахуванням порівнянь з еталонними значеннями центрів кластерів і класів, обчисленими за умов, заданих для формування навчальної вибірки.

За схемою, наведеною на рис. 1, нами виконано експериментальні дослідження. Метою проведення експерименту було виявлення стану, який визначається алгоритмом обробки даних, обчислювального вузла на основі оцифрованих показників завантаження обчислювальних ресурсів. В якості послідовності, що формує поведінковий шаблон, були виділені синхронізовані за часом відсоткові показники монітора системного завантаження.

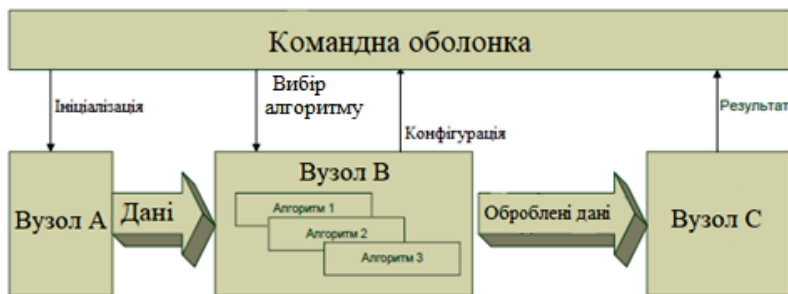


Рис. 1 – Схема проведення експерименту

При проведенні експерименту вибірка шаблонів сигнальних трас для станів, що розглядаються, була розділена на “навчальну” і “тестову”.

Ідентифікація стану виконувалася на основі методу кластеризації k -середніх. Як міра близькості використана Евклідова відстань:

$$r(x, \dot{x}) = \sqrt{\sum_{\rho=1}^n (x_{\rho} - \dot{x}_{\rho})^2},$$

де $x, \dot{x} \in R^n$; R – простір спостережень.

Висновки

1. Широке практичне використання концепції IoT обмежується необхідністю вирішення проблеми безпеки мереж IoT в спектрі захисту від загроз зловмисників. Моніторинг стану інформаційної безпеки пристроїв інформаційно-телекомунікаційних систем та мереж у концепції IoT обумовлює необхідність пошуку та вдосконалення підходів до виявлення різного виду загроз.

2. Використання часових рядів для математичного опису стану пристроїв в мережі IoT надає можливість ідентифікувати стан безпеки мереж IoT без збільшення обсягу інформації, що зберігається і обробляється у внутрішніх обчислювальних ресурсах.

3. Іншим напрямом розвитку подібних рішень, враховуючи відносну обмеженість ресурсів пристроїв, є організація зовнішніх центрів обробки даних, на які пристрої IoT можуть надсилати інформацію про своє функціонування для подальшого аналізу стану.

Список літератури:

1. Farwell J. P., Rohozinski R. (2011). Stuxnet and the Future of Cyber War. (Vol. 53. № 9. P. 23-40) *Surviva*
2. Yeung D. Y., Ding Y. (2003). Host-based intrusion detection using dynamic and static behavioral models (Vol. 36. P. 229-243).
3. Gao D., Reiter M., Song D. (2009). Beyond output voting: Detecting compromised replicas using HMM-based behavioral distance (Vol. 6. № 2. P. 96-110). *IEEE Transactions on Dependable and Secure Computing*.
4. Макаренко С. И., Олейников А. Я, Черницкая Т. Е. (2019). Модели интероперабельности информационных систем (№ 4. С. 215-245). *Системы управления, связи и безопасности*.
5. Bevir M. K., O'Sullivan V. T., Wyatt D. G. (1981). Computation of electromagnetic flowmeter characteristics from magnetic field data (Vol. 14. № 3. P. 373-388). *Journal of Physics D Applied Physics*.
6. Semenov V. V., Lebedev I. S., Sukhoparov M. E., Salakhutdinova K. I. (2019). Application of an Autonomous Object Behavior Model to

Classify the Cybersecurity State. Internet of Things, Smart Spaces, and Next Generation Networks and Systems (pp. 104-112).

УДК 004.056.53

**РОЗРОБКА БЛОКУ КІБЕРЗАХИСТУ ДЛЯ КСЗІ
НА ОБ'ЄКТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ВОДНОТРАНСПОРТНОГО КОМПЛЕКСУ**

***Автор:** Майгур О.І., студент, Національний університет
кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Нужний С.М., к.т.н., доцент, зав. каф. КТІБ,,
Національний університет кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна*

Вступ.

Розробка комплексної систем захисту інформації (КСЗІ) для об'єктів критичної інфраструктури (ОКІ) воднотранспортного комплексу (ВТК) є однією з пріоритетних задач в інформаційно-правовому полі України. Це набуло особливо вагомого значення в умовах збройного нападу Росії на Україну. Захист та відновлення інформаційних ресурсів, протидія кібератакам та деструктивним діям російських диверсійно-розвідувальних груп та їх поплічників можливий тільки при комплексному підході до побудови системи захисту. При цьому об'єкти критичної інфраструктури України після 24 лютого стали основними об'єктами нападу як в фізичному відношенні, так і в кібернетичному.

Порти, як винятково важливі об'єкти господарства, завжди мали значну прилягаючу силу для різних загарбників та зловмисників. Одним з найскравіших прикладів зовнішнього втручання в інформаційну систему морських перевезень є інцидент, який стався в 2012 році в порту Антверпена [1]. Інцидент пов'язаний з контрабандою наркотиків, зброї та грошей в Європу з Латинської Америки. В порту відправки контейнер контрабандою отримував код «легального» контейнера та завантажувався на судно, що прямувало до Європи. По прибутті в порт призначення, «ІТ-департамент» банди перехоплював 9-значові PIN-коди, які викорис-

туються для проведення операцій з контейнерами в системах DP World. Ці коди необхідні для проведення операцій з портовими системами навантаження-розвантаження. Контрабандисти, підключені до однієї з портових бездротових мереж, віддавали команду автоматизованим вантажним системам переміщати контейнер на свою вантажівку [1].

Аналогічні схеми контрабандисти відпрацювали й для перевезення нелегальних мігрантів та навіть бойовиків до держав Європи та Північної Америки.

За останніми оцінками, щорічно по морю перевозиться більш 420 млн контейнерів, і тільки 2% піддаються перевіркам з доглядом, тобто про реальні обсяги контрабанди, що перевозиться навіть в «легальних» контейнерах, важко здогадуватися [2]

Для України, з початком бойових дій (ракетні обстріли та кібератаки на ОКІ ВТК) та перебоями зі світлом (блекаут), ситуація з захистом інформаційних ресурсів суттєво ускладнилась. Це вимагає переведення багатьох систем в режим роботи «локальна мережа» (АС другого класу) або використання Starlink, що вимагає розробки додаткових модулів діагностики мікросервісів Web-застосунків з реєстрацією інцидентів пов'язаних з порушеннями їх доступності.

1. Мета та задачі дослідження

Метою дослідження є розробка програмного модуля, який виконує діагностику мікросервісів Web-застосунку та реєструє інциденти пов'язані з порушеннями їх доступності для блоку кіберзахисту КСЗІ ОКІ ВТК України.

Для досягнення поставленої мети вирішувались такі завдання:

- Гармонізація нормативно-правового забезпечення кіберзахисту України з міжнародними стандартами;
- Реалізація модуля забезпечення доступності Web-застосунку з мікросервісною архітектурою для блоку кіберзахисту КСЗІ ОКІ ВТК України.

2. Гармонізація нормативно-правового забезпечення кіберзахисту України з міжнародними стандартами

В Україні зафіксоване зростання кількості кібератак на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури (ОКІ) [3], в тому числі й тих, що відносяться до водно-транспортного комплексу (ВТК). При цьому Від початку війни тенденція на зростання зберігається.

В II кварталі 2022 року, за допомогою засобів Системи виявлення вразливостей та реагування на кіберінциденти та кібератаки (СВВРКК), було опрацьовано 19 млрд подій [3]. Загальна кількість виявлених та відпрацьованих кіберінцидентів збільшилась від 40 до 64.

Основними цілями хакерів були:

- а) кібершпіонаж,
- б) порушення доступності державних інформаційних ресурсів
- в) знищення інформаційних систем за допомогою програм-вайперів.

У II кварталі 2022 року було зафіксоване значне зростання активності хакерської активності по розповсюдженню шкідливого програмного забезпечення. Це були як програми, які спрямовані на знищення даних, так і ті, що їх викрадають. Порівнянні з I кварталом 2022 року [3]:

г) кількість подій ІБ у категорії «Шкідливий програмний код» збільшилась на 38%.

д) кількість критичних подій ІБ, джерелом яких є ІР-адреси Росії, зменшилась у 8,5 разів.

Фахівці пов'язують це насамперед з блокуванням ІР-адреси, що використовуються рф, постачальниками електронних послуг, які забезпечують доступ до інтернету.

Ці ІР використовувались для проведення кібератак на ОКІ та її інформаційні ресурси, розповсюджувалась фейкова інформація про бездіяльність державних органів під час російсько-української війни.

Незважаючи на те, що найбільша кількість критичних інцидентів ІБ, згідно статистики від системи автоматичного визначення геолокації за ІР-адресами, пов'язана з США, це не прив'язує джерела кібератак до ідентифікованого місцезнаходження [3].

Втім, за атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупованнями, що фінансуються урядом РФ. Зокрема, це UAC-0082/UAC-0113 (пов'язано з Sandworm), UAC-0010 (Gamaredon) та інші [3].

Як вказують в Адміністрації Держспецзв'язку, у II кварталі 2022 року основними цілями хакерів із РФ були українські ЗМІ, Уряд та місцеві органи влади.

В 2021 році наказом Адміністрації Держспецзв'язку ухвалено «Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» [4], який рекомендується запроваджувати для підвищення кіберстійкості інформаційно-комунікаційних систем ОКІ.

Методичні рекомендації розроблені з урахуванням «Настанови для підвищення кібербезпеки критичної інфраструктури» (Framework for Improving Critical Infrastructure Cybersecurity [5]), виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технологій Сполучених Штатів Америки (National Institute of Standards and Technology).

3. Реалізація модуля забезпечення доступності Web-застосунку з мікросервісною архітектурою для блоку кіберзахисту КСЗІ ОКІ ВТК України

У відповідності до нормативно-правової бази України в сфері технічного захисту інформації, будь-який Web-застосунок, в тому числі з мікросервісною архітектурою, оброблюється автоматизованою системою класу 3, в якій, згідно виявлених загроз, пред'являються підвищені вимоги до конфіденційності, цілісності та доступності інформації. Враховуючи вимоги нормативної документації до організації захисту Web-сторінок, комплекс засобів захисту Web- застосунку з мікросервісною архітектурою повинен реалізовувати наступні функціональні послуги безпеки:

а) для організації модуля забезпечення доступності інформаційних ресурсів:

- автоматизоване відновлення після збоїв,
- комплекс засобів захисту з контролем цілісності,
- самотестування в реальному часі;

б) Web-застосунки з мікросервісною архітектурою:

- відмова певного мікросервісу або групи мікросервісів призведе до зниження характеристик обслуговування;
- відмова API-шлюзу призведе до повної відмови Web-застосунку, оскільки взаємодія з клієнтом організована саме через API-шлюз;
- відмова системи управління базами даних призведе до відмови Web- застосунку через неможливість виконання мікросервісами операцій над даними;

– відмова апаратного забезпечення комп'ютерної системи може призвести до зниження характеристик обслуговування або повної відмови Web-застосунку;

– втрата зв'язку між мікросервісом або групою мікросервісів та API-шлюзом призведе до зниження характеристик обслуговування.

Реалізація загрози відмови мікросервісу або групи мікросервісів обумовлена, здебільше, наявністю помилок в їх програмному коді, тобто носить ненавмисний характер. Інші з зазначених вище загроз можуть бути реалізовані як ненавмисно, так і потенційним зловмисником. Таким чином, забезпечення доступності інформаційних ресурсів Web-застосунку з мікросервісною архітектурою розділяється на дві задачі: моніторинг апаратної та програмної складових мікросервісів, і контроль доступу до них[6-3].

Для захисту веб-ресурсів використовуються рішення класу web application firewall (WAF) – міжмережеві екрани рівня додатків. WAF дозволяє захиститися від сучасних атак на web-загроз зі списку OWASP Top 10, DDoS-атак рівня застосунків і інших.

Приймаючи рішення про покупку WAF, важливо враховувати масштаб веб-додатки та потенційні ризики: наприклад, для захисту сайту невеликого салону краси, придбання WAF може бути просто недоцільно. У таких випадках достатньо таких рішень для захисту інтернету, як антивіруси, списки контролю доступу (ACL), anti-DDoS на мережевому і транспортному рівнях. Однак, якщо говорити про більш великі проекти, то тут вступають в справу жорсткі вимоги, зокрема:

1) *Доступність*. Веб-застосунку має бути доступне 99-99,999% часу. Це означає, що час простою протягом року не може бути більше чотирьох днів (99%) або 5,5 хвилин (99,999%). Очевидно, WAF повинен також дотримуватися цих вимог, щоб зберегти показники доступності програми.

2) *Час відгуку*. Процедура розгляду заяв про користувача і видача результату повинні займати від декількох секунд до мілісекунд – в залежності від бізнес-логіки. І WAF не повинен вносити істотну затримку в цей параметр.

3) *Захищеність*. Методи атак змінюються в залежності від трендів, існуючих в розробці додатків, наприклад Web 2.0, SPA, REST API.

Разом з новими технологіями змінюється і ландшафт загроз. Отже, WAF повинен постійно поповнюватися новими методами їх виявлення.

Висновки

Результатами проведеного дослідження є розробка програмного модуля, який виконує діагностику мікросервісів Web-застосунку та реєструє інциденти пов'язані з порушеннями їх доступності для блоку кіберзахисту КСЗІ ОКІ ВТК України.

Для досягнення поставленої мети були вирішені такі завдання:

1. Розглянуто нормативно-правове забезпечення кіберзахисту України та рівень його гармонізації з міжнародними стандартами. Показано, що введені наказом Адміністрації Держспецзв'язку «Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» є адаптацією міжнародного законодавчого документу «Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0»

2. Виконана реалізація модуля забезпечення доступності Web-застосунку з мікросервісною архітектурою для блоку кіберзахисту КСЗІ ОКІ ВТК України.

Список літератури:

1. The Mob's IT Department: How two technology consultants helped drug traffickers hack the Port of Antwerp, J. Robertson, M. Riley, Bloomberg Businessweek, 07.07.2015. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/964-15>.

2. Кибербезопасность на бескрайних морях. Блог компании Positive Technologies. Информационная безопасность. 14.06.2016. – Режим доступу: <https://habr.com/ru/company/pt/blog/303198/>

3. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. 2022. Q2. Оперативний Центр Реагування на кіберінциденти державного центру кіберзахисту Державної Служби спеціального зв'язку та захисту інформації України. – Режим доступу: <https://scpc.gov.ua/api/docs/19b0a96e-8c31-44bf-863e-cd3e0b651f20/19b0a96e-8c31-44bf-863e-cd3e0b651f20.pdf>

4. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Адмі-

ністрація Держспецзв'язку; Наказ, від 06.10.2021 № 601. – Режим доступу: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciiinoyi-infrastrukturi>

5. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. National Institute of Standards and Technology. February 12, 2014). – Режим доступу: <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

УДК 681.391

АНАЛІЗ МЕТОДИК ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗВУКОІЗОЛЯЦІЇ В ЗАХИСТІ МОВНОЇ ІНФОРМАЦІЇ

***Автор:** Сизов М.О., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Сірівчук А.С., к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Роботи з побудови системи захисту мовної інформації від витоків віброакустичними каналами традиційно починається з оцінки існуючої та забезпечення необхідної звукоізоляції виділених приміщень, оскільки звукоізоляція є основним пасивним засобом захисту акустичної інформації і спрямована на локалізацію акустичних сигналів всередині приміщень.

Звукоізоляція – ослаблення звуку при його проникненні через огороження будівель; у ширшому сенсі – сукупність заходів щодо зниження рівня шуму, що проникає у приміщення ззовні або виходить з нього. Кількісна міра звукоізоляції огорожувальних конструкцій, що виражається в децибелах (дБ), називається звукоізолюючою здатністю. Розрізняють звукоізоляцію повітряного та ударного шуму.

Звукоізоляція повітряного шуму характеризується зниженням рівня звуку (мова, спів, музика) при проходженні його через огороження та оцінюється частотною характеристикою звукоізоляції в діапазоні частот 100-3200 Гц з урахуванням фонду звукопоглинання в приміщенні, що ізолюється.

Звукоізоляція ударного шуму (звук кроків, рух меблів і т.п.) залежить від рівня звуку, що виникає під перекриттям, і оцінюється частотною характеристикою наведеного рівня ударного шуму в тому ж діапазоні частот при роботі на перекритті стандартної ударної машини, також з урахуванням фонду звукопоглинання в приміщенні, що ізолюється.

Звукоізоляція приміщень забезпечується за допомогою архітектурних та інженерних рішень, а також застосуванням спеціальних будівельних та оздоблювальних матеріалів.

Оцінка ефективності звукоізоляційних конструкцій щодо витоку інформації з обмеженим доступом (ІзОД) акустичними каналами є складовою оцінювання захищеності мовної інформації на об'єктах інформаційної діяльності, що атестуються по вимогах інформаційної безпеки, і проводиться в процесі спеціальних досліджень та технічного контролю ефективності захисту інформації [1–3].

Метою роботи є аналіз існуючих методик оцінювання ефективності звукоізоляції для подальшого розвитку методик та пристосування їх до оцінки захищеності мовної інформації на основі критерію словесної розбірливості.

При виконанні замірів оцінки звукоізоляції кімнати необхідно дотримуватись наступних вимог:

- спрямованість – звук повинен випромінюватися однаково від джерела звуку в усіх напрямках, тобто гучномовець має бути всенаправленим. Ступінь спрямованості визначається стандартами і є функцією виключно гучномовця і не залежить від властивостей вихідної кімнати;

- спектр – незважаючи на те, що вимірювання звукоізоляції є вимірюванням різниці, стандарти передбачають, що різниця між сусідніми 1/3-октавними смугами становить максимум 6 дБ. Частотна характеристика приміщення впливатиме на результат, тому ця вимога стосується вимірювання, а не обладнання. Коротше кажучи, мета полягає в тому, щоб мати якнайплатіший вихідний сигнал кімнати для виконання вимірювань;

- рівень звукової потужності – вихідна звукова потужність гучномовця має бути достатньо високою, щоб рівень звукового тиску в приймальній кімнаті був значно вищим за рівень фонового шуму. Ця вимога залежить як від гучномовця, так і від підсилювача потужності, який його керує;

- стабільність рівня – щоб бути придатним для вимірювання акустики будівлі, потужність звуку не повинна суттєво змінюватися як

функція часу. Коли гучномовець нагрівається, ефект «стиснення» зменшить рівень звуку, цей ефект слід компенсувати, щоб падіння рівня було менше 0,2 дБ/хв.

Стандартна методика інструментально-розрахункової оцінки звукоізоляції огорожувальних конструкцій в галузі інформаційної безпеки базується на методиці оцінки захищеності приміщення від витoku інформації по акустичному каналу і полягає у визначенні коефіцієнтів звукоізоляції огорожувальних конструкцій (ОК) в октавних смугах зі середньгеометричними частотами 125, 250, 500, 1000, 2000, 4000, 8000 Гц і наступним зіставленням отриманих коефіцієнтів з їх нормативними значеннями [2,3].

Суть вимірювання та розрахунку коефіцієнтів звукоізоляції полягає в наступному:

- вимірюється рівень так званого тестового сигналу, випромінюваного акустичною системою;
- вимірюється рівень фонових шумів в контрольній точці;
- вимірюється рівень сумарного акустичного сигналу в контрольній точці та розраховується рівень небезпечного сигналу;
- розраховується коефіцієнт звукоізоляції.

Стандарт ДСТУ Б В.2.6-86:2009 [4] установлює методи вимірювання ізоляції повітряного і ударного шуму внутрішніми і зовнішніми огорожувальними конструкціями і їх елементами будинків і споруд у лабораторних і натурних умовах.

Метод вимірювання ізоляції повітряного шуму полягає у порівнянні середніх рівнів звукового тиску перед та за випробовуваною огорожувальною конструкцією.

Передавальний тракт для створення шуму при вимірюваннях ізоляції повітряного шуму повинен містити: генератор шуму з діапазоном від 20 Гц до 15000 Гц; підсилювачі потужності згідно з ГОСТ 24388; гучномовці (акустичні системи) з робочим діапазоном від 50 Гц до 10000 Гц і нерівномірністю частотної характеристики не більше ніж 15 дБ.

В залежності від місця проведення вимірів методи можуть бути використанням двох суміжних ревербераційних кімнат або з використанням мініатюрної випробувальної камери [5].

Метод із використанням двох суміжних ревербераційних кімнат. Для визначення показника шумопоглинання бар'єрів у діапазоні частот понад 5 кГц. Випробування проводяться в наборі з двох горизонтально суміжних ревербераційних камер. Тестові елементи встановлюються в отвір у перегородці між цими камерами. Розмір пробного отвору 0,7 x 0,7 м.

Визначення звукоізоляції бар'єру полягає у проведенні вимірювань рівнів звукового тиску у вихідній та приймальній кімнатах з подальшим розрахунком різниці між двома значеннями. Вимірювання звукового тиску проводяться в діапазоні частот від 5 кГц до 12,5 кГц. Випробувальний стенд складається з наступних компонентів: звукова система в камері джерела, ланцюжок аналізу та вимірювання та моніторинг випробувань.

Кімната джерела збуджується широкосмуговим шумом (білим шумом), який генерується генератором шуму аналізатора через підсилювач потужності та гучномовець. Акустичні сигнали з обох приміщень одночасно передаються на двоканальний аналізатор і лінійно усереднюються протягом 12 с для кожної точки вимірювання. Загалом вимірювання звукового тиску проводяться у 12 точках вимірювань у вихідній кімнаті та у 12 точках вимірювань у приймальній.

Описаний попередній метод визначення показника шумопоглинання бар'єрів має обмежений діапазон частот вимірювання, тому більш ефективним є другий метод – метод з використанням мініатюрної ревербераційної камери.

Характеристики звукоізоляційних властивостей бар'єрів у діапазоні частот понад 5 кГц було запропоновано новий параметр, а саме індекс звукоізоляції бар'єру [5]. Показник звукоізоляції бар'єру D_U в дБ визначається за формулою:

$$D_U = L_1 - L_2,$$

де L_1 – рівень звукового тиску в 1/3-октавних смугах із центральними частотами в діапазоні від 5 до 25 кГц, виміряний у певному місці, де в отворі вимірювання не встановлено бар'єр, у дБ;

L_2 – рівень звукового тиску в 1/3-октавних смугах із центральними частотами в діапазоні від 5 до 25 кГц, виміряний у певному місці, де встановлено бар'єр у вимірювальному отворі, у дБ.

Для визначеного таким чином показника звукоізоляції бар'єру ключовим елементом випробувального стенду, встановленого для йо-

го визначення, є мініатюрна випробувальна камера у формі куба об'ємом 2,8 м³. Виготовляється з багат шарових пресованих деревних плит. У верхній стінці камери розташований вимірювальний отвір 0,34 x 0,34 м, в якому встановлюється випробуваний бар'єр. Всередині камери встановлено джерело ультразвукового шуму, а саме твітер

Випробувальний стенд встановлювався в акустичній камері, в якій виконувалися умови вільного акустичного поля над звуковідбивною поверхнею. Вимірювальний мікрофон був встановлений в центральному положенні відносно вимірювального отвору, на висоті 0,25 м від поверхні верхньої стінки мініатюрної випробувальної камери.

Висновок.

Аналіз методів методик оцінювання ефективності звукоізоляції показує, основним засобом вимірювання звукоізоляції є вимірювання різниці звукового тиску в кімнаті з вимпромінювачем звуку та дослідній кімнаті на різних частотах. Використання таких методик для визначення ефективності змовної інформації вимагає додаткових обчислень, оскільки мовна інформація на різних частотах сприймається по різному.

Список літератури:

1. Хорев А.А. Оценка возможностей средств акустической (речевой) разведки, Специальная техника. 2009. № 4. 49–63 сс.
2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов, М.: ООО "Издательство Машиностроение", 2009. 508 с.
3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие, М.: Горячая линия-Телеком, 2005. – 416
4. ДСТУ Б В.2.6-86:2009 "Конструкції будинків і споруд. Звукоізоляція огорожувальних конструкцій. Методи вимірювання.", Київ: Мінрегіонбуд України, 2010. 46 с.
5. Pleban D., Mikulski W. Methods of testing of sound insulation properties of barriers intended for high frequency noise and ultrasonic noise protection, Journal of mechanical engineering – Strojnicky časopis, vol 68 (2018), no 4, 55 – 64.

УДК 004.056.5;057.2

АНАЛІЗ ЗАХИЩЕНОСТІ БЕЗДРотовИХ ТОЧОК ДОСТУПУ В МЕРЕЖІ WI-FI

***Автор:** Соболев В.В., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Козирев С.С., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Тенденцією розвитку сучасних Wi-Fi пристроїв є активне впровадження нових більш захищених методів протоколювання Wi-Fi, внаслідок чого з'являються нові протоколи безпеки, а традиційні моделі набувають нового змісту.

Метою даної роботи є дослідження перспектив застосування протоколів бездротової мережі Wi-Fi.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз всіх протоколів;
- визначити типові напрями атаки які можуть використовуватися;
- визначити методи покращення безпеки;

На цей час, існує не так багато протоколів безпеки Wi-Fi, а саме: WEP, WPA, WPA2, WPA3, OWE.

• Протокол WEP. Протокол WEP, представлений у 1999 році, є першою версією сімейства протоколів безпеки бездротової мережі IEEE 802.11. Через два роки після його впровадження цей протокол був зламаний через його довжину ключа та погану структуру та криптографічний алгоритм.

• Протокол WPA. Введено для вирішення проблем попередніх протоколів, а саме WEP. Цей протокол оснащено більш надійним шифруванням протоколу часової цілісності ключа (TKIP), а його довжина ключа становить 128 біт замість ключа на 40 біт.

• Протокол WPA2. Замінив протокол WPA в 2004 році. Цей протокол був оснащений ланцюгом блоків шифрування в режимі лічильника (CCMP) з алгоритмом AES. Є найпопулярнішим протоколом у даний час. З 2017 року став ненадійним після публікації атаки Krack.

• Протокол WPA3 Найсучасніший протокол безпеки, котрий покриває майже всі недоліки минулого зразку, але ще не набув тієї попу-

лярності в розповсюдженні. Оскільки головна уразливість приховувалася у чотирьохсторонньому рукостисканні, у WPA3 додалася обов'язкова підтримка більш надійного методу захисту SAE, також відомого як Dragonfly. У цьому разі довжина ключа може становити 192, для автентифікаційного шифрування 256(GCMP-256) для захисту цілісності кадрів – VIP-GMAC-256, а для передачі і підтвердження ключів використовується HMAC з хешами SHA-384.

• OWE – це стандарт Wi-Fi запроваджений разом із WPA3 але є безпарольним тобто – відкритим, який гарантує, що зв'язок між кожною парою кінцевих точок захищений від інших кінцевих точок. На відміну від звичайного Wi-Fi, він забезпечує «індивідуальний захист даних» таким чином, що трафік даних між клієнтом і точкою доступу «індивідуалізований». Інші клієнти все ще можуть отримувати та записувати цей трафік, але не можуть його розшифрувати.

Чому не варто використовувати протоколи WEP, WPA? Таблиця 1 дасть відповідь на це запитання.

Саме через велику кількість ймовірних атак ці протоколи краще не використовувати.

Таблиця 1. Зведення найпопулярніших атак відновлення секретного ключа на WEP та WPA

Протокол	Атака	Тип	IV-пошук	Рік
WEP	FMS	Статистичний	Рандом	2001
	Korek			2004
	PTV		Рандом	2007
	VV		Рандом	2007
	Klein	Відновлення ключа	Рандом	2008
	BT		Aircraft-ng	2009
WPA	Словникова атака	Відновлення ключа		
	Beck and Tews	QoS		2009
	Ohigashi-Morii	Введення пакетів		2009
	Hole196	Людина посередині		2010

WPA-2 був непоганим протоколом але для нього існувало вже безліч різновидностей атак, одними з таких атак є атака попарного ідентифікатора головного ключа (PMKID). Атака яка зруйнувала захист цього протоколу це атака KRACK Exploit. Перехід до WPA-3 прибрав лазійки майже всіх відомих атак на WPA-2 окрім атаки Evil-Twin, навіть атака KRACK Exploit була безпорадна проти WPA-3.

Підвищити безпеку наявних протоколів можна звичайними методами: Приховування SSID мережі; Вибір надійного пароля та часта його зміна; В жодному разі не використовувати кнопку WPS на Wi-Fi роутері, використання цього засобу дуже сильно знижує безпеку Wi-Fi роутеру і дає можливість дуже простого захоплення контролю небажаним людям; Оновлення бездротового пристрою; Використання вузькосмугових фільтрів є вигідним для підвищення безпеки мережі.

Висновки. В даній роботі проведено аналіз аналіз протоколів мереж Wi-Fi, методів їх злому та обходу захисту, визначені типові методи підвищення безпеки. WEP і WPA це дуже ненадійні протоколи, через невелику довжину ключа і тому хакери який дуже просто отримає доступ як до самої мережі, так і до пакетних даних які ви використовуєте, тим паче що для зламу системи на цих протоколах може вистачити навіть звичайного словникового підбору! WPA-2 можна використовувати але на свій страх і ризик, це не досить надійний протокол на даний час. Єталоном надійності і захищеності можна вважати WPA-3, саме на нього слід звертати увагу при виборі найбезпечнішого хоча і він не захищає від всіх видів атак.

Список літератури:

1. A. Terkawi, and N. Innab, "Major impacts of key reinstallation attack on Internet of Things system." 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018.
2. R. Guo, "Survey on Wi-Fi infrastructure attacks", International Journal of Wireless and Mobile Computing vol.16, no.2, pp.97-101, 2019.
3. A. Sari, and M. Karay, "Comparative analysis of wireless security protocols: WEP vs WPA", International Journal of Communications, Network and System Sciences, vol.8, no.12, p.483, 2015.

РОБОТА ТА МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ В УМОВАХ ВОЄННОГО СТАНУ

***Автори:** Трибулькевич С.Л., ст. викладач; Трибулькевич В.В., аспірантка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Більшість сучасних бізнес та технологічних процесів оцифровані та пов'язані з роботою ІТ-систем, таких як ERP, CRM, SCADA, тощо. Тому будь-які збої в ІТ-інфраструктурі спричиняють фінансові та репутаційні втрати для бізнесу. Робота підприємства в умовах воєнного стану пов'язана з деякими труднощами у функціонуванні ІТ підсистем, якими можуть являтися відсутність електроживлення, труднощі у системах зв'язку, руйнування мережевої інфраструктури через обстріли.

Для безперебійного функціонування мережевого та серверного обладнання у складних умовах необхідно виконання таких заходів:

- резервування живлення за рахунок використання генераторів та оснащення критичного обладнання джерелами безперебійного живлення;
- резервування каналів виходу у мережу Інтернет шляхом використання різних провайдерів, а також мобільних або супутникових технологій;
- надання працівникам, що евакуювалися у інші міста України та світу, захищених каналів доступу до внутрішньої мережі підприємства;
- резервування каналів зв'язку у внутрішній мережі шляхом прокладки кабелів різними маршрутами та використанням бездротових технологій;
- своєчасне копіювання даних у локальні та хмарні сховища резервних копій;
- постійний моніторинг мережі та серверного обладнання, сповіщення про виникнення аварійних ситуацій.

Моніторинг роботи мережевого устаткування та ключового ПО – це одна з найважливіших задач системного адміністрування. Сучасні комп'ютерні системи побудовані на мережі Internet, або об'єднані в локальну мережу з подальшим виходом до Internet. Ураховуючи сучасний стан інформаційних і комунікаційних технологій для концентрації інформації щодо комп'ютерних мереж постає проблема моніторингу. Доцільним є створення програм мережевого моніторингу для

забезпечення доступу до інформації, стосовно мережевого контенту, топології, обладнання як спеціалістів так і користувачів.[1]

Zabbix – це повномасштабний інструмент для мережного й системного моніторингу мережі, який поєднує кілька функцій в одній веб-консолі. Він може бути сконфігурован для моніторингу й збору даних із самих різних серверів і мережних пристроїв, забезпечуючи обслуговування й моніторинг продуктивності кожного об'єкта. Zabbix дозволяє робити моніторинг серверів і мереж за допомогою широкого набору інструментів, включаючи моніторинг гіпервізорів віртуалізації й стеков веб-додатків.

В основному, Zabbix працює із програмними агентами, запущеними на контрольованих системах. Але цей розв'язок також може працювати й без агентів, використовуючи протокол SNMP або інші можливості для здійснення моніторингу. Zabbix підтримує VMWare і інші гіпервізори віртуалізації, надаючи докладні дані про продуктивність гіпервізор і його активності. Особлива увага також приділяється моніторингу серверів додатків Java, веб-сервісів і баз даних.

Zabbix дозволяє набудовувати панелі моніторингу й веб-інтерфейс, щоб сфокусувати увагу на найбільш важливих компонентах мережі. Повідомлення й ескалації проблем можуть ґрунтуватися на діях, що настроюються, які застосовуються до хостів або груп хостів. Дії можуть навіть настроюватися для запуску віддалених команд, тому якийсь ваш сценарій може запускатися на контрольованому хості, якщо спостерігаються певні критерії подій.

Програма відображає у вигляді графіків дані про продуктивність, такі як пропускна здатність мережі й завантаження процесора, а також збирає їх для систем, відображення, що настроюються. Крім того, Zabbix підтримує карти, що настроюються, екрани й навіть слайд-шоу, що відображають поточний статус контрольованих пристроїв.

Zabbix може бути складним для реалізації на початковому етапі, але розумне використання автоматичного виявлення й різних шаблонів може частково полегшити труднощі з інтеграцією. На додаток до встановлюваного пакета, Zabbix доступний як віртуальний пристрій для декількох популярних гіпервізорів.

Дуже зручно переглядати працездатність пристроїв на мапі (рис. 1). Також з вікна мапи можна викликати вікна Dashboard пристроїв для перегляду детальної інформації або запуску простих тестів.



Рисунок 1 – Система моніторингу

Якщо потрібно включити в систему обладнання, що не має мережних інтерфейсів, то можна використати перетворювачі інтерфейсів Ethernet – RS232. У даному випадку інформаційний обмін може бути реалізовано шляхом використання спеціалізованих драйверів віртуальних послідовних портів. Шляхом тестування подібного програмного забезпечення визначено, що найбільш функціональним є Null-modem emulator [2] це драйвер віртуального послідовного порту Windows, який працює в режимі ядра (kernel-mode driver), з відкритим вихідним кодом, доступний під захистом ліцензії GPL. Null-modem emulator дозволяє створювати необмежену кількість пар віртуальних COM-портів. Кожна пара COM-портів складається з двох COM-портів, віртуально з'єднаних один з одним каналом даних. Вихід одного COM-порту пари з'єднується з входом іншого COM-порту пари, і навпаки. Отже, можна використовувати будь-яку пару для з'єднання будь-якої однієї програми, розрахованої на роботу з COM-портом, з іншим додатком, що також працює з COM-портом, і вони будуть передавати дані один одному. Єдиним знайденим недоліком даного програмного забезпечення є відсутність цифрового підпису драйверів, що ускладнює встановлення у сучасних операційних системах.

На стороні ПК за зв'язок відповідають 3 пари послідовних портів, об'єднаних одним концентратором (рис. 2):

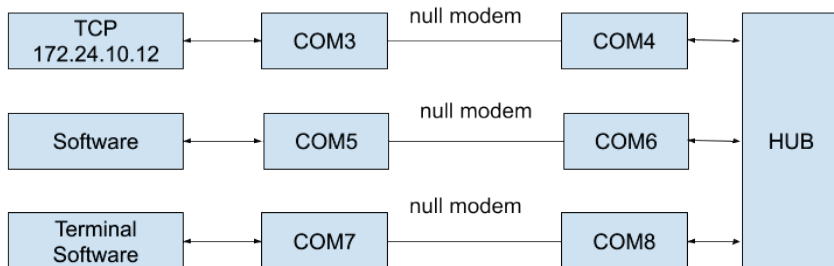


Рисунок 2 – Схема послідовних портів

– Пара COM3-TCP відповідає за зв'язок з обладнанням. 172.24.10.12 – IP адреса перетворювача Ethernet – RS232;

- Пара COM5-Software призначена для опитування та видачі параметрів за допомогою існуючого програмного забезпечення;
- Пара COM7-Terminal Software призначене для діагностики за будь-якого термінального ПЗ, наприклад, Putty.

Дана схема використовується для моніторингу роботи джерел безперебійного живлення APC Smart SMC1500I-2U не оснащених UPS Network management card. Дане рішення дозволяє перекласти роль моніторингу та керування завершенням роботи фізичних серверів на віртуальну машину, подібна ситуація настає у разі складнощів при розгортанні оригінального програмного забезпечення від виробника джерела безперебійного живлення напряму у операційній системі Server Core гіпервізору. Експлуатація даного обладнання показала роботоспроможність даної схеми, стабільність виводу параметрів у стандартне програмне забезпечення для ПК, широкі можливості по маршрутизації потоків даних між віртуальними послідовними портами та можливість перехвату потоку даних, його аналізу та передачі у інше програмне забезпечення, відмінне від стандартного.

