БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 1(6)2023 **НАУКОВИЙ ЖУРНАЛ** **ISSN 2707-1758**

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Представлено результати досліджень за такими напрямами: інформаційна та кібернетична безпека, комп'ютерні науки та інформаційні технології, інформаційно-комунікаційні системи, телекомунікації та радіотехніка.

Для науковців, докторантів, аспірантів, фахівців відповідних напрямів, студентів.

Адреса редколегії

вул. Богдана Гаврилишина, 24, Київ, 04116, Україна
☎ факс (+38044) 481 44 07, e-mail: fit@univ.net.ua

Затверджено

Вченою радою факультету інформаційних технологій Київського національного університету імені Тараса Шевченка 24.04.23 (протокол № 10)

Зареєстровано

**Міністерством інформації України.
Свідоцтво про державну реєстрацію
КВ № 23831-13671Р від 15.03.2019**

Засновник і видавець

**Київський національний університет імені Тараса Шевченка, Видавничо-поліграфічний центр "Київський університет".
Свідоцтво внесено до Державного реєстру
ДК № 1103 від 31.10.02**

Адреса видавця

**ВПЦ "Київський університет",
б-р Тараса Шевченка, 14, м. Київ, 01601, Україна
☎ (38044) 239 31 72, 239 32 22; факс 239 31 28**

INFORMATION SYSTEMS AND TECHNOLOGIES SECURITY

№ 1(6)2023 **SCIENTIFIC JOURNAL** **ISSN 2707-1758**

TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV

The scientific publication presents the results of research in such areas as Information and Cyber Security, Computer Science and Information Technology, Information and Communication Systems, Telecommunications and Radio Engineering.

For scientists, doctoral students, graduate students, specialists, students.

ЗМІСТ

ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

КОМП'ЮТЕРНІ НАУКИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

CONTENTS

INFORMATION AND CYBER SECURITY

COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES

INFORMATION AND COMMUNICATION SYSTEMS

ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

УДК 004.621.68
DOI 10.17721/ISTS.2023.1.5-12

Микола Браіловський, orcid.org/0000-0002-3148-1148,
bk1972@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна,
Володимир Хорошко, orcid.org/0000-0001-6213-7086,
professor_va@ukr.net
Національний авіаційний університет, Київ, Україна

МЕТОДИ ДЕСТРУКТИВНОГО ВПЛИВУ ТА ЗАХИСТУ КОНТЕНТУ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розглянуто актуальну тему захисту суспільства від деструктивних впливів у соціальних мережах. Доведено, що для запобігання подібним впливам, необхідно оцінювати не тільки матеріали, що містяться в текстах, аудіо- та відеоконтентах, а й тональність інформації, що поширюється в них. Тональність є однією з характеристик думки або емоції і нині використовується як основний параметр для класифікації текстів за тематичними категоріями. Це пояснюється зручністю й ефективністю класифікації за цим принципом та значно спрощує інші завдання з класифікації текстових постів. Сформовано категорії тональної оцінки. Доведено можливість оцінювання настрою за одновимірним або багатовимірним параметром. Показано можливість використання для класифікації тональності тексту двох підходів. Перший – це автоматичний аналіз цифрових текстів комп'ютерами з елементами машинного навчання або навчання з учителем. Другий – за допомогою словників (тезаурусів), підключених до програми. Наведено недоліки, які виникають у автоматичних комплексах для визначення тональності. Запропоновано новий алгоритм роботи автоматичних комплексів. Зазначено, якщо якість системи аналізу тональності тексту оцінюється тим, наскільки добре вона узгоджується з думкою людини щодо емоційного оцінювання досліджуваного тексту, то для цього можуть використовуватися такі показники, як точність і повнота. Наведено розрахунки цих параметрів. Під час розгляду публікації, представленої у формі зображення, зазначено необхідність враховувати параметри яскравості, контрасту, а також колірних поєднань, оскільки ці показники потенційно можуть використовуватися розповсюджувачами деструктивного контенту для привернення уваги мережі користувачів. Заявлено, що фотоматеріали можуть містити різні праворадикальні знаки та символи, які можуть стосуватися пропаганди певної забороненої організації чи ідеології. Представлено частоти, завдяки яким можливо дестабілізаційно впливати на організм людини. Проведено аналіз можливих методів впливу на свідомість користувача соціальними мережами.

Ключові слова: *деструктивні впливи аудіо- та відеоконтентів; соціальні мережі; аналіз тональності тексту; методи аналізу.*

1. ВСТУП

Соціальні мережі нині відіграють важливу роль у житті кожної людини. Для них немає кордонів, тому вони об'єднують аудиторію не лише жителів однієї держави, а й усієї планети. За їх допомогою обмінюються різноманітними типами контенту: текстовим, аудіо, фото та відео, що у свою чергу серйозно впливає на світогляд кожної окремої людини. У зв'язку із цим виникає необхідність захисту соціально-інформаційного простору шляхом виявлення деструктивного контенту, який є шкідливим для користувачів та суспільства в цілому [1]. Для запобігання подібним впливам, необхідно оцінювати не тільки матеріали, що містяться в текстах, аудіо- та відеоконтентах, а й тональність інформації, що поширюється в них [2, 3].

2. ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

Аналіз тональності тексту – клас методів контент-аналізу в комп'ютерній лінгвістиці, призначених для автоматичного виявлення емоційно забарвленої лексики в текстах та емоційної оцінки авторів щодо об'єктів, про які йдеться у тексті.

Тональність – емоційне ставлення автора висловлювання до якогось об'єкта, виражене в тексті. Емоційний компонент, виражений на рівні лексеми чи комунікативного фрагмента, називається лексичною тональністю. Тональність усього тексту в цілому можна визначити як функцію лексичної тональності складових його одиниць і правил їхнього поєднання [4].

Тональність є однією з характеристик думки або емоції і нині використовується як основний параметр для класифікації текстів за тематичними категоріями. Це пояснюється зручністю й ефективністю класифікації за цим принципом та значно спрощує інші завдання щодо класифікації текстових постів. Зручність полягає у спрощенні класифікації шляхом зведення її до оцінювання лише одного параметра. Результат визначення класу тексту за настроєм можна уточнити за допомогою інших зазвичай відомих параметрів (наприклад, автора публікації, регіону, в якому вона була написана, спільноти користувачів тощо). Тематичні категорії для класифікації слід визначити заздалегідь. Автор і тема публікації можуть бути відомі, і в цьому випадку головною метою аналізу є визначення їхнього відношення до обговорюваної теми. Якщо автор та/або тема невідомі, то першим завданням є визначення теми обговорення, наступним завданням є оцінювання тональності висловлювань автора, а потім, за потреби, визначення автора публікації [5, 6].

Незважаючи на те, що завдання класифікації зводиться, здавалося б, до одновимірності (визначення одного параметра тексту – його тональності), воно залишається досить складним, оскільки сам параметр може бути як одновимірним, так і векторним, і необхідно вибрати шкалу і правила відповідності її значень. Багатовимірний параметр оцінюється за кількома шкалами. Отже, тональність може відображати як одновимірний емоційний простір, так і багатовимірний. Якщо для відображення емоцій обрано одновимірний простір, то параметр "тональність" може набувати одне з можливих значень n-вимірної шкали. Якщо вибрано багатовимірний простір, то необхідно вибрати основу для цього простору, тобто базові емоції – радість, гнів, страх тощо [5], які перетворюються на шкали оцінок.

Аналіз тональності проводять для того, щоб, по-перше, визначити ставлення автора до предмета обговорення, по-друге, виявити авторську позицію, по-третє, виявити додаткові ознаки думки (наприклад, первинна вона чи запозичена, чи є подібні погляди). Так, у [7] думки поділено на два типи: пряма думка і порівняння.

Безпосередню думку можна формально представити як кортеж [7]:

$$O = (e, f\ op, h, t), \quad (1)$$

де *e (сутність)* – об'єкт настрою, тобто предмет обговорення; *f* (*feature*) – властивості об'єкта тональності (атрибути, частини об'єкта); *op (орієнтація* або *полярність)* – тональна оцінка (емоційна позиція автора щодо згаданої теми); *h (тримач)* – суб'єкт тональності (автор думки); *t (час)* – момент часу, коли була залишена думка.

Порівняння здійснюють відносно будь-яких предметів, явищ, подій або їхніх властивостей. Порівнюють дві або більше думок, кожна з яких може бути представлена як первинна (1). Результатом порівняння є думка про перевагу одного об'єкта над іншим (перевага властивості одного об'єкта над подібною властивістю іншого об'єкта).

Ознакою переваги в тексті є ступені порівняння прикметників, частин мови та морфем (дієслова, прислівники, суфікси тощо). Очевидно, що для різних мов необхідно формувати відповідні набори ознак.

Формальне представлення порівняння залежить від його мети. Наприклад, якщо порівнюють два об'єкти, то формальне представлення може бути таким [7]:

$$C=(O_1, O_2, F, Op, h, t), \quad (2)$$

де O_1, O_2 – об'єкти порівняння; F – набір загальних характеристик, які порівнюються; Op – сукупність уподобань автора думки; h – суб'єкт тональності (автор, тобто той, кому належить ця думка); t – момент часу, в який висловлено порівняльну думку.

Тональну оцінку можна сформувати за такими категоріями [3, 6–8]:

1) позитивна, негативна;

2) позитивна, негативна, нейтральна (відсутність емоційного забарвлення);

3) більше градацій, наприклад, позитивна, середньопозитивна, злегка позитивна, нейтральна, злегка негативна, середньонегативна, негативна.

Оцінювання настрою може здійснюватися за одновимірним або багатовимірним параметром [5, 6, 8].

1. *Класифікація тональності за бінарною шкалою.* Бінарна шкала передбачає дві оцінки: позитивну і негативну. Це найпростіший спосіб класифікації з погляду формалізації завдання, якщо висловлена однозначна думка. Проте автор може висловити свою точку зору, наприклад, аналізуючи об'єкт із різних сторін. Думка може містити ознаки як позитивного, так і негативного емоційного забарвлення. У цьому випадку однозначно оцінити тональність дуже складно і не завжди можливо.

2. *Класифікація тональності за багатовимірною шкалою.* Між полярними оцінками, позитивними та негативними, вводять додаткові градації. Чим більше градацій, тим складніше завдання класифікації. Потрібна поступова класифікація.

Етап 1. Класифікація нейтральної тональності.

Етап 2. Класифікація негативної/позитивної тональності.

Етап 3. Класифікація ступеня позитивності/негативності.

3. *Системи градації (шкалування)* формують шляхом надання різним словам відповідного числа з вибраного інтервалу, наприклад, від мінус 1 до 1. При цьому мінус 1 відповідає найбільш негативній тональності, 0 – нейтральній, а 1 – найбільш позитивній. Тобто кожному слову присвоюється ступінь важливості. Це, по суті, і є формування вектора ваг. Текст, який аналізується, попередньо досліджується за допомогою засобів оброблення мови (інструментів і алгоритмів) з метою виокремлення слів або фрагментів для подальшого оцінювання тональності.

4. *Суб'єктивність/об'єктивність.* Визначення суб'єктивності/об'єктивності тексту – окрема проблема. Складність посилюється тим, що слова або фрази можуть використовуватися в певному контексті. Крім того, слід розрізняти, коли автор цитує чужу думку, з якою він може повністю або частково погоджуватись чи не погоджуватись. Об'єктивним вважається "неупереджений" текст, який не містить судження, а тільки викладає поточний стан речей. Наприклад, стаття новин. Ідентифікацію об'єктивності/суб'єктивності використовують як додатковий етап класифікації змісту: попередньо вилучивши об'єктивні думки (речення), можна отримати точнішу оцінку настрою.

Детальніший аналіз можна провести на основі моделі функції/аспекту. Спочатку встановіть об'єкти (властивості), за якими буде оцінюватися тональність, а потім визначте її якимось чином (наприклад, як функцію). У процесі розв'язування задачі класифікації визначається об'єкт, виокремлюється відповідна йому функція та оцінюється тональність.

Для класифікації тональності тексту використовують два підходи. Перший – це автоматичний аналіз цифрових текстів комп'ютерами з елементами машинного навчання або навчання з учителем [9, 10]. Другий – за допомогою словників (тезаурусів), підключених до програми [11–15]. Відмінності між цими підходами очевидні: перший забезпечує більш точний результат і більший обсяг даних для оброблення, другий – легший у реалізації. Якщо за допомогою другого підходу вдається не повністю завантажувати базу даних, а оптимізувати використання словників, то швидкість оброблення й обсяг оброблених даних можна збільшити.

Усі згадані вище тезауруси були створені для англійської мови. Для української мови подібних розробок практично немає. Тому розглянемо, як приклад, подібні твори для російської мови.

Зараз у Санкт-Петербурзькому державному університеті кафедра математичної лінгвістики розробляє базу даних російською мовою RussNet, подібну до WordNet. Тезаурус RussNet містить 1300 іменників, 1900 дієслів, 1100 прикметників, 200 прислівників. Внутрішньомовна структура мови недостатньо розвинена, тому тезаурус не пов'язаний з Inter-Lingual-Index [16].

Програма Абріаль [17] була розроблена 2004 р. А. І. Пацкіним у Російському науково-дослідному інституті штучного інтелекту з метою аналізу текстів російською мовою. Програма застосовна для широкого кола завдань, включаючи аналіз настроїв, але має істотний недолік: база даних повністю завантажується у віртуальну пам'ять. Тезаурус Роже був використаний як база даних, яка передбачає шість семантичних категорій: абстрактні відносини, простір, матерія, розум, воля, чуттєві та моральні сили. Усередині цих категорій будуються деревоподібні ієрархії підкласів. Для спрощення пошуку слова розташовуються в алфавітному порядку та забезпечуються інформацією про місце в ідеографічній класифікації.

Метрики й інструменти для аналізу деструктивного контенту в соціальних мережах та опис прикладного програмного забезпечення щодо виявлення деструктивного вмісту в постах представлено у [18]. Були зроблені такі кроки: підключення словників, нормалізація слів шляхом стемінгу. Однак основними параметрами у визначенні деструктивності контенту є відгуки користувачів мережі.

Відомі також методи, засновані на пошуку лексичної тональності у тексті за попередньо складеними тональними словниками та правилами з використанням лінгвістичного аналізу, де

спочатку визначається емотивна лексика, а потім текст оцінюється сукупно (наприклад, підсумовуванням значення тональності окремих речень) на основі кількісної шкали, градуйованої від негативної до позитивної оцінки [19]. Для аналізу використовують списки правил, регулярні вирази та спеціальні правила зв'язування тональної лексики в реченні.

Підвищення точності оцінювання тональності тексту можна досягти шляхом введення ваг для термінів. Найбільшу вагу повинні мати терміни, які краще відповідають тематиці тексту [6].

Аналіз показує, що автоматичні комплекси для визначення тональності мають такі недоліки:

- великий обсяг навчальних даних;
- складність навчання та неоднозначність результату навчання: з одного боку, збільшення обсягу навчальних даних дозволяє точніше налаштувати комплекс, з іншого боку, навчання залежить від ходу установки (викладача) і може призвести до різних результатів;
- навчання відбувається за алгоритмом "чорної скриньки", тобто його формалізація неможлива;
- складність складання семантичних словників.

Тому пропонується використовувати автоматизований комплекс оцінювання тональності, який працює за таким алгоритмом:

1) складання списку контенту;
2) формування бібліотек деструктивних конструкцій;
3) завантаження контенту та бібліотек конструкцій;
4) поділ контенту на об'єкти, розділені ключовим словом;
5) порівняння кожного об'єкта контенту з бібліотеками деструктивних конструкцій;
6) згодом записування кількості деструктивних слів у кожному об'єкті контенту до змінної;
7) аналіз і відсоткове оцінювання тональності тексту за такими розділами:
   - антиукраїнська пропаганда;
   - пропаганда екстремізму та тероризму;
   - критика існуючого порядку у країні;
   - розпалювання міжнаціональної ворожнечі;
   - заклики до насильства та суїциду;
   - заклики до повалення влади;
   - підрив духовно-моральних цінностей;
   - пропаганда алкоголізму та наркоманії;
   - інші негативні прояви;
8) візуалізація результату.