Для віддаленого доступу користувачів використовуються різноманітні протоколи VPN. Протокол тунелювання точка-точка (Point-to-Point Tunneling Protocol) – це протокол, винайдений Microsoft для організації VPN через мережі комутованого доступу. PPTP є стандартним протоколом для побудови VPN вже багато років. Хоча PPTP зазвичай і використовується зі 128-бітовим шифруванням, у наступні кілька років після включення цього протоколу до складу Windows 95 OSR2 у 1999 році було знайдено низку вразливостей. Найбільш серйозною з яких стала вразливість протоколу аутентифікації MS-CHAP v.2. Використовуючи цю вразливість, PPTP було зламано протягом 2 днів. І хоча компанією Microsoft було виправлено цю помилку (за рахунок використання протоколу аутентифікації PEAP, а не MS-CHAP v.2), вона сама рекомендувала до використання як VPN проколів L2TP або SSTP.

Протокол тунелювання 2 рівня (Layer 2 Tunnel Protocol) – це протокол VPN, який сам по собі не забезпечує шифрування та конфіденційність трафіку, що проходить через нього. З цієї причини зазвичай використовується протокол шифрування IPsec для забезпечення безпеки та

конфіденційності. L2TP/IPsec вбудований у всі сучасні операційні системи та VPN-сумісні пристрої, і так само легко може бути налаштований як і PPTP (зазвичай використовується той самий клієнт). Проблеми можуть виникнути в тому, що L2TP використовує UDP-порт 500, який може бути заблокований фаїрволом, якщо ви за NAT. Тому може знадобитися додаткове налаштування роутера (перееадресація портів).

Протокол IPsec на даний момент не має жодних серйозних уразливостей і вважається дуже безпечним під час використання таких алгоритмів шифрування, як AES. Однак, оскільки він інкапсулює дані двічі, це не так ефективно, як рішення SSL (наприклад, OpenVPN або SSTP), і тому працює трохи повільніше.

Протокол безпечного тунелювання сокетів (Secure Socket Tunneling Protocol) – був представлений Microsoft у Windows Vista SP1, і хоча він тепер доступний на Linux, RouterOS та та ін., він, як і раніше, використовується значною мірою лише Windows-системами. SSTP використовує SSL v.3 і, отже, пропонує аналогічні переваги, що і OpenVPN (наприклад, можливість використовувати TCP-порт 443 для обходу NAT).

OpenVPN є програмним додатком з відкритим вихідним кодом, який використовує можливості віртуальної приватної мережі (VPN) для створення захищених з'єднань точка-точка або сайт-сайт на всьому маршруті інформації, а також при використанні містків конфігурацій дистанційно. Всередині OpenVPN використовуються протоколи безпеки SSL (Secure Socket Layer – рівень захищених сокетів) або TLS (Transport Layer Security – безпека транспортного рівня), за допомогою яких користувачі можуть обмінюватися ключами.

OpenVPN є досить новою технологією з відкритим кодом, яка використовує бібліотеку OpenSSL та протоколи SSLv3/TLSv1, поряд з багатьма іншими технологіями для забезпечення надійного VPN-рішення. Однією з його головних переваг є те, що OpenVPN дуже гнучкий у налаштуваннях. Цей протокол може бути налаштований на роботу на будь-якому порту, у тому числі на 443 TCP-порту, що дозволяє маскувати трафік усередині OpenVPN під звичайний HTTPS (який використовує, наприклад, Gmail) і тому його важко заблокувати.

Отже OpenVPN має найбільш високу захищеність, можливість використання у будь-яких операційних системах таких, як Windows,

Linux, Android, Mac OS та iOS, можливість використовувати 443 TCP порт для маскування трафіку та обходу блокування провайдером GRE трафіку. Саме тому даний протокол було використано для віддаленого доступу користувачів через канали зв'язку з невизначеними блокуваннями та з будь-яких персональних пристроїв.

OpenVPN сервер легко реалізувати на будь-якій операційній системі Linux та налаштувати одним із готових скриптів. Також можлива реалізація серверу у RouterOS, але щоб повноцінно використовувати OpenVPN-сервер на Mikrotik, потрібно оновити версію прошивки до версії 7.1 і вище, крім того, у Mikrotik OpenVPN трохи урізаний: немає підтримки UDP (додали до стабільної версії RouterOS 7.1), немає LZO-компресії. Тому при готовому середовищі віртуалізації роль сервера віддаленого доступу віддано віртуальній машині Debian (рис. 3).

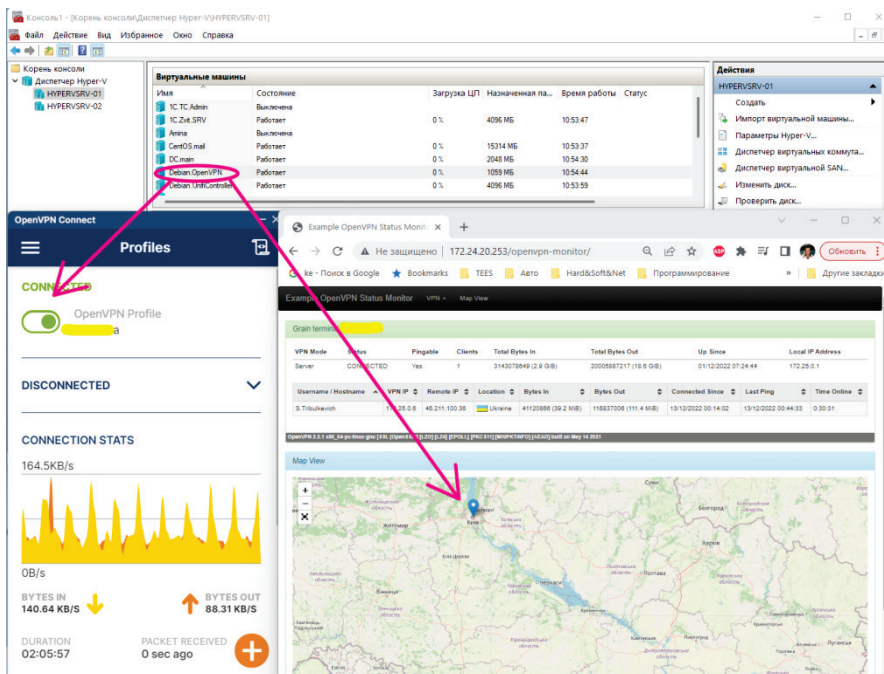


Рисунок 3 – Сервер та клієнт OpenVPN

Секція 2. **Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах**

При використанні стаціонарних провайдерів зв'язку зовнішня «біла» IP адреса може бути визначена за рахунок служб DNS та динамічного оновлення А записів при переключенні між основним та резервними каналами зв'язку. При переході на доступ в інтернет через мережі стільникового зв'язку або тимчасовому переміщенні серверного обладнання у безпечні місця, отримання «білої» IP адреси може бути не можливим, тоді найбільш простим способом побудови роботи мережі VPN є сервер у хмарі, у даному випадку системні вимоги до серверу невисокі та можливе використання не дорогих VPS.

Однією із найбільш ефективних систем резервного копіювання є Veeam Backup and Replication (рис. 4), яка забезпечує бізнес-стійкість, захист даних від зловмисників, запобігання втратам даних і вимушеним простоям. Надійне перенесення даних у хмару та відсутність прив'язки до постачальника завдяки мобільності хмарних рішень. Доступні варіанти інтеграції з більш ніж 100 системами зберігання даних та хмарними інфраструктурами. Це означає максимальну гнучкість та оптимальну сукупну вартість володіння.

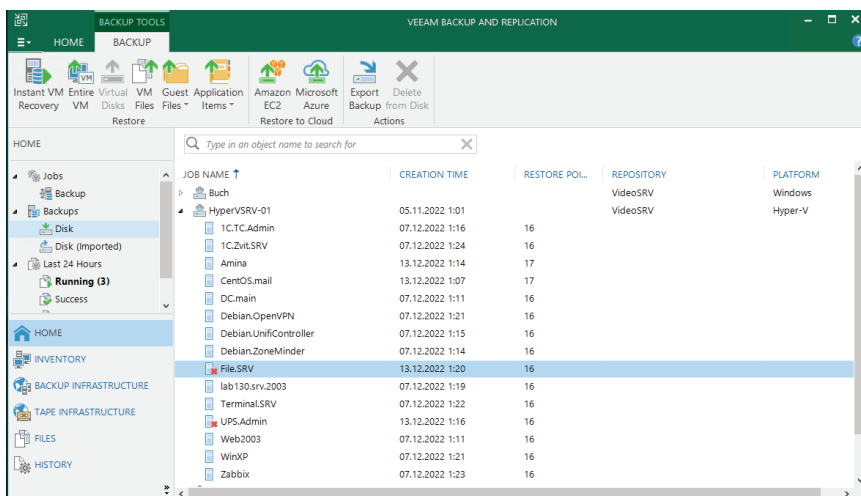


Рисунок 4 – Veeam Backup and Replication

Veeam надає гнучке комплексне рішення, яке захищає дані чотирма різними способами та гарантує дотримання вимог до RPO та RTO.

Для захисту невеликої кількості фізичних та віртуальних машин є безкоштовні редакції.

Висновок: Надано загальні рекомендації по роботі ІТ інфраструктури підприємства малого та середнього бізнесу. Дані рекомендації справедливі незалежно від умов воєнного чи мирного часу, але в умовах саме воєнного часу себе проявляють найбільш тонкі місця ІТ інфраструктури. Своєчасне реагування на сповіщення систем моніторингу дозволяють забезпечити стабільну та безперебійну роботу наскільки це можливо в даних умовах.

Список літератури:

1. Гузій, М. М., Станіславова, О. В., Кадет, М. В. Аналіз технологій моніторингу комп'ютерних мереж. Наукоємні технології, № 1, 2009. Відновлено з <https://jml.nau.edu.ua/index.php/SBT/article/view/5091>
2. Null-modem emulator (com0com). Відновлено з <http://com0com.sourceforge.net/>

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ РЕЖИМНО-СЕКРЕТНОГО ВІДДІЛУ МОРСЬКОГО ПОРТУ

***Автор:** Харченко М.С., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Баронова О.А., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Морський транспортний комплекс є багатофункціональною структурою, що задовольняє потреби національної економіки у транспортному забезпеченні. Від ефективності функціонування морських портів, рівня їх технологічного та технічного оснащення, відповідності системи управління та розвитку інфраструктури сучасним міжнародним вимогам залежить конкурентоспроможність вітчизняного транспортного комплексу на світовому ринку.

Після вторгнення РФ портова галузь України була паралізована. Чотири морські порти – Херсонський, Скадовський, Бердянський та

Маріупольський, частка яких у загальній переробці вантажів усіма морськими портами України у 2021 р. становила 7,2 %, або 11,1 млн т на рік, окуповані. Ще шість портів – Білгород-Дністровський, Одеський, Миколаївський, Чорноморськ, Ольвія та Південний змушені були призупинити роботу на відвантаження через небезпеку морських перевезень та загрозу обстрілів.

Одним з проявлень незаконних дій спецслужб РФ та їх союзників (хакерів з КНДР та Ірану) є масовані кібератаки на інформаційні ресурси України, в тому числі й на об'єкти критичної інфраструктури водно-транспортного комплексу України. За інформацією Голови Держспецв'язку Юрія Щиголя з початку повномасштабного вторгнення Росія здійснила 796 кібератак проти України. З них майже 18,5 % на сервери уряду України та місцеві органи влади та 13 % на сектор безпеки та оборони [1].

Робота присвячена актуальному питанню – аналізу кібернетичних та інформаційних загроз об'єктам критичної інфраструктури портову та розробленню комплексної системи захисту інформації для режимно-секретного відділу.

Об'єктом ОІД для якої створюється КСЗІ є одним із важливіших підрозділів порту задіяних в організації захисту інформації на об'єкті – РСО.

Комплекс ТЗІ створюється за рішенням (наказом) керівника підприємства морської галузі (порту, судноплавної компанії або ін.) про створення комплексу ТЗІ.

Комплекс ТЗІ створюється за такими етапами:

I етап – попередній етап створення комплексу СЗІ;

II етап – проектування і розробка комплексу СЗІ;

III етап – проведення випробувань і передачі в експлуатацію комплексу СЗІ.

Після упровадження проводиться атестація КСЗІ.

Перед створенням комплексу СЗІ визначаються об'єкт інформаційної діяльності та контрольована зона.

У наказі керівника підприємства про визначення об'єкта інформаційної діяльності встановлюється, яка саме інженерно-технічна споруда (приміщення), зона територія або транспортний засіб (із зазначенням відповідної назви, приналежності, адреси, номера приміщення, позначення тощо) є об'єктом інформаційної діяльності, також надається план споруд

ди (зони, території) із зазначенням контуру ОІД, розмірами ОІД та стислим описом розташування ОІД у споруді (місцевості).

У Наказі про визначення контрольованої зони встановлюється межа контрольованої зони навколо ОІД (споруди, в якій розташована ОІД), надається її опис, вказуються відстані від межі КЗ з точною межею (периметром або контуром).

Визначення об'єкта інформаційної діяльності та контрольованої зони, а також прийняття рішення щодо створення комплексу ТЗІ можуть вказуватися в одному наказі.

Розроблюється Положення про Службу захисту інформації, яка визначить завдання, функції, штатну структуру СЗІ в ІТС Метою створення СЗІ є організаційне забезпечення завдань керування КСЗІ в ІТС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

Правову основу для створення і діяльності СЗІ становлять Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, Положення про технічний захист інформації в Україні, Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах.

Розроблюється положення про службу захисту. План захисту є обов'язковим документом в установах, організаціях, в яких здійснюється обробка службової інформації в інформаційно-телекомунікаційних системах (ІТС).

Актуальність роботи обумовлена тим, що підприємства морської галузі відносяться до об'єктів критичної інфраструктури водно-транспортного комплексу [2], від безпеки інформаційних потоків яких залежить сталий розвиток всіх сфер життєдіяльності держави і суспільства [3].

Метою даної роботи є підвищення захищеності підрозділу режимно-секретного органу морського порту від витоку інформації за рахунок впровадженням комплексної системи захисту інформації.

Для реалізації поставленої цілі в даній кваліфікаційній роботі було проведено аналіз нормативно-правових документів у сфері техніч-

ного захисту інформації, проаналізовано особливості морського порту як об'єкту інформаційної діяльності та розроблення проекту по впровадженню комплексної системи захисту інформації режимно-секретного відділу морського порту. Результати роботи призначені для використання при побудові комплексної системи захисту інформації на об'єктах морської інфраструктури та можуть бути використані в навчальному процесі для здобуття студентами практичних навичок у відповідності з напрямками підготовки з кібербезпеки.

Висновки

В роботі було проведено огляд нормативних документів, щодо захисту інформації на об'єктах портової галузі. Виконано аналіз особливостей порту як ОІД основних загроз інформації, було розроблено проект по комплексної системи захисту інформації режимно-секретного відділу морського порту та повний комплект для впровадження .

Було розроблено комплект документів, які пов'язані з технічним захистом інформації при роботі на ПЕОМ. Проведенні випробування інформаційно-телекомунікаційних системах в автоматизованій системі класу «1», які включають в себе наступні види контролю:

а) перевірка ТЗ на створення КСЗІ ІТС на відповідність вимогам типового ТЗ (або наявності типового ТЗ);

б) аналіз та оцінка відповідності організаційно-технічної документації на КСЗІ ІТС вимогам нормативних документів щодо організації обробки ІзОД, НД ТЗІ та вимогам з ТЗІ;

в) перевірка відповідності вихідних даних реальній комплектності ІТС;

г) перевірка впровадження організаційно-технічних заходів захисту інформації та дотримання режиму доступу до ІзОД згідно з вимогами г)ТЗ;

д) перевірка виконання вимог щодо захисту від НСД згідно з вимогами ТЗ;

е) перевірка виконання вимог щодо функціонування системи антитвірусного захисту та контроль цілісності ПЗ (КЗЗ).

Розроблена КСЗІ відповідає вимогам відповідних нормативним правових документів. Показано в результатах, що дана КСЗІ відповідає вимогам і дає можливість продовжити з нею працювати від реєстрації до встановлення на реальному об'єкті інформаційної діяльності пов'язана не лише з морською галуззю, а й із всіма іншими.

Список літератури:

1. Росія – законна ціль. Інтерв'ю Голови Держспецзв'язку України Юрія Щиголя про санкції та невдалі кібератаки РФ. [URL]: <https://glavcom.ua/techno/telecom/golova-derzhspeczvyazku-rozpoviv-pro-kilkist-kiberatak-rf-proti-ukrajini-z-pochatku-vtorgnennya-857009.html>
2. Порядок формування переліку об'єктів критичної інформаційної інфраструктури [Текст]: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 [URL]: <https://zakon.rada.gov.ua/laws/show/943-2020-p>.
3. Про внесення змін до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інфраструктури [Текст]: Наказ адміністрації державно\ служби спеціального зв'язку та захисту інформації України від 10 липня 2021 р. № 343 [URL]: <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601>

СЕКЦІЯ 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***Автор:** Матрасва Д.В., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Забезпечення інформаційної безпеки України, безпеки її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері протидії загрозам цих інтересів та впорядкування відповідного правотворчого процесу.

Створення дієвого механізму забезпечення прав, свобод і законних інтересів фізичних та юридичних осіб належить до пріоритетних напрямів діяльності держави та органів публічної адміністрації зокрема. Це питання є дуже актуальним, адже є пріоритетним не лише для України, а і для всього світового співтовариства, і перестало бути «сферою зацікавленості» окремих держав світу та міжнародних або національних правозахисних організацій. Варто звернути увагу на той факт, що нині однією із серйозних проблем діяльності органів публічної адміністрації у сфері забезпечення інформаційної безпеки є, перш за все, невизначеність та незбалансованість окремих складових частин правового регулювання цієї сфери, зокрема чинного законодавства. У зв'язку з цим останнім часом органи державної влади та науковці приділяють значну

увагу обговоренню проблем удосконалення правового забезпечення інформаційної безпеки України. Дане правове забезпечення створюється сукупністю системи правового регулювання забезпечення інформаційної безпеки та процесу формування цієї системи.

Правова основа забезпечення інформаційної безпеки в теоретичному сенсі – це сукупність різних за юридичною силою права норм, що відносяться до різних галузей і відбивають сутність процесів, що відбуваються в сфері забезпечення інформаційної безпеки, складаючи єдину систему

Правові норми складають базу забезпечення інформаційної безпеки і визначають ефективність діяльності держави, суспільства та окремих громадян із захисту національних інтересів України в інформаційній сфері. У склад цієї бази включаються і норми міжнародних договорів України, закони України, акти Президента України, постанови уряду, нормативні акти органів державної влади, які регулюють відносини у даній сфері.

Аналіз змін в законодавчому забезпеченні інформаційної сфери України з погляду її безпеки після агресії Росії зумовлює аналіз відповідної нормативної бази, яка діяла на етапі від 90-х років і до початку російського втручання у 2014 р. і виявила необхідність її подальшого серйозного коригування відповідно до потреб часу, незважаючи на об'єктивну потребу такого акту в час, коли Україна знаходиться в стані гібридної війни, за умов якої інформаційна безпека є найбільш атакованою і, водночас, найбільш вразливою.

На сьогодні одним із важливих напрямів стратегії адміністративно-правового забезпечення інформаційної безпеки України є аналіз та удосконалення нормативно-правового регулювання в цій сфері. Так, нормативно-правове регулювання інформаційної безпеки у сфері прав та свобод здійснюється Конституцією України і такими базовими законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про поштовий зв'язок». Вказані нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони держав-

ної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів, спрямовані на реалізацію положень Доктрини безпеки особистості, держави і суспільства.

Чітко простежується кількісний пріоритет нормативно-правових актів, спрямованих на врегулювання інформаційно-технічної безпеки щодо інформаційно-психологічної та інформаційної безпеки у сфері прав та свобод, що пов'язано, на нашу думку, з інтенсивним розвитком інформаційних технологій, а отже, з необхідністю оперативного реагування щодо зміни певних стандартів у цій сфері. Особливим недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення його у численних нормативно-правових актах різної юридичної сили. Причому важливі проблеми нормативно закріплюються підзаконними нормативно-правовими актами. Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів як між собою, так і з чинною Конституцією. Характерною рисою національного інформаційного законодавства є декларативність значного масиву норм без указівок на шляхи їх реалізації, внаслідок чого спостерігається низький рівень правореалізації норм права, що регулюють суспільні відносини у сфері забезпечення інформаційної безпеки.

В інформаційній сфері, національну безпеку України, слід розглядати як єдину цілісність чотирьох складових – публічної (суспільної), персональної, корпоративної (комерційної) і державної безпеки. Саме тому, при окресленні характеру ризиків слід брати до уваги наступні елементи:

- основні елементи політичної безпеки, її принципів, стандартів та правил, погоджених із чинним законодавством й принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, корпоративних структур та держави;
- визначення об'єктів та цілей;
- визначення прийнятих з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінки ризиків та управління ризиками.

Особливе місце в системі нормативно-правових актів щодо забезпе-

печення інформаційної безпеки займають міжнародно-правові акти, зокрема: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [9]; Конвенція про кіберзлочинність [10]; Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних [11]; Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру [12]. Важливе значення у регулюванні суспільних відносин у цій сфері займають Укази Президента України, які можна згрупувати за певними сферами регулювання:

- по-перше, акти, що визначають правовий статус суб'єктів забезпечення інформаційної безпеки (зокрема Положення про Національний координаційний центр кібербезпеки, що затверджено Указом Президента України від 7 червня 2016 року № 242/2016). Саме такі акти визначають загальну спрямованість діяльності суб'єкта, а також конкретні права та обов'язки у цій сфері;

- по-друге, акти, що визначають зміст державної політики та стратегічні напрями реалізації державної політики щодо забезпечення інформаційної безпеки. Так, у зв'язку із застосуванням Російською Федерацією технологій гібридної війни проти України, використанням найновіших інформаційних технологій впливу на свідомість громадян, що спрямовані на розпалювання національної і релігійної ворожнечі, пропаганди агресивної війни, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України у 2016 році була затверджена Стратегія кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Наступною групою нормативно-правових актів, що регулюють відносини у сфері забезпечення інформаційної безпеки України, є постанови Кабінету Міністрів України.

Перша група актів Кабінету Міністрів України визначає організаційно-правові засади діяльності органів публічної адміністрації у сфері забезпечення інформаційної безпеки України, зокрема: реалізація

заходів щодо реформування цієї сфери; повноваження органів публічної адміністрації, що встановлюють межі впливу останніх; їх організаційна структура; зміст процедур із надання адміністративних послуг тощо. До цієї групи треба зарахувати постанови Кабінету Міністрів України «Положення про Державний комітет телебачення і радіомовлення України», «Положення про Міністерство оборони України», «Положення про Міністерство юстиції України», «Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України».

Друга група актів Кабінету Міністрів України визначає безпосередній зміст заходів уповноважених органів публічної адміністрації щодо забезпечення інформаційної безпеки. До них можна зарахувати такі: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»; Постанова Кабінету Міністрів України від 11 листопада 2020 р. № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом».

Підсумовуючи вищенаведене, варто зазначити, що нині в Україні вдалося досягти значних успіхів щодо нормативно-правового регулювання забезпечення інформаційної безпеки. Це насамперед зумовлено тим, що забезпечення інформаційної безпеки стало одним із пріоритетних напрямів діяльності органів публічної адміністрації, адже сучасне інформаційне середовище активно впливає на стан політичної, економічної, військової та інших складових частин національної безпеки України.

Нині правове регулювання діяльності органів публічної адміністрації щодо забезпечення інформаційної безпеки має цілісний характер, тобто ця діяльність регулюється як законами, так і указами, постановами, розпорядженнями, наказами – понад 70 нормативними актами.

Проте, незважаючи на позитивні моменти, проаналізовані нормативно-правові акти мають ряд недоліків. По-перше, встановлено, що різні нормативно-правові акти, норми яких регулюють суспільні відносини, об'єктом яких є інформаційна безпека, приймалися в різний час без узгодження понятійного апарату, вони мають низку не досить коректних термінів або взагалі не мають чіткого визначення змісту; по-друге, нині

існує низка нормативно-правових актів, що регулюють таку діяльність. Така кількість чинних нормативно-правових актів призводить до труднощів у застосуванні поданих норм; по-третє, нечітке нормативно-правове регулювання діяльності органів публічного адміністрування значно знижує їх готовність до реалізації закріплених повноважень.

Отже, з метою вдосконалення нормативно-правового регулювання забезпечення інформаційної безпеки пропонуємо провести відповідну роботу щодо систематизації та скасування «формально чинних» норм.

Список літератури:

1. Конституційно-правові засади інформаційної безпеки у парадигмі «війни нового покоління» <http://dspace.onua.edu.ua/bitstream/handle/11300/12940/Nove%20pokolinnya.pdf?sequence=1&isAllowed=y>

2. Нормативно-правове забезпечення інформаційної безпеки в Україні http://www.pravoisuspilstvo.org.ua/archive/2012/3_2012/28.pdf

3. Нуянзин С.В., Нуянзин О.С. Информационная безопасность личности и некоторые организационноправовые меры по ее обеспечению. Юридическая наука и правоохранительная практика. 2018. № 2 (44). URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-lichnosti-i-nekotorye-organizatsionnopravovye-mery-po-ee-obespecheniyu> (дата обращения: 19.01.2021).

4. Ярмоленко Ю.В. Проблеми правового регулювання діяльності ветеринарної міліції : Монографія. Київ : Магістр ХХІ сторіччя, 2010. 146 с.

5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ратифікована згідно із Законом України № 2438–VI від 06.07.2010 р. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_326

6. Статистична інформація 2020. URL: <https://old.gp.gov.ua/ua/statinfo.html>

7. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. Правова інформатика. 2009. № 4(24). С. 5–12.

8. Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. <https://ela.kpi.ua/bitstream/123456789/9686/3/04.pdf>

СЕКЦІЯ 4. МОДЕЛЮВАННЯ ОБ'ЄКТІВ І ПРОЦЕСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.5;057.2

АНАЛІЗ ПРОЦЕСУ ІДЕНТИФІКАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автори: Баронова О.А., ст. викладач; Божаткін С.М., ст. викладач; Турті М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Згідно ISO/IEC 27005:2011 [1] процес оцінки ризиків інформаційної безпеки (РІБ) є ітераційною процедурою і складається з трьох етапів (ідентифікація, аналіз і оцінювання ризику), кожен з яких містить ряд підпроцесів. Кроки ітерації для цього процесу різняться за ступенем деталізації відомостей щодо РІБ, що використовуються на етапі обробки ризиків для визначення комплексу адекватних засобів управління ризиками. При цьому важливою є повнота списків можливих загроз, вразливостей, наслідків успішної реалізації загроз, які формуються на етапі ідентифікації ризиків ІР.

Метою даної роботи є структуризація знань щодо процесу ідентифікації ризиків інформаційної безпеки, для чого необхідно провести аналіз стандартизованого процесу ідентифікації РІБ, визначити структурні компоненти системи знань в цій предметній галузі та їх взаємозв'язки.

Метою ІР є визначення множини потенційно небезпечних для організації подій, їх витоків і наслідків з достатнім для прийняття рішень щодо обробки ризиків ступенем деталізації. До складу процесу ІР ризиків входять, згідно ISO/IEC 27005 п'ять підпроцесів ідентифікації для активів, загроз, засобів контролю, вразливостей і наслідків. На першому кроці ітерації проводиться високорівнева оцінка ризиків за спрощеною процедурою для досягнення субмети – виявлення високих ризиків, інформація щодо яких має бути деталізована. Вхідними даними для ІР є вхідні дані підпроцесу ідентифікації активів, які можуть різнитися на першому і наступних кроках ітерації. На виході процесу ІР в результаті ідентифікації наслідків отримується перелік сценаріїв

інцидентів інформаційної безпеки із визначеними з достатнім ступенем точності ймовірнісними характеристиками та наслідками для окремих активів і бізнес-процесів, що дозволяє провести категоризацію ризиків, визначити прийнятні залишкові ризики, ризики, що не вимагають деталізації і високі ризики, які мають бути деталізовані на наступних кроках ітераційного процесу оцінки РІБ.

Кожен підпроцес процесу ідентифікації РІБ також має власну мету, що підпорядкована цілі процесу ідентифікації РІБ, власні вхідні і вихідні дані та певні принципи проведення. Дерево цілей для процесу ІР наведене на рис.1, а опис вхідних і вихідних даних під процесів разом з визначеними особливостями їх проведення представлені у вигляді табл.1.

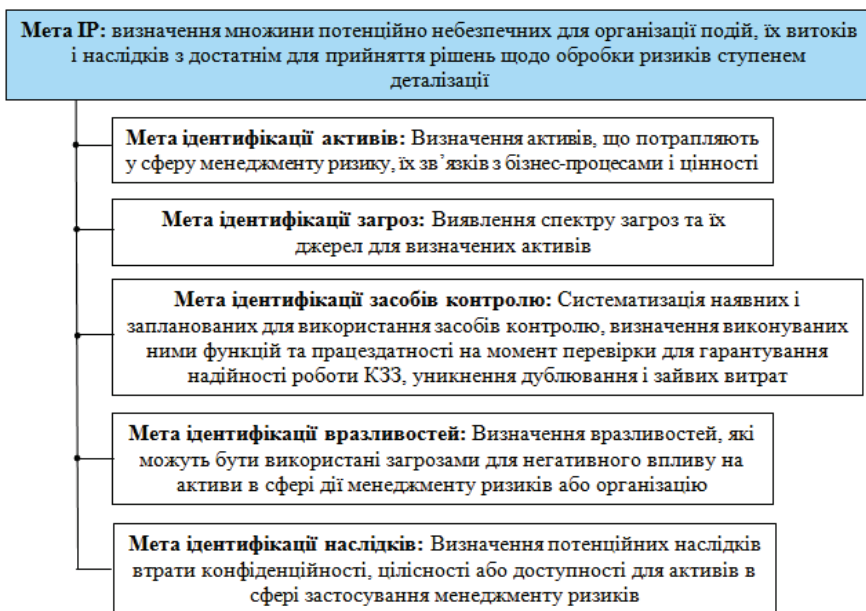


Рисунок 1 – Дерево цілей процесу ідентифікації ризиків

Таблиця 1 – Ідентифікація ризиків

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація активів	Область застосування менеджменту ризиків ІБ, її границя, перелік складових частин із вказівкою їх характеристик, зокрема, функцій, власників, розташування тощо.	Перелік активів, що підлягають менеджменту ризиків ІБ, із визначеною цінністю Перелік пов'язаних з визначеними активами бізнес-процесів із оцінкою їх значимості	Обсяг інформації, що підлягає аналізу, збільшується із поглибленням рівня деталізації Цінність активу найчастіше визначає його власник або особа, що відповідає за отримання, експлуатацію і збереження активу Значимість бізнес-процесів для бізнесу в цілому може визначатися топ-менеджерами
Ідентифікація загроз	Інформація про загрози, отримана при аналізі інцидентів, отримана від власників активів та користувачів, інформація з інших джерел, в тому числі з реєстрів загроз	Перелік загроз із визначеними властивостями (тип загрози, джерело загрози)	Мають бути ідентифіковані випадкові і цілеспрямовані загрози, внутрішні і зовнішні загрози, загрози, що впливають на один актив і на декілька активів різним чином тощо. В ідеалі мають бути ідентифіковані всі загрози. Слід враховувати, що спектр значимих загроз постійно змінюється, особливо при зміні інформаційних технологій і бізнес-середовища.

Продовження таблиці 1

Підпро- цес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація засобів контролю	Список засобів контролю, план реалізації обробки ризиків, документація на засоби контролю,	Перелік наявних і запланованих для використання засобів контролю із визначенням їх розташування, виконуваних функцій, частоти використання і ефективності	Ефективність засобів контролю кількісно може бути оцінена або шляхом аналізу журналів моніторингу та аудиту, або шляхом експерименту, під час якого визначають на скільки знизилася ймовірність успішної реалізації загрози і легкість використання загрозою сукупності вразливостей. Наявний і запланований для використання засіб контролю може бути ідентифікований як: - ефективний; - недостатній; - неефективний; - необґрунтований (економічно недоцільний). Щодо неефективних і недостатніх засобів контролю повинні бути прийняті рішення: - про їх видалення і заміну на ефективніші засоби; - про введення в КЗЗ додаткових засобів контролю; - рішення залишити ситуацію без змін з міркувань вартості

Продовження таблиці 1

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація вразливостей	Перелік активів із визначеною цінністю, перелік загроз із визначенням їх типів та джерел, перелік засобів контролю із визначеною ефективністю	Перелік вразливостей із визначеними їх зв'язками з активами, із загрозами, із засобами контролю Переліки не пов'язаних з загрозою вразливостей для кожної ідентифікованої загрози	Розглядаються вразливості, що є відносно активу: внутрішніми вразливостями зовнішніми вразливостями. Наявність вразливості може бути викликана: порушенням умов експлуатації активу; неефективністю в певних умовах експлуатації засобу контролю. Вразливості можуть ідентифікуватися в таких областях як: організація робіт; прийняті в організації норми управління; процеси і процедури; персонал; фізичне середовище; конфігурація ІКС, апаратні і програмні засоби, засоби зв'язку; зовнішні впливи. Вразливість, яка не експлуатується жодною загрозою: не вимагає впровадження засобів контролю; вимагає проведення моніторингу з метою своєчасного виявлення небезпечних змін. Загроза, яка не має відповідної вразливості, не спричиняє появу ризику.

Продовження таблиці 1

Підпроцес	Вхідні дані	Вихідні дані	Принципи
Ідентифікація наслідків	Перелік активів, перелік бізнес-процесів, перелік загроз, перелік вразливостей із визначеними показниками значимості елементів переліків і їх зв'язками (в разі наявності) з елементами інших переліків.	Перелік сценаріїв інцидентів інформаційної безпеки із визначеними наслідками для активів і бізнес-процесів	Будуються сценарії інцидентів, в яких певна загроза експлуатує певну вразливість. Сценарії можуть будуватися для активу, частини активу, групи активів. Визначаються потенційні збитки від реалізації сценаріїв за всіма критеріями впливу (типами наслідків), прийнятими на етапі визначення контексту. При визначенні операційних наслідків сценаріїв приймають до уваги: - час, необхідний для розслідування інциденту; - час, необхідний для відновлення системи; - втрати ресурсу робочого часу організації внаслідок інциденту; - порушення охорони праці і безпеки; - втрачені можливості (економічні і неекономічні); - фінансові витрати, необхідні для забезпечення спеціфічних навичок персоналу з ліквідації негативного результату сценарію тощо. Наслідки сценаріїв можуть бути тимчасовими і постійними (приклад – руйнування активу).

Слід зазначити, що реалізація процедур підпроцесів суттєво залежить від типу вхідних і вихідних даних і може здійснюватися на основі різних методів [2, 3].

Висновки

В даній роботі проведено аналіз стандартизованого процесу ідентифікації РІБ, визначені структурні компоненти системи знань в цій предметній галузі та їх взаємозв'язки, зокрема побудовано дерево цілей процесу ідентифікації РІБ, визначені принципи організації підпроцесів процесу ідентифікації РІБ, визначено взаємозалежність вхідних і вихідних даних підпроцесів, що в сукупності являє собою структуру знань щодо процесу ідентифікації ризиків інформаційної безпеки.

Список літератури:

1. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. [URL]: <https://www.iso.org/standard/56742.html>
2. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально.-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с.
3. Турти М.В, Книжник Р.О. Методика визначення оптимальності інформаційних моделей в галузі інформаційної безпеки //Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».- Миколаїв: НУК, 2013. – С.148-153.

УДК 004.056.5

КРИТЕРІЙ ВИБОРУ МЕТОДІВ ОЦІНЮВАННЯ РИЗИКІВ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: Божаткін С.М., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Задача оцінювання ризиків є наріжним каменем управління інформаційною безпекою (ІБ). Методологія оцінювання ризиків ІБ стрімко розвивається, зокрема, згідно Плану реалізації Стратегії кібербезпеки України у другому півріччі 2025 року на державному рівні мають бути

розроблені методики ідентифікації та оцінки кіберризиків, стандартизовані процедури аудиту кіберризиків. Ефективність моніторингу та аудиту стану інформаційної безпеки ІКС суттєво впливає на своєчасність прийняття рішення щодо модернізації систем захисту інформації (СЗІ) і, відповідно на сталість показників якості СЗІ в часі.

Вибір методу оцінювання ризиків для конкретної ІКС має відповідати поставленій задачі аудиту: вхідні дані повинні адекватно відображати стан ІКС та її об'єктів, характеристики її оточуючого середовища, а вихідні дані повинні містити інформацію, яка є достатньою для прийняття рішень, що адекватні задачі аудиту. На даний час існує низка стандартів з менеджменту ІБ (МІБ), однак удосконалення методології оцінювання ризиків залишається актуальною задачею, вирішенням якої займаються науковці як закордоном [1, 2], так і у вітчизняних наукових закладах [3-6]. Зокрема, на даний час відсутні методики вибору методу аналізу і оцінювання ризиків (АОР) в ІБ і не визначені критерії такого вибору.

Метою даної роботи є підвищення ефективності процедури дослідження ризиків при вирішенні задач інформаційної безпеки шляхом визначення оптимальної системи критеріїв для вибору методу оцінювання ризиків.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- проаналізувати нормативно-правову базу МІБ і визначити атрибути вхідної і вихідної інформації для АОР за стандартизованими методиками;
- визначити сукупність критеріїв вибору методу АОР в ІБ.