Для текстового контенту аналіз базується насамперед на вивченні його структури, а саме наявності та частоти вживання слів, пов'язаних із різними темами деструктивного змісту (ДК) (екстремізм, націоналізм тощо). Важливу роль в аналізі відіграє знакова організація тексту, яка, у свою чергу, включає три компоненти:

- синтактика, яка порівнює різні знакові системи часової послідовності;
- семантика, яка демонструє відношення семантичного значення з пропозиціональним змістом тексту;
- прагматика, яка порівнює текст із його комунікативними установками.

Наступним критерієм може бути визначення емоційного забарвлення тексту. Існують алгоритми автоматизованого оцінювання тональності тексту, в якій значення обчислюється в діапазоні від 0 до 100 %, але це призводить до великого розкиду значень. Тому зручніше використовувати оцінку параметра настрою в діапазоні від 0 до 1, де 1 – позитивна оцінка, тобто вміст не є деструктивним, а 0 – негативна (деструктивна).

Точність і якість системи аналізу тональності тексту оцінюється тим, наскільки добре вона узгоджується з думкою людини щодо емоційного оцінювання досліджуваного тексту. Для цього можуть використовуватися такі показники, як точність і повнота.

Формула для знаходження повноти:

$$Entirety = \frac{CEO}{TNO}, \quad (3)$$

де CEO (*correctly extracted opinions)* – правильно розпізнані думки, TNO (*total number of opinions)* – загальна кількість думок (як знайдених системою, так і не знайдених).

Точність обчислюється за формулою

$$Veracity = \frac{CEO}{TNOFS}, \quad (4)$$

де CEO (*correctly extracted opinions)* – правильно розпізнані думки, TNOFS (*total number of opinions found by system)* – загальна кількість думок, знайдених системою.

Таким чином, точність виражає кількість досліджуваних текстів, речень або документів, в оцінюванні яких думка системи аналізу тональності збіглася з думкою експерта. Причому, згідно з дослідженнями, експерти зазвичай погоджуються в оцінках тональності конкретного тексту в 78,4 % випадків. Тобто програма, яка визначає тональність тексту з точністю 70 %, робить це майже так само добре, як і людина.

У розгляді публікації, представленої у формі/або зображенні, необхідно враховувати параметри яскравості, контрасту, а також колірних поєднань, оскільки ці показники потенційно можуть використовуватися розповсюджувачами деструктивного контенту для привернення уваги мережі, користувачів.

Для визначення яскравості зображення використовують вираз [20]

$$Y = 0{,}299R + 0{,}578G + 0{,}114B. \quad (5)$$

Яскравість зображення виражають як середню яскравість усіх пікселів. Яскравість одного пікселя розраховують за формулою

$$Y = R_p + G_p + B_p,, \quad (6)$$

де Y_p – яскравість пікселя; R_p – червоний колір; G_p – зелений колір; B_p – синій колір; p – індекс числа пікселів.

Тоді фізичну яскравість зображення (видимого), що містить N пікселів, можна обчислити за формулою

$$Y = \frac{1}{N}\sum_{p=1}^{N} 0{,}299R_p + 0{,}578\,G_p + 0{,}114B_p, \quad (7)$$

де Y – яскравість зображення; p – індекс підсумовування; N – кількість пікселів зображення.

Для оцінювання контрастності можна використовувати дисперсію яскравості пікселів зображення:

$$\sigma^2 = \frac{1}{N}\sum_{p=1}^{N}(Y_p - Y)^2, \quad (8)$$

де σ – стандартне відхилення.

Параметри для оцінювання яскравості та контрастності змінюються на інтервалі від [0; 1].

Відношення стандартного відхилення σ до максимально можливого значення яскравості $Y_{\max}$ дозволить виміряти контраст яскравості C:

$$C = \frac{2\sqrt{N}\sum_{p=1}^{N}(Y_p - Y)}{\sum_{p\max=1}^{N} 0{,}299R_{p\max} + 0{,}578\,G_{p\max} + 0{,}114B_{p\max}}, \quad (9)$$

де C – контраст яскравості зображення; $R_{P\max}$, $G_{P\max}$, $V_{P\max}$ – значення R_p, G_p, V_p, що відповідають максимальному значенню яскравості зображення $Y_{\max}$.

Критерій (9) є інтегральним і змінюється в межах від 0 до 1, де 0 – одноколірне зображення, а 1 – найбільш насичене.

Однак, аналізуючи вміст фотоконтенту щодо його помітності, має сенс розглядати значення контрасту яскравості (C) лише в діапазоні від 0,5 до 1, який характеризує зображення, бо завдяки своїй яскравості та контрастності привертають більше уваги користувачів порівняно із зображенням зі значенням параметра від 0 до 0,5.

Згідно з науковими дослідженнями в галузі психології, кольори можуть впливати на сприйняття інформації людиною [21, 22]. З погляду деструктивного впливу на користувача соціальної мережі, особливу увагу слід звернути на такі кольори:

• чорний – деструктивність, придушення, депресія, порожнеча, застосування сили як прояв слабкості й егоїзму;

• червоний – фізичне насильство, нетерпимість, хтивість;

• синій – ідеалізм, фанатизм, субординація.

Основним інструментом поєднання кольорів є коло кольорів [23], сконструйоване таким чином, що поєднання будь-яких кольорів, обраних із нього, добре виглядатиме разом. Головне, правильно використовувати поєднання кольорів.

Відповідно до теорії кольору гармонійні поєднання кольорів виходять:

• із будь-яких двох кольорів, розташованих один навпроти одного на колірному колі;

• у разі використання будь-яких трьох кольорів, рівномірно розподілених на колірному колі з утворенням трикутника;

• у випадку використання будь-яких чотирьох кольорів, що утворюють прямокутник.

Гармонійні поєднання кольорів називають колірними схемами. Ці схеми залишаються гармонійними незалежно від кута повороту, що дозволяє розширити можливі комбінації маніпуляцій свідомістю.

Якщо необхідно на чомусь зосередити увагу користувача, вони використовують техніку з компліментарними або додатковими кольорами. Це будь-які два кольори, один проти одного розташовані на колірному колі. Наприклад, синій і помаранчевий, червоний і зелений. Ці кольори створюють високий контраст, тому їх використовують, коли ви хочете щось виділитися. В ідеалі один колір застосовують як фон, а інший – як акцент.

Класична тріада – це поєднання трьох кольорів, які рівновіддалені один від одного на колірному колі. Наприклад, червоний, жовтий і синій. Схема тріади також має високу контрастність, але більш збалансована, ніж додаткові кольори. Принцип тут полягає в тому, що один колір домінує і підкреслюється на фоні двох інших. Така композиція виглядає живою навіть під час використання блідих і ненасичених кольорів.

Крім того, фотоматеріали можуть містити різні праворадикальні знаки та символи, які стосуються пропаганди певної забороненої організації чи ідеології. Це може бути як відомий символ свастики або якихось рун, так і менш відомі знаки, які є символами заборонених екстремістських організацій. Крім того, це можуть бути кількісні символи, якими користується певна група людей. Усе вказане пов'язано з тим, що в багатьох країнах заборонено діяльність деяких неонацистських організацій, а в громадських місцях заборонено демонструвати символіку праворадикальних активістів. Щоб обійти ці заборони, екстремістські групи й окремі особи використовують шифри для передачі своїх повідомлень та уникнення судового переслідування.

Такий спосіб обману завжди можна зустріти на футбольних стадіонах, де вболівальники носять футболки або вивішують плакати з подібними шифрами. Цифри часто належать до порядкового значення букв в алфавіті. Наприклад, найчастіше вживають цифри 14, 18, 28 і 88 або їхню комбінацію, що є закодованим гаслом білих нацистів, яке часто використовують як привітання, і досить часто його зустрічаємо в інтернеті.

Аудіоконтент теж має особливості. Перш за все, варто зазначити, що люди можуть сприймати аудіоконтент на ходу, що дозволяє довготривало впливати на користувача.

Відомо, що низькочастотні звуки, близькі до нижньої межі зони чутності, можуть викликати дискомфорт, страх, занепокоєння і навіть паніку, якщо діють на людину досить довго і з необхідною інтенсивністю [24].

У таблиці наведено кілька прикладів впливу на людину звуку певних частот.

Таблиця

Залежність стану людини від несучої частоти

Значення несучої частоти, Гц	**Вплив на людину**
1–2	Серцебиття
41	Підвищення рівня метаболізму
62	Збільшення фізичної сили
131, 147, 165–169	Важка депресія
170–185	Дискомфорт
196, 247	Комфортний стан
333	Натхнення
349, 698	Любов
440, 880	Уява
523	Бар'єр страху

Яскравим прикладом звукового впливу є відома гра, яка має різні назви: "Тихий дім", "Розбуди мене о 4:20", "Море китів", "U19", "F57", "Синій кит" та ін. Можливо, сама назва пов'язана зі співом кита. Частота звуку, який видає синій кит, становить від 8 до 20 Гц, він не чутний людським вухом, але викликає занепокоєння, паніку і страх. За даними ЗМІ, завдання з 30 по 49 у цій грі пов'язані саме з прослуховуванням звуків певної частоти та нанесенням собі фізичної травми різанням. У цьому контексті видається цілком очевидним, що на учасників гри – дітей – вплинули, змушуючи їх слухати низькочастотний спів китів.

Тексти пісень також можуть становити загрозу. Його слід аналізувати за методами, наведеними вище. Тут постає додаткове завдання розпізнавання слів у аудіоконтенті.

Оцінювання відеоконтенту є найскладнішим, оскільки відеоматеріали є поєднанням текстового контенту, аудіоконтенту та зображень, які динамічно змінюються. Тому він повинен не тільки об'єднати всі перераховані вище показники, але й врахувати швидкість зміни кадрів, тобто різкі переходи від одного зображення до іншого, що супроводжується різними візуальними ефектами.

Однак найважливішим критерієм для будь-якого типу контенту є наявність у публікації ознак забороненого матеріалу. Якщо система виявить подібність цього контенту з відомими негативними матеріалами, його необхідно негайно передати на контент-аналіз.

3. ВИСНОВКИ

Представлені в роботі ознаки первинного оцінювання текстового, аудіо- та відеоконтенту соціальних мереж, а головне, тональність, з якою в них подається інформація, дозволять знизити ступінь суб'єктивності в оцінюванні і тим самим зменшать помилки розпізнавання деструктивного змісту.

Наступним важливим кроком у боротьбі з деструктивним контентом є створення відповідного вітчизняного програмного забезпечення з використанням представлених методів і параметрів, яке має застосовуватися як інструмент для моніторингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Браіловський М. М., & Толюпа С. В. (2021). Проблеми аналізування та прогнозування інформаційно-психологічних впливів у соціальних мережах, міжнар. наук.-практ. конф. *"Інформаційна безпека та інформаційні технології":* матеріали конференції". Харків – Одеса: Харківський нац. екон. ун-т ім. Семена Кузнеця. 99–103.

[2] Yue L., Chen W., Li X., Zuo W., & Yin M. (2018, Jul.). A survey of sentiment analysis in social media. *Knowl. Inf. Syst.*, vol. 60, 617–663.

[3] Tedmori, S., & Awajan, A. (2019). Sentiment analysis main tasks and applications: A survey *J. Inf. Process. Syst.*, vol. 15, no. 3, pp. 500–519.

[4] Stefano B. (2010). Sentiwordnet 3.0: An enhanced lexical resource for sentiment analysis and opinion mining, *Proceedings of LREC :conference*, pp. 2200–2204.

[5] Pang, B., & Lee, L. (2004). A Sentimental Education: Sentiment Analysis Using Subjectivity Summarization Based on Minimum Cuts // *Proceedings of the Association for Computational Linguistics (ACL)* : article, pp. 271–278.

[6] Liu, B. (2010). Sentiment Analysis and Subjectivity. Eds.: N. Indurkhya, F. J. Damerau. *Handboor of Natural Language Processing*, pp. 38.

[7] Pang, B., & Lee, L. (2008). Opinion Mining and Sentiment Analysis. *Foundations and Trends in Information Retrseval*, 2. 16–17.

[8] SenticNet (2009). http://sentic.net/about/.

[9] Cambria, E., Poria, S., Bajpai, R., & Schuller, B. (Dec. 2016). SenticNet 4: A semantic resource for sentiment analysis based on conceptual primitives. *In Proc. 26th Int. Conf. Comput. Linguistics, Tech. Papers (COLING).* Osaka, Japan: The

COLING 2016 Organizing Committee, pp. 2666–2677. https://www.aclweb.org/anthology/C16-1251.

[10] Gatti, L., Guerini, M., & Turchi, M. (Oct. 2016). SentiWords: Deriving a highprecision and high coverage lexicon for sentiment analysis, IEEE Trans. *Affect. Comput.*, vol. 7, no. 4, 409–421.

[11] Гофайзен О. В., & Пилявський, В. В. (2012). Область кольорів, передаваних системами цифрового телебачення. *Цифрові технології*, 11, 47–70.

REFERENCES

[1] Brailovsky M. M., & Tolyupa S. V. (2021). Problems of analyzing and forecasting informational and psychological influences in social networks, International Scientific and Practical Conference [Information Security and Information Technologies]: conference materials. Kharkiv – Odesa: Semyon Kuznets Kharkiv National University of Economics [in Ukrainian].

[2] Yue L., Chen W., Li X., Zuo W., & Yin M. (2018, Jul.). A survey of sentiment analysis in social media. *Knowl. Inf. Syst.*, vol. 60, 617–663.

[3] Tedmori, S., & Awajan, A. (2019). Sentiment analysis main tasks and applications: A survey *J. Inf. Process. Syst.*, vol. 15, no. 3, pp. 500–519.

[4] Stefano B. (2010). Sentiwordnet 3.0: An enhanced lexical resource for sentiment analysis and opinion mining, *Proceedings of LREC :conference*, pp. 2200–2204..

[5] Pang, B., & Lee, L. (2004). A Sentimental Education: Sentiment Analysis Using Subjectivity Summarization Based on Minimum Cuts // *Proceedings of the Association for Computational Linguistics (ACL)* : article, pp. 271–278.

[6] Liu, B. (2010). Sentiment Analysis and Subjectivity. Eds.: N. Indurkhya, F. J. Damerau. *Handboor of Natural Language Processing*, pp. 38.

[7] Pang B., & Lee L. (2008). Opinion Mining and Sentiment Analysis. *Foundations and Trends in Information Retrseval*, 2. 16–17.

[8] SenticNet (2009). http://sentic.net/about/.

[9] Cambria, E., Poria, S., Bajpai, R., & Schuller, B. (Dec. 2016). SenticNet 4: A semantic resource for sentiment analysis based on conceptual primitives. In Proc. 26th Int. Conf. Comput. Linguistics, Tech. Papers (COLING). Osaka, Japan: The COLING 2016 Organizing Committee, pp. 2666–2677. https://www.aclweb.org/anthology/C16-1251.

[10] Gatti, L., Guerini, M., & Turchi, M. (Oct. 2016). SentiWords: Deriving a highprecision and high coverage lexicon for sentiment analysis, IEEE Trans. *Affect. Comput.*, vol. 7, no. 4, pp. 409–421.

[11] Hofeisen, O. V., & Pylyavskyi, V. V. (2012). The range of colors transmitted by digital television systems. *Digital technologies*, 11, 47–70 [in Ukrainian].

Стаття надійшла до редколегії 20.01.2023

Methods of destructive influence and content protection in social networks

The work is devoted to the topical issue of protection of society from destructive influences in social networks. It has been proven that in order to prevent such influences, it is necessary to evaluate not only the materials contained in texts, audio and video content, but also the tone of the information disseminated in them. Tonality is one of the characteristics of thought or emotion and is currently used as the main parameter for classifying texts by thematic categories. This is due to the convenience and efficiency of classification according to this principle and greatly simplifies other tasks for the classification of text posts. Formed categories of tonal assessment. The possibility of assessing mood by one-dimensional or multidimensional parameter is proved. The possibility of using two approaches to classify the tonality of the text is shown. The first is the automatic analysis of digital texts by computers with elements of machine learning or teacher training. The second - with the help of dictionaries (thesauri) connected to the program. The shortcomings that occur in automatic systems for determining the key are given. A new algorithm for automatic complexes is proposed. It is noted that if the quality of the text analysis system is assessed by how well it agrees with a person's opinion on the emotional assessment of the studied text, then such indicators as accuracy and completeness can be used. Calculations of these parameters are given. When considering a publication presented in the form of an image, it is necessary to take into account the parameters of brightness, contrast, and color combinations, as these indicators can potentially be used by distributors of destructive content to attract the attention of the network. users. It is noted that the photo materials may contain various radical signs and symbols that may relate to the propaganda of a particular prohibited organization or ideology. The analysis of possible methods of influence on consciousness of the user by social networks is carried out.

Keywords: *destructive effects of audio and video content; social networks; analysis of the tonality of the text; methods of analysis.*

Микола Браіловський,
канд. техн. наук, доц.
Доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Mykola Brailovsky,
PhD (Engin.), Associate Prof.
Associate Professor of the Department of Cyber Security and Information Protection, Faculty of Information Technologies, Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Володимир Хорошко,
д-р техн. наук, проф.
Професор кафедри безпеки інформаційних технологій Національного авіаційного університету. Київ, Україна.

Volodymyr Horoshko,
Dr. Sci. (Engin.), Prof.
Professor of the Information Technology Security Department of the National Aviation University. Kyiv, Ukraine.

УДК 004.056.5
DOI 10.17721/ISTS.2023.1.13-20

Сергій Бучик, orcid.org/0000-0003-0892-3494,
buchyk@knu.ua
Оксана Хоменко, orcid.org/0000-0002-6821-2240,
ksenyahomenk@gmail.com
Юрій Серпінський, orcid.org/0000-0001-5354-195X,
yuriy.nelkmen@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

СТЕГАНОГРАФІЧНА СИСТЕМА ПРИХОВУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ В АУДІОФАЙЛАХ

Стеганографію аудіофайлів можна використовувати як ефективний і дієвий метод приховування повідомлень. У цій статті представлено вдосконалений підхід до приховування секретної текстової інформації повідомлення в аудіофайлах, що поєднує методи стеганографії та криптографії. Як алгоритм стеганографічного перетворення використано метод найменш значущих бітів (LSB), один із найпоширеніших та основних методів стеганографії. Описана суть цього методу полягає в заміні наймолодших бітів звукового контейнера бітами повідомлення, що містять дуже мало корисної інформації, тому їхнє заповнення додатковою інформацією практично не впливає на якість сприйняття. Такий вагомий недолік, як низький рівень надійності, покращується впровадженням криптографічного шару, доцільність чого обґрунтовано у статті. Криптографічний захист додано у вигляді одного із сучасних симетричних алгоритмів шифрування – алгоритму AES в режимі CBC. Для створення стійкого криптоключа використано псевдовипадкові числа. Алгоритм застосовано для захисту повідомлення, що після криптографічного перетворення приховується в аудіофайл за допомогою стеганографічного методу LSB. Проаналізовано основні характеристики стегосистеми. У цій роботі прикладна система стеганографічного захисту інформації в аудіофайлах із використанням криптографічного алгоритму реалізована за допомогою використання середовища Microsoft Visual Studio 2019 та криптографічних бібліотек, мовою програмування обрано C++. У ролі цифрового контейнера використано аудіофайл формату WAV. NIST-тести застосовано для оцінювання стійкості до стегоаналізу, що за результатами є кращою з використанням удосконаленого методу порівняно з класичним підходом LSB. Крім того, стеганографічний алгоритм оцінюється візуально шляхом порівняння початкового аудіофайлу та стегофайлу з прихованим повідомленням. Результати аналізу вказують на відсутність слідів стеганографії. На основі отриманих результатів можна стверджувати про надійність та ефективність використання запропонованого підходу, тому використання LSB-AES техніки може бути запропоновано для забезпечення безпечної передачі даних.

Ключові слова: *стеганографія; шифрування; Least Significant Bit; алгоритм AES-CBC; NIST-тести.*

1. ВСТУП

Для забезпечення конфіденційності застосовують не лише методи криптографії, а й методи стеганографії. Хоча кожна із цих наук має свої сфери застосування, вони можуть поєднуватися для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів) або ж для формування надійної безпечної системи зв'язку [1].

Стеганографія – наука приховування повідомлень, але не шляхом їхнього перетворення на щось нерозпізнаване, як це відбувається у криптографії, а шляхом того, щоб вони залишалися непоміченими [2]. Загалом, стеганографія може використовувати у вигляді контейнерів будь-що від таких цифрових носіїв інформації, як зображення, аудіо та відео, до мережних протоколів еталонної моделі OSI.

У цьому дослідженні увага приділяється лише стеганографії в аудіосередовищі. Застосування стеганографії в аудіо є складним, оскільки слухова система людини (HAS) чутливіша до невеликих змін у аудіоданих, ніж візуальна система людини (HVS) [3].

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Деякі з досліджень, опублікованих в області аудіостеганографії, розглядають набір таких загальних підходів, як *Least Significant Bit (LSB), Echo Hiding, Spread Spectrum (SS), Phase Coding*, розглянутих у [4].

Схема приховування даних у відео- та аудіофайлах, запропонована в [5], використовує 4LSB та алгоритм фазового кодування для збереження якості відеофайлу навіть після вбудовування секретних даних. Застосування аудіостеганографії з текстом шифрування потокового шифру RC4 розроблено в [6]. Запропонований підхід [7] до аудіостеганографії використовував комбінацію обчислення коефіцієнта DCT і схеми шифрування AES для покращення безпеки модуля. У [15] запропоновано метод заокруглення значень елементів зображення для модифікації найменшого біта у задачах стеганографічного захисту.

Розроблені стеганографічні методи можна застосовувати як для прихованого зберігання інформації, так і для захисту авторських прав на різноманітні об'єкти інтелектуальної власності шляхом укладення цифрових ідентифікаційних міток і "водяних знаків".

Більшість програмних рішень, де в ролі контейнера використовується звуковий сигнал, пропонує для вбудовування інформації тільки метод LSB, що можна спробувати пояснити складністю реалізації альтернативних методів. Запропонований у цій статті підхід реалізовано комбінацією двох – стеганографічної та криптографічної – технік.

3. МЕТА РОБОТИ

Метою цієї роботи є покращення алгоритму LSB для приховування текстової інформації у звукових файлах шляхом додаткового використання криптографічного методу та псевдовипадкових чисел для створення стійкого криптоключа, а також оцінювання, як удосконалення підходу впливає на основні критерії стеганографічної системи.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У розробленій програмній реалізації вдосконалено один із базових методів стеганографії – техніку Least Significant Bits. Класична інтерпретація методу заміни найменш значущого біта можлива шляхом заміни останніх значущих бітів у контейнері на біти приховуваного повідомлення. Нижче наведено загальні основні кроки техніки LSB [8]: байти аудіофайлу перетворюються на бітову послідовність; усі символи повідомлення перетворюються на еквівалентну двійкову систему; найменш значущий біт аудіо замінюються на біт повідомлення.

Для вдосконалення стеганографічної техніки впроваджено додатковий криптографічний захист у вигляді алгоритму AES-CBC, за яким секретне повідомлення перед убудуванням шифрується на основі криптоключа-пароля.

Алгоритм AES реалізовано в режимі роботи CBC (Cipher Block Chaining), що дозволяє шифрувати повідомлення більшої довжини шляхом сегментування інформації блоками фіксованої довжини і застосуванням до першого сегменту операції XOR із випадковим значенням вектора ініціалізації. Указаний вектор ініціалізації може бути рівним нулю, що не є нерекомендованим з погляду алгоритму. Результат цієї операції зашифрований за допомогою ключа, і, таким чином, маємо новий зашифрований блок. Далі до наступного блоку повідомлення застосовується XOR разом з отриманим на попередньому кроці зашифрованим текстом, що також шифрується для наступних блоків.

Як варіант, значення вектора ініціалізації можна було зробити програмно фіксованим, проте в цьому програмному рішенні його значення генерується під час кожної спроби та використовується для отримання прихованого повідомлення з аудіофайлу в подальшому.

Таким чином, відповідно до рис. 1, на вхід програми подається аудіофайл-контейнер, повідомлення та криптоключ. Вхідний аудіофайл та зашифроване криптографічним алгоритмом повідомлення програмно конвертуються до бінарного представлення. Потім за стеганографічним алгоритмом біти повідомлення замінюють визначені біти вхідного аудіофайлу, що формують вихідний аудіофайл з убудуванням.

Враховуючи, що кожен семпл аудіофайлу містить 1 біт повідомлення, послідовність після вкладення не буде відрізнятися від вихідної за умови, що найменш значущий біт вихідної послідовності збігається з вкладеним бітом інформації. Інакше, значення останнього біта буде з імовірністю 50 % збільшено, або зменшено, на 1.

Процес знаходження прихованого повідомлення, що схематично зображено на рис. 2, є зворотним. Користувачу потрібно знати пароль, вектор ініціалізації (IV). З використанням правильного пароля та значення IV біти повідомлення буде відновлено, розшифровано і перетворено на текстову форму.

Щодо пароля, то він формується на вибір: задається користувачем або, за бажанням, генерується, з використанням псевдовипадкових чисел. Для отримання псевдовипадкового числа поєднано два генератори:

• mersenne twister – "Вихрь Мерсенна", а точніше mt19937, заснований на властивості простих чисел;

• std::random_device – рівномірно розподілений генератор випадкових чисел, для генерації істинно випадкових чисел, що виробляє недетермінований випадкове число.

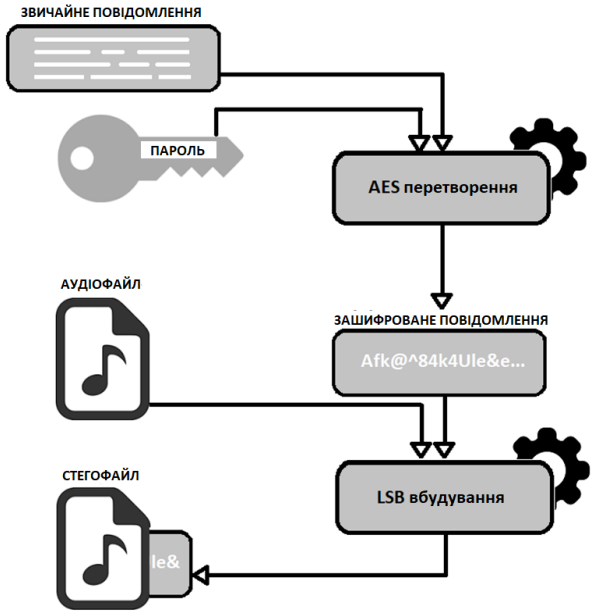


Рис. 1. Схема процесу приховування повідомлення за алгоритмом LSB-AES

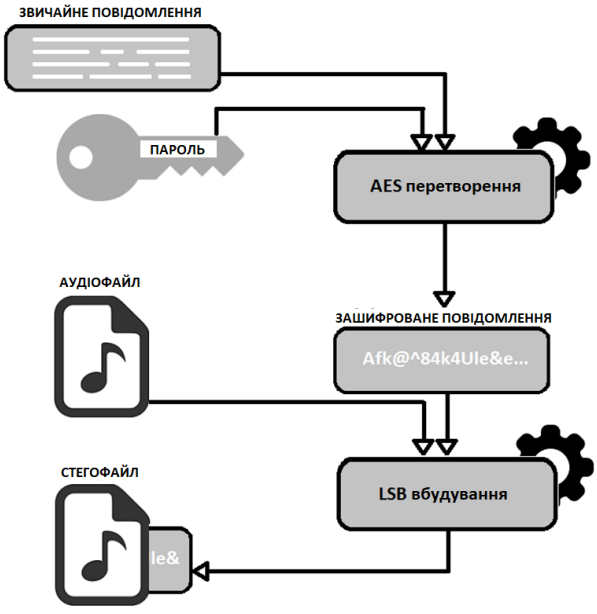


Рис. 2. Схема процесу витягування повідомлення за алгоритмом LSB-AES

У програмі для формування псевдовипадкових послідовностей один ГПВЧ ініціалізується результатом дії іншого ГВЧ (рис. 3), потім згенероване число використовується для генерації пароля.

Згенероване число безпосередньо застосовується для генерації пароля у разі вибору із 6 масивів цифр, англійських літер верхнього та нижнього регістрів, деяких знаків пунктуації чи спеціальних символів із повторенням операції до досягнення обраної довжини пароля.

```
std::random_device rd{};
std::mt19937 mersenne(rd());
```

Рис. 3. Ініціалізація генераторів

Загальний інтерфейс програми, яка була представлена в [14], зображено на рис. 4, 5.

5. ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ

У процесі застосування стеганографії важливими є такі характеристики [9]: пропускна здатність (capacity) – характеризує об'єм секретних даних відносно розміру файлу, в який можна вбудувати контейнер за допомогою визначеного методу; стійкість (robustness) – свідчить про стійкість стегофайлів до навмисних і ненавмисних атак; невидимість (invisibility) – описує схожість заповненого контейнера та пустого, являє собою рівень деградації контейнерів після приховування секретного повідомлення. Дотримання балансу всіх характеристик є важливим та дещо складним для реалізації. Загалом LSB є дуже простим методом і має перевагу у критерії невидимості, але цей метод стає слабким і передбачуваним, якщо виконувати його традиційно.

Пропускну спроможність стегоканалу можна знайти, використавши формулу

$$size = \frac{F}{BPS} - 132, \qquad (1)$$

де F – розмір файлу-контейнера, BPS – кількість байт на семпл (ця програма розрахована на BPS, яке дорівнює 16 байт).

Оскільки відбувається просто заміна молодшого біта, логічним є твердження, що додавання криптографічної складової до методу ніяк не впливає на пропускну здатність створюваного системою захищеного каналу зв'язку, яка може бути збільшена лише у випадках підвищення ступеня заповнення контейнера.

Розроблений стеганографічний інструмент побудовано таким чином, що він не змінює властивості аудіофайлів задля вбудування бітів повідомлення, не залишає жодних підозрілих підписів. Тому у разі аналізу стегофайлу таким способом не можна виявити наявність прихованих повідомлень, і тим більше, ідентифікувати використання саме цієї утиліти, що і є перевагою.