АОР є складовою процесу визначення якості комплексної системи захисту інформації організації, то при її проведенні повинні враховуватися нормативно-правові акти, що стосуються:

- якості товарів і послуг вцілому;
- якості менеджменту організації вцілому;
- якості СЗІ вцілому, зокрема НД ТЗІ, що визначають вимоги до політики безпеки організації і профілів захищеності ІКС, методики їх визначення та експертизи;
- якості систем управління інформаційною безпекою;
- оцінки будь-яких ризиків;

- оцінки ризиків саме інформаційної безпеки;
- деталізації та оптимізації окремих процедур оцінки ризиків ІБ.

При цьому слід враховувати, що існують міжнародні нормативно-правові акти, які можуть бути імплементовані і неімплементовані в Україні, національні і відомчі нормативно-правові акти. Нормативні документи можуть містити обов'язкові до виконання вимоги; рекомендації, що застосовуються за бажанням користувача; вимоги, що є обов'язковими для організацій, які відповідають певному критерію, наприклад, в їх ІКС циркулює інформація, яка містить державну таємницю, або організація є складовою критичної інфраструктури.

Таким чином, кожна організація має власну множину актуальних для неї нормативно-правових актів, частина яких визначається як обов'язкова на рівні держави, частина є обов'язковою в певній галузі чи відомстві, а частина – може використовуватися за бажанням. Всі методи, методики і програмні засоби аналізу та оцінювання ризиків базуються на певних міжнародних і/або національних стандартах і можуть враховувати досвід певної компанії-розробника у формі списків параметрів, варіантів сценаріїв і рекомендованих рішень.

Нормативно-правову базу оцінювання якості СЗІ і АОР складають:

- законодавчі акти: Конституція України; Стратегія національної безпеки України; Конвенція про кіберзлочинність; Доктрина інформаційної безпеки України; Стратегія кібербезпеки України; План реалізації Стратегії кібербезпеки України; Закони України «Про національну безпеку України», «Про критичну інфраструктуру», «Про інформацію», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про критичну інфраструктуру», «Про Державну службу спеціального зв'язку та захисту інформації України» тощо;
- нормативні документи з технічного захисту інформації: НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»; НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»; НД ТЗІ 2.6-002-2015 «Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99»; НД ТЗІ 2.6-003-2015

«Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99»; НД ТЗІ 2.7-013-2016 «Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99»; НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах»

– міжнародні стандарти, частина з яких імплементована в Україні як ДСТУ: ISO 31000:2018 «Risk management – Guidelines» (ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови»); ISO/TR 31004:2013 «Guidance for the implementation of ISO 31000» (ДСТУ ISO/TR 31004:2018 «Менеджмент ризиків. Настанови з впровадження ISO 31000»); ISO/IEC 31010:2019 «Risk management – Risk assessment techniques» (ДСТУ ISO/IEC 31010:2013 «Керування ризиком. Методи загального оцінювання ризику»); ISO/IEC 27001:2015 «Information technology – Security techniques – Information security management systems – Requirements» (ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги»); ISO/IEC 27002:2013 «Information technology – Security techniques – Code of practice for information security management» (ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки»); ISO/IEC 27005:2022 «Information Technology – Security Techniques – Information Security Risk Management» (ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки»); ISO/IEC 15408 «Common Criteria for Information Technology Security Evaluation» (відповідає НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»);

– національні стандарти окремих країн, які широко використовуються поза їх межами: NIST 800-30 «Risk Management Guide for Information Technology Systems» (США); BSI-Standard 100-3 «Risk Analysis based on IT-Grundschutz» (Німеччина) – розроблений Federal Office for Information Security – BSI; AS/NZS 4360:2004 «Risk management» – стандарт Австралії і Нової Зеландії; ISO/FDIS 31000

«Risk management – Principles and guidelines» – стандарт з аналізу і обробки ризиків Швейцарії орієнтований на бізнес-процеси і політику ризик-менеджменту організації;

– накази Адміністрації Державної служби спеціального зв'язку та захисту інформації, наприклад, Наказ від 06 жовтня 2021 року № № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури»;

– галузеві нормативні документи і законодавчі акти, що стосуються певної галузі, наприклад: Закони України «Про платіжні системи та переказ коштів в Україні», «Про банки і банківську діяльність», «Про Національний банк України»; Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України; СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності, система управління інформаційною безпекою. Вимоги»; СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» тощо.

Проведений аналіз нормативно-правової бази МІБ дозволив визначити атрибути вхідної і вихідної інформації для АОР за стандартизованими методиками [7, 8] і побудувати ієрархічну систему критеріїв вибору методу АОР в ІБ, наведену на рис.1.

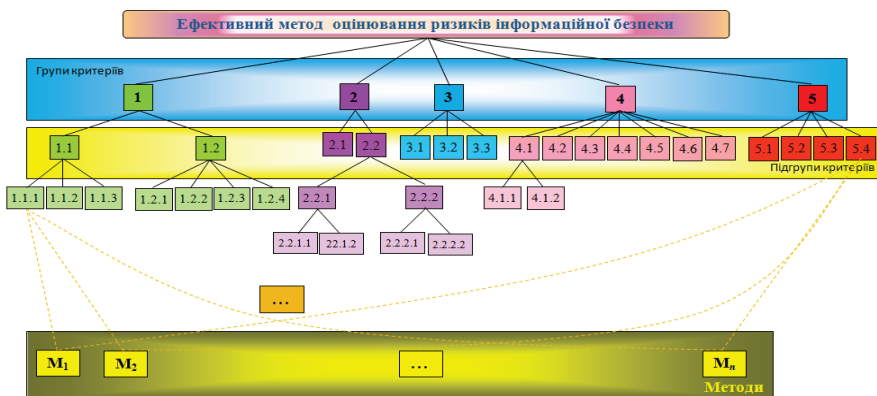


Рисунок 1 – Система критеріїв вибору ефективного методу АОР

На рис.1 M1, M2, ..., M – методи АОР, з яких потрібно обрати оптимальний за сукупністю критеріїв метод. Критерії вибору об'єднані у 5 груп:

1. Тип вирішуваної задачі:

1.1 Дослідження соціотехнічних аспектів інформаційної безпеки: дослідження впливу на окрему людину (1.1.1), на окремі соціальні групи (1.1.2), на окремі професійні групи (1.1.3).

1.2 Дослідження впливу інформаційної безпеки на безпечність бізнесу: дослідження стану безпеки інформації на підприємстві (1.2.1), в галузі (1.2.2), в країні (1.2.3), в світі (1.2.4).

2. Типи даних:

2.1 Реальні і віртуальні статистичні дані.

2.2 Дані експертного опитування: дані експертного опитування в натуральних одиницях вимірювання (2.2.1) (2.2.1.1 – детерміновані дані, 2.2.1.2 – нечіткі дані) і в рангових оцінках (2.2.2) (2.2.2.1 – детерміновані дані, 2.2.2.2 – нечіткі дані).

3. Джерела даних про об'єкт дослідження: дані експертної оцінки (3.1), реальні статистичні дані (3.2), віртуальні статистичні дані (3.3).

4. Програмне забезпечення (ПЗ): умови використання (4.1) (вільнорозповсюджене ПЗ (4.1.1), ліцензоване ПЗ (4.1.2)), докладність опису активів (4.2), складність впровадження (4.3) і використання (4.4), вартість використання (4.5), ступінь автоматизації процедур (4.6), орієнтованість на процес проектування чи експертизи (4.7).

5. Інтегральні оцінки: граничні ризики (5.1), середні ризики (5.2), критичні активи (5.3) ефективні та неефективні засоби і заходи захисту інформації (5.4).

Висновки. В даній роботі проведено аналіз нормативно-правової бази МІБ, визначені атрибути вхідної і вихідної інформації для АОР за стандартизованими методиками та сукупність критеріїв вибору методу АОР в ІБ.

Список літератури:

1. Carfora M., Martinelli F. Cyber Risk Management: An Actuarial Point of View //Journal of Operational Risk. 2021. – Vol.4. – №4. – [URL]: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778061

2. Svilicic B., Kamahara J., Rooks M., Yano Y. Maritime Cyber Risk Management: An Experimental Ship Assessment // The Journal of Navigation. – 2019. – Volume 72. – Issue 5. – pp. 1108 – 1120. DOI: <https://doi.org/10.1017/S0373463318001157>

3. Баронова О.А., Турти М.В. Методика визначення комплексу методів системного аналізу для оцінювання об'єктів і процесів ТЗІ //Тези доповідей Третьої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 29-31 травня 2012 року. – Вінниця: ВНТУ, 2012. – С.180-181.

4. Богданова В.В. Нечітка модель оцінювання ризиків інформаційної безпеки на основі однозначної нечіткої логіки і методології IRAM //Матеріали VI Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». -Миколаїв: НУК, 2016. – С.63-69.

5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. – К.ДУТ, 2015. – 288 с.

6. Корченко А.Г., Архипов А.Е., Казимирчук С.В. Анализ и оценивание рисков информационной безопасности. – К.: ООО «Полиграф-Лазурит», 2013. – 275 с.

7. ISO/IEC 27005:2022 «Information technology – Security techniques – Information security risk management».

8. ДСТУ ISO/IEC 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» (ISO/IEC 31010:2009, IDT).

УДК 004.056.5

АНАЛІЗ РИНКУ ПРОГРАМНИХ ІНСТРУМЕНТІВ ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автори: Божаткін С.М., ст. викладач; Сірівчук А.С., к.т.н.; Турти М.Ю., магістр, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Аналіз і оцінювання ризиків інформаційної безпеки (АОРІБ) є складною процедурою [1, 2] і може виконуватися на основі різних методів [3]. Для автоматизації АОРІБ на даний час на ринку існує різноманітне спеціалізоване програмне забезпечення (СПЗ), яке відрізняється

як за спектром виконуваних функцій, так і за умовами розповсюдження. Вибір СПЗ для АОРІБ є досить складною задачею.

Метою даної роботи є визначення критеріїв вибору СПЗ АОРІБ. Для досягнення цієї мети необхідно визначити перелік наявних на ринку СПЗ АОРІБ, їх характеристики, що є важливими для користувача і становлять критерії вибору СПЗ АОРІБ, провести порівняльний аналіз наявних СПЗ.

Як показав проведений аналіз, СПЗ для АОРІБ може бути вільно розповсюджуваним і платним, може мати тріал-версії, а також може бути програмним продуктом чи власністю організації. СПЗ для певної організації адаптується під завдання АОРІБ та управління ризиками в цій організації, враховує специфіку її інформаційних потоків. Якщо ПЗ розробляється як програмний продукт, то воно найчастіше є універсальним.

Наявне на ринку СПЗ може базуватися на якісних і кількісних методах аналізу ризиків, причому застосовуваний метод або методика є часто розробкою авторів СПЗ, що особливо характерне для СПЗ, яке спочатку розроблялося для потреб певної організації, а потім знайшло поширення на інші галузі.

Якісні методи аналізу ризиків ІБ реалізовані в COBRA, RA Software Tool, Risk Advisor, Digital Security Office 2006 (має дві складові – КОНДОР для управління політикою безпеки і ГРИФ для аналізу ризиків). В системах CRAMM (CCTA Risk Analysis and Managment Method), АванГард, RiskWatch реалізуються кількісні і комбіновані методи аналізу ризиків (табл.1).

При цьому СПЗ, наведені в табл.1 можуть проводити АОР з різним ступенем деталізації, видавати узагальнені і вибіркові звіти, ілюстрації результатів у вигляді діаграм, використовуючи різні методики і показники. Так у RiskWatch в якості критеріїв управління ризиками використовуються прогнозовані річні втрати ALE та оцінка повернення від інвестицій ROI, а для визначення ризиків, крім інших параметрів, використовуються запропоновані Американським інститутом стандартів NIST оцінки середніх частот реалізації загроз на рік в певній частині світу SAFE (Standard Annual Frequency Estimate) і в певному місці LAFE (Local Annual Frequency Estimate).

Таблиця 1 – Характеристики СПЗ АОР ІБ

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
COBR А	Базовий. Рівні ризиків не визначаються	BS7799, ISO/IEC 17799	Перевірка стану ІБ на відповідність вимогам стандартів, в тому числі ідентифікація ризиків	Якісний	Відповіді аналітика на декілька десятків питань анкети	Якісний опис результатів аналізу анкетування	Великобританія	+Можливість доповнення вбудованих баз знань
RA Software Tool (RA2 art of risk)	Підвищений (базовий з елементами високого)	ISO/IEC 17999, ISO/IEC 13335, BS7799, керівні документи BSI	Оцінка ризиків як на базовому рівні, так і за більш детальними специфікаціями згідно керівництва PD 3002 Британського інституту стандартів (BSI)	Якісний	Відповіді аналітика на питання анкети	Якісний опис результатів аналізу анкетування	Великобританія	+ Можливість розробки користувачами власних методик аналізу і оцінювання ризиків

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
Risk Advisor	Високий	AN/NZS 1360, ISO/IEC 17799	Ідентифікація загроз, збитків, ризиків Перевага: опис різних зв'язків (зовнішніх і внутрішніх, в тому числі – з бізнес-процесами), адекватний облік багатьох факторів ризику, відносно невисока тривалість, докладний звіт з 100 розділами Недолік: аналіз факторів ризику відсутній	Якісний	Якісний опис загроз, втрат, ризиків та їх взаємозв'язків	Оцінка ризику в якісних шкалах. Оцінка ефективності контрзаходів Граф ризиків	Нова Зеландія	-

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
КОН ДОР 2006	Високий	ISO/IEC 17799, ISO/IEC 27001	Розробка та управління політикою безпеки. Містить з бази стандартів управління ІБ, у вигляді переліку вимог, що мають вагу, визначену за досвідом експертів Digital Security на момент поставки. Дозволяє виявити недоліки політики безпеки і визначити ефективність планових контрзаходів, ранжувати контрзаходи за ефективністю з метою визначення пріоритетів їх впровадження. Складово Digital Security Office 2006	Якісний	Відповіді аналітика на питання анкети щодо дотримання в політиці безпеки вимог стандартів управління ІБ Обмеження знизу на вагу вимог для визначення вимог, що є критичними для організації Планові контрзаходи	Невиконані вимоги і рекомендації щодо усунення недоліків Множина невиконаних вимог, що є критичними для організації Оцінки ефективності планових контрзаходів	Росія	+Бази стандартів управління ІБ у вигляді переліку зважених вимог можуть регулюватися і доповнюватися: користувач може змінити перелік вимог та їх ваги

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
ГРИФ 2006	Високий	ISO/IEC 17799, ISO/IEC 27001	Аналіз захищеності активів і управління ризиками ІБ за результатами аналізу співвідношення витрати/ефективність. Дозволяє провести повний аналіз ризиків, визначити рівні ризиків активів і причини ризику. Складово Digital Security Office 2006	Якісний	Відповіді аналітика на питання анкети, які дозволяють ідентифікувати ризики	Оцінка ризиків за якісними і кількісними шкалами Ефективність витрат Причини ризиків	Росія	,

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
CRA MM	Високий	BS7799, прийнятий як державний стандарт Великобританії	Аналіз і управління ризиками ІБ для великих і дрібних організацій, де циркулює несекретна інформація, на всіх стадіях життєвого циклу інформаційно-комунікаційних систем. CRAMM зручніший для аудиту вже діючих ІКС, ніж для аудиту проєктів ІКС на стадії розробки. Універсальне СПЗ, що має версії для комерційних і для урядових організацій, які різняться за своїми базами знань. Містить сотні рекомендацій і прикладів організації захисту інформації		Якісні дані Цінність активів за 10-бальною шкалою за критеріями, що різняться для фізичних ресурсів і ПЗ. Цінність фізичних ресурсів визначається як вартість відновлення після руйнування, а цінність даних та ПЗ – для випадків порушення доступності на певний час; втрати інформації після останнього	Кількісні дані Рівні ризиків за дискретною шкалою. Переліки контрзаходів, обраних із списків рекомендаційних контрзаходів. Оцінки загроз і вразливостей за непрямыми факторами за 5-ти бальною шкалою	Великобританія	-

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
			Недоліки: використання методу CRAMM вимагає спеціальної підготовки та високої кваліфікації аудитора; процес аудиту є трудомістким і тривалим; вбудовані бази знань, шаблони звітів не користуються користувачем показники захищеності за національними нормативами визначити неможливо.	Комбінований	резервного копіювання тощо. 16 класів активів фізичних, 5 класів програмних активів. Бінарні відповіді на питання анкети щодо загроз і вразливостей. Сценарії реалізації загроз Оцінки наслідків за 7 критеріями за розроблюваними для них власними 10-бальними шкалами.			

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
Аван-Гард	Високий		Управління інформаційною безпекою Недоліки: вибір якісних оцінок не піддається верифікації; наявні рекомендації розроблені на основі статистичних даних лише щодо закордонних компаній	Кількісний	Якісні і кількісні дані Кількісне значення збитку і його ймовірності Ієрархічна схема АОР для об'єктів, підсистем, регіонів і моделей в цілому з врахуванням процесів і середовища	Оцінка ризику як добутку і збитку і ймовірності Ризик у монетарній формі	Росія	-
Risk Watch	Високий	ISO/IEC 17799, US Healthcare Insurance Portability	Аналіз ризиків, обґрунтування вибору засобів захисту Управління ризиками за показниками ALE та ROI. Містить бази з оцінками LAFE і SAFE, а також з узагальненими описами різних типів засобів захисту		Визначення контексту шляхом вибору із вбудованих списків категорій ресурсів, втрат, загроз, уразливостей та заходів захисту.	Опис ризиків як очікуваних наслідків реалізації загроз за рік Оцінка вигоди нових засобів контролю	США	+Вибір способу введення вихідних даних. Модифікація

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
		and Accountability Act	Переваги: можливість оцінити вигоди впровадження нових засобів контролю; наочність представлення результатів у вигляді звітів і діаграм; відносна простота опису моделі; можливість коригування окремих вбудованих баз даних; можливість імпорту результатів аналізу комп'ютерних мереж інструментальними засобами дослідження вразливостей Недоліки: тільки англійськомовний інтерфейс; відсутність комплексного підходу до оцінки ризиків (аналіз ризиків, головним чином, на технічному		Дані, щодо характеристик системи, можуть вводитися вручну або імпортуватися із звітів, створених засобами дослідження вразливості комп'ютерних мереж. Відповіді на питання анкети з 600 питань для виявлення можливих уразливостей. Введення показників LAFE і SAFE.	Класи інцидентів Звіти різних типів: короткі підсумки, результати аудиту безпеки, звіти з вибірковою інформацією про цінність активів, очікувані втрати, загрози, ефективність інвестицій ROI		назв і описів категорій у списках ресурсів, що захищаються, втрат, загроз, вразливостей та засобів захисту, а також додавання нових категорій. Коригування

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації

СПЗ	Рівень деталізації	Нормативна база	Призначення	Метод	Дані		Країна-розробник	Здатність до модифікації
					Вхідні дані	Вихідні дані		
			рівні захисту); використання параметрів LAFE і SAFE, які невідомі вітчизняним користувачам (відсутня статистика)	Кількісний	Сценарії впровадження засобів захисту «що, якщо:»			питань анкети щодо вразливостей

В табл.1 неведено результати аналізу СПЗ для АОР за критеріями, які пропонується використовувати вибору СПЗ:

1. Рівень деталізації – рівень глибини аналізу ризиків:

- базовий рівень – виконується узагальнений аналіз ризиків. При цьому можуть застосовуватися різні методи, але найчастіше в СПЗ базового рівня використовуються якісні методи АОР;
- підвищений рівень – окремі процедури виконуються з високим ступенем деталізації;
- високий рівень – виконується докладний аналіз ризиків якісними або кількісними методами, розв’язуються задачі оптимального управління ризиками.

2. Нормативна база – міжнародні і національні нормативні документи, на основі яких розроблена методика АОР, реалізована в СПЗ. Більшість поширеного СПЗ базується на ISO/IEC 17799 (ISO/IEC 27002).

3. Призначення СПЗ, його функціональні переваги та недоліки.

4. Метод АОР, що реалізований в СПЗ: якісний, кількісний, комбінований.

5. Особливості вхідних і вихідних даних, зокрема, зміст даних, тип даних (якісний або кількісний), способи введення даних (анкету-

вання, введення вручну, імпорт з іншого СПЗ) і формати представлення результатів АОР (номенклатура звітів, використання діаграм).

6. Країна-розробник. Цей критерій у сукупності з критеріями 2 та 7 визначає доцільність використання СПЗ для АОР ІБ в певній країні.

7. Здатність до модифікації, тобто можливість адаптувати вбудовані бази даних і алгоритми роботи СПЗ, формати і склад звітів до вимог АОР ІБ в певній країні для певного об'єкту аналізу.

Слід зазначити, що методики, які реалізовані в наявному на ринку, СПЗ можуть також різнитися за складністю, і, відповідно, висувати додаткові вимоги до кваліфікації персоналу та ресурсів часу на проведення АОР. Результати АОРІБ, отримані за будь-якою методикою будь-яким СПЗ, мають деякий ступінь невизначеності, однак різняться за ступенем суб'єктивності отриманих оцінок і за можливостями верифікації результатів. Наприклад, АванГард та RiskWatch суб'єктивність реалізованих методик не завжди дозволяють отримати адекватні результати АОР.

Висновки

В даній роботі проведено аналіз наявних на ринку СПЗ АОРІБ, критерії їх вибору користувачем, за якими проведено порівняльний аналіз СПЗ АОРІБ.

Список літератури:

1. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально-наукових та науково-практичних видань НА СБ України, 2014. – 190 с.
2. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. [URL]: <https://www.iso.org/standard/56742.html>
3. ДСТУ ISO/IEC 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» (ISO/IEC 31010:2009, IDT). [URL]: <https://khoda.gov.ua/image/catalog/files/dstu%2031010.pdf>

УДК 004.056.5;057.2

МОДЕЛЬ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ОРГАНІЗАЦІЇ

Автори: Божаткін С.М., ст. викладач; Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Будь-яка організація намагається знизити залишкові ризики інформаційної безпеки (ІБ) [1] за допомогою економічно доцільних систем захисту інформації (СЗІ) [2, 3].

З точки зору системного аналізу СЗІ є підсистемою організації і має власну мету – запобігання загрозам її ІБ, яка підпорядкована цілям організації як системи в цілому. СЗІ впливає на виробничу діяльність всіх підрозділів організації, забезпечуючи цілісність і доступність інформації, яка необхідна для функціонування організації, та забезпечуючи конфіденційність інформації, яка захищається згідно загальнодержавних вимог або на вимогу власника. Відповідно, існують прямі непрямі зв'язки СЗІ з іншими підрозділами організації і з зовнішнім середовищем, які впливають на ефективність СЗІ і показники якості функціонування організації і можуть бути представлені у вигляді моделей різного типу [4].

Метою даної роботи є побудова узагальненої суб'єктно-об'єктної мотиваційної моделі процесів інформаційної безпеки організації.

Для досягнення поставленої мети необхідно визначити типи процесів ІБ організації, об'єкти і суб'єкти цих процесів та мотивацію їх поведінки.

Серед процесів ІБ організації можна виокремити ряд наступних стандартних процедур:

- віднесення інформації до категорії інформації з обмеженим доступом (ІЗОД);
- виявлення загроз безпеці активів організації;
- створення механізмів оперативного реагування на загрози, відшкодування та локалізації збитків, послаблення негативного впливу наслідків порушень ІБ на стратегічні цілі організації;
- розслідування інцидентів ІБ;
- прогнозування подій ІБ з метою попередження інцидентів;

- планування модернізації і впровадження засобів управління ризиками ІБ;
- впровадження засобів управління ризиками;
- контроль ефективності СЗІ, виявлення і усунення недоліків.

В розроблюваній моделі в якості об'єктів розглядаються:

- активи, що мають для організації певну цінність та власні множини вразливостей;
- цінність активу, яка може бути виражена в монетарній бальній чи якісній формі і може бути повністю або частково втрачена внаслідок успішної експлуатації загрозами певних вразливостей;
- вразливості інформаційно-комунікаційної системи (ІКС) та вразливості СЗІ, що впливають на ймовірність реалізації загрози;
- збитки або втрати, спричинені негативними наслідками реалізації загрози для бізнесу і витратами на відновлення активу і СЗІ;
- ризик – ймовірний збиток організації в разі реалізації загрози ІБ.

Суб'єктами в розроблюваній моделі є:

- власник активів, який створює СЗІ з метою їх захисту;
- джерела загроз, зокрема, зловмисник, що створює цілеспрямовані загрози, а також природні події, технічні відмови, помилки персоналу, фізичні пошкодження, що мають випадковий характер;
- загрози ІБ, які ініціюють процес експлуатації вразливостей;
- СЗІ, яка протидіє загрозам.

Кожен суб'єкт моделі може застосовувати різні стратегії для досягнення власних цілей.

Метою власника є отримання максимального прибутку, для чого необхідно зберігати ресурси і репутацію організації, та зменшувати поточні витрати і потенційні втрати. Тому дії власника мотивуються його бажанням зберегти активи, знизити ризики і не витратити надмірні кошти на СЗІ, тобто власник в своїх діях керується принципом «розумної достатності». Власник визначає інформаційні ресурси, що містять ІзОД, цінність активів, критерії прийняття ризиків; ініціює створення СЗІ і приймає участь у процесах створення механізмів оперативного реагування на загрози, відшкодування та локалізації збитків, послаблення негативного впливу наслідків порушень ІБ, плануванні модернізації і впровадження засобів управління ризиками.

Діяльність зловмисника може бути мотивована бажанням помсти, бажанням отримати конкурентні переваги чи реалізувати певну шахрайську схему тощо. В будь-якому разі зловмисник зацікавлений в організації несанкціонованого використання активів шляхом створення загроз, що збільшують ризики в ІКС організації і прямим чи непрямим чином впливають на бізнес-процеси.

Кожна загроза намагається успішно реалізуватися за рахунок експлуатації вразливостей, асоційованих з активами, і наявних недоліків СЗІ, тобто вразливостей СЗІ.

Головною метою діяльності СЗІ є зниження або утримування ризиків на прийнятному для організації рівні, для чого необхідно виявляти і усувати вразливості, вчасно виявляти загрози і зменшувати їх негативний вплив. Відповідно СЗІ приймає участь у всіх процесах ІБ організації після свого створення, що є окремою процедурою.

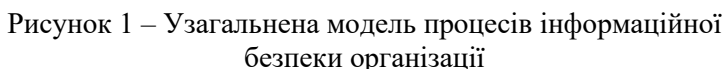
Суб'єкти моделі, що є стохастичними процесами не мають мотивації для здійснення цілеспрямованого негативного впливу, однак вони здатні ініціювати техногенні, антропогенні і природні загрози і створювати ризики ІБ в ІКС.

На рис.1 наведена розроблена узагальнена суб'єктно-об'єктна мотиваційна модель процесів ІБ організації, яка побудована на основі стандарту ISO/IEC 27005:2011 [5]. На рис.1 суб'єкти позначені овалами, об'єкти – прямокутниками, причинно-наслідкові зв'язки – суцільними лініями, а цільові відношення суб'єктів системи – пунктирними лініями.

Наведена на рис.1 модель відображає сукупність об'єктивних і суб'єктивних зовнішніх і внутрішніх факторів, які впливають на стан інформаційної безпеки, що характеризується ризиком, зумовленим однією загрозою, яка в загальному випадку формується в результаті цілеспрямованих дій зловмисника і впливу випадкових факторів різної природи. Для множини загроз повинен розглядатися сумарний ризик, спричинений множиною загроз, асоційованою з активом.

Отримана модель є семантичною мережею, в якій використовуються такі типи зв'язків як «має», «прагне», «створює», «знижити», «збільшити», «зберегти», «використовує».

Висновки. В даній роботі визначено типів процесів ІБ організації, об'єкти і суб'єкти цих процесів та мотивацію їх поведінки.



1. Arnold R. Cybersecurity: A Business Solution: An executive perspective on managing cyber risk. Winston-Salem: Threat Sketch, LLC, 2017. – 100 с. [URL]: https://books.google.com.ua/books?id=z44DwAAQBAJ&pg=PA22&redir_esc=y#v=onepage&q&f=false
2. Архипов О.Є., Архипова Є.О. Ризиковий підхід до визначення обсягу оптимальних інвестицій у безпеку інформації / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность. Материалы XV Международной научно-практической конференции ИТБ-2015. (21 жовтня 2015 р., м. Київ). – К.: ИПРИ НАН України, 2015. –

250 с. – С.12-17. [URL]: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-15_AA_risk2_konf.pdf

3. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально.-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с.

4. Турти М.В, Книжник Р.О. Методика визначення оптимальності інформаційних моделей в галузі інформаційної безпеки //Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».- Миколаїв: НУК, 2013. – С.148-153.

5. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. [URL]: <https://www.iso.org/standard/56742.html>

УДК 004.056.5; 057.2

ІНФОРМАЦІЙНА МОДЕЛЬ ОЦІНЮВАННЯ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

***Автор:** Гайванюк І.О., магістр, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

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

Сучасний кіберпростір є середовищем, яке дозволяє здійснювати електронні комунікації у фаховій діяльності людини або в процесі реалізації суспільних відносин. Безпека кіберпростору держави повинна забезпечуватися так саме, як безпека її території на суші, в повітрі і морі. Кіберпростір утворюється в результаті функціонування сумісних комунікаційних систем з використанням глобальних і локальних мереж передачі даних.

Для захисту інформації застосовуються комплексні системи захисту інформації (КСЗІ), необхідність застосування, порядок впровадження і оцінювання ефективності котрих регламентується низкою законів України, міжнародними нормативними документами, норма-

тивними документами з технічного захисту інформації (НД ТЗІ), галузевими нормативними документами.

Динаміка розвитку методів і засобів КСЗІ зумовлена неперервними і швидкими змінами, що спостерігаються в галузі інформаційних технологій, і, в свою чергу зумовлює постійне вдосконалення методів, методик і спеціалізованих програмних засобів оцінювання ефективності КСЗІ [1]. Загрози інформації при цьому можуть бути представлені різними моделями.

Метою даної роботи є розробка інформаційної моделі оцінювання загроз безпеці інформації з обмеженим доступом на основі їх формалізованих моделей.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

- провести аналіз нормативно-правової бази і визначити критерії класифікації загроз безпеці інформації, доцільні для застосування у даній роботі;
- провести аналіз формалізованих моделей загроз і визначити вхідні вихідні дані інформаційної моделі оцінювання загроз безпеці інформації з обмеженим доступом (ІзОД) на їх основі;
- розробити основні алгоритми і побудувати інформаційну модель оцінювання загроз безпеці ІзОД на основі їх формалізованих моделей.

Згідно ISO/IEC 27005 [2] загрози класифікуються за наступними критеріями 1, 2, 3:

1. За природою виникнення загрози поділяються на:

- навмисні загрози. Позначення *D*. Використовуються для всіх навмисних акцій, спрямованих на інформаційні активи;
- випадкові загрози. Позначення *A*. Використовуються для всіх дій людини, що можуть пошкодити інформаційні активи;
- природні (екологічні) загрози. Позначення *E*. Використовуються для всіх впливів зовнішнього середовища, що не пов'язані з діями людини.

2. За типом загроз. Причому одна й та ж сама загроза може мати різню природу виникнення. В ISO/IEC 27005 загрози згруповані за наступними типами:

а) фізичні пошкодження: вогонь, пошкодження водою, забруднення, знищення обладнання або носіїв, пил, корозія, зледеніння тощо. Всі загрози цього типу можуть бути природними, або можуть бути викликані випадковими чи цілеспрямованими діями людини. Відповідно, всі цього типу можуть позначатися *A, D, E*;

б) природні події: кліматичні, сейсмічні, вулканічні, метеорологічні явища, повинь тощо. Всі загрози цього типу є природними і позначаються *E*;

в) втрата необхідних сервісів: відмова телекомунікаційного обладнання, відмова системи кондиціонування або системи водо забезпечення (категорії *A, D*), втрата електроживлення з будь-якої причини (категорії *A, D, E*);

г) несправності внаслідок негативного впливу випромінювання різної природи: теплового, електромагнітного, радіаційного випромінювання, електромагнітних імпульсів (категорії *A, D, E*);

д) компрометація інформації:

- категорія *D*: перехоплення і відправлення скомпрометованого сигналу; дистанційне шпигування; підслуховування; крадіжка носіїв інформації, документів або обладнання, відновлення інформації з бракованих або відправлених на переробку носіїв; виявлення місця розташування; втручання в роботу апаратних і програмних засобів;

- категорії *A, D*: дані з ненадійних джерел, виявлення (розкриття);

е) технічні відмови:

- категорія *A*: відмови і збої обладнання, програмні збої,

- категорії *A, D*: насичення інформаційної системи, втрата ремонтпридатності інформаційної системи;

ж) несанкціоновані дії:

- категорія *D*: несанкціоноване використання обладнання, шахрайське копіювання програмного забезпечення, викривлення даних, несанкціонована обробка даних;

- категорії *A, D*: використання контрафактного або скопійованого програмного забезпечення;

з) компрометація функцій:

- категорія *A*: помилка у використанні;

- категорія *D*: фальсифікація прав, заперечення дій;

- категорії *A, D*: зловживання правами;
 - категорії *A, D, E*: порушення працездатності персоналу.
3. За джерелами загроз, викликаних людською діяльністю (типами зловмисників):
- хакер, крекер;
 - комп'ютерний злочинець;
 - промислове шпигування (компанії, іноземні уряди, інші урядові інтереси);
 - інсайдер (співробітники недостатньої кваліфікації; невдоволені, зловмисні і недбалі співробітники, нечесні або звільнені співробітники).
- Кожна людина-джерело загрози має власну мотивацію дій, що різняться за типами і критичністю наслідків (табл.1).

Таблиця 1 – Мотивація і наслідки дій зловмисників різних типів

Тип зловмисника	Мотивація	Наслідки
Хакер, крекер	Грошова вигода; статус; виклик (бунтарство); его (зарозумілість); повстання	Хакерство, несанкціонований доступ в систему; вторгнення в систему, злам; соціальна інженерія
Комп'ютерний злочинець	Руйнування інформації, незаконне розкриття інформації; грошова вигода, в тому числі кредитна; викривлення даних (несанкціонована модифікація)	Комп'ютерний злочин (наприклад, кіберпереслідування); інформаційний підкуп; імітація; шахрайство (наприклад, перехоплення, підrobка, відтворення); вторгнення в систему
Терорист	Помста; розвідка; шантаж; руйнування; розголошення в засобах масової інформації; політичні преференції;	Тероризм; інформаційна війна; системна атака (наприклад, розподілена DDoS-атака); вторгнення в систему; втручання в роботу системи

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації

Тип зловмисника	Мотивація	Наслідки
Промисловий шпигун	Конкурентні переваги; економічний зиск	Крадіжка інформації; крадіжка персональних даних; економічна розвідка; несанкціонований доступ до інформаційних активів, що містять ІзОД, в тому числі службову та технологічну інформацію; соціальна розробка (замах на недоторканність особистого життя)
Інсайдер	Ненавмисні помилки і упущення (наприклад, помилки введення даних, логічні помилки програмування); цікавість; его; грошова вигода; помста; розвідка	Напад на співробітника; шантаж; ознайомлення з секретами фірми; неправильне використання апаратних і програмних засобів обробки інформації; шахрайство і крадіжка; інформаційний підкуп; введення фальсифікованих даних, руйнування даних, несанкціонована модифікація даних; перехоплення; впровадження шкідливого коду (наприклад, вірусів, троянських коней, логічних бомб); системні помилки; системний саботаж; продаж персональних даних (розголошення персональних даних); несанкціонований доступ в систему; вторгнення в систему

4. За порушуваними властивостями захищеної інформації (за НД ТЗІ 2.5-004-99 [3] – а), б), в), г):

а) загрози конфіденційності:

– за місцем розташування інформації в активі:

• загрози доступу до інформації на зовнішніх запам'ятовуючих пристроях (наприклад, загрози несанкціонованого доступу (НСД) до ІзОД на жорсткому диску, на флеш-накопичувачах, в RAID-масивах, на мобільних пристроях);

• загрози доступу до інформації в оперативній пам'яті (наприклад, до залишкової інформації в оперативній пам'яті; до інформації з певних областей оперативної пам'яті, що використовуються операційною системою і її підсистемою захисту, іншими користувачами, прикладними програмами);

• загрози доступу до інформації в каналах зв'язку;

• загрози доступу до інформації на периферійних пристроях в процесі її обробки згідно використовуваних технологій (наприклад, загрози НСД до інформації, що відображається на дисплеї, друкується на принтері, сканується і розпізнається тощо);

– за способом доступу до інформації в активах:

• загрози НСД до інформаційних ресурсів стандартним шляхом за рахунок використання реквізитів доступу лігітимних користувачів (наприклад, одержання паролів і логіків легітимних користувачів агентурним шляхом, шляхом використання недбалості користувачів, підбором, імітацією інтерфейсу входу в систему з блоком автентифікація тощо);

• загрози НСД до інформаційних ресурсів нестандартним шляхом за рахунок використання не документованих можливостей операційної системи, в тому числі завантаження сторонньої операційної системи для оминання засобів захисту зі змінних носіїв.

б) загрози цілісності;

в) загрози доступності;

г) загрози спостережуваності (керованості);

5. За впливом на функціонування ІКС: активні і пасивні загрози.