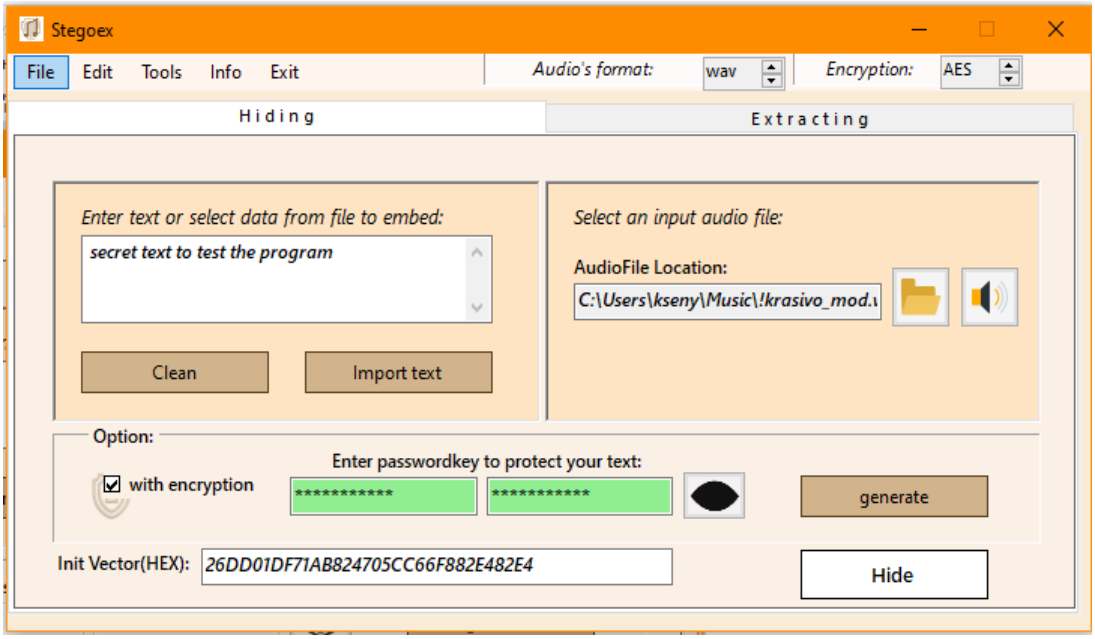


Рис. 4. Загальний інтерфейс прикладної програми. Модуль приховування з прикладом заповнення даних

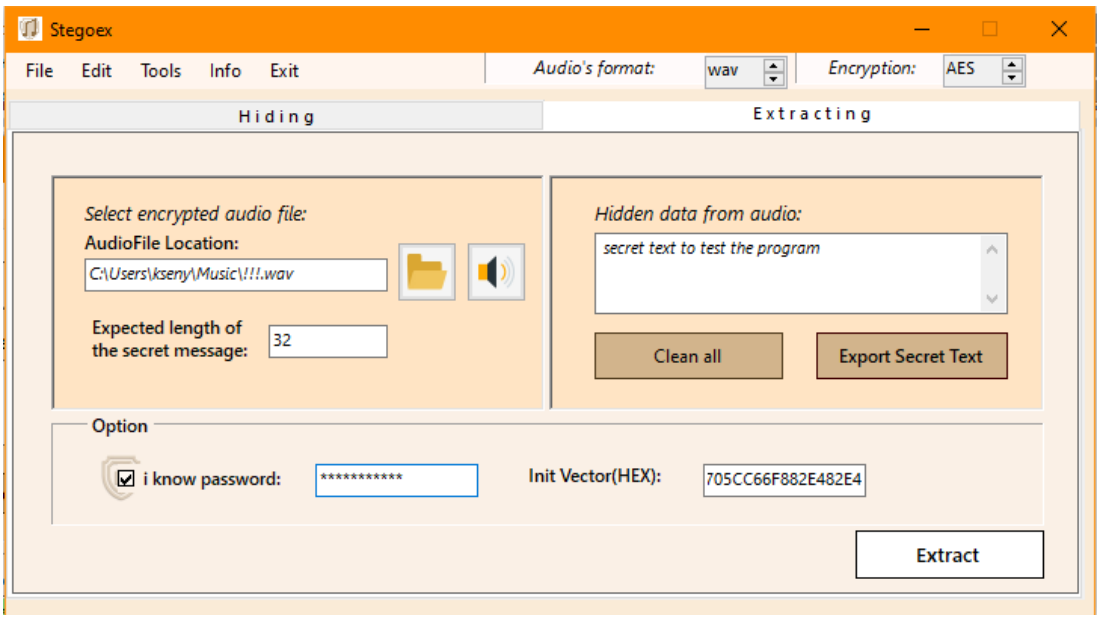


Рис. 5. Загальний інтерфейс прикладної програми. Модуль витягнення з прикладом заповнення даних

Як відомо, молодші розряди містять дуже мало корисної інформації. Їхнє заповнення додатковою інформацією практично не впливає на якість сприйняття. Тому загалом різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини. Якість сигналу збільшується зі збільшенням розміру сигналу, оскільки пропорція відношення бітів сигналу до кількості бітів повідомлення збільшується, таким чином, спотворення зменшується.

Спотворення, що вносяться методом заміни найменш значущого біта в реальному звуковому сигналі, можна візуально виявити шляхом аналізу спектра сигналу. Перевірка чутності спотворень (іншими словами, можливості виявлення вкладень) проводиться візуально за допомогою звукового редактора Audacity 1.3 (рис. 6). На основі порівняння осцилограм можна стверджувати про відсутність прихованих повідомлень.

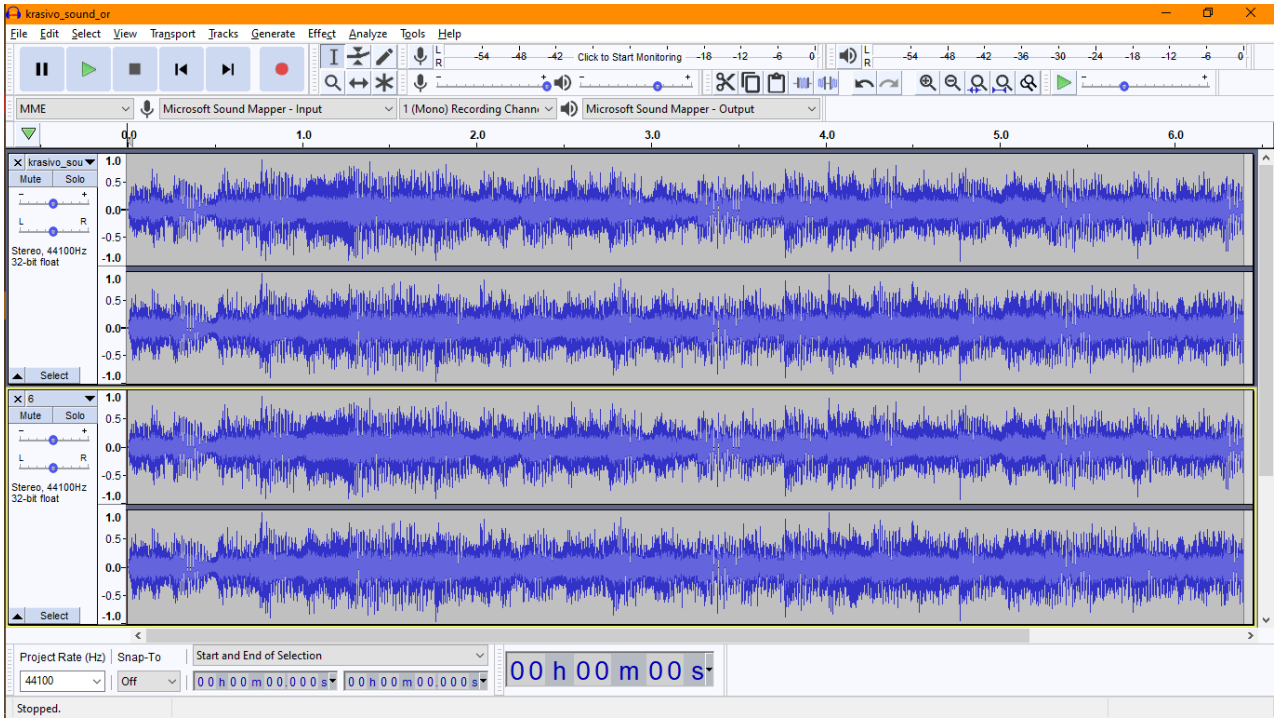


Рис. 6. Осцилограма "пустого" аудіофайлу (зверху) з прихованим повідомленням (знизу)

Основна ідея – використання методу з криптографією замість звичайного в покращенні статистичних властивостей об'єкта, таким чином, цей метод вкладення стає стійкішим, зокрема і до статистичних методів стегоаналізу. Ще більшої стійкості надає використання саме алгоритму AES, що також передбачає вектор ініціалізації, який використовується із секретним ключем аби уникнути повторів у процесі шифрування даних, що робить неможливим для хакерів, що використовують атаку за словником, розшифрувати за-шифроване повідомлення шляхом виявлення шаблона.

Відомо, що існують різні стегоаналітичні методи, у тому числі такі, що засновані на дослідженні статистичних властивостей видобутих повідомлень [10, 11]. Тому для оцінювання стійкості досліджуваного методу вбудовуване повідомлення піддається тестуванню на псевдовипадковість за допомогою так званих NIST-тестів [12], на основі яких розроблене готове рішення [13] використовується в роботі. Ці тести зосереджено на різних типах невипадковості, які можуть існувати в послідовності і їхньою ціллю є визначення міри випадковості отриманих двійкових послідовностей.

Було проведено тестування на псевдовипадковість криптографічно перетвореного повідомлення (рис. 7) та звичайного (рис. 8) завдовжки 40 кб. На основі отриманих результатів можна стверджувати про відсутність стеганографічних вкладень у вбудуванні зашифрованого повідомлення, оскільки кількість успішно пройдених тестів становить більшість, а точніше – 86,67 %, чого не можна сказати про результат тестування для звичайного повідомлення, де цей показник становить лише 20 %.

6. РЕЗУЛЬТАТИ

Варто розуміти, що використання поширених стеганографічних методів знижує ентропію бітів аудіофайлу, що може бути причиною тверджень щодо присутності секретних убудувань. Убудування секретного повідомлення, зашифрованого AES-CBC у аудіосигналі за допомогою методу LSB дозволяє усунути будь-які шаблони, що можуть бути створені у процесі застосування стеганалітичних методів. Попереднє шифрування прихованого повідомлення робить виявлення складнішим, оскільки зашифровані дані зазвичай мають більший ступінь випадковості. Відновлення прихованого повідомлення додає ще один рівень складності порівняно зі звичайним виявленням наявності прихованого повідомлення.

Результати проходження NIST-тестів показують перевагу застосування представленого підходу. Порівнюючи осцилограми, можна помітити візуальну відсутність відмінностей між гістограмами вихідного та стегосигналу.

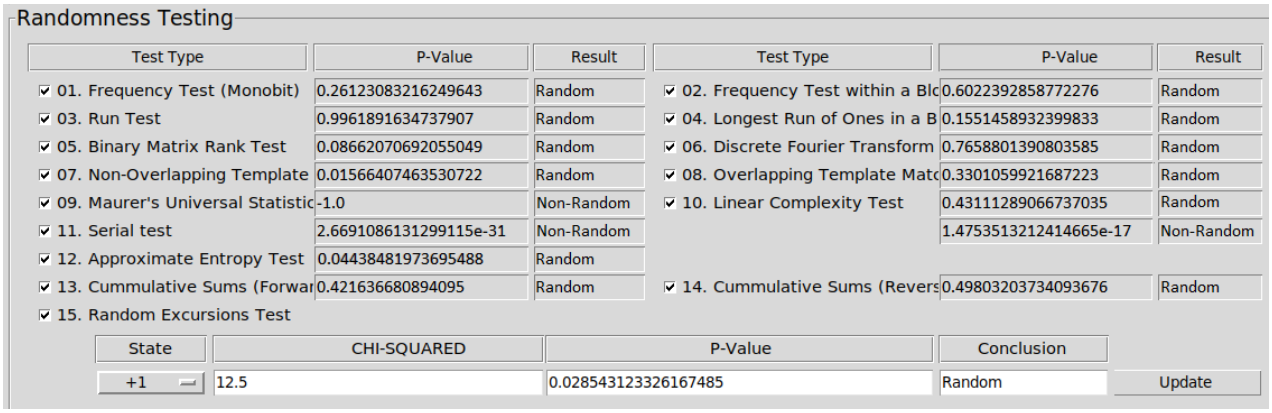


Рис. 7. Результати тестування зашифрованого повідомлення (86,67 % пройдено успішно)

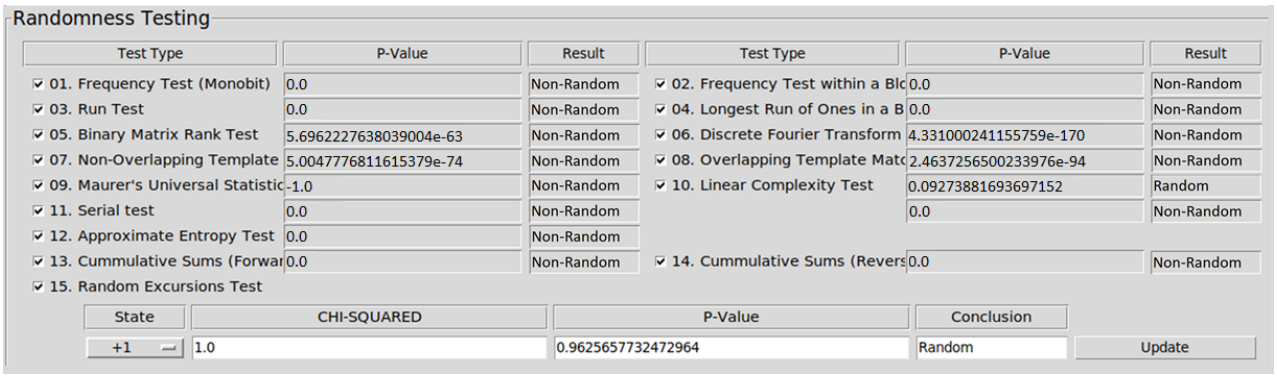


Рис. 8. Результати тестування звичайного повідомлення (лише 20 % пройдено успішно)

7. ВИСНОВКИ

У силу своєї простоти і прозорості реалізації метод LSB широко застосовують у стеганографії. Проте головним недоліком є надійність, яка може бути покращена з використанням надійного криптографічного алгоритму AES для захисту повідомлення. На основі покращеного стеганографічного алгоритму шляхом додаткового використання криптографічного методу розроблено та реалізовано стеганографічну утиліту для приховування текстової інформації у звукових файлах. Зокрема, використання елементів криптографії покращує статистичні властивості, таким чином, цей метод вкладення стає стійкішим до статистичних методів стегоаналізу, як показують результати NIST-тестів. Результати візуального аналізу вказують на відсутність слідів стеганографії. Тому запропонована вдосконалена техніка приховування зашифрованих даних у аудіосигналах характеризується кращою надійністю, що уможливлює її використання для забезпечення безпечної передачі даних між відправником та одержувачем у незахищених мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Hazra, T. K., Samanta, R., Mukherjee, N., & Chakraborty, A. K. (2017). Hybrid image encryption and steganography using SCAN pattern for secure communication. *In 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pp. 370–380. Bangkok.

[2] Katzenbeisser, S., Petitcolas, F. A. P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking (pp. 121–148). Artech.

[3] Basu, P. N., & Bhowmik, T. (2010). On embedding of text in audio-a case of steganography. In Proceedings. *Of International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 203–206.

[4] Navneet, K., & Sunny, B. (2014, May). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International Journal of Engineering Trends and Technology*, *IJETT*, VII(8), 388–392.

[5] Bhagat, V. B., Kulurkar, P. N. (2015). Audio And Video Steganography. *Using Lsb And Phase Encoding Algorithm*, *IJPRET*, vol. 3, no. 9, 1640–1648.

[6] Jian, C. T., Wen, C. C., Binti Ab Rahman, N. H. & Hamid, I. R. B. A. (2017). Audio Steganography with Embedded Text. *IOP Conf.*, vol. 226, no. 1, pp. 1–10.

[7] Bandi, S., & Manjunatha Reddy, H. S. (2019). Combined audio steganography and AES encryption to hide the text and image into audio using DCT. *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, 1732–1738.

[8] Pooyan, M., & Delforouzi, A. (2007, Dec.). LSB-based Audio Steganography Method Based on Lifting Wavelet Transform. *ISSPIT'07*. Egypt.

[9] Al-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., Alanazi, & Overview, H. O. (2010). Main fundamentals for steganography. *J. Comp*, 2(3), 158–165.

[10] Korzhik, V., Fedyanin, I., Godlewski, A., & Morales-Luna, G. (2017). Steganalysis Based on Statistical Properties of the Encrypted Messages. Computer Network Security. MMM-ACNS 2017. *Lecture Notes in Computer Science*, vol. 10446, Springer, Cham. https://doi.org/10.1007/978-3-/319-65127-9_23.

[11] Akhrameeva, K., Korzhik, V., & Nguyen, C. (2020). Detection of Video Steganography with the Use of Universal Method Based on NIST-Tests. *Proc. of Telecom. Universities*, 6(1). 72–78.

[12] National Institute of Standards and Technology (2010), p. 131. (02.01.2023) https://www.nist.gov/publications/statistical-/test-suite-random-and-pseudorandom-numbergenerator-cryptographic.

[13] Python implementation of NIST's A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (02.01.2023) https://github.com/stevenang/ randomness_testsuite

[14] Бучик, С. С., & Хоменко, О. В. (2021, 30 вер.). Прикладна програма приховування текстової інформації в аудіофайлах. *Прикладні системи та технології в інформаційному суспільстві: V Міжнар. наук.-практ. конф.,* К., pp. 27–32.

[15] Buchyk, S., Tolyupa, S. Symonychenko, Y., Symonychenko, A., & Platonenko, A. (2021, January 28). Improvement of Steganographic Methods based on the Analysis of Image Color Models. *Cybersecurity Providing in Information and Telecommunication Systems*, K., 2021, 11–124.

REFERENCES

[1] Hazra, T. K., Samanta, R., Mukherjee, N., & Chakraborty, A. K. (2017). Hybrid image encryption and steganography using SCAN pattern for secure communication. *In 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pp. 370–380. Bangkok.

[2] Katzenbeisser, S., Petitcolas, F. A. P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking (pp. 121–148). Artech.

[3] Basu, P. N., & Bhowmik, T. (2010). On embedding of text in audio-a case of steganography. In Proceedings. *Of International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 203–206.

[4] Navneet, K., & Sunny, B. (2014, May). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International Journal of Engineering Trends and Technology, IJETT*, VII(8), 388–392.

[5] Bhagat, V. B., Kulurkar, P. N. (2015). Audio And Video Steganography. *Using Lsb And Phase Encoding Algorithm, IJPRET*, vol. 3, no. 9, 1640–1648.

[6] Jian, C. T., Wen, C. C., Binti Ab Rahman, N. H. & Hamid, I. R. B. A. (2017). Audio Steganography with Embedded Text. *IOP Conf.*, vol. 226, no. 1, pp. 1–10.

[7] Bandi, S., & Manjunatha Reddy, H. S. (2019). Combined audio steganography and AES encryption to hide the text and image into audio using DCT. *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, 1732–1738.

[8] Pooyan, M., & Delforouzi, A. (2007, Dec.). LSB-based Audio Steganography Method Based on Lifting Wavelet Transform. *ISSPIT'07*. Egypt.

[9] Al-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., Alanazi, & Overview, H. O. (2010). Main fundamentals for steganography. *J. Comp*, 2(3), 158–165.

[10] Korzhik, V., Fedyanin, I., Godlewski, A., & Morales-Luna, G. (2017). Steganalysis Based on Statistical Properties of the Encrypted Messages. Computer Network Security. MMM-ACNS 2017. *Lecture Notes in Computer Science*, vol. 10446, Springer, Cham. https://doi.org/10.1007/978-3-/319-65127-9_23.

[11] Akhrameeva, K., Korzhik, V., & Nguyen, C. (2020). Detection of Video Steganography with the Use of Universal Method Based on NIST-Tests. *Proc. of Telecom. Universities*, 6(1). 72–78.

[12] National Institute of Standards and Technology (2010), p. 131. (02.01.2023) https://www.nist.gov/publications/statistical-/test-suite-random-and-pseudorandom-numbergenerator-cryptographic.

[13] Python implementation of NIST's A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (02.01.2023) https://github.com/stevenang/randomness_testsuite

[14] Buchyk, S. S., & Khomenko, O. V. (2021, September 30). Applied program for hiding text information in audio files, Applied systems and technologies in the information society: V International Scientific and Practical Conference. K., pp. 27–32 [in Ukrainian].

[15] Buchyk, S., Tolyupa, S. Symonychenko, Y., Symonychenko, A., & Platonenko, A. (2021, January 28). Improvement of Steganographic Methods based on the Analysis of Image Color Models. *Cybersecurity Providing in Information and Telecommunication Systems*, K., 2021, 11–124.

Стаття надійшла до редколегії 27.01.2023

Steganographic system for hiding text information in audio files

Audio file steganography can be used as an effective and efficient method to hide messages, but it is a complex process because the human auditory system is sensitive to small changes in audio data. In this article an improved approach for hiding secret text message in audio is presented, combining steganography and cryptography. The Least Significant Bits (LSB) technique, one of the most common and basic methods of steganography, is used as an algorithm for steganographic transformation. The described point of this method is to replace the least significant bits of the audio container with message bits that contain not very useful information, so filling them with additional information has little effect on the quality of perception. Such a significant disadvantage as the low level of reliability is improved by the introduction of a cryptographic layer, the feasibility of which is justified in the article. Cryptographic protection has been added in the form of one of the modern symmetric encryption algorithms – the AES algorithm in the CBC mode. Pseudo-random numbers are used to create a stable cryptokey. The cryptoalgorithm is used to protect the message, which after cryptographic conversion is hidden in the audio file using the steganographic LSB method. The main characteristics of the stegosystem are analyzed. In this paper, the application system of steganographic protection of information in audio files using a cryptographic algorithm is implemented using the environment of Microsoft Visual Studio 2019 and cryptographic libraries, the programming language is C ++. A WAV audio file was used as the digital container. NIST tests were used to assess resistance to stegoanalysis, which according to the results is better using an improved method compared to the classical LSB approach. In addition, the steganographic algorithm is evaluated by visual analysis by comparing the original audio file and the stegofile with the hidden message. The results of the analysis indicate the absence of traces of steganography. Based on the obtained results, it can be argued about the reliability and efficiency of the proposed approach, so the use of LSB-AES technique can be proposed to ensure secure data transmission.

Keywords: *cteganography; encryption; Least Significant Bit; AES-CBC algorithm; NIST tests.*

Сергій Бучик,
д-р техн. наук, проф.
Професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Serhii Buchyk,
Dr. Sci. (Engin.), Prof.
Professor at the Department of Cyber Security and Information Protection, Faculty of Information Technologies Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Оксана Хоменко,
студентка Київського національного університету імені Тараса Шевченка. Київ, Україна.

Oksana Khomenko,
Student of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Юрій Серпінський,
студент Київського національного університету імені Тараса Шевченка. Київ, Україна.

Yuriy Serpinsky,
Student of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

УДК 004.056
DOI 10.17721/ISTS.2023.1.21-27

Наталія Лукова-Чуйко, orcid.org/0000-0003-3224-4061,
lukova@ukr.net
Тетяна Лаптєва, orcid.org/0000-0002-7291-1829,
tetiana1986@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ НЕЛЕГАЛЬНИХ ТОЧОК ДОСТУПУ ДО БЕЗДРОТОВОЇ МЕРЕЖІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Широке використання мобільних пристроїв привело до збільшення підключень до інтернету і розгортання нових бездротових локальних мереж. Згідно з останніми дослідженнями компанії Cisco, до кінця 2023 р. в усьому світі користувачами інтернету стануть 66 % населення Землі. До глобальної мережі будуть підключені більше 28 млрд пристроїв. В останні два десятиліття ми стали свідками народження і розвитку технології, яка істотно змінила нашу роботу і життя, – IEEE 802.11, також відому як Wi-Fi. Технологія Wi-Fi є улюбленим способом підключення до інтернету через простоту використання і гнучкість. Для підключення до бездротової мережі лише необхідно перебувати в радіусі її дії. Тобто споживачі і бізнес будуть усе більше покладатися на мобільні мережі. Однак слід зазначити, що кожна нова можливість цифровізації також дає нові можливості кіберзлочинцям і тому проблема безпеки бездротових мереж нині є однією з головних проблем IT-технологій. Неминуче поширення бездротових мереж і зростаючий трафік у цих мережах, може призвести до безлічі інцидентів інформаційної безпеки. Основні загрози спрямовані на перехоплення, порушення конфіденційності і цілісності переданих даних, здійснення атак на доступність вузлів каналу передачі та їхню підміну. У статті проведено аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації. Удосконалено метод виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності. Проведено натурне моделювання виявлення несанкціонованого втручання в інформаційну бездротову мережу підприємства. Натурне моделювання підтвердило точність локалізації відкритої точки доступу до інформації у мережі Wi-Fi – до 2 м. Це дозволить своєчасно виявляти та локалізувати несанкціоновані точки доступу до інформації у бездротовій мережі підприємств та установ.

Ключові слова: *атака; радіосигнал; метод; загроза; витікання інформації.*

1. ВСТУП

Широке використання мобільних пристроїв привело до збільшення підключень до інтернету та розгортання нових і модернізації існуючих комп'ютерних мереж з акцентом на бездротові локальні мережі – WLAN (Wireless Local Area Network). Упровадження нових стандартів розширило зону покриття з меншими витратами, забезпечуючи водночас мобільність користувачів. Підключення до мережі Wi-Fi є улюбленим способом підключення до мережі інтернету. Для підключення до бездротової мережі лише необхідно перебувати в радіусі дії бездротової мережі.

З кожним днем кількість абонентів, які використовують пристрої з бездротовим виходом в інтернет, безперервно зростає. Згідно з останніми дослідженнями компанії Cisco, до кінця 2023 р. в усьому світі користувачами інтернету стануть 66 % населення Землі. До глобальної мережі будуть підключені більше 28 млрд пристроїв. Тобто споживачі й бізнес будуть все більше покладатися на мобільні мережі. Однак слід зазначити, що кожна нова можливість цифровізації також дає нові можливості кіберзлочинцям, і тому проблема безпеки бездротових мереж нині є однією з головних проблем IT-технологій. Серед усіх загроз безпеці бездротової мережі найсерйозніша – це шахрайські нелегальні точки доступу, які встановлюються зловмисником, без дозволу адміністратора бездро-

тової локальної мережі, з метою використовувати їх для конкурентної розвідки й атак. Загроза нелегальних точок доступу останнім часом стала важливою проблемою безпеки в бездротових локальних мережах.

Тому питання захисту інформаційних бездротових мереж, саме визначення сигналів несанкціонованих точок доступу, з метою виділення сигналів нелегальних точок доступу на фоні легальних радіосигналів бездротових мереж стає дуже гострим. А розроблення нових і вдосконалення існуючих методів виявлення нелегальних точок доступу у локальних бездротових мережах дуже актуальне.

2. МЕТА СТАТТІ

Метою роботи є аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації, а також удосконалення методу виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності.

3. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питанням захисту інформації, розроблення моделей виявлення каналів витікання інформації та засобів нелегального отримання інформації присвячено значну кількість публікацій. Так у роботі [1] розглянуто різні методи перехоплення інформації дешифрування й аналіз Wi-Fi-активності без будь-якого підключення до бездротової мережі. Хакери, намагаючись зламати захист на бездротових маршрутизаторах, можуть використовувати найрізноманітніші методи для отримання доступу до вашої конфіденційної інформації: від ресурсомістких атак грубої сили, що здійснюються за допомогою різних програм із підбору простих "словникових" паролів, до витончених схем соціальної інженерії, таких як фішинг Wi-Fi-паролів шляхом блокування з'єднання та створення підроблених точок доступу, проти яких безсилі навіть найнадійніші паролі. Як тільки облікові дані Wi-Fi будуть отримані, у зловмисників з'являються величезні можливості щодо прихованого захоплення й аналізу мережного трафіка скомпрометованої бездротової мережі. Але сам методологічний апарат не розкривається, методика наведена не в повному обсязі.

У роботах [2, 3] приділяється основна увага злому паролів бездротової мережі. Вразливі мережні пристрої та різноманітні помилки конфігурації роблять цей спосіб досить простим для зловмисника. Проникнувши в мережний периметр, порушник зможе розвинути атаку й отримати доступ до корпоративних ресурсів і критичних сфер інфраструктури. Дослідження безпеки Wi-Fi дозволить оцінити рівень захищеності бездротових мереж, знайти та усунути наявні проблеми. Проте методів виявлення каналів витікання інформації та локалізації можливих місць витікання інформації не наводиться.

У роботах [4–7] наведено можливі сценарії, які будуються на найбільш поширених векторах атак: безпосередньо на точки доступу; на канал взаємодії точки доступу з клієнтом (перехоплення та розшифрування трафіка); на процес аутентифікації (викрадення аутентифікаційних даних користувачів). Методологію припинення сценарію цих атак не наведено, методи виявлення вторгнень у бездротову мережу не розглянуто.

У роботах [8, 9] розглядається організація підроблених точок доступу, вихід із гостьової Wi-Fi-мережі в корпоративну або експлуатація вразливостей небезпечних протоколів автентифікації – лише частина можливих атак із арсеналу зловмисників, які експлуатують бездротові мережі. Тому завершеного характеру робота не отримала.

У роботі [10] доводиться, що зловмисник, метою якого є атака на корпоративну інфраструктуру, крім достатнього рівня кваліфікації може мати у своєму розпорядженні набір спеціалізованих інструментів. У його арсеналі можуть бути потужні Wi-Fi-адаптери для роботи в різних частотних діапазонах, антени, мікрокомп'ютери для створення підробленої точки доступу, обладнання для прихованого аналізу бездротових мереж і різноманітне програмне забезпечення, що дозволяє активно аналізувати безпеки Wi-Fi-мереж. Тобто більше уваги приділено апаратно-програмній частині атак, а не методу виявлення нелегального вторгнення.

У роботах доводиться, що атака на Wi-Fi точки доступу з глобальної та локальної мереж є недооцінена проблема. Вона базується на помилках налагоджування обладнання. Як правило, далі налаштування інтернету та Wi-Fi мало хто доходить. Мало хто дбає про те, щоб змінити пароль адміністратора, і вже зовсім одиниці вчасно оновлюють прошивку пристроїв. І всі це безліч пристроїв з обліковими даними admin: password прекрасні видно для сканерів у локальній або глобальній мережі ... (є винятки, наприклад, не видно пристрої із сірими адресами, за NAT тощо. Тобто їх не видно з глобальної мережі, але ніхто не скасовував їх видимість у локальних мережах). І вже є реалізації масової атаки на дефолтні облікові дані та відомі вразливості роутерів: Router Scan by Stas'M. Але це вторгнення у бездротову мережу цілком залежить від кваліфікації як користувача, так і зловмисника. Проблемі виявлення вторгнення у бездротову мережу не приділено уваги.

У цих роботах не повною мірою відображено питання методологічного визначення сигналів несанкціонованих точок доступу до інформації у бездротових мережах підприємств.

Таким чином, нині у практиці і теорії побудови систем захисту інформації у бездротових мережах загострилося протиріччя між необхідністю швидкого й гарантованого визначення та точної локалізації несанкціонованих точок доступу, що працюють на фоні легальних радіосигналів у бездротових мережах, і можливостями існуючих методів, які використовуються для виявлення та блокування нелегальних точок доступу у бездротових мережах.