6. За ступенем залежності від функціонування ІКС:

- загрози, що виникають незалежно від подій, що відбуваються в ІКС в процесі її функціонування;
- загрози, що виникають в разі настання певних подій в ІКС.

Моделі загроз можуть бути формалізованими і неформалізованими. Формалізовані моделі використовуються головним чином при застосуванні кількісних методів оцінювання ризиків, відповідно їх вхідні і вихідні дані є кількісними. Вхідними даними моделі є ймовірнісні характеристики виникнення загроз, ймовірності експлуатації загрозами недоліків КСЗІ і описана будь яким чином структура шляхів успішної реалізації загрози за рахунок експлуатації різних вразливостей системи, а вихідними – ймовірності порушення певних властивостей ІЗОД та інформаційної безпеки в цілому. Відповідна інформаційна модель наведена на рис.1.

Ймовірність порушення інформаційної безпеки $P_{ІБ}$, тобто ймовірність того, що засоби управління ризиками не зможуть протистояти сукупності загроз і якась із загроз конфіденційності, цілісності або доступності інформації буде успішно реалізована зловмисником згідно цієї моделі визначається за формулою

$$P_{ІБ}=1-(1-P_K)(1-P_{Ц})(1-P_D).$$

Висновки

В даній роботі проведено аналіз нормативно-правової бази і формалізованих моделей загроз; визначені критерії класифікації загроз безпеці інформації, вхідні вихідні дані інформаційної моделі оцінювання загроз безпеці інформації з обмеженим доступом на їх основі; розроблені основні алгоритми і побудовано інформаційну модель оцінювання загроз безпеці інформації з обмеженим доступом на основі їх формалізованих моделей.

Список літератури:

1. Корченко О.Г., Гнатюк С.О, Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально-наукових та науково-практичних видань НА СБ України, 2014. – 190 с.

2. ISO/IEC 27005:2022 Information technology – Security techniques – Information security risk management. [URL]: <https://www.iso.org/standard/80585.html>

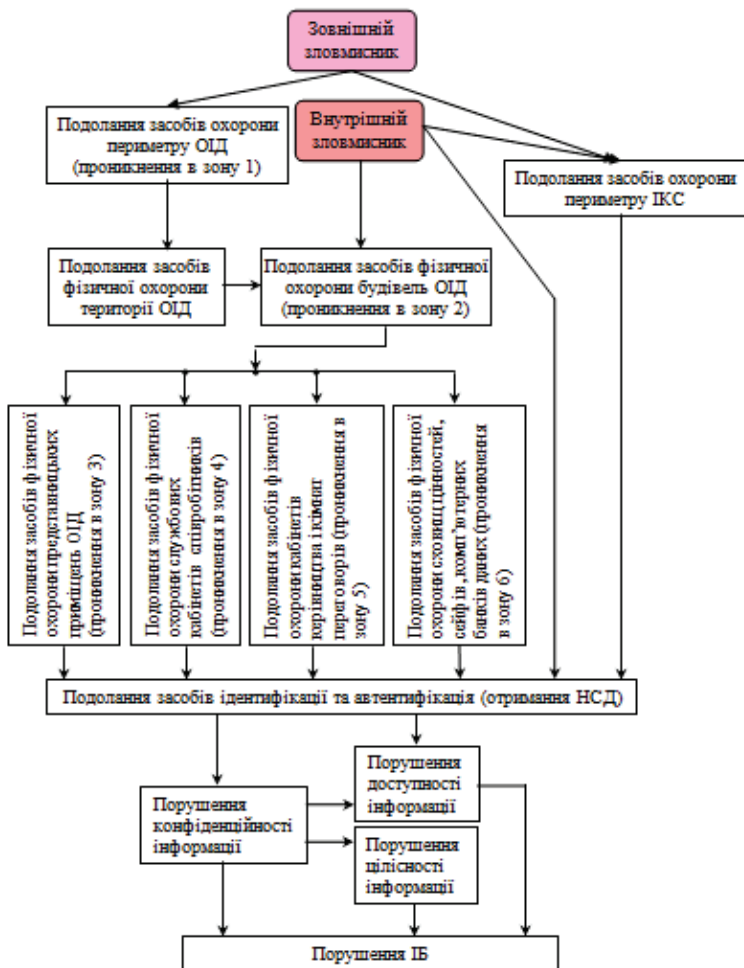


Рисунок 1 – Узагальнена інформаційна модель

3. НДТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [URL]: <http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342>

УДК 004.056.53: 534.8/78

ВРАХУВАННЯ ПІДВИЩЕННЯ ЗАЛИШКОВОЇ РОЗБІРЛИВОСТІ МОВИ В КАНАЛІ ВИТОКУ ПРИ БАГАТОРАЗОВОМУ ПРОСЛУХОВУВАННІ

Автори: Касьянов Ю.І., ст. викладач; Іванова А.В., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. Одним з основних джерел отримання інформації про особисте життя людини, фінансової, адміністративної або виробничої діяльності організації, тобто відомостей, що не підлягають широкому розголошенню є мовна інформація. За допомогою технічних засобів або шляхом безпосереднього прослуховування може здійснюватися несанкціонований доступ до мовної інформації з обмеженим доступом. Внаслідок цього захист мовної інформації є однією з найважливіших задач в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта.

Наразі в провідних країнах світу для оцінювання захищеності мовної інформації використовується критерій словесної розбірливості мови, який є інваріантним до виду завади [1, 2]. В сертифікованих методиках найчастіше використовується об'єктивний формантний метод визначення розбірливості мови [3, 4]. При цьому, не дивлячись на зростаючі можливості запису перехопленої розмови, залишається недостатньо проробленим питання врахування в оцінюванні впливу на розбірливість мови фактору багаторазового прослуховування. Це може привести до зниження ступеня захищеності мовної інформації у виділеному приміщенні.

Метою роботи є визначення впливу багаторазового прослуховування на розбірливість мовного повідомлення для врахування даного фактору в методиці оцінювання захищеності мовної інформації формантним методом.

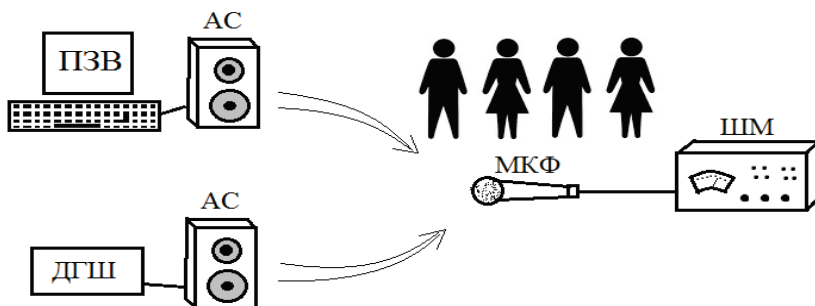
Основна частина. Враховуючи, що фактор впливу багаторазового прослуховування на сприйняття і, відповідно, розбірливість мовного повідомлення визначається суб'єктивними людськими характеристиками, то для дослідження було вибрано найбільш універсальний суб'єктивний метод – метод артикуляційних випробувань [3, 5].

Дослідження проводились за методикою, описаною в [6], яка включає підготовчу, інструментальну (вимірювальну), розрахункову та аналітичну стадії.

Підготовча стадія полягала у підборі текстового матеріалу для зачитування та запису фонограм.

В якості текстового матеріалу було використано артикуляційні таблиці слів (5 таблиць), взяті з ГОСТ 16600-72 [5]. Це забезпечило фонетичну та статистичну збалансованість. Кожна таблиця містить по 50 слів загального вжитку. Для запису фонограм було задіяно 2 диктори (молоді жінка і чоловік), без вад дикції. Диктори читали текст (слова) рівним голосом, з постійним рівнем мови, чітко без підкреслювання окремих звуків. Темп зачитування слів: 15...20 слів за хвилину з паузами між ними 2...3 секунди для їх запису аудитором. Фонограми записувались на комп'ютері з допомогою програми Sound Forge в режимі "Моно" у форматі нестисненого цифрового звуку (44100 Гц, 16 біт).

Схема проведення експериментальної стадії наведена на рис.1



ПЗВ - пристрій запису та відтворення (ПК або диктофон);
АС - активна акустична система;
ДГШ - джерело генерованого шуму;
МКФ - мікрофон;
ШМ - шумомір.

Рисунок 1 – Схема проведення експериментальної стадії

Відповідно до даної схеми було обрано конкретні засоби для проведення досліджень. Апаратні засоби включають два персональних комп'ютера (ПК) з відповідним програмним забезпеченням (програвач Windows Media та програма обробки звуку Sound Forge) та виходом на активні акустичні системи (SoundStorm та F&D-600) і шумомір ВШВ-003. Фонограми відтворювались ПК з програвачем Windows Media та АС F&D-600. Кожна фонограма повторювалась 4 рази. Інтегральний рівень мовного сигналу в точці прослуховування задавався рівним 70 дБ, що вимірювалось шумоміром. Шумова завада типу "білий" шум генерувалась програмою Sound Forge і відтворювалась АС SoundStorm. Відношення сигнал/шум: +10, +5, +0, -5, -10 дБ задавались зміною рівня шуму.

У прослуховуванні приймали участь 5 аудиторів, що розміщувались на відстані 2 м від акустичних систем. Перед прослуховуванням проводилася попередня адаптація аудиторів до шуму на протязі 3...5 хвилин. Аудитори при кожному значенні відношення сигнал/шум прослуховували аудіозапис таблиці слів 4 рази, записуючи при кожному прослуховуванні зрозумілі слова, доповнюючи чи коригуючи записаний при попередніх прослуховуваннях набір слів. При зміні рівня шуму таблиця слів змінювалась.

Обробка результатів на розрахунковій стадії проводилась шляхом порівняння записаного з оригіналами артикуляційних таблиць та розрахунком розбірливості мови для кожного аудитора і кожного прослуховування, як відношення правильно сприйнятих слів до загальної кількості в артикуляційній таблиці. Слова з помилками, які не змінювали їх смисл, за принципом найгіршого варіанту захищеності вважались розпізнаними.

Далі було проведено статистичне усереднення між аудиторами значень словесної розбірливості для кожного прослуховування.

На аналітичній стадії проводився аналіз результатів та побудова графіків відповідних залежностей.

Графіки залежності словесної розбірливості від відношення сигнал/шум для різної кількості прослуховувань, побудовані у середовищі MathCad приведено на рис. 2.

Як бачимо, збільшення розбірливості за рахунок багаторазового прослуховування при розглянутих відношеннях сигнал/шум становить

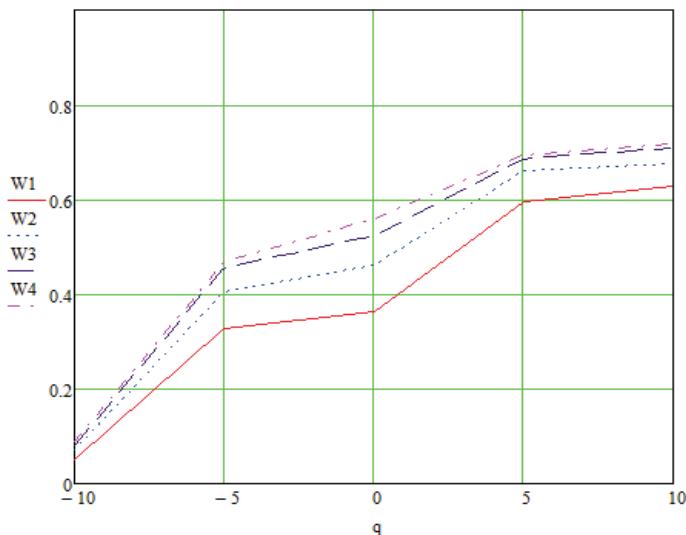


Рисунок 2 – Графіки залежності словесної розбірливості від відношення сигнал/шум для різної (від 1 до 4) кількості прослуховувань

5...20%, причому найбільший вплив має місце при сумірності інформативного сигналу і завади (відношеннях сигнал/шум від -5 до 5 дБ). Це пояснюється високою розбірливістю вже при першому (безпосередньому) прослуховуванні при малих рівнях завади і низькою максимально можливою розбірливістю при значному перевищенні рівня завади над рівнем інформативного сигналу в контрольній точці.

Було отримано також графіки залежності приросту розбірливості мови за рахунок багаторазового прослуховування від відношення сигнал/шум (рис.3). Використовуючи ці залежності можна коригувати значення розбірливості мови, отримані формантним методом, для врахування фактору багаторазового прослуховування.

Враховуючи висновок, зроблений в [6], що збільшення кількості прослуховувань більше 4-х не дає суттєвого приросту розбірливості, для корекції можна взяти приріст в результаті 4-х прослуховувань.

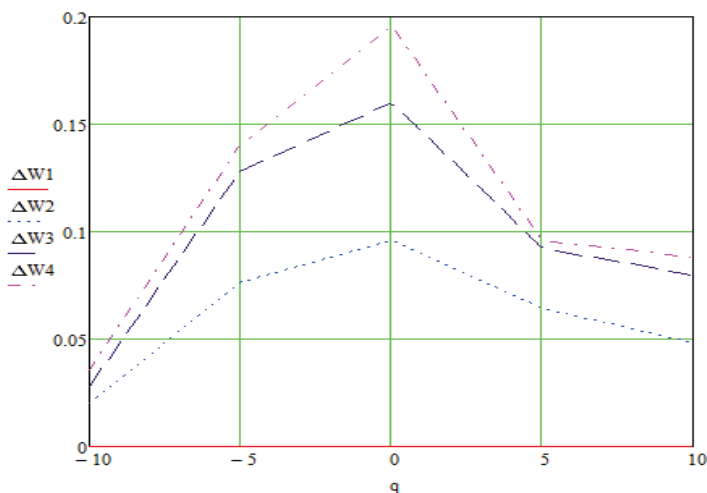


Рисунок 3 – Графік залежності приросту словесної розбірливості від відношення сигнал/шум для різної кількості прослуховувань

Висновки: При заваді типу «білий шум» збільшення розбірливості за рахунок багаторазового прослуховування може досягати 20%, причому найбільший вплив має місце при відношеннях сигнал/шум від -5 до 5 дБ.

Отримані в роботі залежності дають можливість враховувати вплив багаторазового прослуховування при оцінюванні захищеності мовної інформації формантним методом.

Список літератури:

1. Дворянkin С.В. Обоснование критериев эффективности защиты речевой информации / С.В. Дворянkin, Ю.К. Макаров, А.А. Хорев // Защита информации. Инсайд. – М.: 2007. -№2. – С.39-45.
2. Касьянов Ю.І. Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови / Ю.І. Касьянов, С.М. Нужний // Вісник НУ "Львівська політехніка": Автоматика вимірювання та керування. – 2016. – №.852 – С. 105 – 110.
3. Покровский Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.

4. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А.Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.

5. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений: ГОСТ 16600-72. – М.: ИПК Издательство стандартов, 1973. – 90 с.

6. Касьянов Ю.І. Дослідження впливу багаторазового прослуховування на словесну розбірливість мови / Ю.І. Касьянов, А.В. Сафіуліна //Сучасні проблеми інформаційної безпеки на транспорті: Матеріали VI всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2016. – С. 28 – 34.

УДК 004.056.5: 534.[784: 835]: 621.391.883

РОЗРАХУНОК БАЖАНИХ ХАРАКТЕРИСТИК ЗВУКОІЗОЛЯЦІЇ ТА ШУМОВОЇ ЗАВАДИ ЗА ОКТАВНИМИ РІВНЯМИ ФОРМАНТНОЇ РОЗБІРЛИВОСТІ МОВИ

***Автори:** Касьянов Ю.І., ст. викладач; Золотченко В.В., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Роботи з побудови системи захисту мовної інформації від витоку віброакустичними каналами ґрунтуються на оцінці існуючої та забезпечення необхідної звукоізоляції виділених приміщень (ВП), а також, при необхідності на застосуванні активних акустичних шумових завад, які створюються спеціальними генераторами і маскують інформативний сигнал.

Враховуючи, що пасивні та активні засоби захисту, як правило використовуються в комплексі і доповнюють один одного, для забезпечення заданого ступеня захищеності мовної інформації у ВП необхідно вирішувати задачі визначення необхідної характеристики звукоізоляції при відомій (заданій) шумовій заваді та визначення необхідних рівнів спектру шумової завади при наявній звукоізоляції.

Метою роботи є розробка методики розрахунку необхідних характеристик звукоізоляції та шумової завади за октавними рівнями бажаної формантної розбірливості мови для заданого ступеня захищеності мовної інформації.

Основна частина. Враховуючи, що в провідних країнах світу наразі для оцінювання захищеності мовної інформації використовується критерій розбірливості мови і впровадження цього критерію в Україні є лише питанням часу, за основу при розробці даної методики було взято методики оцінювання за критерієм розбірливості мови ефективності звукоізоляційних огорожувальних конструкцій [1] та генераторів реальних мовоподібних завад [2].

Розроблена методика дозволяє вирішувати дві взаємозалежні задачі.

Перша задача – при відомому рівні мовного сигналу у виділеному приміщенні і відомому рівні шуму та його спектру (октавних рівнів) в контрольній точці (з урахуванням активної шумової завади) визначається частотна характеристика звукоізоляційної конструкції, яка разом з даним шумом забезпечить необхідний ступінь захисту мовної інформації (необхідні октавні рівні формантної розбірливості і загальні значення формантної та словесної розбірливості в контрольній точці).

Друга задача – при відомому рівні мовного сигналу у ВП і відомій частотній характеристиці звукоізоляції визначаються октавні рівні шумової завади (рівень та спектр завади), яка разом з даною звукоізоляційною конструкцією забезпечить необхідний ступінь захисту мовної інформації.

Вхідними даними для розрахунку є:

- інтегральний та октавні рівні мовленнєвого сигналу у виділеному приміщенні (L_{Σ} та L_{Mi});
- середньгеометричні (125, 250, 500, 1000, 2000, 4000, 8000 Гц) та граничні (f_{ni} та f_{vi}) частоти октавних смуг мовного діапазону;
- октавні рівні формантної розбірливості в контрольній точці A_i , які необхідно забезпечити;
- частотна характеристика звукоізоляції $Q_i(f)$ або октавні рівні шумової завади в контрольній точці L_{wi} , в залежності від того яка (перша чи друга) задача вирішується.

В розрахунку використовуються графіки і формули з [3, 4].

Розрахунок виконується в наступному порядку:

з емпіричної функції розподілу появи формант $A_m(f)$ (рис. 1), або з апроксимуючого співвідношення

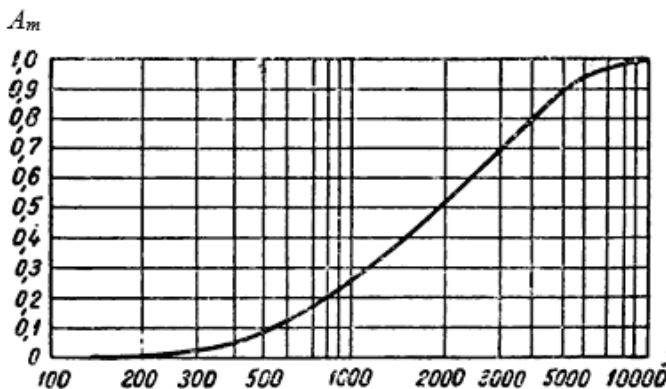


Рисунок 2.5 – Емпірична функція розподілу формант

$$A_m(f) = \begin{cases} 2,57 \cdot 10^{-8} \cdot f^{2,4}, & \text{якщо } 100 < f \leq 400 \text{ Гц;} \\ 1 - 1,074 \exp(-10^{-4} \cdot f^{1,18}), & \text{якщо } 400 < f \leq 10000 \text{ Гц.} \end{cases} \quad (1)$$

визначаються значення $A_m(f_{vi})$ і $A_m(f_{ni})$ та за формулою

$$A_{mi} = k_i = A_m(f_{vi}) - A_m(f_{ni}). \quad (2)$$

розраховуються максимальні значення формантної розбірливості в октавних смугах A_{mi} (ваговий коефіцієнт кожної смуги k_i);

– за формулою

$$\Delta B_i = \begin{cases} 200 / f_{cpi}^{0,43} - 0,37, & \text{якщо } f_{cpi} \leq 1000 \text{ Гц;} \\ 1,37 + 1000 / f_{cpi}^{0,69}, & \text{якщо } f_{cpi} > 1000 \text{ Гц.} \end{cases} \quad (3)$$

яка є аналітичною апроксимацією графіка різниці між спектрами мови й формант, отриманим Н.Б. Покровським за результатами артикуляційних випробувань (рис. 2) визначаються значення форматних параметрів ΔB_i ;

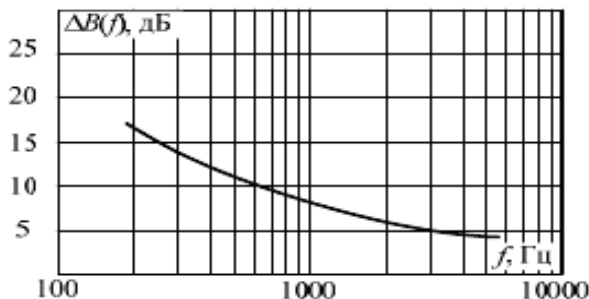


Рисунок 2 – Різниця між спектрами мови і формант

– визначаються ймовірності сприйняття формант, як відношення заданих (бажаних) октавних рівнів формантної розбірливості до вагових коефіцієнтів кожної смуги k_i (максимальних значень формантної розбірливості в октавних смугах A_{mi})

$$P_i = \frac{A_i}{A_{mi}} = \frac{A_i}{k_i} ; \quad (4)$$

– розраховуємо рівні відчуття формант E'_i в октавних смугах за формулою

$$E'_i = \begin{cases} -5.63 \cdot \ln(1-P_i) + 18.5 \cdot P_i - 13.2, & \text{якщо } P_i \geq 0.5 \\ 5.63 \cdot \ln(P_i) + 18.5 \cdot P_i - 5.5, & \text{якщо } P_i < 0.5 \end{cases} \quad (5)$$

яка є аналітичною апроксимацією залежності рівня відчуття формант від ймовірності їх сприйняття і отримана в програмі Advanced Grapher шляхом побудови функції $E'_i(P_i)$ за функцією $P_i(E'_i)$, приведеною в [3], та регресійного аналізу при її апроксимації логарифмічною залежністю;

– розраховуємо октавні відношення сигнал/шум q_i в контрольній точці за формулою

$$q_i = E'_i + \Delta B_i \quad (6)$$

– при розрахунку необхідної частотної характеристики звукоізоляції визначаємо октавні рівні інформативного сигналу в контрольній точці, а потім частотну характеристику звукоізоляції за формулами

$$L_{ci} = q_i + L_{\text{шi}} ; \quad (7)$$

$$Q_i = L_{\text{mi}} - L_{ci} ; \quad (8)$$

– при розрахунку необхідних октавних рівнів шумової завади в контрольній точці визначаємо октавні рівні інформативного сигналу в контрольній точці, а потім октавні рівні шумової завади за формулами

$$L_{ci} = L_{\text{mi}} - Q_i ; \quad (9)$$

$$L_{\text{шi}} = L_{ci} - q_i . \quad (10)$$

Розроблено програму розрахунку в Mathcad та проведено апробаційні розрахунки для дверної звукоізоляційної конструкції, які підтвердили працездатність розробленої методики.

Висновок: Розроблено методику розрахунку необхідних характеристик звукоізоляції та шумової завади за октавними рівнями бажаної формантної розбірливості мови для заданого ступеня захищеності мовної інформації. Проведено її апробацію.

Методика дає можливість оптимально компенсувати недостатню дію звукоізоляції активною шумовою завадою та навпаки.

Список літератури:

1. Касьянов Ю.І. Визначення впливу шумової завади та звукоізоляції на розбірливість мови формантним методом / Ю.І. Касьянов // Комп'ютерні технології друкарства. – 2014. – №31. – С.85-93.
2. Касьянов Ю.І. Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови / Ю.І. Касьянов, С.М. Нужний // Вісник НУ "Львівська політехніка": Автоматика вимірювання та керування. – 2016. – №.852 – С. 105 – 110.

3. Покровский Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.

4. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А.Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.

УДК 004.056.5: 534.843: 621.391.883

ОСНОВНІ АСПЕКТИ ОБ'ЄКТИВНОГО ТОНАЛЬНОГО МЕТОДУ ВИЗНАЧЕННЯ РОЗБІРЛИВОСТІ МОВИ

Автори: Касьянов Ю.І., ст. викладач; Трізно С.О., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вступ. Захист мовної інформації є однією з найважливіших задач у загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єктів інформаційної діяльності. При створенні та експлуатації систем технічного захисту суттєвим фактором є оцінка ефективності засобів захисту та ступеня захищеності мовної інформації у виділених приміщеннях від витоку акустичним каналом, яка проводиться при атестаційних випробуваннях та в процесі оперативного контролю.

В сучасних методиках для нормування і оцінювання захищеності мовної інформації від витоку акустичним каналом використовується значення словесної розбірливості мови у точках можливого знімання інформації (контрольних точках). При цьому для визначення розбірливості мови, як правило, використовують різновидності формантного методу [1–3].

Однак цей метод не дозволяє повністю врахувати ряд факторів, що впливають на розбірливість мови і пов'язані з суб'єктивними властивостями і характеристиками людської слухової системи. Тому перспективною видається об'єктивізація окремих суб'єктивних методів, зокрема, тонального методу визначення розбірливості мови, який використовують для оцінки якості телефонного зв'язку [4, 5].

Метою роботи є об'єктивізація тонального методу визначення розбірливості мови для адаптації його до задачі оцінювання захищеності мовної інформації.

Основна частина. Тональний метод визначення розбірливості мови вже давно використовується для оцінювання якості каналів телефонного зв'язку і базується на властивості людського слуху чітко визначати момент зникнення та появи звуку на рівні порогу чутливості. При вимірюванні генеруються тональні сигнали з частотами, рівними середньо-геометричним частотам октавних смуг, та аудитором визначаються пороги відчуття тону (середній рівень зникнення та появи сигналу), за якими розраховуються рівні відчуття тону, як різниця між рівнем сигналу і визначеним пороговим рівнем та за допомогою таблиць і розрахунків визначається формантна та словесна розбірливість.

Однак, для використання цього методу для оцінювання захищеності мовної інформації необхідно щоб він забезпечував адекватність результатів при характерних для контрольних точок відношеннях сигнал/завада та оперативність і мінімум затрат при проведенні оцінювання.

Було розроблено методику досліджень, яка описана в [6], та проведено дослідження можливостей тонального методу при відношеннях сигнал/завада, характерних для акустичних каналів витоку мовної інформації при заваді "білого" шуму. Результати досліджень і їх порівняння з результатами, отриманим формантним методом підтвердили можливість використання. Різниця не перевищувала 5%, що пояснюється різними умовами експериментів.

Забезпечення оперативності і мінімуму затрат при проведенні оцінювання захищеності мовної інформації тональним методом вирішується його об'єктивізацією.

Концепція об'єктивізації полягала у заміні суб'єктивного оцінювання порогу відчуття тону за допомогою аудиторів їх визначенням з використанням узагальнених характеристик порогу чутності тонових сигналів для середньостатистичного слухача.

Основні етапи інструментально-розрахункового тонального методу оцінювання захищеності мовної інформації за критерієм словесної розбірливості мови полягають в наступному:

1. Визначаються можливі акустичні каналів витоку мовної інформації та контрольні точки для вимірювання.

2. Знімається частотна характеристика шуму в контрольній точці (вимірюються рівні шуму в 7-ми октавних смугах мовного діапазону з середньгеометричними частотами 125, 250, 500, 1000, 2000, 4000, 8000 Гц).

3. У виділеному приміщенні почергово генеруються та відтворюються тонові тестові сигнали з частотами, що відповідають середньгеометричним частотам октавних смуг, і рівнями, що відповідають октавним рівням спектру довготривалого мовленнєвого сигналу при заданому (характерному для даного приміщення) його інтегральному рівні. Може бути згенерований єдиний тестовий сигнал з відповідним дискретним спектром.

4. Вимірюються сумарні рівні сигналу та визначаються рівні тестових сигналів в контрольній точці на середньгеометричних частотах октавних смуг.

5. Визначаються пороги чутності тону в контрольній точці на середньгеометричних частотах октавних смуг за частотною характеристикою порогу чутності тону при заданому виді та рівні шумової завади.

6. Розраховуються рівні відчуття тону як різниця між рівнем тестового сигналу та порогом чутності тону на середньгеометричних частотах октавних смуг.

7. Визначається форматна розбірливість в октавних смугах за залежністю від рівня відчуття тону.

8. Розраховується загальна формантна розбірливість та словесна розбірливість.

9. Отримане значення словесної розбірливості порівнюється з нормативним значенням і робиться висновок щодо ступеня захищеності мовної інформації та подальших дій.

Таким чином для об'єктивізації тонального методу потрібно мати значення порогів чутності тону тональних сигналів з частотами, що відповідають середньгеометричним частотам октавних смуг мовного діапазону (частотну характеристику порогу чутності тональних сигналів) при заданій шумовій заваді.

Частотні характеристики порогу чутності тональних сигналів можна отримати:

– чисто розрахунком – для типових видів шуму (з відомими спектрами) при різних інтегральних рівнях шуму;

– експериментально-розрахунковим способом – коли частотна характеристика шуму знімається експериментально, а пороги чутності тональних сигналів розраховуються;

– чисто експериментально – коли пороги чутності тональних сигналів визначаються акустичним експериментом за допомогою аудиторів.

Було отримано частотні характеристики порогу чутності тональних сигналів при заваді "білий" шум розрахунковим та експериментальним шляхом.

Оскільки слух реагує не на загальну енергію сигналу, а на його енергію в критичних смугах слуху, то маскування тонального сигналу широкосмуговим шумом відбувається лише за рахунок енергії завади в межах критичної смуги слуху з центральною частотою, що відповідає частоті тону. Тому при розрахунку слід частотну характеристику шуму представляти у вигляді залежності рівнів шуму в критичних смугах слуху з центральними частотами, рівними середньгеометричним частотам октавних смуг від частоти. Такі характеристики були розраховані для "білого" шуму при різних спектральних рівнях шумової завади $N(R)_{\text{БШ}}$ (рис.1). Розрахунок виконано за формулою:

$$L_{\text{БШ кр}} = N(R)_{\text{БШ}} + 10 \lg(\Delta f_{\text{кр}} / 1 \text{Гц}) \quad (1)$$

Рівень порогу чутності буде знаходитись на декілька децибел нижче рівня маскувального шуму у тій критичній полосі, де знаходиться корисний тоновий сигнал. В [7] сказано, що ця різниця складає 4...5 дБ.

Величина спектральних рівнів шумової завади може бути перерахована у інтегральний (сумарний) рівень інтенсивності за формулою:

$$L_{\Sigma} = 10 \lg \int_{f_{\text{Н}}}^{f_{\text{В}}} 10^{0,1N(R)_{\text{БШ}}} df, \quad (2)$$

де $f_{\text{В}}, f_{\text{Н}}$ – верхня та нижня границі частотного діапазону.

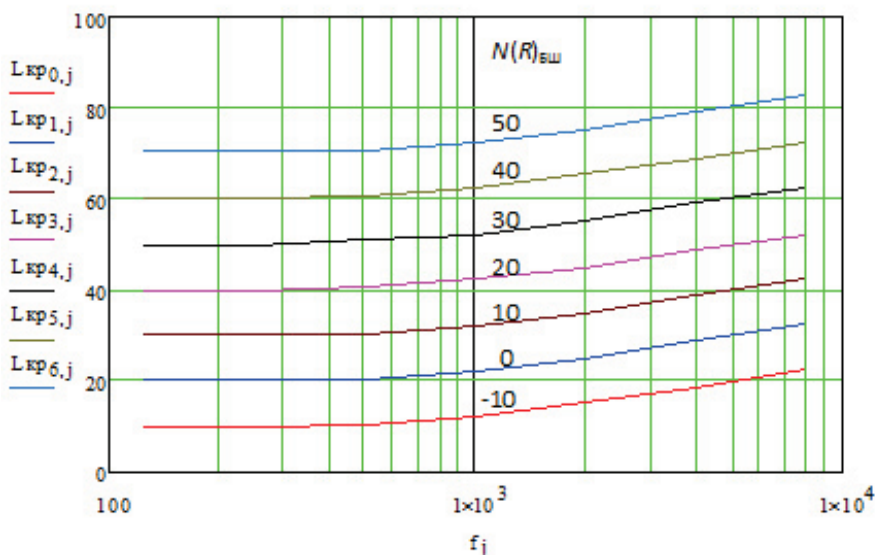


Рисунок 1 – Залежність рівнів інтенсивності "білого" шуму в критичних смугах слуху від частоти

Частотні характеристики порогу чутності тонових сигналів при різних рівнях інтенсивності завади "білий шум", отримані в експериментальних дослідженнях за участі аудиторів для визначення порогів чутності, приведені на рис. 2. "Білий" шум генерувався на персональному комп'ютері за допомогою програми Sound Forge і відтворювався активною акустичною системою F&D 600. Тоновий сигнал генерувався генератором сигналів низької частоти ГЗ-118. Рівень сигналу і шуму вимірювався шумоміром ВШВ-003.

Висновок: Визначено основні аспекти створення інструментально-розрахункового тонального методу визначення розбірливості мови та етапи методики його використання для оцінювання захищеності мовної інформації. Отримано ряд характеристик необхідних для використання методу.

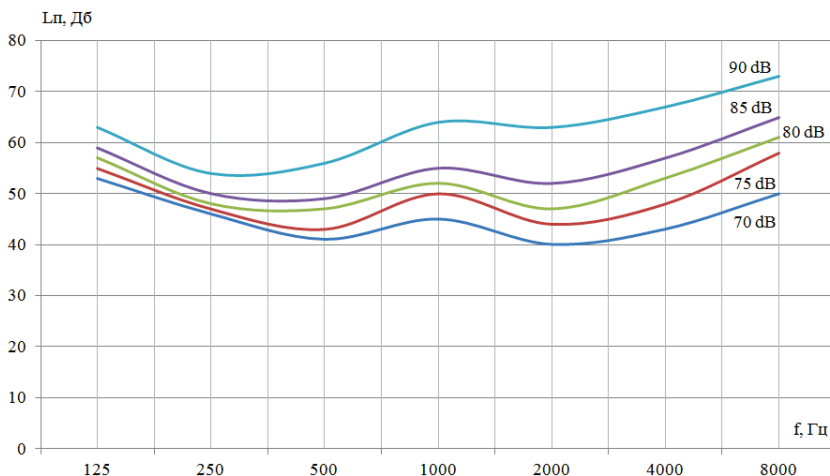


Рисунок 2 – Поріг відчуття тону в контрольній точці
на середньгеометричних частотах

Список літератури:

1. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. Eastern-European Journal Of Enterprise Technologies, 5 (9 (95)), 26–34. doi: <http://dx.doi.org/10.15587/1729-4061.2018.144146>
2. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А.Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.
3. Акустическая экспертиза каналов речевой коммуникации. Монография / Дидковский В.С., Дидковская М.В., Продеус А.Н. – Киев: Имэкс-ЛТД, 2008. – 420 с.
4. Покровский Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.

5. Аппараты телефонные. Тональный метод измерения разборчивости речи: ГОСТ 8031-78. – М.: ИПК Издательство стандартов, 1998. – 6 с.

6. Касьянов Ю.І. Використання тонального методу визначення розбірливості мови для задачі оцінки захищеності мовної інформації / Ю.І. Касьянов, С.В.Дума // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали V всеукраїнської науково-практичної конференції з міжнародною участю. – Миколаїв: НУК, 2015. – С. 32 – 38.

7. Сапожков М.А. Электроакустика. Учебник для вузов / М.А. Сапожков. – М.: Связь, 1978. – 272 с.

УДК 004.056.5: 534.[784: 835]: 621.391.883

ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ ТИПОВИМИ ЗВУКОІЗОЛЯЦІЙНИМИ КОНСТРУКЦІЯМИ ЗА ЇХ ЧАСТОТНИМИ ХАРАКТЕРИСТИКАМИ

***Автор:** Кучер В.С., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Касьянов Ю.І., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Вступ. Існуючі методики оцінки ефективності звукоізоляції, в тому числі в області інформаційної безпеки, побудовані на співставленні рівня сигналу до і після огорожувальної конструкції в октавних смугах мовного діапазону. При цьому визначається як інтегральний рівень звукоізоляції, так і залежність коефіцієнта звукоізоляції від частоти (частотна характеристика звукоізоляції). Такий підхід є оправданим при використанні в якості критерію для оцінювання та нормування захищеності мовної інформації відношення сигнал/шум.

Однак через неінваріантність критерію відношення сигнал/завада до виду завади та введення в практику оцінювання та нормування захищеності мовної інформації критерію розбірливості мови у провідних країнах світу, постала задача переходу на цей критерій і у оцінюванні ефективності звукоізоляційних огорожувальних конструкцій. Це потребує вирішення задач пов'язаних з встановленням залежності

між звукоізоляцією (частотною характеристикою звукоізоляційної конструкції) та втратами розбірливості мови при проходженні інформативного мовленнєвого сигналу через ці конструкції [1].

Метою роботи є розробка методики розрахунку інтегральних показників звукоізоляції та втрат розбірливості мови за частотними характеристиками звукоізоляційних конструкцій.