З урахуванням викладеного вище, розроблення й удосконалення моделей для виявлення та локалізації нелегального отримання інформації на об'єктах інформаційної діяльності є актуальними.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розглядаючи історію виникнення Wi-Fi, слід зазначити, що в основу технології покладено методику передачі даних радіоканалом на частоті 2,4 ГГц із використанням кодування сигналу робочими частотами і спеціальними додатками. Технологія Wi-Fi використовується для організації високошвидкісних бездротових локальних мереж, які працюють у міжнародному неліцензованому діапазоні частот (ISM) 2,4 ГГц і 5 ГГц. Основною перевагою Wi-Fi перед іншими технологіями є висока швидкість передачі інформації – до 1300 Мбіт/с. Тому ця технологія широко застосовується в різних бездротових телеметричних системах і на транспорті. Нині важко знайти іншу подібну за активністю використовувану ділянку радіочастотного спектра, частоти якого використовуються більше ніж діапазон Wi-Fi. Звісно, чим більш використовуваним є діапазон радіочастотного спектра, тим складніше його контролювати й аналізувати. Ця обставина є найвагомішим фактором для вибору зловмисниками середовища з метою маскування роботи своїх точок доступу, призначених для перехоплення інформації обмеженого доступу. Використовуючи для роботи несанкціонованих точок доступу сильно завантажені частотні діапазони бездротових мереж, зловмисник має намір максимально ускладнити їхнє виявлення. Логічно застосовувати для цього загальноприйняті й поширені в цих діапазонах стандарти зв'язку. Але найголовніше – важко відрізнити роботу двох пристроїв, що використовують один і той самий цифровий стандарт зв'язку, без виявлення їхніх унікальних ідентифікаторів (ID). У випадку з Wi-Fi таким ідентифікатором є MAC-адреса. MAC-адреса – це унікальний ідентифікатор мережного інтерфейсу (зазвичай мережної карти) для реалізації комунікації пристроїв у мережі на фізичному рівні. Це унікальний номер, який зберігається у постійній пам'яті, що доступна тільки для читання, і який призначений конкретній мережній карті її виробником. Також унікальним ідентифікатором може бути LLC (Logical link control) – підрівень керування логічним зв'язком – за стандартом IEEE 802 – верхній підрівень канального рівня моделі OSI, який керує передачею даних і забезпечує перевірку і правильність передачі інформації по з'єднанню. У цьому випадку нас цікавить використання технології Wi-Fi, а також вимоги, які необхідно пред'являти до сучасних засобів аналізу мереж Wi-Fi стосовно області пошуку і локалізації несанкціонованих точок доступу для запобігання витікання інформації радіоканалом Wi-Fi.

Актуальність викладеного підтверджується, крім теоретичного обґрунтування, ще і реальними спектрограмами. Реальні спектрограми, що доводять складність визначення несанкціонованих точок доступу існуючими методами, зображено на рис. 1 та 2.

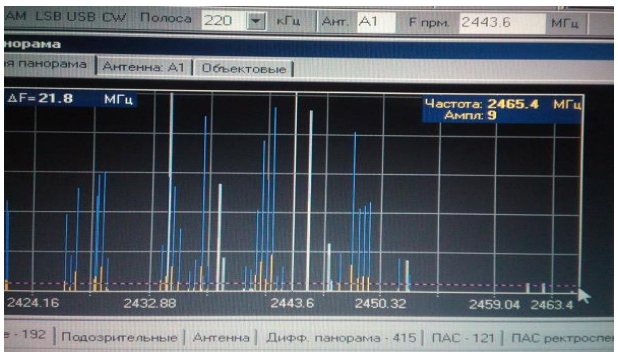


Рис. 1. Спектр сигналів діапазону Wi-Fi, отриманий АПК зі сканувальним приймачем

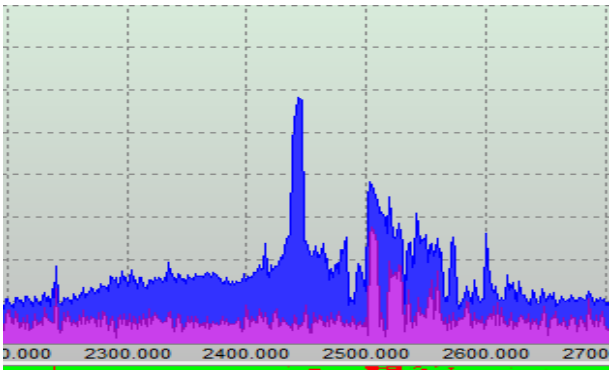


Рис. 2. Спектр сигналів діапазону Wi-Fi, отриманий АПК зі сканувальним приймачем іншого АПК

На рис. 1–3 показано графіки спектрів сигналів, отриманих різними АПК. На рис. 1 та 3 бачимо, що виявити та розпізнати сигнал, який не належить до легальних сингалів, неможливо. Якщо аналоговий сигнал можна виявити за акустичним відгуком, установивши сканувальний приймач на частоту сигналу, то цифровий сигнал так виявити неможливо, тому що він закодований. Замість акустичного сигналу ми будемо чути імпульси цифрового сигналу, без визначення його походження.

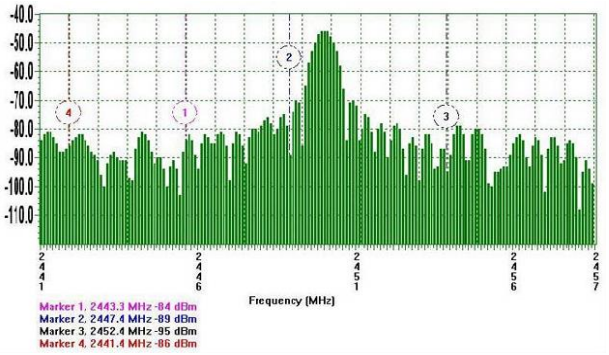


Рис. 3. Спектр сигналів діапазону Wi-Fi, отриманий АПК за допомогою спектр-аналізатора

Отже, сканування цифрового радіодіапазону не дозволить остаточно виявити, а тим більше розпізнати сигнал несанкціонованої точки доступу.

Якщо брати до уваги, що ринок зараз наповнюється високоякісними мініатюрними диктофонами з убудованими Wi-Fi-передавачами, які поєднують у собі диктофон і передавач Wi-Fi, тоді зрозуміло, що цей діапазон буде ще більше завантажуватися.

Беручи до уваги, що у комплекті з Micro Wi-Fi диктофоном поставляється мінімаршрутизатор, який можна конфігурувати так, щоб він автоматично виявляв мережу диктофона, підключався до неї і завантажував аудіозапис, тоді оператору досить наблизитися з ноутбуком із підключеним маршрутизатором на відстань дії мережі Wi-Fi (до 50 м у приміщеннях), щоб завантажити всю накопичену інформацію. Завантаження добового аудіоспостереження, у разі якісного Wi-Fi-з'єднання, з диктофона такого типу займає всього декілька хвилин. Виявити такі пристрої дуже складно. Але таких передавачів частот Wi-Fi, які зовсім не можна виявити, не існує.

Отже, виявити пристрій найімовірніше саме у момент передачі накопиченої інформації по мережі Wi-Fi.

Після тестування такого диктофона, у реальних умовах можна підтвердити основні ТТХ та відмітити його особливості:

1) диктофон може бути виявлено в мережі як точку доступу по SSID. Тут SSID (Service Set Identifier) – унікальний ідентифікатор бездротової мережі, що відрізняє одну мережу Wi-Fi від іншої. У налаштуваннях усіх пристроїв, які повинні працювати в одній бездротовій мережі, має бути зазначений однаковий SSID. Причому SSID можна привласнити будь-яке ім'я;

2) передавання півгодинного запису розмови здійснюється за 30 с.

Це дуже важливе спостереження щодо необхідності повного перегляду концепції моніторингу мереж Wi-Fi. Постійний і безперервний у часі аналіз мереж Wi-Fi тепер стає актуальним, як і постійний радіомоніторинг на об'єктах із наявністю інформації обмеженого доступу.

На нашу думку, велику загрозу мають також Wi-Fi-відеокамери. Як приклад, розглянемо доступну модель Defender MULTICAM WF-10HD. Достатньо розглянути її ТТХ, щоб зрозуміти, що в руках досвідченого зловмисника цей пристрій цілком може стати суттєвою проблемою для фахівців із захисту інформації. Прикладом може бути налагодження з можливістю доступу до камери з будь-якої точки світу через спеціалізований ресурс. У цьому випадку головним є можливість підключення камери до мережі інтернет, що нині виконати не важко. Модифіковані зразки такого типу відеокамер можуть працювати аналогічно прикладу з диктофоном, тобто використовувати передачу по Wi-Fi на короткі відстані.

Проблеми виявлення таких пристроїв виникають з урахуванням можливостей сучасних аналізаторів Wi-Fi, які зазвичай використовуються пошуковими бригадами під час пошукових заходів і в моніторингу контрольованих об'єктів. Більшість аналізаторів із широкими можливостями мають досить великі габарити і прив'язані до комп'ютера. Якщо останній і існує, то у кращому випадку, він розміщений на посту контролю, який може бути значно віддалений від контрольованого приміщення, де зазвичай немає можливості встановити окремий аналізатор.

На підставі викладеного, а також аналізу нових загроз, сформуємо методику пошуку за допомогою автоматизованого програмного комплексу (АПК) мереж Wi-Fi на наявність нелегальних сигналів.

Основою методики виявлення, розпізнавання та локалізації пристроїв і каналів витікання інформації, що працюють у діапазоні Wi-Fi, є аналіз спектральної щільності сигналів. Він базується на

тому, що в активному режимі трансляції інформації спектральна щільність збільшується значно помітніше ніж спектр. Це пов'язано з тим що, залежність спектральної щільності сигналу від звичайного спектра сигналу – квадратична. Тобто зростає значно швидше ніж звичайний спектр.

Оскільки у мережах Wi-Fi завжди використовують маршрутизатори й комутатори, то ці мережі дуже добре захищені та програмно керовані, і проводити перевірку можливо двома способами. Перший, практично відкритий, спосіб – коли всі точки доступу Wi-Fi будуть виключені, тоді "чужі" точки доступу працюватимуть. "Чужі" сигнали дуже просто буде виявити та локалізувати за допомогою запропонованого АПК. Але, якщо потрібно проводити пошукові роботи приховано, тоді цей метод використати неможливо. Потрібно буде застосовувати програмний засіб АПК, що дозволяє аналізувати покриття приміщення, визначати MAC-адреси всіх точок доступу Wi-Fi. Потім цей програмний засіб визначає LLC. На карту приміщення наносить розташування всіх точок доступу та робить карту покриття сигналом Wi-Fi.

Далі аналізує базу MAC-адрес та LLC, виконуючи порівняльний аналіз, виявляє та розпізнає сигнал цифрових засобів негласного отримання інформації.

З огляду на те, що на першому етапі перевірки в базу АПК завантажується, у чіткому масштабі, схематичний план приміщення, визначення "чужого" випромінювання та місце його розташування чітко визначатиметься на схематичному плані приміщення. Алгоритм роботи запропонованого АПК наведено на рис. 4. Слід зазначити, що вказаний алгоритм і наведена методика є частиною цілої методики виявлення, розпізнавання та локалізації цифрових засобів нелегального отримання інформації. Тобто, процес сканування за запропонованою методикою проходить обов'язково, тому що цифровий діапазон складається з багатьох піддіапазонів, деякі вже були розглянуті, а інші розглядатимемо пізніше.

Методика пошуку цифрових засобів нелегального отримання інформації у діапазоні частот мережі Wi-Fi накладає умови, які повинні відповідати таким вимогам:

1. Неперервний (цілодобовий), за допомогою АПК, контроль мережі Wi-Fi усіх стандартів (IEEE 802.11 a / b / g / n) [9], з прив'язкою всіх вимірювань до часу (якщо є така можливість, то контроль приміщень потрібно здійснювати постійно, мати в наявності АПК і спеціаліста із захисту інформації).

2. Пошукові модулі АПК мають бути розміщені безпосередньо в контрольованих приміщеннях (без необхідності установки у приміщенні додаткових ПК) та з'єднані в єдину мережу.

3. Оператор має здійснювати роботи з локалізації мобільно, без необхідності підключення до стаціонарних ПК, накопичений архів даних у цьому разі повинен зберігатися тривалий час.

4. АПК має вести список легальних MAC-адрес для швидкого виявлення й ідентифікації нових передавачів Wi-Fi, та виявляти всі MAC-адреси всіх приладів.

5. Для остаточного виявлення та локалізації цифрових засобів негласного отримання інформації оператору потрібно мати легкий, мобільний та економічний приймальний пеленгаційний модуль. Цей модуль потрібен для розв'язання оперативних завдань.

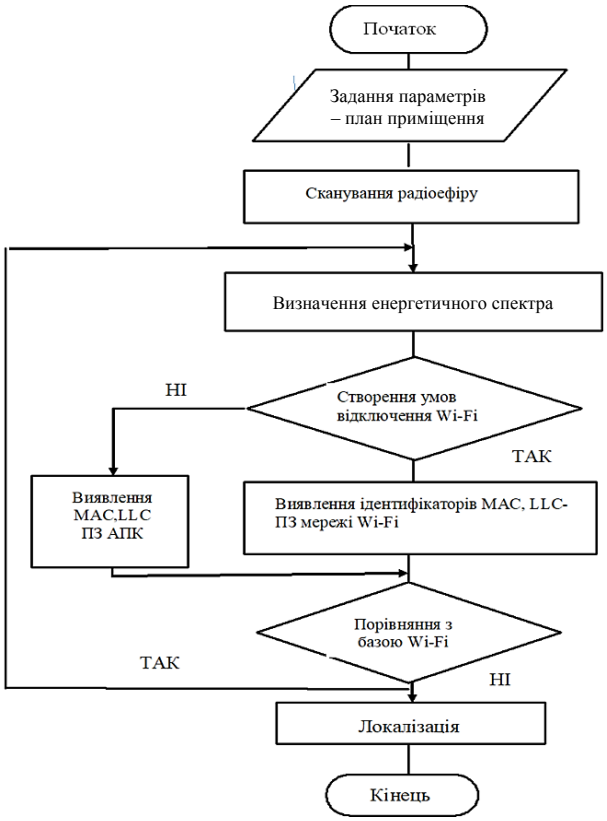


Рис. 4. Алгоритм роботи пошуку цифрових засобів нелегального отримання інформації у діапазоні частот мережі Wi-Fi

Для постійної роботи з протидії незаконним методам отримання інформації необхідна наявність мережного програмного забезпечення, підтримка зонального розміщення необхідної кількості пошукових модулів, які будуть виконувати задачі з пошуку цифрових засобів негласного отримання інформації на постійній основі.

З метою підтвердження алгоритму пошуку цифрових засобів негласного отримання інфор-

мації в діапазоні частот Wi-Fi проведено натурне моделювання пошуку цифрових засобів негласного отримання інформації. Використавши мережне програмне забезпечення, яке імітувало ПЗ АПК, установили імітатори пошукових модулів, це точки доступу Wi-Fi, які були переведені в режим сканування, у лабораторному приміщенні на рис. 5.

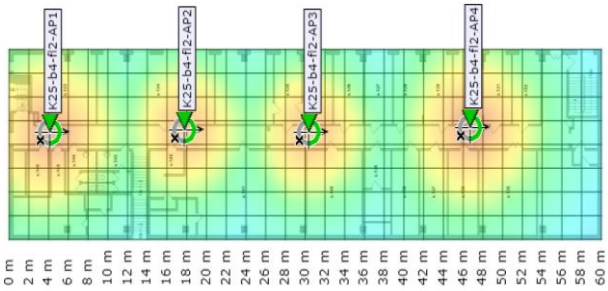


Рис. 5. Приміщення з розташованими пошуковими модулями

Провели сканування приміщення, з метою уточнення розташування пошукових модулів, отримали схему приміщення з рівнем покриття сигналами пошукових модулів (рис. 6).

Далі у лабораторному приміщенні було встановлено нештатний пристрій Wi-Fi. Проведено повторне сканування та отримано схему приміщення, з визначенням "чужого" сигналу. На рис. 6 показано реальну роботу вдосконаленої методики та програмного засобу виявлення, розпізнання та локалізації імітатора цифрових засобів негласного отримання інформації.