Основна частина. Методика оцінки звукоізоляції за критерієм розбірливості мови, описана і використана в [1] базується на інструментально-розрахунковому методі оцінки захищеності мовної інформації від витоку акустичним каналом, розробленому під керівництвом А.А. Хорева [2], та стандартній методиці оцінки звукоізоляції за зниженням рівня сигналу [3] і служить для оцінки ефективності звукоізоляційних конструкцій щодо захисту мовної інформації уже існуючого виділеного приміщення (ВП). Розроблена на її основі методика розрахунку втрат розбірливості мови за частотними характеристиками звукоізоляційних конструкцій дозволяє оцінити звукоізоляції огорожувальних конструкцій на стадії проектування виділеного приміщення.

Вхідними даними для розрахунку є:

- характерний інтегральний рівень мовного сигналу у виділеному приміщенні $L_{ВП\Sigma}$;
- частотна характеристика звукоізоляційної конструкції $Q(f)$, (краще, якщо вона отримана при тестовому сигналі зі спектром довготривалої мови, але може використовуватись і звичайна частотна характеристика для сигналу "білого" чи транспортного шуму);
- спектр шумової завади та її характерний інтегральний рівень в контрольній точці.

Порядок розрахунку наступний:

- визначаються рівні мовного сигналу у виділеному приміщенні на середньгеометричних частотах октавних смуг $L_{ВПi}$ за спектром довготривалого мовного сигналу [2, 4], виходячи з характерного інтегрального рівня мовленнєвого сигналу в приміщенні ;
- визначається рівень інформативного сигналу $L_{КТ i}$ в контрольній точці для кожної i -ої частотної смуги за формулою:

$$L_{\text{КТИ}} = L_{\text{ВПИ}} - Q_i, \quad (1)$$

де Q_i – звукоізоляція огорожувальної конструкції в i -й октавній смузі;

- виходячи з спектру шумової завади та відношення її інтегрального рівня, при якому отримано цей спектр, до характерного інтегрального значення рівня завади в КТ, визначаються рівні шуму в октавних смугах $L_{\text{ши}}$;

- визначається відношення сигнал/шум q в КТ для кожної i -ої частотної смуги;

- далі розрахунок повторює розрахунковий етап описаної в [1] методики експериментального оцінювання ефективності звукоізоляції за критерієм втрат розбірливості. Розраховуються ефективні рівні відчуття формант, коефіцієнт сприйняття формант, формантна розбірливість в октавних смугах, загальна формантна та словесна розбірливість мови, зниження розбірливості мови.

Для апробації методики було зроблено контрольний розрахунок втрат розбірливості в контрольній точці при проходженні інформативного сигналу через двері звукоізолюючі важкі, частотна характеристика звукоізоляції яких була взята з [5]. Октавні рівні фонового шуму взято з [6] на рівні NC-15. Октавні рівні мовного сигналу у виділеному приміщенні визначались за спектром довготривалої мови [2] для інтегрального рівня 64 дБ.

Для розрахунку розбірливості було використано програму, розроблену в MathCad відповідно створеній методиці. Отримані графіки втрат формантної розбірливості в октавних смугах від частоти для огорожувальної конструкції наведено на рис. 1. В результаті розрахунку визначено, що при використанні даної дверної конструкція втрати словесної розбірливості складають приблизно 72%.

Одночисловими показниками звукоізоляції огорожувальної конструкції є індекс звукоізоляції повітряного шуму R_W та інтегральне (загальне) значення звукоізоляції Q_Σ .

Індекс звукоізоляції повітряного шуму розраховується за стандартною методикою, прийнятою в будівництві [6].

Загальне значення звукоізоляції огорожувальної конструкції визначається як

$$Q_{\Sigma} = L_{\text{ВПС}} - L_{\text{КТ}\Sigma}, \quad (2)$$

де інтегральний рівень інформативного сигналу в контрольній точці розраховується за формулою

$$L_{\text{КТ}\Sigma} = 10 \lg \sum_{i=1}^n 10^{0,1 L_{\text{КТ}i}}, \quad (3)$$

в якій n – кількість октавних смуг; $L_{\text{КТ}i}$ – октавний рівень інформативного сигналу в контрольній точці, визначений за формулою (1).

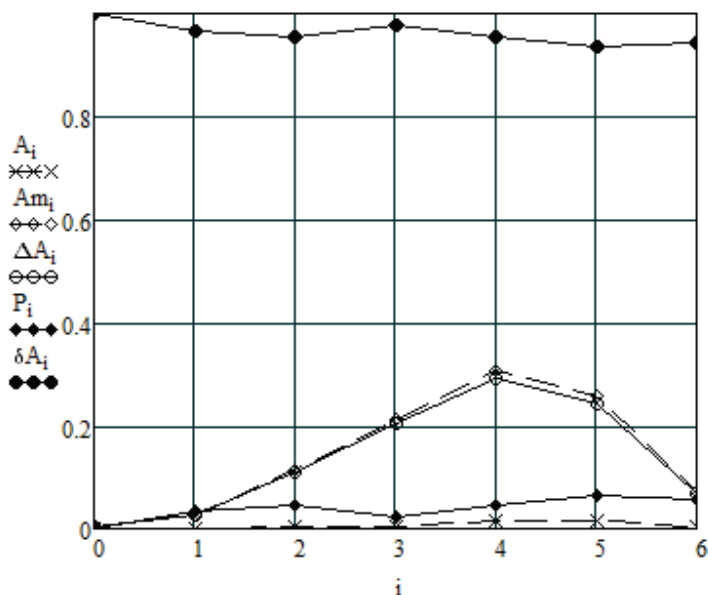


Рисунок 1 – Частотні залежності розбірливості формант (A_i), ймовірності появи формант (A_{m_i}), ймовірності сприйняття формант (P_i) та абсолютних (ΔA_i) і відносних (δA_i) втрат формант у октавних смугах.

Для досліджуваних дверей звукоізоляційних важких розрахований індекс звукоізоляції повітряного шуму $R_w = 42.87$, а інтегральне значення звукоізоляції $Q_\Sigma = 39.4$.

Висновок: Розроблено методику розрахунку втрат розбірливості мови в контрольній точці та інтегральних показників звукоізоляції огорожувальних конструкцій за частотною характеристикою звукоізоляції. Проведено її апробацію.

Методика дає можливість оцінювання ефективності звукоізоляції огорожувальних конструкцій щодо захисту мовної інформації від витоку прямим акустичним каналом на стадії проектування виділених приміщень.

Список літератури:

1. Касьянов Ю.І. Визначення впливу шумової завади та звукоізоляції на розбірливість мови формантним методом / Ю.І. Касьянов // Комп'ютерні технології друкарства. – 2014. – №31. – С.85-93.
2. Хорев А.А.(2001) Методы защиты речевой информации и оценки их эффективности. Специальная техника, № 4, С. 22 – 33.
3. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. – М.: ООО "Издательство Машиностроение", 2009 – 508 с.
4. *Yurii Kasianov, Viktoriia Khivrich, Anastasiia Mykhailychenko.* Research of the Ukrainian speech signal spectrum to assess the security of speech information. Proceedings of the VIII-th International science and technical conference «Information Security and Information Systems Security» ISSS-2021. – Lviv: Lviv Polytechnic Publishing House, 2021, pp.117–118.
5. Торокин А.А. Инженерно-техническая защита информации / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
6. ДСН допустимих рівнів шуму в приміщеннях житлових та громадських будинків і на території житлової забудови – Київ: МОЗ України, 2019. – 5с.
7. ДСТУ Б В.2.6-85:2009 "Конструкції будинків і споруд. Звукоізоляція огорожувальних конструкцій. Методи оцінювання." – Київ: Міністерство будівництва, 2010. – 30 с.

УДК 004.056.53: 534.781

ДОСЛІДЖЕННЯ СПЕКТРІВ ДОВГОТРИВАЛИХ УКРАЇНСЬКИХ МОВЛЕННЄВИХ СИГНАЛІВ

Автори: Михайличенко А.В.; Троценко С.С., студенти,
Національний університет кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна

Науковий керівник: Касьянов Ю.І., ст. викладач, Національний
університет кораблебудування імені адмірала Макарова, м. Миколаїв,
Україна

Вступ. Захист мовної інформації є одним з найважливіших завдань у загальному комплексі заходів щодо забезпечення інформаційної безпеки. Для обґрунтованого вибору інженерно-технічних заходів та засобів захисту мовної інформації потрібно проводити оцінювання ступеня її захищеності від витоку технічними каналами, зокрема прямим акустичним (повітряним) каналом.

До недавнього часу єдиним і загальноприйнятим критерієм оцінювання та нормування захищеності мовної інформації було відношення сигнал/шум в точці можливого знімання інформації. В Україні цей критерій використовується і сьогодні. Однак, цей показник є неінваріантним щодо виду шумової завади, що стримує впровадження в практику ефективних генераторів реальних мовоподібних завад [1, 2]. Тому наразі в ряді провідних країн світу в якості критерію нормування і оцінювання захищеності взято словесну розбірливість перехопленого мовного повідомлення, яка є безпосередньою мірою зрозумілості.

Сертифіковані методики оцінювання захищеності мовної інформації за критерієм розбірливості мови, як правило, базуються на використанні різновидностей формантного методу, які ґрунтуються на розрахунку відносної кількості сприйнятих формант мовного повідомлення і для визначення формантної розбірливості використовують такі характеристики мови, як спектр довготривалого мовленнєвого сигналу та функцію розподілу формант за частотою [3-5].

Впровадження критерію розбірливості мови для нормування і оцінювання захищеності мовної інформації в Україні видається лише питанням часу. Тому актуальною задачею є дослідження спектральних характеристик української мови.

Метою роботи є отримання узагальненого спектра довготривалого українського мовленнєвого сигналу шляхом проведення акустичних експериментів та за допомогою сучасних програмних засобів обробки звуку.

Основна частина. При дослідженнях спектру українського довготривалого мовленнєвого сигналу методом фізичного експерименту цей спектр представляється октавними рівнями довготривалого мовленнєвого сигналу (рівнями звукового тиску) в октавних смугах мовного діапазону частот з середньгеометричними частотами 125; 250; 500; 1000; 2000; 4000; 8000 Гц.

Для проведення досліджень було розроблено методику, яка включає 4 етапи (підготовчий, інструментально-вимірювальний, розрахунковий та аналітичний) і описана в [6, 7].

За даною методикою було проведено дослідження при використанні фонограм українських мовленнєвих сигналів з телевізійних новин [6] та фонограм безпосередньо "живих" голосів дикторів, які читали довільні уривки літературних та публіцистичних текстів [7]. Однак довільний вибір текстового матеріалу як у першому, так і у другому випадку приводив іноді до значного розкиду спектрів одного й того ж диктора. Крім того у першому випадку на спектр впливало ще й налаштування звукової апаратури телевізійних каналів.

Було проведено дослідження впливу підбору текстового матеріалу на спектральні характеристики, які показали, що при використанні фонетично і статистично збалансованого текстового матеріалу, зокрема артикуляційних таблиць слів, спектр окремого диктора був практично стабільним. Тому в даних дослідженнях були використані фонограми зачитування артикуляційних таблиць українських слів, взятих з [8], оскільки, нажаль, державного стандарту з такими таблицями нема.

На стадії підготовки були записані аудіо файли тривалістю 15...20 с при читанні реальними дикторами артикуляційних таблиць українських слів. Запис сигналів робився для двох груп дикторів: чоловіків і жінок. Для запису мовних сигналів використовувався конденсаторний мікрофон BOYA BY-MM1. Запис проводився на ноутбуці MacBook Pro, програмою WavePad у форматі нестисненого цифрового звуку Wav (44000 Гц, 16 біт). Було записано 16 фонограм.

Інструментально-вимірювальний етап проводився в лабораторії за стандартною схемою (рис.1). Підготовлені звукові файли відтворюва-

лись програмою Sound Forge на персональному комп'ютері (ПК) і через звукову карту Realtek High Definition Audio сигнал подавався на активну акустичну систему (AAC) Primax Soundstorm. Вимірювання рівнів сигналу в октавних смугах виконувалось шумоміром ВШВ-003 з конденсаторним мікрофоном в режимі «повільний». Відстань між AAC і мікрофоном шумоміра було встановлено 0,25 м, щоб мінімізувати вплив відбитого звуку на результат.

Перед вимірюваннями проведено налаштування та калібрування відтворювальної апаратури, з метою зниження інструментальних похибок, що вносяться АЧХ елементів каналу. Нерівномірність АЧХ не перевищувала 0,5 дБ.

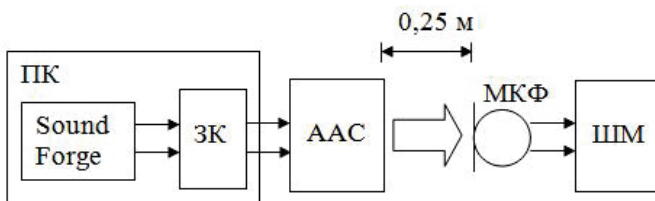


Рисунок 1 – Схема експериментальної установки:

ПК – персональний комп'ютер; ЗК – звукова карта;

AAC – активна акустична система; МКФ – мікрофон; ШМ – шумомір

Звучання усіх фонограм перед проведенням вимірювань в октавних смугах регуляторами гучності приводились до однакового інтегрального рівня звукового тиску в 70 дБ, що забезпечило перевищення рівня мовного сигналу над рівнем фонового шуму не менше 20 дБ.

На розрахунковому етапі було проведено статистичне усереднення спектрів жіночих та чоловічих голосів і отримано узагальнений спектр українського довготривалого мовленнєвого сигналу.

Графіки усереднених спектрів довготривалих жіночих і чоловічих мовленнєвих сигналів та узагальнений спектр української довготривалої мови наведено на рис. 2.

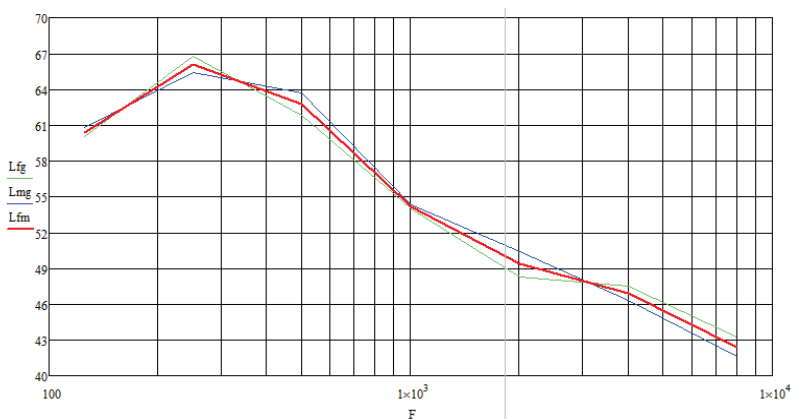


Рисунок 2 – Усереднені та узагальнений спектри української довготривалої мови

Було проведено також аналіз можливостей стандартних програм Sound Forge та RightMark Audio Analyzer щодо дослідження спектрів довготривалих мовленнєвих сигналів з використанням спектральних аналізаторів цих програм.

Спектроаналізатор програми Sound Forge дозволяє не тільки отримати спектри мовленнєвих сигналів, але і сформувати їх масив, що суттєво полегшує порівняльний аналіз та узагальнення. В програмі Sound Forge було проведено дослідження розкиду спектрів у випадку читання одним диктором різних артикуляційних таблиць слів та при читанні різними дикторами однієї і тієї ж таблиці. В дослідженнях використовувались ті ж фонограми, що і у фізичному експерименті. Результати досліджень показали, що спектри різних дикторів при читанні однакової артикуляційної таблиці можуть суттєво різнитись (рис. 3), в той час, як при читанні одним диктором різних артикуляційних таблиць отримані спектри практично співпадають.

Спектральний аналіз фонограм довготривалих мовленнєвих сигналів був також проведений у програмі RightMark Audio Analyzer. Однак дана програма не дозволяє формувати масив спектрів, що ускладнює порівняльний аналіз та узагальнюючі процедури.

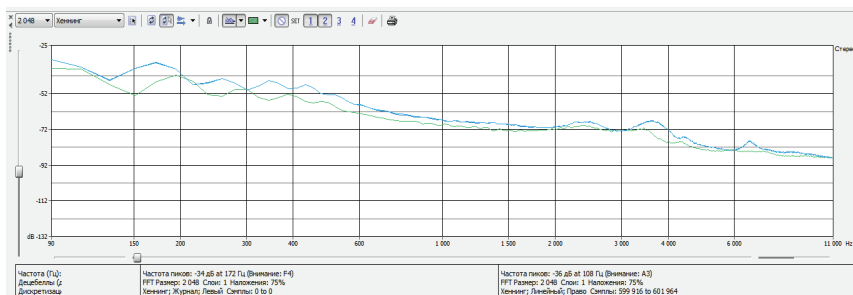


Рисунок 3 – Спектри мови двох чоловіків при зачитуванні однієї й тієї ж артикуляційної таблиці українських слів

Висновки:

1. Отримано узагальнений спектр українського довготривалого мовленнєвого сигналу, що дозволить враховувати особливості національного мовлення при використанні формантних методів для оцінювання захищеності мовної інформації за критерієм розбірливості мови.
2. При використанні для отримання узагальненого спектру мови фонетично та статистично збалансованого текстового матеріалу, яким є артикуляційні таблиці слів, можна мінімізувати кількість текстового матеріалу збільшивши за рахунок цього кількість дикторів і отримавши більш точні статистичні узагальнення при тій же кількості фонограм.

Список літератури:

1. Касьянов Ю.І. Оцінювання ефективності генератора реальної мовоподібної завади за критерієм розбірливості мови / Ю.І. Касьянов, С.М. Нужний // Вісник НУ "Львівська політехніка": Автоматика вимірювання та керування. – 2016. – №.852 – С. 105 – 110.
2. Volodymyr Blintsov, Sergey Nuzhnyi, Liubomyr Parkhuts, Yurii Kasianov (2018) . The objectified procedure and a technology for assessing the state of complex noise speech information protection. Eastern-European Journal of Enterprise Technologies. 5/9 (95), p. 26–34. DOI: 10.15587/1729-4061.2018.144146
3. Покровский Н. Б. Расчет и измерение разборчивости речи / Н. Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.

4. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А.Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.

5. Акустическая экспертиза каналов речевой коммуникации. Монография / Дидковский В.С., Дидковская М.В., Продеус А.Н. – Киев: Имэкс-ЛТД, 2008. – 420 с.

6. Касьянов Ю.І. Спектр довготривалої української мови в оцінюванні захищеності мовної інформації за критерієм розбірливості / Ю.І. Касьянов, В.В. Плютенко. // Інформаційні системи та технології ICT-2019: Матеріали 8-ї міжнародної науково-технічної конференції. – Харків: ХНУРЕ, 2019. – С. 243–245.

7. Yurii Kasianov, Viktoriia Khivrich, Anastasiia Mykhailychenko. Research of the Ukrainian speech signal spectrum to assess the security of speech information. Proceedings of the VIII-th International science and technical conference «Information Security and Information Systems Security» ISSS-2021. – Lviv: Lviv Polytechnic Publishing House, 2021, pp.117–118.

8. Архипова О.О., Журавльов В. А., Кумейко В. Артикуляційні таблиці слів української мови / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, випуск 2(19), 2009. – С. 13 – 17.

УДК 004.056.5; 004.89; 514.743.4

ІНТЕЛЕКТУАЛЬНІ ЗАСОБИ В СИСТЕМАХ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ

***Автор:** Стефанюк Ю.О., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

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

У сучасному світі інформація стає стратегічним ресурсом та кількість самої інформації збільшується. Швидкі темпи розвитку та розповсюдження інформаційних технологій, проникнення їх до усіх сфер життя, викликають виникнення потреби у обробці великих об'ємів

даних та захисту цих даних. Однією з головних причин проникнення до комп'ютерних систем та їх ураження є наявність великої кількості індикаторів (інформації), за якою людина сама прослідкувати не в змозі. Тому зараз все більше починають впроваджуватися нейронні мережі та штучний інтелект до систем виявлення та запобігання вторгнень [1], які використовуються наприклад, як класифікатори (фішингові посилення), фільтри спаму, для виявлення шкідливого програмного забезпечення, тощо [2].

Метою даної роботи є визначення методики використання інтелектуальних засобів та нейронних мереж у системах виявлення та запобігання вторгнень

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- проаналізувати можливості використання інтелектуальних засобів для вирішення задач виявлення та запобігання вторгнень;
- визначити проблемні аспекти застосування машинного навчання у вирішенні задач кібербезпеки та шляхи їх нівелювання.

Інтелектуальні засоби все частіше починають використовуватися у системах захисту інформації. Методи машинного навчання мають великий потенціал використання у сфері кібербезпеки, тому починають розвиватися та впроваджуватися все більшою кількістю компаній у свої продукти [3].

Існують певні обмеження, щодо використання інтелектуальних засобів для вирішення задач кібербезпеки, що спричинені такими факторами:

- Наявність великої кількості алгоритмів для вирішення різних завдань та відсутність одного універсального алгоритму;
- Проблема представлення даних;
- Великі вимоги до об'єму ресурсів системи.

Основними напрямками використання інтелектуальних засобів для вирішення задач кібербезпеки зазвичай є:

- Виявлення аномалій.
- Аналіз шкідливого програмного забезпечення.
- Аналіз мережевого трафіку.
- Захист користувацького веб-середовища.

Під виявленням аномалій, у контексті забезпечення безпеки мереж та хостів, розуміють виявлення випадків непередбаченого вторгнення та раніше не помічених вразливостей. Зокрема такий метод може використовуватися для:

- Виявлення вторгнень на хост.
- Виявлення вторгнень до мережі.
- Виявлення вторгнень у веб-додаток.

Проблемою використання інтелектуальних засобів у виявленні аномалій, є виникнення хибнопозитивних спрацьовувань. Оскільки їх виникнення може швидко знизити ступінь довіри до системи й стати причиною критичних вразливостей у системі. Тому майже немає автоматизованих систем з виявлення аномалій, що працюють лише на методиках машинного навчання – майже завжди у робочий цикл залучена людина.

Аналіз шкідливого програмного забезпечення – це область дослідження функціональних можливостей, мети, походження і потенціального впливу шкідливого програмного забезпечення. Оскільки ця задача зазвичай виконується вручну та пов'язана з великими трудовитратами, все частіше для її вирішення починають використовувати даталогію та машинне навчання для автоматизації певних етап аналізу. Їх методики головним чином пов'язані з визначенням найбільш важливих ознак з даних.

Інтелектуальні засоби можуть допомогти у усуненні деяких типів проблем створених шкідливим ПО, головним чином завдяки таким своїм характеристикам:

- Не чітке порівняння;
- Автоматизований вибір властивостей;
- Адаптованість.

Головною проблемою використання інтелектуальних систем для аналізу шкідливого програмного забезпечення залишається збір, аналіз та форматування даних для подальшого їх ефективного використання.

Найбільш ймовірним способом, яким зловмисники можуть проникнути до інфраструктури – є шлях через мережеве середовище. Забезпечення безпеки мережі являє собою велику практичну область діяльності із захисту комп'ютерних мереж та кінцевих пунктів мереж-

ного доступу від шкідливих дій, некоректного використання та критичних відмов.

У забезпеченні захисту мережі, інтелектуальні засоби використовуються зазвичай для:

- Класифікації мережевих пакетів.
- Виявлення атак та вторгнень до мережі.
- Виявлення загроз у мережевому середовищі.
- Захист від ботнету та DDoS атак.

Захист користувацького веб-середовища є досить великим напрямом для роботи, оскільки під визначення користувацьке веб-середовище підпадає будь-який сервіс, який є доступним для всіх через Інтернет, який надає свою продукцію чи послуги індивідуальним споживачам. Інтелектуальні засоби зазвичай використовуються для:

- Захисту користувацьких облікових записів від злому.
- Аналіз користувацьких облікових записів для виявлення підозрілих, або шкідливих.
- Дослідження та розробка нових методів автентифікації користувачів.

Уявлення про те, що методи машинного навчання у будь-яких випадках їх практичного використання дають позитивні результати – є абсолютно неправильним. У реальній практиці не існує універсальних алгоритмів машинного навчання, які б однаково добре працювали у будь-яких предметних сферах, але наявна певна низка проблем з якою неодмінно стикаються під час розробки та використання інтелектуальних засобів.

Такими проблемами є:

- Проблема необ'єктивності даних та неточності міток, що спотворює подальші результати робіт інтелектуальної системи [4]. Шляхом вирішення цієї проблеми є звуження «області роботи» інтелектуальної системи, або ручне підвищення якості даних та виправлення помилок.
- Проблема відсутніх (втрачених) даних у наборах. Шляхом вирішення цієї проблеми є визначення відсутнього (втраченого) значення у наборі за допомогою аналізу інших, пов'язаних з ним даних.

– Проблема оптимізації гіперпараметрів, параметрів, що мають найбільший вплив на поведінку інтелектуальної системи та задаються перед початком тренування, тобто неможливо завчасно знати правильне значення того чи іншого гіперпараметра. Шляхом вирішення цієї проблеми є метод «грубої сили», тобто тренування системи з різними значеннями гіперпараметра.

Висновки. В роботі розглянуто можливості використання інтелектуальних засобів для вирішення задач виявлення та запобігання вторгнень, визначено проблемні аспекти застосування машинного навчання у вирішенні задач кібербезпеки та шляхи їх нівелювання.

Інтелектуальні системи дозволяють машинам виконувати завдання, для яких необхідний людський інтелект, такі як, візуальне сприйняття, розпізнавання мови, прийняття рішень. Сьогодні область використання інтелектуальних систем у кібербезпеці хоч і не виглядає досить об'ємною, вона розвивається та збільшується з кожним днем. Все частіше можна зустріти процеси автентифікації користувачів, що використовують алгоритми розпізнавання мови або обличчя, дієві спам-фільтри або аналізатори мережевого трафіку [3].

Список літератури:

1. <https://heroic.com/about/>
2. Чіо К., Фрімен Д. Машинне навчання та безпека / пер. з анг. А. В. Снастіна. – М.Ж ДМК Пресс, 2020. – 388 с.
3. Стефанюк Ю.О. Тензоры и искусственный интеллект в системах защиты информации // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали ІХ Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2021. – С.193-197. URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf
4. Штучний інтелект у кібербезпеці. <https://dou.ua/lenta/articles/ai-in-cybersecurity/>

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 інформації 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.

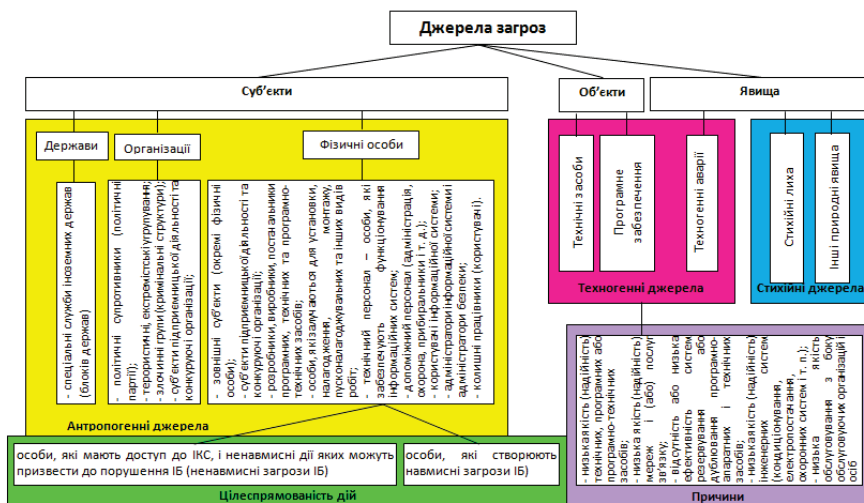


Рисунок 1 – Класифікація джерел загроз

Антропогенні загрози можуть 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.

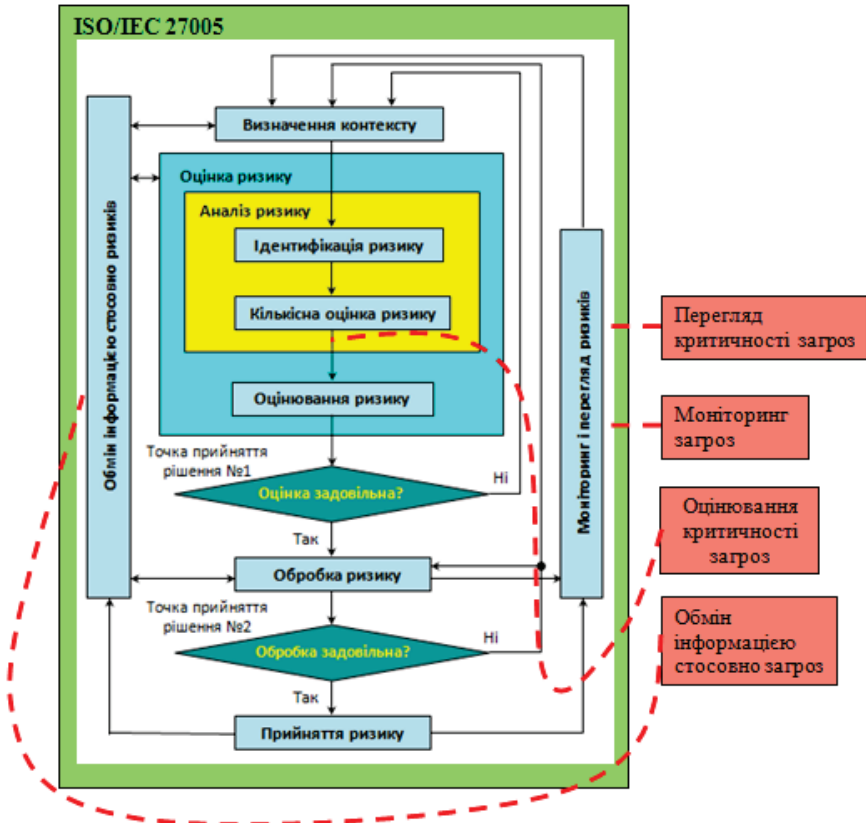


Рисунок 2 – Оцінювання загроз в ітераційному процесі менеджменту ризиків

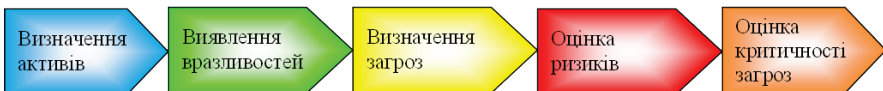


Рисунок 3 – Етапи ранжування загроз

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.

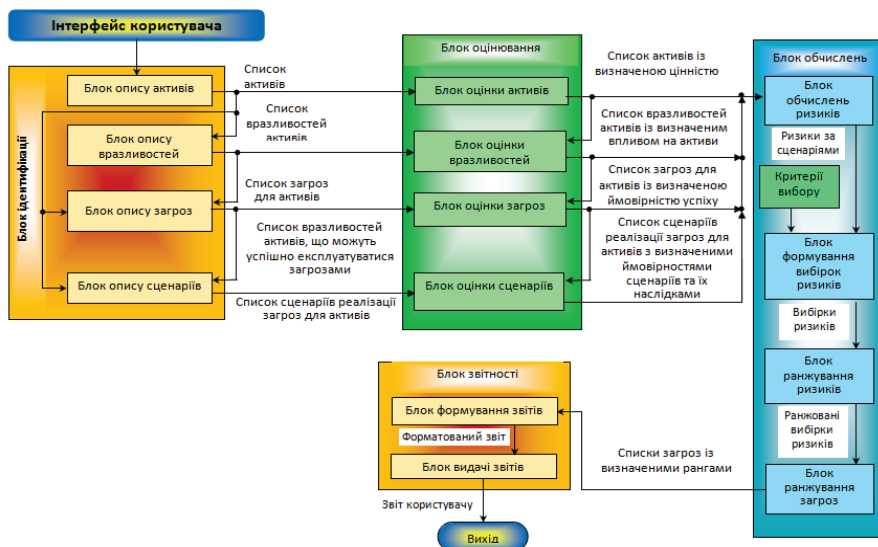


Рисунок 4. – Інформаційні потоки

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.

The screenshot displays a risk assessment form with the following fields and values:

Field	Value
Код сценарію	21
Актив	База клієнтів
Цінність активу	1
Оцінка впливу	3
Оцінка рівня ймовірності реалізації сценарію	4
Рівні ймовірностей успішної експлуатації	2
Рівні ймовірностей вибору вразливостей	3
Рівні ймовірностей виникнення загроз	2
Ризик	144
Ранг ризику	5
Категорія ризику	2
Категорія загрози	1

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 критеріїв, 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. С., 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. Розв'язку 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 ДССЗІ 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 категоризованих 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).

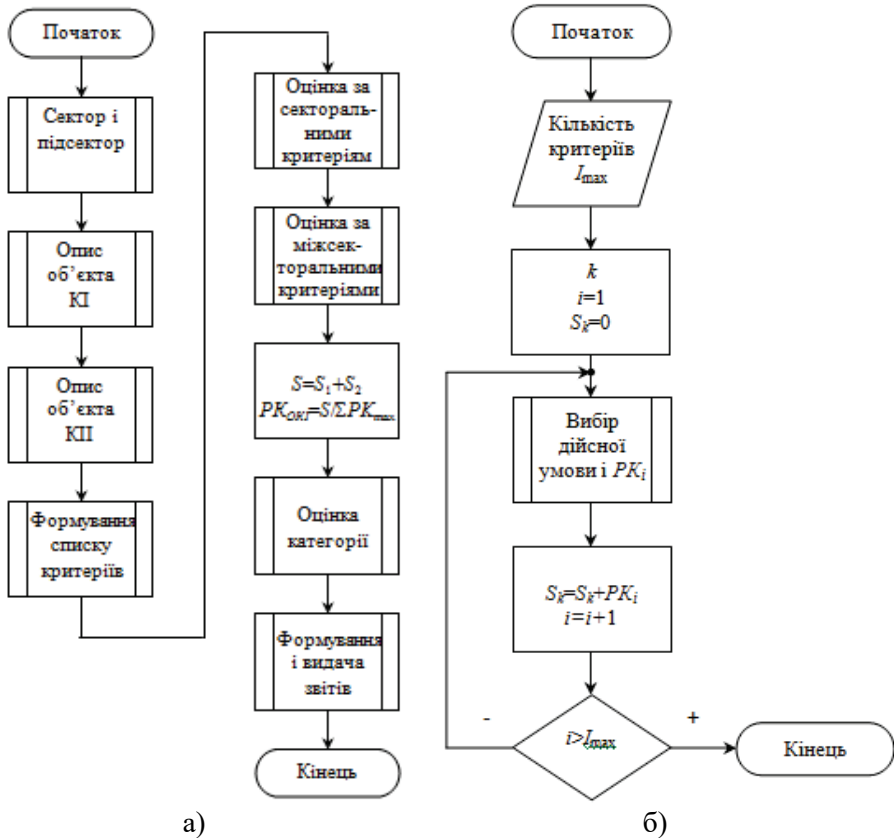


Рисунок 1 – Основні алгоритми

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 представлення

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.

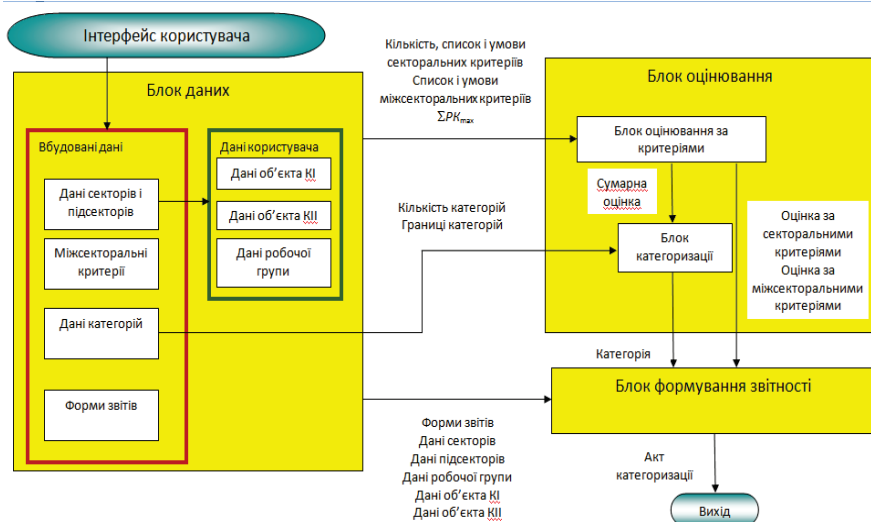


Рисунок 2 – Інформаційна модель

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:

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації

Склад вбудованих блоків даних



Склад даних користувача

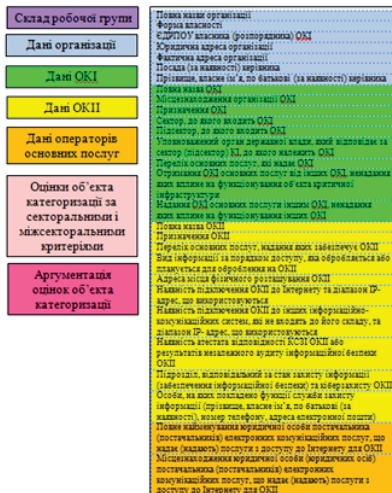


Рисунок 3 – Деталізація вхідних даних

Номер критерію	РК10	РК11	РК12	РК13	РК14	РК15	РК16	РК_max	Сума балів	Категорія	Значущість об'єкта КІ для забезпечення національної безпеки та обороноздатності країни
РСК_1	2								36	3	11
РСК_2	0										6
РК1	3										8
РК2	2										3
РК3	4										6
РК4	0										
РК5	2										
РК6	3										
РК7	1										
РК8	2										
РК9	1										
РК_max								72			
Сума балів	36										
РК_ОКІ	0,5										
Категорія										3	

Рисунок 4 – Вихідні дані моделі

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

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; арозроблені 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\(12\)](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_r_303_79299367.pdf
5. Рогов П.Д., Ворочив 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-cvsvd.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:

- провести аналіз методів оптимізації інвестицій в інформаційну безпеку і визначити вхідні та вихідні дані для цих методів, особливості отримуваних результатів;
- визначити критерії оптимізації інвестицій в інформаційну безпеку;
- розробити інформаційну модель визначення оптимальних інвестицій в інформаційну безпеку за сукупністю критеріїв, що обираються користувачем, і структуру відповідної структури автоматизованої системи.

Як показав проведений аналіз відкритих літературних джерел [1-8] показав, що на даний час оптимізація інвестицій в інформаційну безпеку може бути здійснена за допомогою наступних методів:

- наближена оцінка за долею вартості інформаційно-комунікаційної системи (ІКС), яка може вважатися достатньою на підставі досвіду проектування, впровадження та експлуатації аналогічних ІКС [3, 5, 6];
- методи багатокритеріальної оптимізації;
- методи нечіткої логіки [6, 7];
- оцінка за моделлю Гордона-Лоеба [2, 5, 8], яка може будуватися із застосуванням різних функціональних залежностей, які мають відповідати певним вимогам;
- оцінка за моделлю Архіпова [4], яка базується на ризик-орієнтованому підході і додатково враховує мотивацію дій суб'єктів інформаційних відносин.

Ці методи різняться за теоретичними основами, за способом отримання і формою представлення вхідних і вихідних даних, за способом формування і змістом критеріїв оптимізації, за алгоритмами, але всі вони в якості складової вхідної інформації використовують вартість ІКС, а на виході видають інформацію щодо оптимальних інвестицій у кількісній або якісній формі, зокрема, граничні значення інвестицій з точки зору економічної доцільності і ефективності захисту інформації (обмеження діапазону інвестицій зверху і знизу) або визначена категорія обсягу інвестицій за якісною шкалою «недостатній» – «завищений», яка може мати різну кількість градацій.

Критерії оптимальності обсягу інвестицій в інформаційну безпеку визначаються застосуванням методом аналізу:

– при наближеному оцінюванні визначається точкова оцінка обсягу інвестицій за єдиним критерієм – достатнім (з досвіду) відсотком від вартості ІКС. Практично визначається обмеження інвестицій знизу, верхня межа доцільності інвестицій не визначається, фактори, що впливають на ефективність інвестицій не аналізуються, але їх поточний і прогнозований вплив на ефективність інвестицій в узагальненій формі враховується в розмірі відсотка вартості ІКС;

– при використанні методів багатокритеріальної оптимізації визначається точкова оцінка обсягу інвестицій при досягненні бажаного значення функції мети при заданих обмеженнях, однак для формування такої функції необхідно проводити детальний аналіз ризиків;

– при використанні методів нечіткої логіки критерієм оптимальності є належність обсягу інвестицій нечіткій множині «оптимальні інвестиції» лінгвістичної змінної ОБСЯГ ІНВЕСТИЦІЙ із значенням функції належності не менше заданого рівня прийняття гіпотези. Одночасно можуть бути визначені значення функцій належності обсягу інвестицій іншим нечітким множинам зазначеної лінгвістичної змінної, наприклад, «недостатній обсяг». Таким чином, отримується множина нечітких точкових оцінок;

– при використанні моделі Гордона-Лоеба критерієм оптимальності є максимум відношення обсягу інвестицій до можливих збитків, а оптимальний обсяг інвестицій визначається як певний відсоток від потенційних втрат;

– при використанні моделі Архіпова критерієм оптимальності є мінімальний ризик, а на виході визначається діапазон розумних інвестицій з врахуванням мотивації дій зловмисника і сторони, що захищається.

Розроблена узагальнена інформаційна модель автоматизованої системи, призначеної для визначення оптимальних інвестицій в інформаційну безпеку за сукупністю критеріїв, що обираються користувачем, і структура автоматизованої системи наведені на рис.1.

Блок «Рекомендації» формується на основі аналізу навчальної літератури, нормативних документів і наукових публікацій і коригується в разі потреби адміністратором системи.

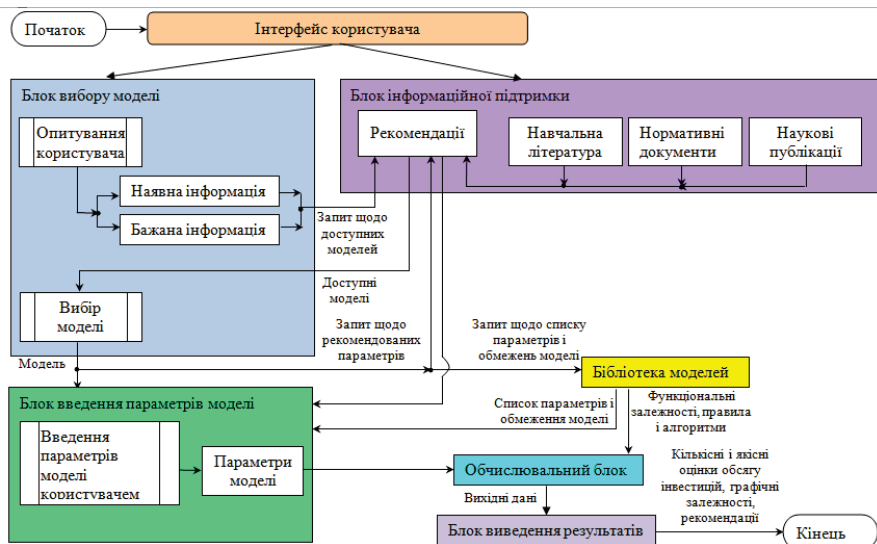


Рисунок 1 – Узагальнена інформаційна модель і структура автоматизованої системи

Вибір моделі здійснюється на основі результатів опитування користувача щодо наявних у нього даних, які необхідні для проведення обчислень за всіма типами моделей, і бажаної для користувач вихідної інформації (визначення граничних обсягів інвестицій, отримання висновків щодо доцільності інвестицій тощо).

Бібліотека моделей містить блоки перелічених вище моделей, які характеризуються списком параметрів моделі, обмеженнями, правилами, функціональними залежностями і алгоритмами отримання вихідної інформації, яка може бути представлена залежно від моделі кількісними і якісними оцінками обсягу інвестицій, графічними залежностями і рекомендаціями щодо засобів підвищення ефективності інвестицій в інформаційну безпеку. Моделі одного типу, що характеризуються різними функціональними залежностями, об'єднані в групу, з якої користувач обирає потрібний підтип моделі.

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 критеріїв, що обираються користувачем.

Список літератури:

1. Arnold R. Cybersecurity: A Business Solution: An executive perspective on managing cyber risk. Winston-Salem: Threat Sketch, LLC, 2017. – 100 с. [URL]: https://books.google.com.ua/books?id=zu44DwAAQBAJ&pg=PA22&redir_esc=y#v=onepage&q&f=false
2. Gordon L. A., Loeb M.P. The Economics of Information Security Investment. – 2002. – 20 с. – URL:https://www.researchgate.net/publication/288351571_The_Economics_of_Information_Security_Investment?enrichId=rgreq-4d47f3f962a06d00a8dc80eb22fbe10d-XXX&enrichSource=Y292ZXJQYWdlOzI4ODM1MTU3MTtBUzozMjAyOTkyNDM5MDA5MjhAMTQ1MzM3NjY5ODU5Mw%3D%3D&el=1_x_3&esc=publicationCoverPdf.
3. Архипов О.Є., Архипова Є.О. Особливості визначення обсягу інвестицій в систему захисту інформаційних ресурсів // Інвестиції: практика та досвід. – 2015. – №11. – С. 71-74. [URL]: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-15_Investitsiyi-v-SZI_DU.pdf
4. Архипов О.Є., Архипова Є.О. Ризиковий підхід до визначення обсягу оптимальних інвестицій у безпеку інформації / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность. Материалы XV Международной научно-практической конференции ИТБ-2015. (21 жовтня 2015 р., м. Київ). – К.: ИПРИ НАН України, 2015. – 250 с. – С.12-17. [URL]: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-15_AA_risk2_konf.pdf
5. Верескун М.В. Ефективність інвестицій в інформаційну безпеку: проблеми і рішення // Вісник Приазовського державного технічного університету. Серія : Економічні науки. – 2015. – Вип. 30. – С. 220-227. URL: http://nbuv.gov.ua/UJRN/VPDTU_ek_2015_30_30

6. Корченко А.Г., Архипов А.Е., Казимирчук С.В. Анализ и оценивание рисков информации безопасности. – К.: ООО «Полиграф-Лазурит», 2013. – 275 с.

7. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. – К.: Центр навчально.-наукових. та науково-практичних видань НА СБ України, 2014. – 190 с.

8. Супруненко І.О. Практичні способи застосування підходу, орієнтованого на ризики, в галузі інформаційної безпеки // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». Секція «Системи та технології кібернетичної безпеки». – Київ: ВПІ ВПК «Політехніка», 2018. Т.2. – С.126-129.

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

УДК 629

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК ДжЕРЕЛА ЖИВЛЕННЯ НА БАЗІ ФОТОЕЛЕКТРИЧНОГО ПЕРЕТВОРЮВАЧА

***Автор:** Бинкало С.Ф., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Сонячна енергія – це енергія, яку може використовувати людина практично в необмежених масштабах. Тієї кількості тепла та енергії, що виділяє Сонце на поверхню Землі, вистачило б, щоб забезпечити енергії не лише нинішні, а й майбутні потреби людини в електроенергії. Приблизно третина енергії відбивається безпосередньо у космос в атмосферу. Час, коли сонячна енергія доступна, є денний час.

Тому що енергія сонця не може бути збережена для використання в інший час, нам потрібно перетворити цю енергію. Одним із можливих способів зберігання сонячної енергії є нагрівання води, які можуть бути використані надалі. Вода нагрівається шляхом пропускання через порожнисті панелі. Чорне покриття пластини використовуються, тому що темні кольори більш ефективно поглинають тепло. Однак цей метод тільки забезпечує достатню кількість енергії для таких заходів, як миття та купання.

Сонячні панелі генерують "низкосортне" тепло, тобто, вони виробляють низькі температури для тієї кількості тепла, яка необхідна в день. Для того, щоб виробити тепло "високого сорту", достатньо сконцентрувати енергію сонця, щоб перетворити воду на пару під високим тиском, яка потім може бути використана для включення електрогенераторів. Концентровані промені сонячного світла збираються в пристрої, названому геліоелектростанцією, яка діє на тих же принципах, що і велика лупа Сонячна електростанція приймає сонячне світло з великої площі і за допомогою лінз і дзеркал можна сфокусувати світло в дуже невеликій площі.

Ця система може забезпечити значні обсяги електроенергії та створюють надзвичайно високі температури, понад 6000 градусів за Фаренгейтом. Сонячні генератори енергії дуже екологічно чисті, мало відходів виділяється з генераторів в навколишнє середовище.

Використання вугілля, нафти та бензину є постійним стоком, економічно та екологічно. Чи буде сонячна енергія енергією майбутнього. Чи може тривання світової енергії бути виконане за допомогою "електростанцію" на сонячних модулях. Автомобілі в майбутньому, ймовірно, працюватиме на сонячній енергії, і вдома будуть мати сонячні нагрівачі.

Висновки: Сонце завжди було поки що жила людина: і одного разу люди навчилися добувати вогонь, після чого вони почали палити деревину. Потім на зміну деревини прийшло кам'яне вугілля. Запаси дерева здавалися безмежними, але парові машини вимагали дедалі більше задля забезпечення енерговитрат людини.

Це був лише етап. В результаті вугілля змінилося нафтою. І в наш час основним видом одержання енергії є газ та нафта. Але кожен новий літр нафти чи кубометр газу перебуває все далі і далі. Не дивно, що відбувається подорожчання нафти та газу щороку.

Настав час змінити лідера та знайти нове джерело енергії. І результат такий: на зміну приходить АСЕ, на які виявляється потрібно витратити в тисячі разів менше коштів і праці, щоб отримати енергію. І АСЕ у вигляді ядерної енергії приходить також на зміну вугілля та нафти.

Але часи змінилися. Зараз нам потрібне джерело енергії, яке зможе покрити нові потреби людини в енергії, електриці, тепла. І Сонце один із ідеальних варіантів отримання енергії. Головною його перевагою є його безмежність та екологічність.

Список літератури:

1. Андреев С.В. Солнечные электростанции. М.: Наука 2002
2. Охоткин Г.П., Серебрянников А.В. Основные принципы построения автономных солнечных электростанций. Чеб.: Внир 2003.
3. Охоткин Г.П., Методика расчета мощности солнечных электростанций/ М.: Энергия 2013.

4. Михеев Г.М. Электростанции и электрические сети. Диагностика и контроль электрооборудования. М.: ИД «Додэка ХХ1», 2010.
5. Воронин С.М. Автономная система электроснабжения на основе солнечной электростанции. Б.: Журнал 2007.
6. Рубан С.С. Нетрадиционные источники энергии. М.: Энергия, 2003.
7. Самойлов М.В. Основы энергосбережения. Минск: БГЭУ, 2003.
8. Аипов Р.С. Повышение эффективности работы гелиоэнергетических установок. У.: УУВШ, 2007.

УДК 629

СИНТЕЗ СИСТЕМИ КЕРУВАННЯ РУХОМ АВТОНОМНОГО ПІДВОДНОГО АПАРАТА

***Автор:** Гузій О.В., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На сьогоднішній день дослідження океану є одним з найбільш пріоритетних напрямків робототехніки в багатьох країнах світу. За найоптимістичнішими оцінками людиною вивчено лише 5-7% океану.

Вивчення Світового океану є одним із найперспективніших напрямів наукових досліджень з низки причин, основною з яких є питання видобутку палива, оскільки простір Світового океану містить велику кількість родовищ корисних копалин. Оскільки питання нестачі енергоресурсів на сьогоднішній день є одним із найгостріших, дослідження та експлуатація підводних родовищ позитивно позначиться на житті населення та економіці країн, у яких приділяється достатня увага розвитку підводної робототехніки. Також Світовий океан є найбільшою частиною біосфери Землі, і дослідження морського середовища дозволить людині гармонійно співіснувати з морськими мешканцями, не руйнуючи їх місце існування.

Дослідження простору океану з використанням підводної робототехніки дозволяє складати карти дна світового океану, збирати дані та

проводити моніторинг підводного середовища, вивчати підводну флору і фауну та досліджувати морське дно на наявність затонулих суден. Окремим пунктом слід виділити дослідження та використання вуглеводнів та інших мінералів та ресурсів у важкодоступних місцях, таких як великі глибини океану та підлідний простір.

Вирішенням викладених проблем може стати розробка підводних апаратів, здатних занурюватися на велику глибину, що мають високу маневреність і автономність, здатні виконувати широкий спектр завдань, як цивільних, так і військових.

Сьогодні головним напрямом розвитку підводної робототехніки є розробка автономних безлюдних підводних апаратів (АНПА). Цей клас підводної робототехніки розвивається досить давно, проте, нещодавно він отримав новий поштовх у розвитку. Це пов'язано з низкою економічних причин, таких як відкриття підводних родовищ корисних копалин та деяких інших.

Автономні безлюдні підводні апарати є багатофункціональними пристроями, здатними при відповідному оснащенні виконувати завдання, що є небезпечними для життя людини. Головною особливістю апаратів даного типу можна вважати наявність автономної рушійної установки, що дає апарату широкий оперативний простір, власної енергетичної установки, що забезпечує електроенергією всі агрегати апарату і бортового комп'ютера, що забезпечує керування всіма агрегатами апарату, підвищення рівня автономності та надійності апаратів.

При створенні АНПА перед розробником стоїть низка важливих питань, одним із яких є вибір рушійної установки. Її правильна робота та ефективність багато в чому визначають швидкодію АНПА та чіткість виконання покладених на АНПА функцій.

Вибір рушійної установки включає вибір типу рушія і вибір управління ним. Важливим аспектом розробки рушійної установки є питання управління рушієм. При несправності або відмові рушія оператор, керуючий апаратом, повинен бути негайно сповіщений про проблему.

Вирішенням цієї проблеми є блок управління рушієм. Даний пристрій дозволить не тільки керувати кожним рушієм АНПА окремо, що

позитивно позначається на його ходових характеристиках і маневреності, а й стежити за станом кожного рушія, отримувати своєчасні відомості про його стан і несправності.

Висновки: У роботі було розглянуто питання розробки блоку управління електрорушієм АНПА. Застосування цього пристрою позитивно позначиться на управлінні АНПА, підвищить його надійність та швидкодію.

Метою роботи було вивчення питання управління рушіями автономного безлюдного підводного апарату, розробка блоку управління електродвигуном автономного безлюдного підводного апарату та розробка математичної моделі автономного безлюдного підводного апарату.

В результаті виконання даної роботи вивчено питання управління рушіями АНПА, розроблено зменшену модель АНПА та блок управління рушіями АНПА. Було розроблено математичну модель АНПА серед Simulink, де було проведено тести з управління рухом АНПА. Також було розроблено екранний інтерфейс управління АНПА.

У подальших дослідженнях цю роботу можна доповнити доопрацюванням програми управління АНПА, розробкою методів управління рушіями АНПА на різних траєкторіях та доповненням екранного інтерфейсу ширшими функціональними можливостями.

На сьогоднішній день дослідження океану є одним з найбільш пріоритетних напрямків робототехніки в багатьох країнах світу. АНПА є найкращим інструментом у вивченні морського середовища та подальше вивчення питань, розглянутих у даній роботі, може надати поштовх нашим морським дослідженням.

Список літератури:

1. Лукомський, Ю.А. Системи управління морськими рухомими об'єктами: підручник/Ю.А. Лукомський, В.С. Чавунів, – Л.: Суднобудування, 1988. – 272 с.
2. Бочаров, Л.Ю. Ненаселені підводні апарати: стан та загальні тенденції розвитку / Електроніка: наука, технологія, бізнес. – 2009. – №7. – С. 62 – 69.
3. Бахарев, С.А. Використання автономних безлюдних підводних апаратів у процесі вивчення світового океану / С. А. Бахарев, В. В. Карасев, А.В. Карасьов/ Наукові праці Дальрибвтуза. – Владивосток, 2015. – с. 47 – 49.

4. П'ятницький ЄС. Синтез ієрархічних систем управління механічними та електромеханічними об'єктами на принципі декомпозиції. Ч. 1 Автоматика та телемеханіка. 1989. № 1. С. 87 – 98.

5. T. Fossen, Guidance and Control of Ocean Vehicles. Chichester, UK: Wiley, 1994

УДК 629

ДОСЛІДЖЕННЯ СИСТЕМИ КЕРУВАННЯ РУШІЙНО-КЕРМОВИМ КОМПЛЕКСОМ ПІДВОДНОГО АПАРАТА

Автор: Захараш А.М., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Зараз дослідження світового океану стає все більш актуальним та важливим завданням у сучасному світі. Завдяки сучасним технологіям суттєво зросли можливості для освоєння.

Підводні апарати можна розділити на два великі класи, кожен із яких має свої особливості. Перший клас складається з населених підводних апаратів, що пілтуються безпосередньо людиною, а другий – з безлюдних підводних апаратів (НПА), які, у свою чергу, поділяються на телескопічні, керовані за допомогою кабелю з судна (ТПА) та автономні (АНПА).

Завдання щодо дослідження розташування природних копалин, вивчення флори та фауни світового океану, екологічні дослідження, пошуково-рятувальні операції, технічне обслуговування споруд, що знаходяться під водою (нафтові платформи, мости та ін.). Активно використовують підводні роботи з метою військової розвідки. Для цих та багатьох інших цілей розробляються досконаліші апарати для підводної роботи. На сьогоднішній день застосовуються різні типи підводних апаратів, які відрізняються за сферою застосування та за технологічними рішеннями.

Пріоритетним є застосування безлюдних підводних апаратів (АНПА). Автономні безлюдні апарати виключають присутність лю-

дини у небезпечних середовищах. Відсутність у підводних апаратах даного типу систем життєзабезпечення людини суттєво зменшують їх у габаритах, що збільшує їхню прохідність у важкодоступних місцях, а також мають інші переваги.

У той самий час, виключаючи присутність людини, виникає у застосуванні якісної системи управління (СУ), враховую всю складність управління у підводному середовищі. Проблеми синтезу СУ полягає у нелінійності як самого АНПА, так і середовища, що впливає на всі ступеня рухливості АНПА, у складності чи неможливості визначення його параметрів.

Питання створення якісного математичного опису є найважливішим у проектуванні безлюдних підводних апаратів. У цій галузі працюють спеціалізовані відділи суднобудування, як зарубіжні та вітчизняні.

У ході огляду робіт, було виявлено два типи підводних роботів: перші, що обслуговують підводні споруди (мости, бурові установки, газопроводи, проводять огляд суден), дані тип НПА повинні мати високу точність при переміщенні різними траєкторіями, якість переміщення багато в чому залежить від СУ.

При проектуванні СУ НПА необхідно проводити велику кількість експериментів саме на практиці, тобто. у реальних умовах або наближених до них, що є фінансово витратним. Виходячи з цього виникає необхідність створення спеціалізованих інструментів, що дозволяють проводити експерименти в напівнатуральному режимі, коли об'єктом управління (ОУ) для СУ НПА є його математична модель. Даний підхід дозволяє знизити витрати та збільшити швидкість отримання результатів.

Багато робіт присвячено математичному опису НПА як вітчизняних [1, 3, 4], так і зарубіжних [5, 6, 7]. Варто зауважити, що математичні описи можуть відрізнятися через різне взаємоположення рухомої та нерухомої системи координат, прийняття будь-яких припущень (спрощень) у ході математичного опису. Також впливає вибір СК. Вітчизняні автори дотримуються кутів Ейлера, які називають «літаками» [1, 3, 4, 8] у зарубіжній літературі вибір системи координат може відрізнятися. Наприклад, у роботах [7] та [8] у рівняннях опису динаміки НПА у знаки при деяких членах рівняння відрізняються, деякі члени відсутні.

Висновки: Дослідження Світового океану є важливим критерієм економічної розвиненості держави. Запаси з корисними копалинами у надрах світового океану ще вивчені. Також залишається загадкою флора і фауна, затонули судна, які є цінними історичними об'єктами. І, зрозуміло, під водою вже знаходяться об'єкти, які вимагають технічної підтримки (газо- та нафтопроводи, бурові установки, дослідницькі станції та ін.). Для цих та багатьох інших цілей необхідно використовувати підводні апарати різної спрямованості. У деяких необхідно використовувати точні переміщення для виконання робіт з технічної експлуатації споруд, подібні характеристики мають

телескопічні безлюдні апарати, для дослідження застосовуються автономні безлюдні апарати.

Дані типи підводних апаратів відрізняє відсутність людини управителя, тому необхідно забезпечити якісну СУ. У результаті синтезу СУ виникають певні проблеми, які потрібно враховувати.

У ході цієї роботи було зроблено математичний опис АНПА. Виділено відмінності в математичному описі з різних джерел: зарубіжних та вітчизняних. Було розглянуто різні типи управління. Було зроблено кілька дослідів з імітаційною моделлю, де реалізовано адаптаційне управління з урахуванням динаміки системи. Також був розроблений графічний інтерфейс користувача для безлюдного підводного апарату, який може застосовуватися для інших типів робототехнічних систем. Проведено підбір контролера, рушіїв, типи драйвера та акумуляторну батарею.

Список літератури:

1. Юхимец Д.А. Методы формирования программных сигналов и высокоточного управления скоростным движением подводных аппаратов. Дисертация на соискание ученой степени доктора технических наук.-Владивосток: ИАПУ., 2014.- 315 с.
2. Агеев М.Д. Автоматические подводные аппараты/ М.Д. Агеев, Б.А Касаткин., Л.В. Киселев и др. – Л.: Судостроение, 1981., – 224 с.: ил.
3. Лукомский Ю.А., Чугунов В.С., Системы управления морскими подвижными объектами: Учебник – Л.: Судостроение, 1988. – 272 с., ил.

4. Блшцов С.В. Онлайн-идентифікація параметрів підводного апарата як нестационарного об'єкта в системі керування на базі шверсної моделі [Електронний ресурс] // Електронне видання «Вюник Національного університету кораблебудування». – Миколаїв : НУК, 2012. – № 3. – Режим доступу: <http://ev.nuos.edu.ua>
5. Antonelly G. Underwater Robots. – Springer-Verlag, 2012.- 265 p.
6. Fossen T.I. Guidance and control of oceanic vehicles. – John Wiley and Sons, 2004. – 494 p.
7. Макарычев В.П. Разработка и исследование системы управления космическим манипуляторами. Диссертация на соискание ученой степени кандидата технических наук.- СПб: ЦНИИ РТК, 2011. – 203 с.
8. Рождественский В.В. Динамика подводной лодки, Л.: Судостроение, 2-х томах, 1987. – 387с.

УДК 629

АНАЛІЗ СТРУКТУРИ СИСТЕМИ КЕРУВАННЯ ПОВОРОТОМ ПАЛУБНОГО МЕХАНІЗМУ

***Автор:** Казаєв В.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Перша у світі система відеоспостереження була розроблена 1942 року в Німеччині компанією Siemens для того, щоб спостерігати за випробуваннями ракет на полігоні Пенемюнде.

Перші поворотні камери стали з'являтися у 90-х роках і мали тоді примітивний привід із зубчастою передачею. Він був відносно недорогим. Відповідно, точність позиціонування у приводу із зубчастою передачею не висока. Сьогодні такий механізм практично не використовується. Його можна зустріти лише у дешевих китайських моделях.

Поворотна камера є роботизованою керованою камерою відеоспостереження з вбудованим електронно-механічним приводом, який керує поворотом або нахилом камери. Управління камерою відбува-

ється віддалено за допомогою спеціального пульта керування або спеціалізованого програмного забезпечення (Web-сервер, CMS) у випадку, якщо камера підключена до мережного протоколу.

Актуальність:

У наш час поворотні камери набули широкого застосування в системах безпеки і займають особливу позицію серед камер відеоспостереження. Використання камер такого типу дозволяє вирішити завдання відеоконтролю за широкою відкритою ділянкою шляхом управління положенням зон огляду. Поворотні камери можуть експлуатуватись як усередині приміщення, так і на вулиці.

Предметом розробки ВКР є поворотний пристрій камери відеоспостереження суднового базування та система керування цим пристроєм.

Метою даної ВКР є розробка системи управління поворотного пристрою камери відеоспостереження, яка здійснює поворот камери при спрацьовуванні датчика об'єму.

Для досягнення поставленої мети мають бути виконані такі основні завдання:

1. Здійснити огляд існуючих систем управління.
2. Здійснити огляд електричних двигунів, які можуть бути використані в поворотному пристрої. За результатами аналізу та розрахунку, вибрати оптимальний для поворотного механізму двигун.
3. Вибрати та запрограмувати відповідний для двигуна контролер та драйвер пристрою керування двигуном.
4. Розробити систему керування поворотною камерою відеоспостереження під час спрацьовування датчика об'єму.

У нашому випадку реалізовуватиметься спостереження за капітанською рубкою та приміщенням спецзв'язку на борту корабля. Розміщення камер такого типу забезпечить широкі кути огляду і, безсумнівно, збільшить безпеку об'єкта, що охороняється.

Висновки: У ході проведеної роботи було отримано такі результати:

1. Було здійснено огляд існуючих систем управління, а саме: система дистанційного управління та система управління на базі чотириобмотувального крокового двигуна.

2. Огляд електричних двигунів, які можуть бути використані в поворотному пристрої. Досліджувалися такі електричні двигуни: сельсин, мотор-редуктор та кроковий двигун. За результатами аналізу та розрахунку, було обрано кроковий двигун. Такий двигун найбільш оптимальний для приводу поворотного механізму.

3. Для керування кроковим двигуном було обрано контролер та драйвер пристрою керування двигуном. Також вибрано корпус камери з вбудованою поворотною платформою та сама камера відеоспостереження.

Щоб наочно показати, як працює система управління, було побудовано математичну модель керованого крокового двигуна.

Список літератури:

1. Дам'янівський В. CCTV біблія охоронного телебачення. Цифрові та мережеві технології". Ай-Ес-Ес-Прес, 2006. – 480с.

2. Дубровський, І.Л., Мікропроцесорне управління електроприводами промислових робіт: навчальний посібник / І. Л. Дубровський, А. П. Дамбраускас, А. А. Рибін. – Красноярськ, КДТУ, 1993 – 88с.

3. Такаші, К. Крокові двигуни та їх мікропроцесорні системи управління: Пер. з англ., М: Енергоатоміздат, 1987 – 199с.

4. Лебедев, Н.І., Вентильні електричні машини/Н. І. Лебедев, В. М. Гандшу, Я. І. Явдошак. – СПб.: Наука, 1996 – 352 с.

УДК 629

ДОСЛІДЖЕННЯ СИСТЕМИ КЕРУВАННЯ МОРСЬКОГО РУХОМОГО ОБ'ЄКТУ

***Автор:** Кузьмін М.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Підводний апарат – невелике судно або технічний пристрій, що використовується для виконання різноманітних завдань у товщі води і на морському дні. На відміну від підводного човна, як правило, має обмежені можливості по автономності і тому працює у взаємодії з за-

безпечує судном-носієм. Підводні апарати можуть працювати на глибині недоступною для підводних човнів та водолазів

За останні 30 років у різних країнах, які займають провідне становище в області морських технологій, було створено понад 9 тис. самохідних ненаселених підводних апаратів (НПА) для вирішення широкого кола завдань. Ці апарати вже продемонстрували свою ефективність при виконанні аварійно-рятувальних, оглядово-пошукових, науково-дослідницьких та інших видів робіт. НПА – одна з найбільш важливих і швидкопрогресуючих областей мікроробототехніки. Але динаміка розвитку цього напрямку в багато чому обумовлена сучасними електронними технологіями.

Сучасні самохідні НПА є окремий клас робототехнічних об'єктів з притаманними їм завданнями, особливостями технології, складом систем і функціональними властивостями. При всій різноманітності НПА (за цільовим призначенням, масогабаритними характеристикам, конструктивності, типу енергосилової установки і т.д. і т.п.) їх можна класифікувати наступним чином.

Всі самохідні НПА поділяють на два великих підкласи: неавтономні (прив'язні) НПА та автономні незаселені підводні апарати (АНПА). До неавтономні НПА відносять буксируємі і самохідні прив'язні підводні апарати.

Треба зазначити, що поділ НПА за ознакою автономності сформувалося в процесі еволюції цього виду техніки, і під автономністю розуміється, насамперед, енергетична незалежність апарату від судноносія. Таким чином, телекерованими можуть бути як автономні, так і неавтономні апарати.

Самохідні НПА вже сформувалися в досить представницький клас робототехнічних засобів, нараховує понад 500 різних проектів (моделей).

До 2011 року за кордоном було створено більше 7500 неавтономних НПА. У розробці і виробництві самохідних НПА лідирують США, Великобританія, Канада, Франція, Німеччина і Японія. Але і вітчизняні науково-технічні інститути (насамперед в Україні є Національний Університет Кораблебудування імені адмірала Макарова з його прові-

дними фахівцями в цій галузі) також мають вагомий досвід у створенні підводних технічних засобів.

Сучасний підводний апарат обладнаний різними корабельними системами. Ці системи забезпечують занурення та спливання судна, змінюють його плавучість, крен та диферент, ведуть боротьбу за живучість при пожежах та надходження заборотної води. Життєдіяльність екіпажу забезпечують системи вентиляції, кондиціювання, регенерації, а також очищення та контролю газового складу повітря. Для забезпечення екіпажу прісною водою використовують електролізні установки, а зберігання продуктів – холодильні установки. Велика кількість тепла, що виділяється під час роботи апаратури, визначає наявність систем водяного охолодження. На судні повсякденно використовують систему підсушування трюмів та систему очищення стічних вод.

Висновки: У цій роботі буде розглянуто інтегровану систему управління підводним апаратом, досліджено її структуру та проведено розрахунок її параметрів надійності. Також буде вивчено питання синтезу та мінімізації логічних пристроїв.

У цьому роботі було проведено аналіз інтегрованої системи управління підводним апаратом. Інтеграційні процеси є одним із найбільш очевидних тенденцій у розвитку сучасних автоматизованих систем управління кораблем. Невипадково у назві подібних систем різних країн загальною є наявність слова Integrate – об'єднана, сукупна, загальна. Причому найактуальніша проблема інтеграції для автоматизованих систем керування підводним човном.

Вивчено приладовий склад цієї системи, а також приладів вводу/виводу, приладів живлення, панелей керування, що входять до цієї системи. Вивчено компонування центрального пульта управління інтегрованою системою управління технічними засобами корабля

Було вивчено структурну схему інтегрованої системи управління технічними засобами корабля і наведено її опис. Для зв'язку приладів системи використовувалася міжвідсічна мережа Mil STD, яка для забезпечення заданих вимог щодо надійності є резервованою. Також було вивчено відеокадри для загальнокорабельної системи (система гідравліки), електроенергетичної системи (ЕЕС) та головної енергетичної установки (дизель-генератори). Також представлений повний опис вищезазначених відеокадрів.

Список літератури:

1. Автоматизированные информационно-управляющие системы. – В.В. Киселев, К.Ю. Шилов – СПб.: Издательство политехнического университета, 2011
2. Интегрированные системы управления технических средств транспорта / В.М. Амбросовский, О.В. Белый, Д.А. Скороходов, С.Н. Турусов. – СПб.: “Элмор”, 2001 г.
3. Автоматизация судовых систем. / П.П. Федорко – СПб.: «Судостроение», 1967
4. Основы теории и расчёта надёжности судовых электроэнергетических систем / И. А. Рябинин. – Ленинград: "Судостроение", 1967 г.
5. Проектирование логических устройств судовой автоматики. / З.Я. Вирьянский – СПб.: «Судостроение», 1979

УДК 629

РОЗРОБКА СТЕНДУ ДОСЛІДЖЕННЯ СИСТЕМИ КЕРУВАННЯ РУХОМ

***Автор:** Листопад М.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Управління судном здійснює людина завдяки здатності оцінити ситуацію за багатьма непрямими ознаками, накопиченим досвідом управління, здатністю змінювати цілі управління і приймати нетривіальні рішення на основі наявних знань. Однак людина не завжди здатна швидко і оперативно приймати рішення, внаслідок чого робляться помилки, що іноді призводять до трагічних наслідків, і тоді говорять про людський чинник як про причину катастрофи.

З появою сучасних обчислювальних засобів багато функцій, що раніше здійснювалися людиною, стало можливо передавати інтелектуальним системам управління. Інформацію стали структурувати та подавати у наочному та зручному вигляді, що полегшує прийняття раціональних

рішень. Скорочується чисельність персоналу, оптимізуються процеси керування судном, що дозволяє заощадити значні кошти [1].

У цій роботі докладніше буде розглянуто автоматизацію управління рухом судна – як систему керування рухом судна (СКРС). Під СКРС розумітимемо систему управління тими технічними засобами, які забезпечують постійність або зміну за законом кінематичних параметрів руху, що характеризують положення судна в заданій координатній системі, його швидкість руху, кутову орієнтацію і швидкість її зміни.

Автоматизацією керування судами почали займатись ще на початку 20 ст. Проте перші системи автоматизації вимагали від судноводителя як підготовленості, а й великого мистецтва, т.к. багато судна не стійкі на курсі, математичні моделі руху суден сильно відрізняються і змінюються в процесі плавання, а реакція судна на вплив виконавчих органів уповільнена, керуючі на порядок слабші обурень від сильного морського хвилювання. У результаті це ускладнювало управління судном, особливо у специфічних режимах, як-от швартування, розбіжність із перешкодами та інших [2]. Сучасні СКРС дозволяють повністю автоматизувати багато завдань судноводіння, що вимагають безпосередньої уваги екіпажу.

В даний час набули широкого поширення такі СКРС, як [3]:

- авторульовий (АР), призначений для автоматизації та оптимізації процесу управління кораблем під час руху за заданим курсом та заданим маршрутом;

- система динамічного позиціонування (СДП), що дозволяє здійснювати автоматичне утримання судна у заданій точці океану без постановки якір;

- штурвально-рульова система (ШРС), що забезпечує дистанційно-автоматичне керування кермовими машинами судна за допомогою штурвала або рукояток;

- джойстикова система (система координованого управління), в якій виконання маневрів зводиться до управління плоскопаралельним переміщенням судна за допомогою джойстика та управління його орієнтацією по курсу за допомогою штурвала. Вибір відповідних режимів роботи силових засобів за командами джойстика виконує комп'ютер. Ці системи встановлюються на судах, діяльність яких пов'язана з

частими маневрами при малих швидкостях руху або необхідність забезпечення підвищеної безпеки;

– система стабілізації качки, яка призначена для керування бортовими кермами з метою зменшення бортової качки судна. Використання системи стабілізації качки покращує керованість судна під час хвилювання, підвищує ступінь комфорту для екіпажу та пасажирів судна, а також створює сприятливі умови для використання обладнання судна.