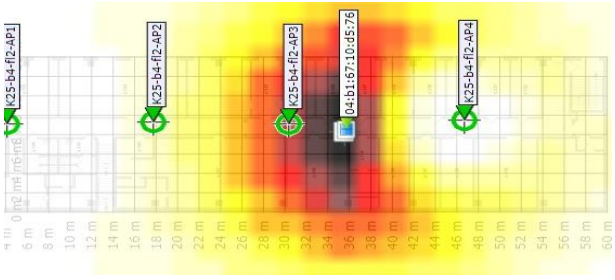


Рис. 6. Схема виявлення імітатора цифрових засобів негласного отримання інформації з використанням запропонованої методики

На рис. 6 темним кольором позначено місце локалізації імітатора цифрових засобів негласного отримання інформації. Отже, одержано результати, які цілком підтверджують запропоновану нами методику пошуку цифрових засобів негласного отримання інформації у цифровому діапазоні Wi-Fi.

Саме таким чином, згідно із запропонованою методикою та за допомогою нових розроблених ПЗ АПК, які можуть виконувати ці завдання, можна виявити й локалізувати цифрові засоби негласного отримання інформації, що працюють під прикриттям легального частотного діапазону Wi-Fi.

5. ВИСНОВКИ

Проведено аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації. Удосконалено метод виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності. Виконано натурне моделювання виявлення несанкціонованого втручання в інформаційну бездротову мережу підприємства. Натурне моделювання цілком підтвердило запропонований нами вдосконалений метод виявлення та локалізації несанкціонованих точок доступу до інформації у бездротовій мережі підприємства. Натурне моделювання підтвердило точність локалізації несанкціонованої точки доступу до інформації у мережі Wi-Fi – до 2 м. Це дозволить своєчасно виявити та локалізувати несанкціоновані точки доступу до інформації у бездротовій мережі підприємств та установ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Барсуков, О. М., Кав'юк, В. В., & Потапенко, В. В. (2018). Виділення аудіосигналу на фоні шуму з використанням методу сингулярного спектрального аналізу. *Системи озброєння і військова техніка,* 1(53). 61–66.

[2] Лаптєв, О. А. (2018). Модель інформаційної безпеки на основі марковських випадкових процесів. *Зв'язок.* К., ДУТ, 6(136). 45–49.

[3] Барабаш, О. В., Лаптєв, О. А., & Зозуля, С. А. (2019). Векторні аналізатори сигналів для удосконалення методики пошуку засобів негласного отримання інформації. *Телекомунікаційні та інформаційні технології.* К., ДУТ, 1. 55–61.

[4] Лаптєв, О. А. (2019). Методика виявлення та локалізації засобів негласного отримання інформації, працюючих у цифровому діапазоні. *Сучасний захист інформації.* К., ДУТ, 2(38). 25–31.

[5] Половінкін, І. М., Лаптєв, О. А., Чумаченко, С. Н., & Гуйда, О. Г. (2019). Визначення основних характеристик випадкових сигналів моделі пошуку засобів негласного отримання інформації. *Вчені записки Таврійського нац. ун-ту ім. В. І. Вернадського*, т. 30 (69), № 6. 101–105.

[6] Павлов, І. М., & Хорошко, В. О. (2013). Функторність і граничність відображень об'єктів множин у системах захисту інформації. *Інформаційна безпека,* 1. 107–116.

[7] Хорошко, В. А. (1999). Вибір критеріїв для оптимізації системи технічного захисту інформації. *Захист інформації: зб. наук. пр.* К., КМУГА, 1999, 7–9.

[8] Хорошко, В. О. Хохлачова, Ю. Є., & Тимченко, М. П. (2017). Оцінка захищеності систем зв'язку. *Системи обробки інформації.* Х., ХНУПС, 2., 134–137.

[9] Лужецький, В. А., & Дудатьєв А. В. (2017). Концептуальна модель системи інформаційного впливу. *Безпека інформації,* т. 23, № 1, С. 45–49.

REFERENCES

[1] Barsukov, O. M., Kavyuk, V. V., & Potapenko V. V. (2018). Isolation of an audio signal against a background of noise using the method of singular spectral analysis. *Weapon systems and military equipment*, 1 (53). 61–66 [in Ukrainian].

[2] Laptev O. A. (2018). Model of information security based on Markov random processes. *Zvyazok: Scientific and practical magazine*., K.: DUT, 6(136). 45–49 [in Ukrainian].

[3] Barabash, O.V., Laptev, O. A., & Zozulya, S. A. (2019). Vector signal analyzers for improving the method of finding means of tacitly obtaining information. *Telecommunications and information technologies: a scientific journal*, K., DUT, 1. 55–61 [in Ukrainian].

[4] Laptev, O. A. (2019). The method of detection and localization of means of secretly obtaining information working in the digital range. *Modern information protection: scientific and technical journal*, K., DUT, 2(38). 25–31 [in Ukrainian].

[5] Polovinkin, I. M., Laptev, O. A., Chumachenko, S. N., & Guida, O. G. (2019). Determination of the main characteristics of random signals of the model of the search for means of obtaining information secretly. *Scientific Notes of V. I. Vernadskyi Tavra National University: jour*., vol. 30(69), no. 6., 101–105 [in Ukrainian].

[6] Pavlov, I. M., & Khoroshko, V. O. (2013). Functority and finiteness of mappings of set objects in information protection systems. *Informational security*, 1. 107–116 [in Ukrainian].

[7] Khoroshko, V. A. (1999). Selection of criteria for optimization of systems of technical protection of information. *Protection of information: a collection of scientific works*, K., KMUGA, pp. 7–9 [in Ukrainian].

[8] Khoroshko, V. O., Khokhlacheva, Yu. E., & Tymchenko, M. P. (2017). Evaluation security of communication systems. *Information Processing Systems*. Kharkiv, KhNUPS, no. 2, 134–137 [in Ukrainian].

[9] Luzhetsky, V. A., & Dudatiev, A. V. (2017). Conceptual model of the system of information influence. *Information security*, vol. 23, no. 1., 45–49 [in Ukrainian].

Стаття надійшла до редколегії 12.02.2023

Improvement of the method of detection and location of illegal access points to the wireless network of information activity objects

Extensive use of mobile devices has led to increased Internet connections and the deployment of new wireless LANs. According to the latest Cisco research, by 2023, 66% of the world's population will be Internet users worldwide. More than 28 billion devices will be connected to the global network. In the last two decades, we have witnessed the birth and development of a technology that has significantly changed our work and life - IEEE 802.11, also known as Wi-Fi. Wi-Fi is a favorite way to connect to the Internet because of its ease of use and flexibility. To connect to a wireless network, you only need to be within range. That is, consumers and businesses will increasingly rely on mobile networks. However, it should be noted that each new opportunity of digitalization also gives new opportunities to cybercriminals and therefore, the problem of security of wireless networks today is one of the main problems of IT technologies. The inevitable proliferation of wireless networks and the growing traffic in these networks can lead to many information security incidents. The main threats are aimed at interception, breach of confidentiality and integrity of transmitted data, attacks on the availability of transmission channel nodes and their substitution.

The article analyzes the existing methods of detecting unauthorized access points to information. The method of detection and localization of unauthorized access points to information circulating in the wireless network at the objects of information activities has been improved. Natural modeling of detection of unauthorized interference in the information wireless network of the enterprise was carried out. Full-scale simulation confirmed the accuracy of localization of an unauthorized point of access to information in the Wi-Fi network – up to 2 m. This will allow timely detection and localization of unauthorized access points to information in the wireless network of enterprises and institutions.

Keywords: *attack; radio signal; method; threat; flow of information*

Наталія Лукова-Чуйко,
д-р техн. наук, проф.
Завідувачка кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Nataliya Lukova-Chuiko,
Dr. Sci. (Engin.), Prof.
Head of the Department of Cyber Security and Information Protection of the Faculty of Information Technologies Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Тетяна Лаптєва,
Аспірантка кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Tetyana Lapteva,
PhD Student Department of Cyber Security and Information Protection of the Faculty of Information Technologies of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

УДК 004.415.056.5(075)
DOI 10.17721/ISTS.2023.1.28-36

Сергій Толюпа, orcid.org/0000-0002-1919-9174,
tolupa@i.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна,
Сергій Штаненко, orcid.org/0000-0001-9776-4653,
shsergei@ukr.net
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ ВЗАЄМОВІДНОСИН СИСТЕМИ КЕРУВАННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Результативне розв'язання задач аналізу і синтезу систем керування інформаційною безпекою не можна забезпечити одними лише способами простого опису їхньої поведінки в різних умовах – системотехніка виявила проблеми, які потребують кількісного оцінювання характеристик. Ті дані, що отримані експериментально або шляхом математичного моделювання, повинні розкривати властивості систем керування інформаційною безпекою. Основним у них є ефективність, під якою розуміють ступінь відповідності результатів захисту інформації поставленій меті. Остання, залежно від наявних ресурсів, знань розробників та інших факторів, може бути досягнута тією або іншою мірою, причому можливі альтернативні шляхи її реалізації. У ряді публікацій авторами запропоновано основи категорійного апарату теорії множин, які дозволяють пояснити процес взаємовідносин множин загроз і множин системи захисту інформації, що дозволяє будувати різні математичні моделі з метою аналізу систем інформаційного обміну в системах критичного застосування. Нині створення систем керування інформаційною безпекою неможливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їхніх складових підсистем, одними з ключових серед яких є системи захисту інформації та протидії вторгненням в інформаційну систему. Складовими математичного забезпечення таких систем є моделі процесів нападу на механізми захисту та блокування або знищення самих кіберзагроз. Базою таких моделей є математичний апарат, який має забезпечити адекватність моделювання процесів захисту інформації за будь-яких умов впливу кіберзагроз. Під час визначення математичного апарату необхідно чітко розуміти, як будуються ті або інші множини кіберзагроз та як здійснюються взаємовідносини самих множин кіберзагроз, множин елементів системи захисту та множин систем виявлення кібератак, які мають контролювати правильність роботи процесу захисту інформації. У статті проаналізовано різні варіанти побудови моделей системи керування інформаційною безпекою та створено математичну модель, яка враховує внутрішні взаємозв'язки різних підмножин складових системи захисту інформації за впливу кіберзагроз.

Ключові слова: *граф, діаграми, кіберзагрози, множини, моделі, функції, підмножини, проєктування, система захисту інформації, керування інформаційною безпекою.*

1. ВСТУП

Процес розвитку й упровадження новітніх інформаційних технологій забезпечує безпрецедентні умови для накопичення і використання інформації, а також створює фундаментальну залежність від їхнього нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем та об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кіберпросторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам й інформаційним системам. Експерти передбачають, що в прийдешньому році повністю зміниться структура кібероперацій і методи їхнього проведення.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів і систем

протидії. Для виявлення мережних вторгнень використовують сучасні методи [1–3], моделі [4, 5], засоби [6–9] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [9–12], які можуть залишатись ефективними у разі появи нових або модифікованих видів кіберзагроз. Проте на практиці під час появи нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди є ефективними і вимагають тривалих часових ресурсів для їхньої відповідної адаптації.

Сьогодні вирішення питань забезпечення безпеки в інформаційних системах (ІС) та керування станом їхньої захищеності описують роботи вітчизняних і зарубіжних дослідників: В. Л. Бурячок, С. О. Гнатюк, О. Г. Корченко, О. О. Кузнецова, І. Ю. Субача, В. О. Хорошко, С. П. Євсеєва, В. Б. Дудикевич, Л. Т. Пархуця, T. Ptaceka, G. Elmasry, P. Albers, O. Camp та ін.

Нині створення систем керування інформаційною безпекою неможливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їхніх складових підсистем, одними з ключових яких є системи захисту інформації та протидії вторгненням в інформаційну систему. Складовими математичного забезпечення таких систем є моделі процесів нападу на механізми захисту та блокування або знищення самих кіберзагроз. Базою таких моделей є математичний апарат, який має забезпечити адекватність моделювання процесів захисту інформації для будь-яких умов впливу кіберзагроз.

2. ПОСТАНОВКА ПРОБЛЕМИ

У визначенні математичного апарату необхідно чітко розуміти, як будуються ті або інші множини кіберзагроз та як здійснюються взаємовідносини самих множин кіберзагроз, множин елементів системи захисту та множин систем виявлення кібератак, які повинні контролювати правильність роботи процесу захисту інформації. У статті запропоновано математичний апарат теорії топосів, який дозволяє на рівні спеціальних категорій будувати моделі для теоретико-множинних конструкцій етапу ескізного проєктування систем захисту інформації [13, 14].

3. ОСНОВНА ЧАСТИНА

Моделлю для множин процесу захисту інформації з повним перекриттям загроз є структура $\mu = \langle A, R, c\rangle$, яка складається з непорожньої множини A (множини процесу захисту інформації у загальному інформаційному процесі), відношення $R = t \times m \times v; R \subseteq A$ (де t – підмножина кіберзагроз, m – множина механізмів захисту, v – множина областей захисту), та c – конкретного індивіду підмножин R, зазначимо, що $c \in A$.

Для формулювання варіантів підходів до створення моделей необхідно ввести обмеження, при якому $m \geq 1, v \geq 1$, при $m = u \times b \times h$; $m \subseteq\subseteq R$ (де u – уразливості бар'єрів захисту, b – бар'єри захисту інформації, h – підсистема аналізу кіберзагроз).

Згідно з інтерпретацією змінних у моделі $\mu \Longrightarrow x$ – вільна функція, яка ставить у відповідність кожному позитивному числу n деякий елемент $x(n)$. Це є μ-оцінкою і представляється у вигляді послідовності $x = \langle \overline{x_1, x_i}\rangle$, i-й член якої – значення змінної v_i, яке дає оцінка x.

Покладемо істинність моделі $\mu \vDash \varphi[\overline{x_1, x_m}]$, якщо $\mu \vDash \varphi[y]$ для деякої (еквівалентним чином, для будь-якої) оцінки y, такої, що $y_i = x_i$ у будь-якому разі, коли v_i входить вільно у φ. Ця модель $\mu = \langle A, R, c\rangle$, вимога φ^m (належне φ число m – кратного добутку), тобто $\varphi^m = \{\langle \overline{x_1, x_m}\rangle : \mu = \varphi[\overline{x_1, x_m}]\}$ являє собою множину всіх m-послідовностей, на яких у моделі μ виконується вимога φ.

Знати множини φ^m для належних m – це знати все про виконання вимог у моделі μ. Причому правила, які визначають виконання для пропорційних зв'язків, відповідають булевим операціям на підмножинах множини A^m. Так, доповнення до φ^m (тобто множина послідовностей, які не задовольняють φ) є множиною послідовностей, які задовольняють ∼φ, перетин множин φ^m іншого перетину множин ψ^m складається з послідовностей, які задовольняють вимогу $\varphi \wedge \psi$. Отже, отримуємо

$$(\sim\varphi)^m = -\varphi^m, (\varphi \wedge \psi)^m = \varphi^m \cap \psi^m,$$
$$(\varphi \vee \psi)^m = \varphi^m \cup \psi^m \text{ і т. п.} \quad (1)$$

Тобто, якщо m є необхідним для φ і ψ числом, то воно буде необхідним і для $\varphi \wedge \psi$.

Розглянемо підоб'єкти і їхні характеристичні стрілки.