Незважаючи на різноманіття існуючих рішень, безліч вітчизняних та зарубіжних компаній продовжують дослідження та розробки в галузі систем керування рухом суден. Їх мета – створення універсальних, високопродуктивних, багатфункціональних та відмовостійких систем, із застосуванням передових технологій та сучасної елементної бази.

Проектування – найважливіша та найскладніша частина розробки нової системи. Насправді проектування систем рідко носить односпрямований характер. Як правило, воно розвивається ітераційним шляхом, коли на будь-якій стадії проекту доводиться звертатись до попередніх стадій для уточнення попередніх рішень. Особливо це характерно для стадії робочого проекту, на якій система, що розробляється, проходить налагодження, налаштування та тестування алгоритмів роботи.

На цьому етапі в інженерів виникає потреба перевірки правильності прийнятого рішення, не чекаючи на встановлення зразка на судно. Як вирішення даної проблеми – налагодження та налаштування проектованої системи не в польових умовах, а також для перевірки працездатності системи при різних вихідних даних, доцільно розробити стенд, який:

1. Імітує роботу органів управління судна;
2. Дозволяє задати параметри зовнішніх впливів;
3. Дозволяє задати початкові дані руху (курс, швидкість та ін.);
4. Візуалізує поточні параметри судна.

Створення стенду дозволить провести всі необхідні роботи на завершальних стадіях СКРС. Більше того, це обладнання може використовуватися підприємством-виробником для проходження різних ви-

пробувань своєї системи, для подальшої її сертифікації та пред'явлення замовнику.

Таким чином, метою роботи є розробка налагоджувального стенду для проведення налагодження та налаштування систем управління рухом судна, що розробляються, зокрема АР і ШРС.

Висновки: У роботі було розглянуто налагоджувальний стенд для систем управління рухом та основні етапи його проектування. Розробка стенду складалася з етапів дослідження існуючих СУДС, особливу увагу було приділено системам АР та ШРС як найбільш поширеним; складання структури стенду, розробка вимог до апаратної та програмної частини стенду. На даному етапі було розглянуто кілька можливих структур і обрано з використанням мікроконтролера як оптимальну. Далі було розроблено ескізи відеокадрів для програмного забезпечення стенду. Були складені відеокадри як для випадку з наявністю математичної моделі судна та кермової машини, так і для відсутності математичної моделі судна та кермової машини. Дані відеокадри були реалізовані за допомогою Matlab GUI, що надає широкі можливості в галузі математичного моделювання та реалізації людино-машинних інтерфейсів. В останньому розділі роботи наведено економічне обґрунтування проведеним дослідженням, розроблено бізнес-план проекту та доведено його актуальність.

Список літератури:

1. Лукомский, Ю.А. Логопедия. Управление морскими подвижными объектами [Текст] / Ю.А. Лукомский, В.М. Корчанов. – М.: Элмор, 1996. – 317 с.
2. Интегрированные системы управления технических средств транспорта [Текст]:/ В.М. Амбросовский, О.В. Белый, Д.А. Скороходов, С.Н. Турусов. – М.: Элмор, 2001. – 287 с.
3. Дорри, М.Х. Автоматизация управления морскими подвижными объектами [Текст] / М.Х. Дорри // Проблемы управления. – 2009. – № 3.1. – С. 94 – 102.
4. Садырин, И. А. Методические указания по технико-экономическому обоснованию выпускных квалификационных работ магистров технических направлений «Составление бизнес плана по коммерциализации результатов НИР магистранта» [Текст] / И.А. Садырин. – М.: СПбГЭТУ «ЛЭТИ», 2013. – 41 с.

5. Створення універсальних транспортних суден і засобів океанотехніки: Монографія [Текст] / С.С. Рижков, В.С. Блінцов, Г.В. Єгоров, Ю.Д. Жуков, В.Ф. Квасницький, К.В. Кошкін, І.В. Кривцун, В.О. Некрасов, В.В. Севрюков, Ю.В. Солоніченко; за ред. С.С. Рижкова. – Миколаїв: Видавництво НУК, 2011. – 340 с.

6. The Navy Unmanned Surface Vehicle (USV) [Text] Master Plan. U.S. Department of the Navy .– 2007. – 122 p.

УДК 629

ДОСЛІДЖЕННЯ МЕТОДІВ ОРГАНІЗАЦІЇ КЕРУВАННЯ РУХОМ РУХОМИХ ОБ'ЄКТІВ

Автор: Московченко О.В., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Науковий керівник: Бабкін Г.В., к.т.н, доцент НУК, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

Вода займає 70,8% площі всієї землі, а саме понад 361 мільйон квадратних кілометрів. Сам факт цього залучає вчених до вивчення, дослідження та знаходження практичного застосування особливостей гідросфери для життя людини.

В даний час у світі проводиться великий обсяг робіт з дослідження морського і океанського дна, з виявлення затонулих об'єктів і підйому їх, з контролю прокладених по дну трубопроводів. Кількість цих трубопроводів незмінно зростає, розробка нафтових родовищ у шельфової зоні проводиться все активніше, тому контроль за загальним станом мережі є нагальною проблемою, вирішення якої пов'язане з проектуванням новітніх механічних систем, здатних переміщати під водою прилади для контролю стану труб, що забезпечують надійну роботу з достатньою точністю позиціонування.

Найактуальніші сфери застосування підводного робота з маніпулятором:

1) Оглядово-пошукові роботи, включаючи пошук та обстеження затонулих об'єктів, інспекцію підводних споруд та комунікацій (трубопроводів, водопроводів, кабелів);

2) Підлідні роботи, у тому числі прокладання кабелю на арктичному дні, обслуговування систем спостереження та освітлення підлідної обстановки;

3) Океанографічні дослідження, моніторинг водного середовища;

4) Роботи військового призначення, що включають, зокрема, протичовнову розвідку, патрулювання, забезпечення безпеки об'єктів військової техніки, пошук та знешкодження мін.

Тенденціями розвитку підводних робіт йде використання універсальних робототехнічних комплексів, створених із застосуванням простих, малих і дешевих агрегатів. У цьому маніпулятор сприймається як найважливіша складова частина підводного робота.

Підводні маніпулятори є частиною великого сімейства промислових робіт. Вони встановлюються на населених і безлюдних підводних апаратах, самопідйомних платформах, гирловому обладнанні морських свердловин.

У сукупності маніпулятора та підводного апарату народжується поняття підводного Апарату-робота. До 80% заселених підводних апаратів і 50% безлюдних озброєні, як мінімум, одним маніпулятором, а значна частина їх числа має по два і більше маніпуляторів.

У зв'язку з проблемою автоматизації різних виробничих процесів через труднодоступність та небезпеки для людини вирішується завдання автоматичної орієнтації (маніпулювання) робочого органу, виробу або інструменту. Повною мірою це стосується цілого ряду робіт під водою, чим і пояснюється широке впровадження маніпуляторів у підводну техніку та підводні технології.

Групу робіт та її систему управління часто слід виділяти як подальшу еволюцію мобільних та інтелектуальних властивостей окремих робіт. Нині використання груп робіт до виконання простих спільних маніпуляційних операцій досить складно реалізувати.

Групове управління створює нові можливості, а також деякі проблеми, без вирішення яких група робіт не може функціонувати нормально.

Для групи робіт додатково з'являються специфічні завдання: побудова загальної карти, розподіл цілей на підзавдання окремих робіт, планування дій групи, складання мережевих графіків і розкладів, спільне побудова траєкторій, організація мережевого інформаційного взаємодії.

Основними цілями цієї роботи є:

- розгляд методів організації руху у групі роботів
- розробка структурної схеми організації руху групи роботів.

Актуальність даної роботи полягає в наступному:

- координація руху групи роботів
- ефективність мультиагентного підходу та надійність у поєднанні з відносною простотою.

Висновки: У роботі досліджувалась методи організації руху на групі роботів. Використання груп роботів дозволяє підвищити продуктивність, можливість виконання завдання, знизити час необхідний роботи .

В результаті виконання роботи було здійснено аналіз існуючих рішень, розроблено структурну схему руху робота в середовищі з перешкодами, математичну модель руху у групі роботів, розглянуто питання безпеки.

Результати досліджень групової взаємодії торкаються багатьох областей. В даний час активно впроваджуються в наше життя та підлягають подальшому вивченню.

Список літератури:

1. Бабкін, Г.В. Математичні моделі та методики будівництва безекіпажних підводних апаратів: Методичні вказівки / Г. В. Бабкін, Ж. Ю. Бурунина, А. М. Войтасик, О. П. Клочков, В. І. Корицький, А. С. Сіривчук // Під загальною редакцією д.т.н. Блінцова В. С. – Миколаїв: НУК, 2018. – 52 с.

2. Blintsov V.S., Babkin G.V. Theoretical basis of design and production of marine robotics / Prospects and priorities of research in science and technology: Collective monograph. Vol. 1. Riga, Latvia : "Baltija Publishing", 2020. 320 p. P.25-43.

3. Zlot R., Stentz A., Dias M.B., Thayer S. Multi-Robot Exploration Controlled By A Market Economy, IEEE International Conference on Robotics and Automation (ICRA), May 2002.

4. Зенкевич С.Л. Планирование задания и управление группой роботов / С.Л. Зенкевич, А.В. Назаров, И.А. Сандлер // Таганрог: Изд-во ТРТУ, 2002.

УДК 629

РОЗРОБКА СТРУКТУРИ СИСТЕМИ КЕРУВАННЯ РУХОМ ПІДВОДНОГО АПАРАТА ПАТРУЛЬНОГО ТИПУ

*Автор: Сірівчук А.С., к.т.н., Національний університет
кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Патрулювання морських акваторій є важливою складовою обороноздатності морської країни. Одним з ефективних засобів прихованого патрулювання морської акваторії є використання спеціалізованих підводних апаратів. Такі спеціалізовані підводні апарати мають особливості конструкції, що надають йому швидкість руху 2-3 м/с, довгу тривалість роботи.

Дані підводні апарати мають потужну установку маршового руху, що забезпечує високу швидкість пересування, та відносно слабку систему вертикального руху (SeaOtter MKII, Talisman L) або зовсім без неї (ALISTAR, SeaWolf, ВСПНЗ).

В підводних апаратах без системи вертикального руху використовується структура рушійно-кормового комплексу (РКК), що складається з 4 маршових рушіїв, які розміщені відповідно до схеми (рис. 1).

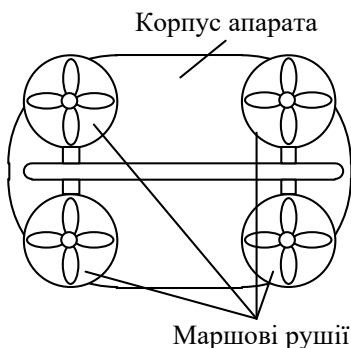


Рисунок 1 – Структура РКК

Використання такої структури РКК може забезпечувати три типи руху: маршовий хід, поворот для зміни курсу і зміну диференту. Однак оскільки всі ці види рухів забезпечуються одними й тими ж руші-

ями виникає необхідність використання спеціалізованого алгоритму розподілення тяги рушіїв під час комбінованого руху (два або три типи руху одночасно).

Метою роботи є розробка структури системи керування рухом підводного апарата з 4 маршовими рушіями та алгоритму розподілення тяги для кожного виду руху.

Для забезпечення прямолінійного руху всі рушії повинні працювати з однаковою силою, яка забезпечується сигналом p_m . Для руху вперед сигнал p_m повинен мати позитивне значення.

Для зміни диференту необхідно забезпечити різницю сили між верхнім і нижнім рушіями, рівень цієї різниці задається сигналом p_p . Позитивний рівень сигналу p_p забезпечується диферент на ніс апарата.

Для зміни курсу передбачена різниця сили між лівими і правими рушіями і задається сигналом p_h . Позитивний рівень сигналу забезпечує обертання проти годинникової стрілки.

Для реалізації керування апаратом пропонується наступна структура системи керування (рис. 2). Існує три режими керування рухом: ручний, автоматизований і автоматичний.

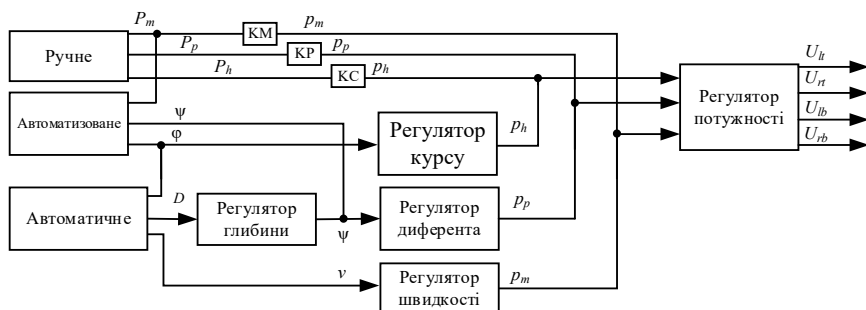


Рисунок 2 – Структура системи управління рухом

Для забезпечення ручного і автоматизованого керування на пульті керування (рис. 3) встановлені два стики керування (грибки): одновісний і двовісний.

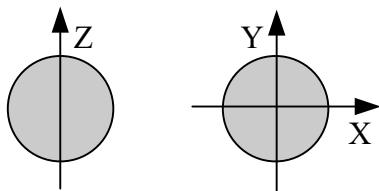


Рисунок 3 – Позначення осей грибків керування

При ручному керування для зміни диференту використовується кут осі Z вказує на значення різниці сил верхніх і нижніх приводів P в діапазоні $\pm 100\%$. Для приведення до відносних одиниць pp (які використовуються при розрахунках системи управління) використовується коефіцієнт K_P , який приводить сигнал в значення у відносних одиницях може бути менше 1, що дозволить більш плавно управляти в ручному режимі.

Вісь Y в пульті керування відповідає за маршовий рух сигналу рівня P_m , який змінюється в проміжках в $\pm 100\%$. За аналогією з сигналом керування диференту отриманий сигнал доводиться до відносних одиниць за допомогою коефіцієнта K_M . Максимальний керуючий сигнал також може бути обмежений заданим коефіцієнтом.

Вісь X в пульті керування відповідає за зміну ходу шляхом установки сигналу P_h , який змінюється в частинах $\pm 100\%$. За аналогією з іншими сигналами керування отриманий сигнал доводиться до відносних одиниць за допомогою коефіцієнта K_C . Максимальний керуючий сигнал також може бути обмежений заданим коефіцієнтом.

Результатом роботи системи керування (у всіх режимах управління) є сила сигналу для кожного окремого рушія. Оскільки рівень сигналу у відносних одиницях не може перевищувати 1, необхідно передбачити обмеження сигналу для кожного двигуна при збереженні пріоритету керуючих сигналів. Найвищим пріоритетом є зміна курсу, другим пріоритетом – зміна диференту і найнижча забезпечення швидкості маршового руху. Цей пріоритет обумовлений розрахунком тривалість режимів роботи (менша тривалість – більш високий пріоритет).

Виходячи з перерахованого вище, керуючі сигнали розраховуються за такими залежностями:

$$U_{lt} = \begin{cases} p_m - p_h + p_p & \text{при } |p_m| + |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h| - |p_p|) - p_h + p_p & \text{при } |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h|(1 - |p_p|)) - |p_p| - p_h(1 - |p_p|) + p_p & \text{при } |p_h| + |p_p| \geq 1; \end{cases}$$

$$U_{rt} = \begin{cases} p_m + p_h + p_p & \text{при } |p_m| + |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h| - |p_p|) + p_h + p_p & \text{при } |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h|(1 - |p_p|)) - |p_p| + p_h(1 - |p_p|) + p_p & \text{при } |p_h| + |p_p| \geq 1; \end{cases}$$

$$U_{rb} = \begin{cases} p_m + p_h - p_p & \text{при } |p_m| + |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h| - |p_p|) + p_h - p_p & \text{при } |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h|(1 - |p_p|)) - |p_p| + p_h(1 - |p_p|) - p_p & \text{при } |p_h| + |p_p| \geq 1; \end{cases}$$

$$U_{lb} = \begin{cases} p_m - p_h - p_p & \text{при } |p_m| + |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h| - |p_p|) - p_h - p_p & \text{при } |p_h| + |p_p| \leq 1; \\ p_m(1 - |p_h|(1 - |p_p|)) - |p_p| - p_h(1 - |p_p|) - p_p & \text{при } |p_h| + |p_p| \geq 1; \end{cases}$$

де U_{lt} – рівень сигналу лівого верхнього двигуна від -1 до 1;

U_{rt} – рівень сигналу правого верхнього двигуна від -1 до 1;

U_{lb} – рівень сигналу нижнього лівого двигуна від -1 до 1;

U_{rb} – рівень сигналу нижнього правого двигуна від -1 до 1.

При автоматичному керуванні в якості сигналів керування виступає: курс, диферент та сигнал спільного керування машовими двигунами.

Рівень диференту, що встановлюється ψ , задається кутом відхилення по осі Z і може бути встановлений в діапазоні $\pm 20^\circ$. Для формування безпосередньо сигналу, який повинен забезпечити установку заданої обрізки p_p , використовується ПІД-регулятор (тип регулятора визначається обраним автопілотом).

Установка і зміна курсу забезпечується поворотом грибка по осі Х. Відхилення грибка формує сигнал про швидкість зміни заданого курсу φ за такими залежностями:

$$\varphi' = \varphi + X \cdot \Delta t;$$
$$\varphi = \begin{cases} \varphi' \text{ при } -180 \leq \varphi' \leq 180; \\ \varphi' - 360 \text{ при } \varphi' \geq 180; \\ \varphi' + 360 \text{ при } \varphi' \leq -180; \end{cases}$$

де φ' ; – проміжне значення ставки;

Δt – час опитування сигналу пульта керування.

Для стабілізації курсу апарата передбачений ПД-регулятор (будова регулятора визначається обраним автопілотом), на виході якого виробляється сигнал p_h .

Управління маршовим рухом повністю збігається з ручним режимом.

В автоматичному режимі всі сигнали надходять з більш високого рівня системи автоматичного управління. Хід φ розраховується виходячи з поточних і заданих координат. Глибина занурення D_i швидкість наступних v задаються в залежності від поточного режиму (рух до цілі, регулювання координат і т. Д.). Для забезпечення заданої швидкості використовується ПД-регулятор, на виході якого формується сигнал p_m .

Для зміни глибини пристрій повинен йти маршовим ходом з диферентом, відмінним від 0, тому на виході значення регулятора глибини знаходиться потрібний ψ корпусу підводного апарату. Установка цього значення диференту забезпечується тим же регулятором, що і в гібридному режимі керування.

Висновок. Розроблена структура системи керування рухом забезпечує рух апарата в трьох режимах роботи. Два режима роботи забезпечують керування апаратом коли він знаходиться на поверхні для керування підходом апарата до заданої точки з керуванням від оператора та автоматичний режим.

Додатково представлений математичний опис розподілення сигналів керування на електрорушійні пристрої при одночасному здійсненні декількох рухів апарата.

**СЕКЦІЯ 6. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАНЬ
«ІНФОРМАЦІЙНА БЕЗПЕКА»**

УДК 316.485.26:316

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

***Автор:** Кальваровська Б.М., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

В умовах гібридної війни, інформаційно-комунікаційна сфера стає провідним театром військових дій. Інформаційне суспільство не тільки наступило, але і почало розвиватися та набувати все нових, більш складних форм [1]. Тому сьогодні, необхідність дослідження тенденцій, закономірностей та перспектив розвитку національної інформаційної безпеки в умовах гібридної війни є дуже важливим.

Концепція гібридної війни не є особливо новою, вона являє собою поєднання звичайних і нетрадиційних воєн, виходячи за межі поля бою, охоплюючи економічну, дипломатичну, інформаційну (включаючи психологічну, кібернетичну та дезінформаційну) та політичну війну. В першу чергу, вона базується на здатності вражати віддалені об'єкти та процеси, які є критично важливими для державних і військових функцій. Як асиметричний підхід, гібридна війна намагається досягти широкомасштабних наслідків, використовуючи скромні засоби, такі як стримування військових операцій супротивника або запобігання політичній підтримці.

У сучасних умовах інформаційна безпека є важливою складовою національної безпеки. Її актуальність особливо помітна під час «гібридних війн».

Одним із основних засобів ведення «гібридної війни» є так звана інформаційна зброя, яка за своєю ефективністю та наслідками становить суттєву загрозу для будь-якої держави, яка бере участь у гібридному протистоянні, зокрема для України.

Такою зброєю можуть бути кібератаки, спрямовані проти країни у рамках повномасштабного військового вторгнення, чи використовуватися на набагато нижчих сходах ескалації як спосіб тиску, будь то державні чи приватні організації, і змусити їх до бажаних дій противника. Навіть інформаційні операції та пропаганда можуть спрямовуватися, щоб вплинути на наші дії.

Яскравим прикладом використання інформаційного продукту як зброї є діяльність Російської Федерації, що веде війну проти нашої країни. Чи не головним методом цієї війни є інформаційна агресія, розв'язана Російською Федерацією з метою створення викривленої реальності та системи цінностей на користь агресора, послаблення та руйнування національної ідентичності і громадянської свідомості українців.

Слід зазначити, що успіх гібридної війни досягається завдяки не лише докладно розробленому плану дій, а й слушно обраному моменту для його реалізації, зокрема:

- ослаблення центральної влади та часткове «безвладдя» на тлі зміни влади;
- зростання суперечностей (актуалізація вже наявних) між центром і регіонами;
- незадовільний психологічний і матеріально-технічний стан структур безпеки;
- антагонізм між різними силовими структурами;
- активна інформаційно-пропагандистська робота протягом довгого періоду часу[1].

Важливість забезпечення інформаційної безпеки в умовах гібридної війни є дуже актуальною в питанні впливу маніпулятивних комунікаційних технологій на свідомість громадян України, визначення механізмів та засобів запобігання маніпулятивного впливу на населення[6].

Враховуючи складний характер і динаміку гібридної війни, експерти запропонували ряд політичних і стратегічних заходів. Деякі з них стосуються заходів щодо виявлення, стримування, протидії та ретельного реагування на гібридні загрози. Забезпечення інформаційної безпеки завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії значною мірою може сприяти за-

безпеченню досягнення успіху при вирішенні завдань у сфері гібридної війни.

Гібридні загрози часто пристосовані до вразливості цільової держави або міждержавних політичних спільнот. Мета полягає в тому, щоб використовувати їх настільки, наскільки вони поглиблені, для створення та посилення поляризації як на національному, так і на міжнародному рівнях.

Саме з цієї причини розбудову довіри слід вважати ключовим оплотом проти гібридних загроз, особливо тих, які спрямовані на підірив демократичних держав і держав. Крім того, довіра залишається обов'язковою умовою для реалізації будь-якої політики чи стратегічної відповіді на гібридні загрози.

Розбудова, відновлення та зміцнення довіри залишається критично важливим для створення тривалої стійкості перед обличчям гібридних загроз, які гостро загрожують безпеці на рівні держави та суспільства. Розбудова довіри всередині та між громадами має стати стрижнем зусиль із нейтралізації гібридної війни та загроз. Це вимагає постійних зусиль на структурному та політичному рівнях для розвитку міцних зв'язків між державою та людьми, які ґрунтуються на суттєвій прозорості, власності та інклюзивності[5].

Загалом політика інформаційної безпеки як суспільне явище має комплексний характер, включаючи внутрішньо та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вимагає комплексного підходу. В умовах гібридної війни, діяльність органів державної влади повинна спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися єдиною метою – надання належних умов для реалізації забезпечення інформаційної безпеки України [2].

Список літератури:

1. Гібридна війна: сутність, виклики та загрози, (2021) URL: https://academy.ssu.gov.ua/uploads/p_57_28744724.pdf
2. Бєлай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави, (2018). 408 с

3. Гуржій Тарас. Інформаційне право: виклики гібридної війни, (2019) URL: [http://zt.knute.edu.ua/files/2018/04\(99\)/04.pdf](http://zt.knute.edu.ua/files/2018/04(99)/04.pdf)
4. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України, (2019) URL: http://lsej.org.ua/2_2020/54.pdf
5. Arsalan Bilal. Hybrid Warfare – New Threats, Complexity, and «Trust as the Antidote», (2021) URL: <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>
6. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. – Київ : ТОВ «Видавничий дім «АртЕк», (2018) – 446 с. URL: http://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf

УДК 316.485.26:316.77

ІНТЕРНЕТ-МЕРЕЖІ В ГІБРИДНІЙ ВІЙНІ

***Автор:** Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

В добу інформаційно-комунікаційних технологій будь-яка подія в політичній, економічній, соціальній та інших сферах життєдіяльності суспільства розвивається у двох площинах: фізичному та інформаційному. Причому інформаційний вимір часто набуває першочергового значення, формуючи сприйняття події внутрішньої і зовнішньої громадськістю і як наслідок визначаючи її реакції та поведінку у фізичному просторі. Особливо яскраво ця тенденція проявляється в період криз і конфліктів як на національному так і міжнародному рівнях [1].

Завдяки суттєвому підвищенню актуальності соціальних мереж серед українського населення, інформаційні потоки знаходять своє розповсюдження дедалі з більшою силою. Люди отримали можливість не тільки отримувати та поглинати інформацію, а й обмінюватись нею, своїми поглядами, коментарями щодо тих чи інших подій. В деякому розумінні кожному хто користується соціальними мережами в Інтернеті доводиться опановувати професію журналіста, блогера. Це зумовлено тим, що політичні та економічні проблеми стосуються безпосередньо кожного, а тому бажання поділитись подіями та відношенням до них з іншими є досить обґрунтованим.

Більша частина населення веде віртуальне життя на сторінках соціальних мереж, при цьому відбувається спілкування з однієї сторони світу з іншою.

Завдяки цьому явищу вдається не тільки маніпулювати свідомістю певної частини людей, а й вдало це розповсюджувати. Тобто, завдяки технологіям інформація віддається в маси, а вони вже обробляють отриману інформацію (як їм здається самостійно) та обмінюються нею один з одним при цьому залучаючи навіть тих хто доволі слабо цікавиться політичними новинами. Така дія розповсюджується подібно вірусу тільки в інформаційному просторі.

Така практика надає відповідні результати в процесі ведення інформаційної війни. Досягнення результатів так званого референдуму в Автономній Республіці Крим 2014 року відбулось саме завдяки тривалому розповсюдженню та «зараженню» необхідною інформацією суспільства. Такий самий сценарій можна було спостерігати також на Донбасі.

Використання інтернет-мережі в гібридній війні надає можливість здійснювати різноспрямовані широкомасштабні інформаційні кампанії горизонтального типу. Ефективність таких кампаній зумовлена тим, що вони базуються на схемах міжособистісної комунікації та поширенні повідомлень з начебто незаангажованих джерел. Такий підхід сприяє зниженню критичності у сприйнятті інформації, підвищенні емоційної залученості та довіри до повідомлень. В даному випадку, Росія максимально використовує можливості та переваги мережі для управління громадською думкою і встановленні контролю над внутрішнім і зовнішнім інформаційним простором.

В Інтернет-просторі російські мас-медіа та проросійські організації, активісти, експерти, відомі діячі мистецтва та культури діють за наступними видами :

- публікація численних коментарів в онлайн-медіа під статтями про події в Україні;
- поширення пропагандистських повідомлень (відео та фотоматеріалів у соціальних медіа, соціальні мережі, блоги, форуми, фото і відеохостинги і т.д. [1]).

У рамках першого напряму російські структури організували публікацію величезної кількості тенденційних коментарів у популярних онлайн-медіа. За оцінками глави РТ- агентства «Ревуhtqnt» в період збройних зіткнень на сході України і президентської виборчої кампанії 2014 р., коментарів на сайтах онлайн-ЗМІ залишають не звичайні користувачі, а так звані тролі – анонімні інтернет-провокатори, які розміщують подібні повідомлення за певну плату [3].

Антиукраїнські коментарі публікуються не лише на сайтах українських та російських інтернет-каналах, а й зарубіжних, більш того, коментарі щодо подій в характеризуються категоричністю, агресивністю, зневажливим ставленням до іншої думки.

Аналіз публікацій у соціальних медіа свідчить про те, що в мережі Інтернету російська сторона продовжує пропагандистську кампанію, розпочату в традиційних ЗМІ.

Простір соціальних медіа заповнений інформацією, яка не відповідає дійсності або суттєво спотворює новинний ряд та реальні факти, заповнюючи інформаційним сміттям і неправдивими повідомленнями; приплачені російські користувачі, боти, громадські та культурні діячі здійснюють суттєвий вплив на суспільну думку українського користувачів інтернет-мережами.

Вищезазначені фактори загрожують українському медіа простору через свою непередбачуваність, фальшивість та використання його в якості об'єкта й, одночасно, інструменту агресії. Причетний до її ведення централізований державний механізм РФ активно виступає гравцем в Інтернет-мережах.

Російсько-українська гібридна війна вкотре демонструє що, використовуючи соціальні мережі, можна дестабілізувати ситуацію в країні, змодельовати вигідний противнику соціально-політичний контекст розвитку подій.

Крім того, потужні інформаційні ресурси Росії значною мірою впливають на свідомість громадян європейських держав, особливо їх оцінку подій в Україні та навколо неї. У цьому випадку ліберальні демократії Заходу демонструють уразливість стосовно дезінформації з огляду на відсутність цензури та формальну відповідність російських мас-медіа їх національному законодавству. Некоректний інформаційний супровід впливає не лише на суспільну думку, але й позицію по-

літичних сил, які приймають важливі державні рішення, зокрема ті, які прямо чи опосередковано стосуються України

Потрібно зазначити, що масове поширення інформаційних, соціально-мережних технологій докорінно змінило способи спілкування та методологію впливу на свідомість громадян – з'явилися такі методи роботи, як «ботоферми», «живі свідки», маніпулювання фотодокументами та інше.

Таким чином, стрімкий розвиток віртуального простору постійно змінює проблематику та актуальність проблем, дедалі частіше у фокусі уваги опиняється не реальні події та факти, а символізми. Тому в сучасній, інформаційній реальності такі поняття, як новини та реальні події змінюються політично заангажовані наративи.

Більш того, потрібно брати до уваги, що для ведення інформаційних атак керівництво Росії задіяло значні людські, матеріальні і фінансові ресурси, які направлені на продукування неправдивої інформації, завдяки чому вдалося ефективно впливати на громадську думку більшості споживачів.

В контексті зміни парадигми сучасного устрою, слушною є думка Г. Почепцова, який наголошує на тому, що сьогодні інформаційні війни, перш за все, ведуться за допомогою інтелектуального інструментарію, а соціальні мережі є безпосереднім середовищем для їх використання. Також він відзначає створення нового методу впливу на громадську думку, що отримав назву мікротаргетингу і полягає у публікації персоналізованих повідомлень на рівні окремої людини для привернення її уваги та завоювання прихильності [4].

В цілому, основними методами деструктивного впливу на суспільство через соціальні мережі є мережеві атаки, залученням користувачів до обговорення, імплементація в цей процес «ботів», створення «експертного середовища» тощо.

Охоплюючи велику та різносторонню аудиторію, інтернет, - соціальні мережі перетворюються на інструментарій інформаційної агресії, тому проблеми диверсифікації зазначених ризиків залишаються недостатньо вивченими, потребують ґрунтового аналізу всіх методів, задіяних для здійснення інформаційної складової гібридної війни.

Список літератури:

1. Запорожець О.Ю, Практика використання мережі інтернет в інформаційній війні file:///C:/Users/USER/Downloads/2451-8914-1-PB%20(2).pdf [online] Доступно: http://nbuv.gov.ua/j-pdf/Nzipiend_2014_2_6.pdf
2. Ніколаєнко Н.О., Комарчук О.О., Засоби масової комунікації як детермінанти гібридної війни : монографія, Миколаїв : НУК, 2021., 220 с.
3. Попова М., Боты вернулись: как работает российская интернет, пропаганда [online] Доступно: <http://bkz-nkic-net.cnn.cnn.utctk.163802/bqt>,
4. Почепцов Г.Г., Гібридна війна: інформаційна складова. [online] Доступно: http://www.jimagazine.lviv.ua/2015/Pochepcov_Ros_konteksty_hibridnoj_vijnny.htm

УДК 316.485.26:316

БОРОТЬБА З ІПСО В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

***Автор:** Тимошук Є.І., студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

***Науковий керівник:** Ніколаєнко Н.О., д.п.н., професор кафедри адміністративного та конституційного права, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На початку повномасштабного вторгнення ворог атакував українців не тільки воєнними діями, а й маніпуляціями, фейками та сумнівними новинами. До такої інформаційної навали не були готові ні медіа, ні органи влади, ні тим паче громадяни. Виходячи з цього ми мусимо розрізняти інформаційні вкиди і як внаслідок гідно протистояти атакам окупантів.

ІПСО – інформаційно-психологічна спеціальна операція (англ. Psychological Operations, PSYOPS), метою якої є вплинути на настрої різних груп суспільства задля досягнення поставленої мети [7]. Ознаки ІПСО: спеціальна операція завжди має мету, яка полягає у зміні поведінки конкретної людини чи групи людей; мета повинна реалізовуватися інтересантом – людиною чи організацією, яка отримує виго-

ду від зміни поведінки цих людей; у спеціальних операціях інформація повторюється або доноситься за допомогою специфічних засобів. У практиці роботи спецслужб це є однією з основних ознак розкриття ворожих намірів; якщо в медіа ви бачите повторюваність меседжу, яку не можна пояснити його соціальною значимістю, це має спонукати вас думати, що в цьому може бути ресурс реалізації спецоперації; у рамках спеціальних операцій інформацію важко або неможливо верифікувати, тобто немає об'єктивного підтвердження, що інформація є правдивою [8].

Формування глобального інформаційного суспільства не змогло заблокувати війни як спосіб розв'язання політичних, економічних, територіальних, етнічних, релігійних та інших конфліктів. Більше того, процеси запровадження сучасних інформаційно-комунікаційних, соціально-політичних та соціально-психологічних технологій зробили ці війни більш витонченими і підступними. В умовах інформаційних війн руйнуються суспільні організми (державні, політичні, соціальні інститути і організації), деформується цивілізаційно-культурний код нації і суспільна мораль, руйнується почуття патріотизму, розхищується людська психіка, паралізується здатність народу до спротиву агресії ворога. Домінування інформаційних чинників при веденні інформаційних та гібридних війн визначається сутністю інформаційного суспільства, яке, на думку його ідеологів, визначається якісним переходом людської цивілізації від аграрної та індустріальної до інформаційної стадії розвитку, коли інформаційно-комунікаційні ресурси стають набагато важливішими, ніж матеріально-технічні ресурси суспільства. Відповідно до цієї базової філософської конструкції, в умовах інформаційної та гібридної війни противник активно використовує соціальні структури, які мають достатньо вагомий вплив на глобальну суспільну свідомість та національну суспільну свідомість країни, що стала об'єктом інформаційного нападу відразу чи протягом тривалого часу: • засоби масової комунікації: ефірне, кабельне, супутникове телебачення і радіо, мобільний відео, аудіо та інтернет-зв'язок, соціальні мультимедіа мережі, сайти, паперові та електронні газети, журнали і книги; • релігійні, культурологічні, профспілкові, екологічні, правоза-

хисні, журналістські та інші соціальні організації; • дипломатичні структури (МЗС, посольства та представництва при міжнародних організаціях); • зовнішню розвідку (через своїх таємних та легалізованих агентів в мас-медіа, міжнародних та суспільних організаціях)

Цілі російських ПІСО спрямовані на те, що забезпечити російським військам оптимальні умови для взяття під контроль українських територій, тобто зробити все, щоб українці припинили чинити опір російським окупантам. Часто фейки, чутки та маніпуляції називають ПІСО. Але насправді, вони можуть бути лише частиною ПІСО так само як і дезінформація, пропагандистські наративи, маніпулятивні прийоми, диверсії та кібератаки [6]. Впроваджують ПІСО таким чином: часто це неформальні комунікації, ефіри, інформаційні повідомлення, листівки – загалом, будь-що, що допомагає охопити якомога більшу кількість людей. Спочатку в рамках ПІСО формують певну аудиторію, яку спонукають думати у певному напрямку, даючи потрібні аргументи. Наступний етап – дати аудиторії пряму вказівку, що потрібно робити. Часто ПІСО працює на контрасті патріотичних закликів і шкідливого твердження, і саме шкідлива теза починає ширитися під прикриттям правильних гасел.

Розкол суспільства, підри́в дові́ри та деморалізація – одні із основних цілей психологічних операцій під час війни.

1. Пам'ятаєте повідомлення на початку повномасштабного вторгнення про червоні мітки, які треба знищувати чи засипати землею? Одна із найбільш вдалих спецоперацій початкового етапу. Мітки дійсно були, проте по них не наводилися ракетні удари. Українці шукали «відьом» серед своїх. згодом стало зрозуміло, що мітки не становлять загрози, а спрямовані на максимальне поширення паніки та шпигуноманію.

2. У липні усі українці потрапили під вплив ще однієї ПІСО, яка мала кілька складових: відео, де українського військовослужбовця каструють канцелярським ножем; страта українців в Оленівці. Теми, дуже чутливі і болючі для українців, використали росіяни для розпалювання гніву та провокацій. Проте дуже важливо пам'ятати, що Україна – цивілізована країна. Усі звірства росіян мають бути розслідувані міжнародними та українськими інституціями, а винні у їх вчиненні – покарані.

Дослідниик інформаційної безпеки та російської пропаганди Бен Німо виокремив 4 основні компоненти дезінформаційних кампаній: Dismiss – заперечуй правду та факти; Distract – відвертай увагу та звинувачуй; Distort – спотворюй факти та перекручуй їх; Dismay – залякуй, викликай паніку та тривогу [2]. Саме за цією моделлю працюють ПСГО, інфовкиди та чутки, які поширює РФ. Російська пропаганда спрямована на розпалювання ворожнечі, створення інформаційного хаосу та дискредитацію військових, влади, волонтерів і медіа.

Для того, щоб перемогти систему російської пропаганди, варто дотримуватися таких порад:

1. Аналіз та повторення історії, адже ми знаємо, що путін любить підмінювати історичні факти та прив'язуватися до дат. Яким чином можна аналізувати? Прослуховування подкастів, участь в онлайн-проектах, конференціях.

2. Не переходити за невідомими посиланнями, навіть якщо їх відправляють рідні. Встановіть двофакторну авторизацію у всіх месенджерах.

3. Писати пости, поширювати у своїх соц.мережах правильні новини із достовірних джерел, а також публікувати поради із виживання в інфопросторі, але: не поширювати на українську аудиторію результатів терору росії. Доцільніше злочини рф поширювати на міжнародну спільноту.

4. Оминайте приголомшливих заголовків

5. Ретельно перевіряти сторінки під фото яких ви пишете коментарі. Пост може бути таким: Наші ЗСУ – герої, прокоментуйте на удачу. В майбутньому це можливий бот або ботоферма вже із сформованою аудиторією

6. Використання фактчекінгових ресурсів. Ресурси: «СтопФейк», «Без брехні», «Воксчек», «По той бік новин» [3].

7. Фільтруйте джерела, з яких берете інформацію. Якщо це телеграм, то чи знаєте ви, хто пише новини для конкретного телеграм-каналу? Наприклад, телеграм-канал Укрінформ чи Радіо Свобода ведуть команди відповідних медіа. А хто публікує інформацію у телеграм-каналі Труха чи Інстайдер? Це цілодобова робота, яка потребує значних ресурсів.

8. Відпишіться від анонімних телеграм-каналів, якщо це фейсбук або твіттер, то звідки саме? Це офіційна сторінка якогось відомства чи коментар під постом у якійсь групі? Оберіть кілька медіа, в яких є журналісти, які перевіряють інформацію та дотримуються стандартів. Білий список медіа: Українська правда, Укрінформ, Громадське, Радіо Свобода [5].

9. Якщо якимось повідомленням викликає у вас гнів, злість, жалість чи радість, скажіть собі «Стоп». Відкладіть телефон і підіть, наприклад, на кухню, випити чаю чи кави. Після цього поверніться і перечитайте новину

10. Не вступайте з ботами у дискусію. Не відповідайте і не критикуйте їх. Краще залишати скарги. Перед тим, як відповідати комусь на коментар, подумайте, чи точно по той бік екрану знаходиться людина і з якою метою вас втягують у дискусію [4].

11. Пам'ятайте про шахрайства. Більшість з них пов'язані з нібито виплатами допомоги. Так тільки за останні місяці жертвами такого шахрайства стали понад 5000 українців, які на цьому втратили понад 100 млн гривень. Ціляться, першочергово у людей поважного віку. Обіцяють допомогу нібито від Президента, Євросоюзу і так далі.

Отже, кожен українець під час війни має ретельно ставитися до отримуваної і поширюваної інформації і довіряти насамперед офіційним українським джерелам, фаховим журналістам та українським і світовим ЗМІ з бездоганною репутацією.

Список літератури:

1. О.Мороз. Нація овочів? Як інформація змінює мислення і поведінку українців, К.:Yakaboo Publishing, 2020, 304 с.

2. Бен Німо. Disinformation, Misinformation, and Fake News Teach-Out. URL: <https://online.umich.edu/teach-outs/disinformation-misinformation-and-fake-news-teach-out/lessons/4d-model-disinformation-campaigns/?fbclid=IwAR1FJPnDfe3q8xhZIJAZfHpLeLnZpYrd1a5QZKZyrnx5CE8Xm2IC5gvks1s>

3. О. Набожняк. Інструменти фактчекінгу: як професійно відрізнити брехню від правди. URL : <https://imi.org.ua/articles/instrumenti-faktcheking-u-yak-profesiyno-vidriznyati-brehyu-vid-pravdi-i407>

4. Війна в соцмережах: як працюють ботоферми на мільйон акаунтів та який вплив мають. URL: <https://www.google.com/amp/s/tsn.ua/amp/exclusive/viyna-v-socmerezah-yak-pracyuyut-botofermi-na-milyon-akauntiv-ta-yakiy-vpliv-mayut-2147434.html>

5. Білий список: 10 медіа, що стали найякіснішими URL : <https://imi.org.ua/monitorings/bilyj-spysok-10-media-shho-staly-najyakisnishymy-i41541>

6. Що таке ІПСО, чому важливо це знати і які операції зараз проводить Росія проти України. URL : <https://tyzhden.ua/News/254439>

7. Як рашистські ІПСО ховаються за українською символікою в українському Facebook. URL: <https://armyinform.com.ua/2022/08/03/yak-rashystski-ipso-hovayutsya-za-ukrayinskoyu-symvolikoyu-v-ukrayinskomu-facebook/>

8. Що таке інформаційно-психологічні операції і як їх розпізнати URL : <https://ms.detector.media/manipulyatsii/post/29009/2022-02-23-shcho-take-informatsiyno-psykhologichni-operatsii-i-yak-ikh-rozpiznaty/>

УДК 004.056.5;057.2

ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

***Автори:** Турти М.В., к.т.н., доцент; Баронова О.А., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

План реалізації Стратегії кібербезпеки України [1], затверджений в лютому 2022 року до початку воєнних дій на території України, передбачає досягнення в найближчі роки ряду цілей, частина з яких безпосередньо пов'язана із підготовкою фахівців з інформаційної безпеки (ІБ). В умовах військової агресії підготовка захисників кіберпростору набуває особливого значення.

Метою даної роботи є визначення пріоритетних напрямів і форм підготовки фахівців з інформаційної безпеки в умовах воєнного стану. Для досягнення поставленої мети необхідно провести аналіз актуальної нормативно-правової бази і визначити актуальні напрямки підго-

товки фахівців з ІБ за нормативними вимогами, визначити методики викладання, доцільні для застосування в умовах воєнного стану.

Ціль С.1 «Дієва кібероборона» згідно [1] передбачає, що «Україна створить та забезпечить розвиток (у тому числі кадрово та технологічно) підрозділів із повноваженнями ведення збройного протиборства в кіберпросторі, ...забезпечить ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності». Зокрема передбачається:

1) проведення навчань у сфері кібербезпеки у системі військово-патріотичного виховання та системі територіальної оборони, проведення спільних навчань з підрозділами держав-членів НАТО;

2) запровадження практичних навчань;

3) розробка і впровадження механізмів комунікації між державою та суспільством щодо стримування деструктивної діяльності в кіберпросторі:

– збирання кіберстатистики і щорічне її оприлюднення на офіційних сайтах;

– проведення щорічних соціологічних досліджень спектру загроз у кіберпросторі України та ефективності протидії цим загрозам державних органів;

– проведення «загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів» [1];

– залучення приватного сектору, громадських організацій, наукової спільноти до здійснення заходів протидії загрозам у кіберпросторі;

4) поліпшення матеріально-технічного забезпечення галузі;

5) інтенсифікація наукових досліджень і розробок у галузі кібербезпеки з урахуванням тенденцій розвитку інформаційно-комунікаційних технологій на основі довгострокових програм та програми державної підтримки стратегічно важливих наукових установ та організацій;

6) «створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки» [1];

7) забезпечення в державному секторі матеріального стимулювання фахівців з кібербезпеки «з урахуванням рівнів оплати праці таких фахівців у приватному секторі» [1];

8) підвищення рівня знань з кібербезпеки:

- громадськості шляхом розробки і впровадження Загальнонаціональної програми кіберграмотності,

- здобувачів освіти шляхом включення питань щодо кіберграмотності і кібергігієни до навчальних програм загальної середньої, професійно-технічної та вищої освіти.

- фахівців у сфері кібербезпеки у формі періодичного підвищення кваліфікації, в тому числі залучення «суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу» [1];

- фахівців, які займаються дослідженнями електронних доказів та безпечності апаратних і програмних засобів;

9) розвиток мережі центрів, що виконуватимуть наступні функції:

- реагування на кібератаки та кіберінциденти;

- акумуляція і оперативне розповсюдження вітчизняних і міжнародних нормативно-правових документів в галузі кібербезпеки, зокрема, регламентів і директив Європейського парламенту та Ради ЄС, галузевих нормативних документів, законів і підзаконних актів України, нормативних документів з технічного захисту інформації;

- узагальнення та обмін досвідом у сфері кібербезпеки;

- підтримка інновацій та вітчизняних розробок у сфері кібербезпеки.

- організація періодичного підвищення кваліфікації фахівців у сфері кібербезпеки;

10) створення національної системи управління інцидентами.

Таким чином, ще в мирний час була визначена необхідність модернізації системи управління інформаційною безпекою України і розроблена відповідна система заходів, до яких входить проведення докорінної реформи системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Перші кроки у напрямі реалізації цієї реформи були зроблені протягом 2021-2022 року з метою забезпечення відповідності стандартам ЄС і США, впровадження в освітній процес

найкращих світових практик, досвіду Стратегічної освітньої ініціативи у сфері кібербезпеки США та досвіду розробки і впровадження Європейської рамки кваліфікації.

Тривалий час у Класифікаторі професій були лише дві професії, що безпосередньо стосувалися кібербезпеки і відповідали освітньо-кваліфікаційним рівням «бакалавр» і «магістр» - фахівець та професіонал із організації захисту інформації. 25 жовтня 2021 року у Класифікатор професій за поданням Держспецв'язку було внесено 17 нових професій, серед яких «Фахівець з технічного захисту інформації», «Аналітик загроз безпеки», «Дізнавач сфери кібербезпеки та захисту інформації» та ін. [2]. Для кожної професії мали бути сформульовані кваліфікаційні вимоги і розроблені стандарти. За цими стандартами в кваліфікаційних центрах випускники закладів вищої освіти повинні складати професійні іспити щоб здобути кваліфікацію за конкретним напрямом.

У 2022 році були розроблені, пройшли публічне обговорення та експертизу перші шість професійних стандартів для професій «Адміністратор мереж і систем», «Аналітик з безпеки інформаційно-телекомунікаційних систем», «Інструктор-методист з інформаційної безпеки та кібербезпеки», «Розробник систем захисту інформації», «Фахівець з питань безпеки» та «Фахівець сфери захисту інформації» [3].

Планується [3], що у 2023 році будуть розроблені стандарти для 14 професій, кількість професій у сфері кібер- та інформаційної безпеки буде збільшена до 20, і відкриються перші незалежні кваліфікаційні центри.

В рамках реформи підготовки фахівців у сфері кібербезпеки і в умовах воєнного стану можна вважати дцільною трансформацію освітнього процесу за спеціальністю 125 «Кібербезпека» на наступних засадах:

1. Розширення спектру освітньо-професійних програм у вищих навчальних закладах з метою підготовки вузькоспеціалізованих фахівців згідно новим професіям у Класифікаторі професій.

2. Використання регіональних центрів як баз практик студентів вищих навчальних закладів.

3. Динамічна модифікація робочих програм дисциплін і (за необхідності) навчальних планів) за результатами оприлюднених результатів моніторингу стану кіберпростору України.

4. Підсилення практичної складової освітнього процесу:

- використання на практичних і лабораторних заняттях реальних прикладів застосування новітніх практик рішення задач кіберзахисту за матеріалами регіональних центрів;

- залучення здобувачів освіти за спеціальністю 125 «Кібербезпека» до вирішення практичних завдань Плану реалізації Стратегії кібербезпеки України: збирання кіберстатистики, проведення соціологічних досліджень, участь у заходах протидії загрозам у кіберпросторі, участь у загальнонаціональній інформаційній роз'яснювальній кампанії та створенні апаратних і програмних засобів захисту в рамках студентської наукової роботи, курсових і дипломних проєктів, виробничої практики та наукового стажування;

- залучення здобувачів освіти за спеціальністю 125 «Кібербезпека» до наукових досліджень і розробок у галузі кібербезпеки, що проводяться випусковою кафедрою або іншими організаціями (з відома кафедри), відповідно до наявних у студентів форм допуску.

5. Рациональне використання наукового потенціалу вищих навчальних закладів:

- формування переліків пріоритетних напрямів наукових досліджень в галузі кібербезпеки, які фінансуються Держбюджетом і приватним сектором;

- формування переліків пропозицій щодо напрямів наукових досліджень від науковців;

- розробка механізму створення тимчасових творчих колективів з вітчизняних та закордонних науковців і практиків, що є співробітниками організацій різного підпорядкування;

- скорочення витрат часу науковців навчальних закладів на документальне забезпечення навчального процесу за рахунок використання електронних бібліотечних фондів регіональних центрів, до яких пропонується включити без порушення авторського права електронні конспекти лекцій, методичні вказівки до лабораторних і практичних робіт тощо.

Реалізація запланованих заходів з реформування освіти в галузі кібербезпеки під час воєнного стану ускладнюється ресурсними об-

меженнями. Крім того, дистанційне навчання під час відсутності гарантованого електроживлення і зв'язку вимагає застосування гнучких методів навчання і оцінювання знань студентів:

- відсутність можливості проведення занять в спеціалізованих лабораторіях частково може бути скомпенсована застосуванням файлів зображень і відеороликів, які знаходяться у вільному доступі або можуть бути створені викладачем;

- джерела інформації з дисциплін мають бути надані студентам у формі електронних документів, що дозволяє скоротити час пошуку, наприклад нормативних документів, за посиланнями в мережі і зменшити залежність студента від наявності Інтернет-зв'язку;

- завдання до лабораторних і практичних робіт, модульні контрольні роботи доцільно формувати за варіантами, кількість яких дорівнює кількості студентів, що дозволяє оцінити роботу без процедури захисту;

- усі методичні матеріали, підручники, нормативні документи мають бути сформовані у вигляді кейсу, який розташовується наприклад на Google-диску і протягом семестру в ідеалі не коригується;

- втрачається значимість присутності студента на заняттях, активності студентів на заняттях і дотримання термінів виконання робіт протягом семестру внаслідок унеможливлення об'єктивної оцінки умов, в яких знаходяться студенти, особливо здобувачі освіти, що перебувають на тимчасово окупованих територіях;

- студенти повинні отримувати протягом семестру інформацію про набрані ними бали за всіма формами контролю і причини зниження балів за окремі види робіт, наприклад у вигляді таблиць на Google-диску, що, по-перше, стимулює конкурентну діяльність студентів, а по-друге – дозволяє оперативно виявити загублені при передачі чи не зараховані з якоїсь причини роботи;

- змінюються вимоги щодо форматів представлення робіт: в разі відсутності у студента можливостей створювати документи в текстовому редакторі робота може бути представлена як набір фотографій рукописного тексту (за виключенням кваліфікаційних робіт);

- зростає значення індивідуального підходу до студентів, створення атмосфери дружньої підтримки і взаєморозуміння;

- навчальний процес виходить за стандартні рамки відповідальності викладача за вчасність і якість проведення занять, а стає резуль-

татом спільної роботи колективу кафедра-викладач-студенти, який (в разі необхідності) призначає і узгоджує час проведення додаткових занять у формі консультацій, їх тематику;

– зростає значимість планування навчання на наступних курсах, на наступних освітніх рівнях, участі в науковій роботі, що настрює студентів на отримання невеликих але позитивних результатів у недалекому майбутньому, тобто сприяє створенню психологічного комфорту.

Висновки

В даній роботі проведено аналіз нормативно-правової бази, визначені актуальні напрямки підготовки фахівців з ІБ та методики викладання, доцільні для застосування в умовах воєнного стану.

Список літератури:

1. План реалізації Стратегії кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
2. Олександр Потій: до класифікатора внесено 17 додаткових професій у галузі безпеки інформації та кіберзахисту. URL: <https://cip.gov.ua/ua/news/oleksandr-potii-do-klasifikatora-vneseno-17-dodatkovikh-profesii-u-galuzi-bezpeki-informaciyi-ta-kiberzakhistu>
3. Реформування системи підготовки професійних кадрів у сфері кібербезпеки в Україні: затверджені перші шість професійних стандартів. URL: <https://cip.gov.ua/ua/news/reformuvannya-sistemi-pidgotovki-profesiinikh-kadriv-u-sferi-kiberbezpeki-v-ukrayini-zatverdzheni-pershi-shist-profesiinikh-standartiv>

СЕКЦІЯ 7. ШКОЛА МОЛОДИХ НАУКОВЦІВ

УДК 004.056.5; 004.89; 514.743.4

СУЧАСНІ ЗАСОБИ МОДЕЛЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Автор: Литвиненко О.-Н., студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

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

Оскільки ми живемо в еру інформаційних технологій – діяльність будь-якої сучасної компанії або державної структури не можна уявити без постійного використання інформації та, відповідно, засобів для комунікації. Зі стрімким розвитком технологій паралельно породжуються нові види ризиків, тому перед розробниками інформаційних технологій постала задача забезпечення захисту інформації в комп'ютерних мережах. Сучасний ринок послуг пропонує велику кількість засобів для моделювання загроз. Розробці сучасних засобів моделювання загроз інформації в комп'ютерних мережах та їх ефективного використання також присвячені роботи багатьох вітчизняних та зарубіжних науковців [1 – 3]. Кожна з них має свої переваги та недоліки, і як наслідок цілком природньо виникають труднощі щодо вибору, до того ж, з кожним днем змінюються вимоги щодо захисту інформації. Відповідно, актуальною задачею є вибір оптимальних засобів моделювання для вирішення конкретних прикладних задач інформаційної безпеки.

Метою цієї роботи є ознайомлення із сучасними засобами моделювання загроз інформації в комп'ютерних мережах, методикою їх використання на практиці.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати основне призначення засобів моделювання загроз інформації в комп'ютерних мережах;
- встановити параметри, які необхідно враховувати під час розробки нової методики та програмного комплексу з моделювання загроз в комп'ютерних мережах;

– проаналізувати найкращі практики використання засобів моделювання на сьогоднішній день.

Моделювання загроз – це ітеративна процедура оптимізації безпеки програм, системи або бізнес-процесу шляхом визначення потенційних вразливостей і цілей зловмисника із наступним встановленням контрзаходів для запобігання або пом'якшення наслідків загроз для системи.

З точки зору безпеки програмного забезпечення, моделювання загроз є найважливішою частиною етапів проектування та розробки. Команді розробників необхідно визначити, які засоби необхідні для протидії потенційним загрозам, і як вирішити нагальну проблему саме на ранній стадії. З цього можна встановити, що засоби моделювання забезпечують досить високий рівень безпеки системи з превентивної точки зору, а за рахунок визначення пріоритетів передбачуваних загроз, ресурси використовуються ефективно.

Не дивлячись на різноманіття експертних думок, можна визначити наступні основні етапи побудови моделей і проведення досліджень загроз:

1. **Залучення зацікавлених сторін до команди.** Перший крок в процесі моделювання загроз інформації в комп'ютерних мережах пов'язаний із об'єднанням людей, що мають спільну мету, задля створення надійної системи із врахуванням всіх думок. Це можуть бути: мережеві архітектори (розробники), власники бізнесу, експерти з питань інформаційної безпеки, керівництво найвищої ланки.

2. **Визначення потенційних загроз.** Для усіх компонентів КС необхідно змоделювати потенційний сценарій вторгнення (будь то перехоплення мережевого трафіку, або, наприклад, вплив на співробітників компанії шляхом соціальної інженерії та ін.). Чим більше таких сценаріїв буде розглянуто, тим більш надійну систему отримаємо в підсумку. Саме на цьому етапі обирається відповідний інструмент (утиліта) для моделювання загроз інформації.

3. **Оцінка ризику для кожної із загроз (ранжування).** Тут все досить примітивно: необхідно визначити рівень ризику, що являє со-

бою та чи інша загроза. Цей простий спосіб полягає в множенні потенційної шкоди для системи на ймовірність її виникнення.

4. Реалізація пом'якшення наслідків. Залучаються мережеві архітектори та експерти з питань інформаційної безпеки, які в свою чергу вирішують як саме зменшити або знизити ризики до найменшого рівня для спроектованої системи.

5. Документація результатів. Останній крок полягає в документуванні усіх попередніх етапів задля відстеження певної динаміки в системі. Це надасть змогу в майбутньому впровадити нові моделі захисту інформації в комп'ютерній мережі, тим самим забезпечуючи її цілісність та надійність.

Фахівцями визнано, що з точки зору практики при моделюванні загроз найбільш доцільно дотримуватися наступних правил:

1. Використання багатозадачних (від англ. multitasking tools) додатків. Ринок послуг постійно оновлюється допоміжними засобами для моделювання загроз інформації, однак доцільно розглядати саме багатозадачні додатки. Таким чином система захищається від різних видів атак за рахунок того, що інструмент знаходить найкращі способи реагування на загрози.

2. Загальне розуміння значущості потенційних ризиків. Авжеж, власники бізнесів завжди шукають можливості для заощаджування на будь-чому (і це є нормальним явище), але у випадку стійкості системи дане рішення не панацея. Необхідно розуміти усі ризики у разі вторгнення, щоб обрати правильні шляхи пом'якшення загроз для досягнення бізнес-цілей.

3. Вчасно почати діяти. Моделювання загроз інформації можна виконувати в будь-який час у ході проекту, але краще розпочати якомога раніше. Завдяки цьому забезпечиться безпекова складова, окрім того, можна швидко і вигідно (у фінансовому аспекті) додати елементи керування саме на процесі побудови.

Як вже зазначено вище, існують різні інструменти для моделювання загроз інформації. Відповідно, виникає необхідність ознайомлення з ними:

1. PASTA. Фреймворк, розроблений у консалтинговій компанії з питань інформаційної безпеки VerSprite. Представляє методологію, орієнтовану на ризик та спрямовану на застосування контрзаходів безпеки, порів-

нянних з можливим впливом, який може бути отриманий від певних моделей загроз, вразливостей, слабких місць та моделей атак.



Рисунок 1 – Приклад побудованої моделі загроз з використанням PASTA

2. **CAIRIS**. Платформа з відкритим вихідним кодом, яка використовує дані про потенційні загрози для визначення рівня атаки та перевірки проектів на наявність проблем безпеки та потенційних проблем із відповідністю GDPR (рис. 2).

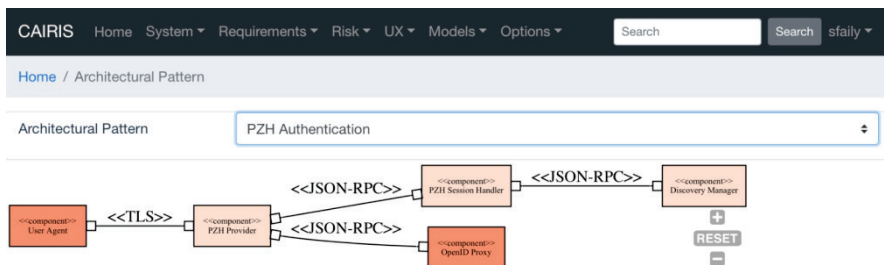


Рисунок 2 – Приклад побудованої моделі загроз з використанням CAIRIS

3. OWASP Threat Dragon. Цей інструмент із відкритим кодом працює як веб-програма або програма для настільного комп'ютера. Вона записує можливі загрози, визначає підходи до пом'якшення та демонструє компоненти моделі і поверхню загроз цих моделей (рис. 3).

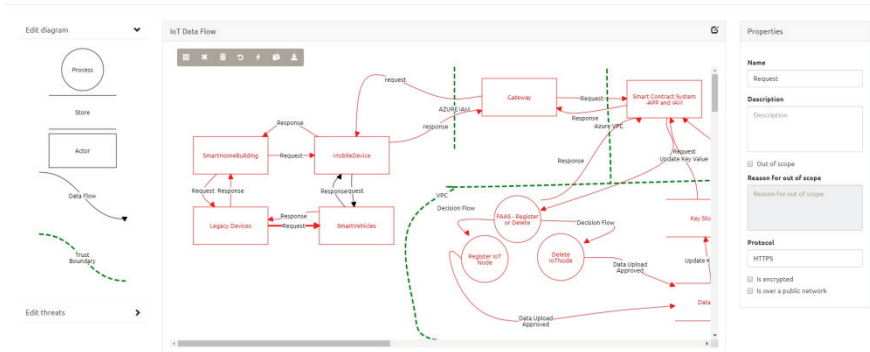


Рисунок 3 – Приклад побудованої моделі загроз з використанням OWASP Threat Dragon

Висновки. В роботі розглянуто основні параметри, які потрібно врахувати під час розробки нової методики та програмного комплексу з моделювання загроз інформації в комп'ютерних мережах, проведено аналіз використання засобів для моделювання загроз на практиці.

Ознайомлено з деякими інструментами для здійснення моделювання загроз інформації та встановлено, що варто використовувати багатозадачні додатки. Варто розуміти, що аналіз загроз потребує часу, зусиль та фінансових вкладень. Краще знайти вразливість і виправити її до виявлення хакерами, і методологія моделювання загроз – найкращий спосіб досягти цього.

Список літератури:

1. Комп'ютерні мережі. Низхідний підхід, Джеймс Куроз, Кіт Росс, 2016. 912 с.
2. Michael Cobb M. Threat modeling. [URL]: <https://www.techtarget.com/searchsecurity/definition/threat-modeling>
3. Моделирование угроз. [URL]: <https://progler.ru/blog/modelirovanie-ugroz>

УДК 004.056.5;057.2

ВИКОРИСТАННЯ ГРАФІВ ПРИ АНАЛІЗІ І ОЦІНЮВАННІ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: Манько С.В., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна

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

На даний час існує багато методів аналізу і оцінювання ризиків (АОР) [1, 2], які можуть бути застосовані для в менеджменті ризиків інформаційної безпеки [3]. Ці методи різняться за типом і обсягом оброблюваних та вихідних даних, складністю, алгоритмами, способами і методами формалізації розв'язуваних задач. Частина загальних методів АОР, описаних в [2] базується на використанні різних типів графів.

Метою даної роботи є визначення критеріїв вибору методу, що базується на графовій моделі, для аналізу і оцінювання ризиків інформаційної безпеки.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз типів графів, методів їх математичного опису та графічного відображення, які застосовуються для АОР;
- визначити критерії вибору методу, що базується на графовій моделі, для аналізу і оцінювання ризиків інформаційної безпеки;
- провести порівняльний аналіз методів за визначеними критеріями.

В ДСТУ ISO/IEC 31010:2013 описані наступні методи АОР, що використовують графові моделі:

- аналізування дерева подій;
- аналізування дерева відмов;
- дерево рішень;
- аналізування причин і наслідків;
- аналізування причинно, наслідкових зв'язків;
- аналізування за схемою «краватка-метелик»;
- Марковське аналізування;
- мережі Байєса.

Таблиця – Властивості методів АОР, що використовують моделі, побудовані за теорією графів

Метод	Застосовність					Вирішувані задачі							Функціональні особливості			
	ідентифікування ризику	аналіз ризику			оцінювання ризику											
		для аналізу наслідків	для аналізу ймовірностей подій	для аналізу рівнів ризиків												
		пошук	аналіз сценарію	функціональний аналіз		оцінювання засобів контролю	статистичний аналіз	організація процесів отримання експертних оцінок	врахування впливу людського фактору	Вимоги до ресурсів і кваліфікації персоналу	Складність	Характер і ступінь невизначеності вхідних і вихідних даних	Здатність обробляти кількісні дані і отримувати кількісні вихідні дані			
Аналіз дерева подій	3	33	3	3	НЗ	-	+	-	+	-	-	-	С	С	С	+
Аналіз дерева відмов	3	НЗ	33	3	3	+	+	+	+	-	-	+	В	С	В	+
Дерево рішень	НЗ	33	33	3	3	-	+	-	-	-	+	-	С	С	С	+
Аналіз причин і наслідків	3	33	33	3	3	+	+	+	+				В	В	С	+
Аналіз причинно-наслідкових зв'язків	33	33	НЗ	НЗ	НЗ	+	+	+	+	-	+	-	Н	С	Н	-
Аналіз за схемою «краватка-метелик»	НЗ	3	33	33	3		+	+	+		+	-	С	С	В	+
Марковське аналізування	3	33	НЗ	НЗ	НЗ	-	+	+	-	+	-	-	В	В	Н	+
Мережі Байеса	НЗ	33	НЗ	НЗ	33	+	-	-	-	+	+	-	В	В	Н	-

В ДСТУ ISO/IEC 31010:2013 не включені методи, засновані на теорії графів, які також можуть бути виористані для АОР, але більше орієнтовані на організацію віртуальних експериментів в галузі управління інформаційною безпекою [4]: когнітивні моделі, мережі Петрі, системи масового обслуговування (СМО), потокові оптимізаційні моделі, семантичні мережі експертних систем, нейронні мережі (наприклад, персептрони), кінцеві і клітинні автомати, фрактали.

Вибір методу АОР є складною задачею і здійснюється за множиною критеріїв, до складу якої можуть входити критерії з наведеної нижче системи:

1. Застосовність методу для загального АОР, що включає: застосовність методу для ідентифікування ризику; застосовність методу для аналізу ризику (для аналізу наслідків, аналізу ймовірностей подій і аналізу рівнів ризиків); застосовність методу для оцінювання ризику.

2. За вирішуваними задачами: пошук; аналіз сценарію; функціональний аналіз; оцінювання засобів контролю; статистичний аналіз; організація процесів отримання експертних оцінок; врахування впливу людського фактору на досліджувані процеси (допоміжні методи).

3. За функціональними особливостями: вимоги до ресурсів і кваліфікації персоналу; складність; характер і ступінь невизначеності вхідних і вихідних даних; здатність обробляти кількісні дані і отримувати кількісні вихідні дані.

Як показав проведений порівняльний аналіз за групою критеріїв застосовності для загального АОР, методи АОР, що використовують моделі, побудовані за теорією графів, мають властивості, представлені в таблиці.

В таблиці використовуються наступні позначення:

- для кожного етапу процесу оцінки ризику: «завжди застосовується» (ЗЗ), «застосовується» (З) і «не застосовується»;
- важливість впливових чинників: «низька» (Н), «середня» (С), висока (В);
- здатність вирішувати певні задачі і здатність обробляти та видавати на виході кількісні дані: Так (+), Ні (-).

Кольором позначені задачі, для яких певний метод рекомендується ДСТУ ISO/IEC 31010:2013, однак практично кожний метод може

бути використаний також для вирішення інших задач, зазвичай з меншою ефективністю.

Висновки

В даній роботі проведено аналіз типів графів, методів їх математичного опису та графічного відображення, які застосовуються для аналізу і оцінювання ризиків; визначені критерії вибору методу, що базується на графовій моделі, для аналізу і оцінювання ризиків інформаційної безпеки; проведено порівняльний аналіз методів за визначеними критеріями. В результаті проведеного аналізу було виявлено, що методи аналізу і оцінювання ризиків, що використовують моделі, побудовані за теорією графів, і розглянуті в ДСТУ ISO/IEC 31010:2013, переважно рекомендуються для аналізу сценаріїв, але окремі методи можуть також застосовуватися для аналізу процесів функціонування і оцінювання засобів контролю ризиків, тобто оцінювання ефективності систем захисту інформації. Найбільш широкий спектр задач може бути вирішений шляхом аналізу дерева відмов, аналізу причин і наслідків та аналізу причинно-наслідкових зв'язків. Найбільш спеціалізованими є методи аналізу дерева подій і дерева рішень.

Список літератури:

1. Корченко А.Г., Архипов А.Е., Казимирчук С.В. Анализ и оценивание рисков информационной безопасности. – К.: ООО «Полиграф-Лазурит», 2013. – 275 с.
2. ДСТУ ISO/IEC 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» (ISO/IEC 31010:2009, IDT))
3. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. [URL]: <https://www.iso.org/standard/56742.html>
4. Манько С.В. Графи та штучний інтелект в системах технічного захисту інформації // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2021. – С.177-183. URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf

ЗМІСТ

Секція 1. Інформаційна безпека транспортних засобів і систем3

Особливості управління проектами інформаційної безпеки об'єктів морської критичної інфраструктури <i>Блінцов В.С., Буруніна Ж.Ю.</i>	3
Особливості формування концепції інформаційної безпеки для ініціативи «Флот морських дронів України» <i>Нужний С.М.</i>	7

Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах16

Дослідження адаптивної системи активного захисту мовної інформації у виділеному приміщенні <i>Демідов І.А.</i>	16
Комбіновані методи забезпечення інформаційної безпеки <i>Кобзєв В.Г.</i>	20
Розробка КСЗІ для об'єкту критичної інфраструктури водотранспортного комплексу <i>Крюк А.С.</i>	23
Ідентифікація стану пристроїв IoT для задач захисту інформації <i>Лисинчук В.В.</i>	29
Розробка блоку кіберзахисту для КСЗІ на об'єкті критичної інфраструктури водотранспортного комплексу <i>Майгур О.І.</i>	34
Аналіз методик оцінювання ефективності звукоізоляції в захисті мовної інформації <i>Сизов М.О.</i>	40
Аналіз захищеності бездротових точок доступу в мережі WI-FI <i>Соболев В.В.</i>	45
Робота та моніторинг комп'ютерних мереж в умовах воєнного стану <i>Трибулькевич С.Л.; Трибулькевич В.В.</i>	48
Розробка комплексної системи захисту інформації режимно-секретного відділу морського порту <i>Харченко М.С.</i>	56

Секція 3. Правові аспекти діяльності в галузі інформаційної безпеки.....61

Правові аспекти діяльності в галузі інформаційної безпеки <i>Матраєва Д.В.</i>	61
--	----

Секція 4. Моделювання об'єктів і процесів технічного захисту інформації.....	67
Аналіз процесу ідентифікації ризиків інформаційної безпеки <i>Баронова О.А.; Божаткін С.М.; Турти М.В.</i>	67
Критерії вибору методів оцінювання ризиків в задачах інформаційної безпеки <i>Божаткін С.М.</i>	73
Аналіз ринку програмних інструментів для оцінювання ризиків інформаційної безпеки <i>Божаткін С.М.; Сірівчук А.С.; Турти М.Ю.</i>	79
Модель процесів інформаційної безпеки на рівні організації <i>Божаткін С.М.; Турти М.В.</i>	91
Інформаційна модель оцінювання загроз безпеці інформації з обмеженим доступом <i>Гайванюк І.О.</i>	95
Врахування підвищення залишкової розбірливості мови в каналі витоку при багаторазовому прослуховуванні <i>Касьянов Ю.І.; Іванова А.В.</i>	103
Розрахунок бажаних характеристик звукоізоляції та шумової завади за октавними рівнями формантної розбірливості мови <i>Касьянов Ю.І.; Золотченко В.В.</i>	108
Основні аспекти об'єктивного тонального методу визначення розбірливості мови <i>Касьянов Ю.І.; Трізно С.О.</i>	113
Визначення ефективності захисту мовної інформації типовими звукоізоляційними конструкціями за їх частотними характеристиками <i>Кучер В.С.</i>	119
Дослідження спектрів довготривалих українських мовленнєвих сигналів <i>Михайличенко А.В.; Троценко С.С.</i>	124
Інтелектуальні засоби в системах виявлення та запобігання вторгнень <i>Стефанюк Ю.О.</i>	129
Інформаційна модель ранжування загроз за BS ISO/IEC 27005:2011 <i>Турти М.В.; Доценко В.В.</i>	134
Інформаційна модель категоризації об'єктів критичної інфраструктури <i>Турти М.В.; Злочевська О.В.</i>	140
Інформаційна модель системи визначення оптимальних інвестицій в інформаційну безпеку <i>Турти М.В.; Осипчук А.В.</i>	147

Секція 5. Створення підводно-технічних засобів для захисту морських об'єктів та акваторій.....	153
Дослідження характеристик джерела живлення на базі фотоелектричного перетворювача <i>Бинкало С.Ф.</i>	153
Синтез системи керування рухом автономного підводного апарата <i>Гузій О.В.</i>	155
Дослідження системи керування рушійно-кормовим комплексом підводного апарата <i>Захараши А.М.</i>	158
Аналіз структури системи керування поворотом палубного механізму <i>Казасев В.С.</i>	161
Дослідження системи керування морського рухомого об'єкту <i>Кузьмін М.С.</i>	163
Розробка стенду дослідження системи керування рухом <i>Листопад М.О.</i>	166
Дослідження методів організації керування рухом рухомих об'єктів <i>Московченко О.В.</i>	170
Розробка структури системи керування рухом підводного апарата патрульного типу <i>Сірівчук А.С.</i>	173
Секція 6. Підготовка кадрів у галузі знань «Інформаційна безпека».....	178
Інформаційна безпека в умовах гібридної війни <i>Кальваровська Б.М.</i>	178
Інтернет-мережі в гібридній війні <i>Ніколаєнко Н.О.</i>	181
Боротьба з ІПСО в контексті російсько-української війни <i>Тимошук Є.І.</i>	185
Проблеми підготовки фахівців з інформаційної безпеки в умовах воєнного стану <i>Турти М.В.; Баронова О.А.</i>	190
Секція 7. ШКОЛА МОЛОДИХ НАУКОВЦІВ	197
Сучасні засоби моделювання загроз інформації в комп'ютерних мережах <i>Литвиненко О.-Н.</i>	197
Використання графів при аналізі і оцінюванні ризиків інформаційної безпеки <i>Манько С.В.</i>	202

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