Замінимо множину φ^m характеристичною функцією $[\![\varphi]\!]^m : A^m \to 2$, де

$$[\![\varphi]\!]^m(\langle \overline{x_1, x_m}\rangle) = \begin{cases} 1, \text{якщо } \mu \vDash \varphi[\overline{x_1, x_m}], \\ 0, \text{в іншому випадку.} \end{cases} \quad (2)$$

На основі теореми про істинність (якщо топос ε булевий, то $\varepsilon \vDash \alpha \vee \sim \alpha$ для будь-якої пропозиції α) маємо рівняння

$$[\![\sim\varphi]\!]^m = \neg \circ [\![\varphi]\!]^m,$$
$$[\![\varphi \wedge \psi]\!]^m = [\![\varphi]\!]^m \cap [\![\psi]\!]^m (= \cap \circ \langle [\![\varphi]\!]^m, [\![\psi]\!]^m\rangle),$$
$$[\![\varphi \vee \psi]\!]^m = [\![\varphi]\!]^m \cup [\![\psi]\!]^m. \quad (3)$$

Розглянемо квантори підмножин. Припустимо, що φ має вільні тільки змінні v_1, v_2, v_3 і (за умови, що m = 3) функція $[\![\varphi]\!]^3: A^3 \to 2$ вже визначена. Необхідно визначити функцію $[\![\forall v_3 \varphi]\!]^3: A^3 \to 2$. Візьмемо вільну трійку $\langle x_1, x_2, x_3\rangle \in A^3$ і припустимо визначення виконуваності:

$$B_2 = \{x \in A: \mu \vDash \varphi[\overline{x_1, x_3}]\} =.$$

$$= \{x \in A: [\![\varphi]\!]^3(\overline{x_1, x_3}) = 1\}.$$

Із цього визначення слідує, що $\mu \vDash \forall v_3 \varphi[\overline{x_1, x_3}]$ тоді і тільки тоді, коли $B_2 = A$. Тому покладемо

$$[\![\forall v_3 \varphi]\!]^3(\langle\overline{x_1, x_3}\rangle) = \begin{cases} 1, \text{якщо } B_2 = A, \\ 0 \text{ в іншому випадку.} \end{cases}$$

Зіставлення $\overline{x_1, x_3}$ підмножини $B_2 \subseteq A$ визначає функцію $|\varphi|_2^3$ з A^3 у $\mathcal{P}(A)$. Уведемо нову функцію $\forall_A: \mathcal{P}(A) \to 2$, маючи

$$\forall_A(B) = \begin{cases} 1, \text{якщо } B = A, \\ 0, \text{якщо } B \neq A. \end{cases}$$

Тоді функцію $[\![\forall v_3 \varphi]\!]^3$ можна записати у вигляді $[\![\forall v_3 \varphi]\!]^3 = \forall_A \circ |\varphi|_2^3$. Ця функція має вигляд, зображений на рис. 1.

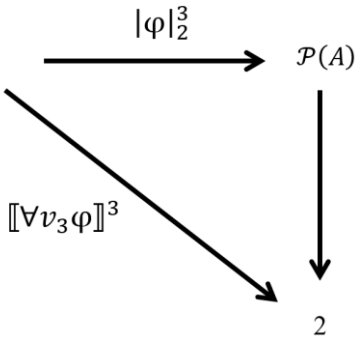


Рис. 1. Граф комутативної діаграми функції $[\![\forall v_3 \varphi]\!]^3$

Необхідно дати категорійне визначення для $\forall_A$. Таке визначення дано в [2], де $\forall_A$ визначається як характеристичне відображення імені функції $true_A$. Тобто визначається $\lceil true_A \rceil: 1 \to 2^A$– ім'я функції $true_A$ – як стрілку (функцію), яка виділяє $true_A$ з множини 2^A. Оскільки $true_A = \chi_A: A \to 2$, ототожнюємо $true_A$ з $\{A\} \subseteq \mathcal{P}(A)$. Характеристичною функцією цього підоб'єкта є $\forall_A$. Функція $\lceil true_A \rceil$ сама є експоненціально приєднаною до композиції, зображеної на рис. 2, де $pr_A(\langle 0, x\rangle) = x$.

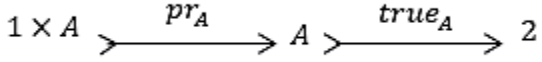


Рис. 2. Категорійне проєктне визначення відображення $|\psi|_2^4$

Таким чином, у рівнянні $[\![\forall v_2 \varphi]\!]^3 = \forall_A \circ |\varphi|_2^3$ через $\forall_A$ визначена характеристична функція підоб'єкта у 2^A, яка визначається вкладенням, експоненціально приєднаним до $true_A \circ pr_A$, а $|\varphi|_2^3$ визначає функцію, експоненціально приєднаною до $[\![\varphi]\!]^3 \circ \langle pr_1^4, pr_4^4, pr_3^4\rangle$.

Для квантора існування аналогічним образом розраховуємо

$$\mu \vDash \exists v_2 \varphi[\overline{x_1, x_3}] \text{ тоді і тільки тоді,}$$

$$\text{якщо } B_2 \neq 0. \quad (4)$$

Тому покладемо

$$[\![\exists v_2 \varphi]\!]^3(\langle\overline{x_1, x_2}\rangle) = \begin{cases} 1, \text{ якщо } B_2 \neq 0, \\ 0 \text{ у іншому випадку.} \end{cases} \quad (5)$$

З (5) випливає, що діаграма графа з рис. 3 є комутативною, де

$$\exists_A(B) = \begin{cases} 1, \text{якщо } B \neq \varnothing, \\ 0, \text{якщо } B = \varnothing. \end{cases} \quad (6)$$

Функція $\exists_A$ є характеристичною для множини

$$C = \{B: B \neq \varnothing\} =$$

$$= \begin{Bmatrix} B: \text{існує } x, \text{який належить } A, \\ \text{такий, що } x \in B \end{Bmatrix}.$$

Якщо $\in_A \hookrightarrow \mathcal{P}(A) \times A$ – відношення належності на A, тобто

$$\in_A = \{\langle B, x\rangle: B \subseteq A \text{ і } x \in B\},$$

і p_A – перша проєкція добутку,

$$\mathcal{P}(A) \times A \text{ у } \mathcal{P}(A): (p_A(\langle B, x\rangle) = B),$$
$$\text{то } p_A(\in_A) = C.$$

Таким чином, $\exists_A$ є характеристичною функцією образу композиції:

$$\in_A \hookrightarrow \mathcal{P}(A) \times A \xrightarrow{p_A} \mathcal{P}(A). \quad (7)$$

Загальне визначення функцій $[\![\forall v_i \varphi]\!]^m$ і $[\![\exists v_i \varphi]\!]^m$ отримуємо підстановкою m замість (4) та i замість (2).

Функцію $[\![t \approx u]\!]^m: A^m \to 2$ визначимо так:

$$[\![t \approx u]\!]^m(\langle\overline{x_1, x_m}\rangle) = \begin{cases} 1, \text{якщо } x_t = x_u, \\ 0, \text{в іншому випадку,} \end{cases}$$

де x – деяка (вільна) оцінка, перші m членів якої збігаються з $\overline{x_1, x_m}$. Таким чином, отримуємо комутативну діаграму графа (рис. 3).

На рис. 3 $p_t^m: A^m \to A, p_u^m: A^m \to A$ і δ_A визначені співвідношеннями:

$$p_t^m(\langle\overline{x_1, x_m}\rangle) = x_t, \quad p_u^m(\langle\overline{x_1, x_m}\rangle) = x_u,$$

$$\delta_A(\langle x, y\rangle) = \begin{cases} 1, \text{якщо } x = y, \\ 0, \text{якщо } x \neq y, \end{cases} x, y \in A.$$

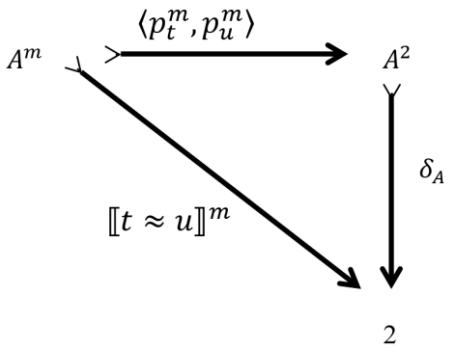


Рис. 3. Граф комутативної діаграми функції $[\![t \approx u]\!]^m$

Функція δ_A є характеристичною функцією тотожного відношення (діагоналі)

$$\Delta = \{\langle x, y\rangle : x = y\} \subseteq A^2.$$

Функція може бути ототожнена з монострілкою $1_A : A \to A^2$, яка переводить x у $\langle x, x\rangle$. Для категорійного визначення p_t^m уведемо функцію $f_c : \{0\} \to A$, покладемо $f_c(0) = c$. Тоді

$$p_t^m = \begin{cases} pr_i^m : A^m \to A, \text{якщо } t = v_i, \\ f_c \circ !: A^m \xrightarrow{1} 1 \xrightarrow{f_c} A, \text{якщо e} = c. \end{cases}$$

Подібні рівняння справедливі і для p_u^m.

Перейшовши до предикатної форми, визначимо через $r : A^2 \to 2$ характеристичну функцію множини $R \subseteq A \times A$. Тоді діаграма на рис. 4 буде комутативною.

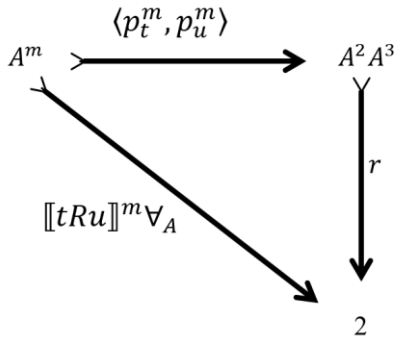


Рис. 4. Граф комутативної діаграми функції $[\![tRu]\!]^m$

Розглянемо наскільки істинна модель і як це можна описати. Нехай формула $\varphi(\overline{v_{i_1}, v_{i_n}})$ має індекс n, тоді визначаючи $[\![\varphi]\!]\mu : A^n \to 2$ умовами

$$[\![\varphi]\!]\mu(\langle \overline{x_1, x_n} \rangle) = \begin{cases} 1, \text{якщо } \mu \vDash \varphi[\overline{x_1, x_n}], \\ 0 \text{ у іншому випадку,} \end{cases}$$

отримуємо: $\mu \vDash \varphi$ тоді і тільки тоді, коли для будь-яких $\overline{x_1, x_n} \in A$ має місце

$$[\varphi]_\mu(\langle \overline{x_1, x_n} \rangle) = 1 \Longrightarrow [\varphi]\mu = \chi_{A^n} \Longrightarrow$$

$$[\varphi]\mu = true A^n.$$

Для опису функції $[\varphi]_\mu$ у вигляді графа визначимо, що існує m – необхідне для φ число, таке, що $\mu \vDash \varphi[\overline{x_1, x_n}]$ тоді і тільки тоді, коли для будь-яких $\overline{y_1, y_m}$ справедливе $\mu \vDash \varphi[\overline{y_1, y_m}]$. Таким чином, для будь-якого f, яке задовольняє рівняння $pr_{i_k}^m \circ f = pr_k^n$ при $1 \le k \le n$, граф діаграми, зображений на рис. 7, буде комутативний.

Цей опис функції $[\varphi]\mu$ придатний для визначення істинності пропозицій, які виникають під час аналізу істинності проєктування впливу загроз на механізми захисту інформації.

Вільний елемент множини A^n, тобто n-членну послідовність, можна розглядати як функцію з ординалу $n = \{0, 1, \dots, n-1\}$ в A. Тому, якщо $n = 0$, то A^0 є множиною функцій з ординалу 0 (початкового об'єкта $\varnothing$) в A. Таким чином,

$$A^0 = A^{\varnothing} = \{\varnothing\} = 1.$$

Якщо індекс φ=0, то $[\![\varphi]\!]_\mu : A^0 \to 2$ є деяким істинним значенням $1 \to 2$; тут

$$[\varphi]_\mu = \begin{cases} true, \text{якщо } \mu \vDash \varphi, \\ false, \text{в іншому випадку.} \end{cases} \quad (8)$$

На основі (8) можна дійти висновку, що для будь-якого $m \ge 1$ і будь-якого $f : 1 \to A^m$ граф діаграми, зображений на рис. 5, є комутативним, і при $\mu \vDash \varphi$ функція $[\![\varphi]\!]^m$ набуває значення 1, якщо не виконуються вимоги, то ця функція набуває значення 0.

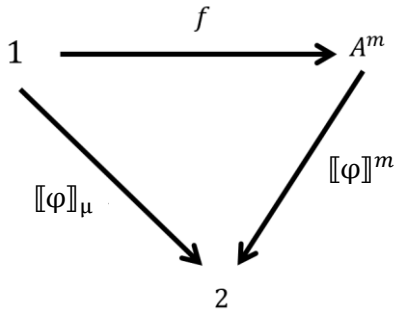


Рис. 5. Загальний граф комутативної діаграми функції $[\varphi]_\mu$ для будь-якого $m \ge 1$ і будь-якого $f : 1 \to A^m$

Звертаючись до моделі системи захисту інформації з повним перекриттям загроз [3], розкриємо порядок впливу загроз на механізми захисту. Для чого визначимо взаємозв'язки між елементами області загроз, механізмами захисту, системою аналізу загроз та областю захисту, як показано на рис. 6, де $t_1, t_2, \dots, t_i$ – загрози з області загроз, $u_1, u_2, \dots, u_d$ – підмножини уразливостей механізмів захисту, $b_1, b_2, \dots, b_d$ – підмножини бар'єрів захисту (фільтрів) ($\overline{1, k}$ – порядковий номер класу механізмів захисту), $h_1, h_2, \dots, h_y$ – підмножин

системи аналізу загроз, $v_1, v_2, \dots, v_j$ – множини областей захисту інформаційної системи.

Усі підмножини тісно взаємно пов'язані між собою.

Якщо об'єднати окремі підмножини у множини (рис. 6), то можна побудувати комутативний граф взаємовідносин множин загроз і підмножин множини системи захисту інформації, який показано на рис. 6.

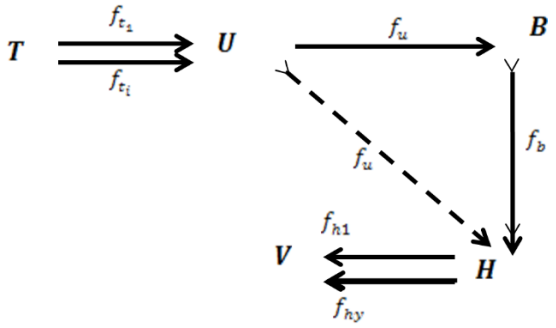


Рис. 6. Комутативний граф взаємовідносин множин загроз і підмножин множини системи захисту інформації

З рис. 7 можна дійти висновку, що згідно з [1] коприрівнювачем пари паралельних β-стрілок f_{t_1}, f_{t_i} є комежа $f_{t_1}, f_{t_i}: \boldsymbol{T} \rightrightarrows \boldsymbol{U}$. Коприрівнювач можна розглядати як таку β-стрілку $f_u: u \to h$ при якій: $f_u \circ f_{t_1} = f_u \circ f_{t_i}$, та будь-яку стрілку $f_u: u \to h$, яка задовольняє рівняння $f_u \circ f_{t_1} = f_u \circ f_{t_i}$, існує одна єдина стрілка $f_b: b \to h$, для якої діаграма комутативна.

У подальшому, розглядаючи місця множини $\boldsymbol{H}$ у системі захисту інформації, згідно з [2], можна побудувати наступний граф, який зображено на рис. 7.

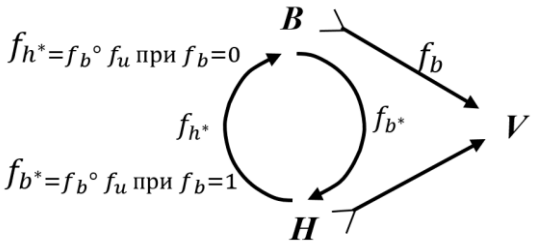


Рис. 7. Діаграма тотожності підмножин при $\boldsymbol{f_b = f_h \circ f_{b^*}}$, $\boldsymbol{f_h = f_b \circ f_{h^*}}$

Якщо $f_b \subseteq f_h$ і$f_h \subseteq f_b$, то f_b і f_h пропускаються один через одного, і $f_b = f_h \circ f_{b^*}$, $f_h = f_b \circ f_{h^*}$.

У цілому, якщо множина $\boldsymbol{M}$ (механізмів захисту) є підмножиною множини $\boldsymbol{A}$ (процесу захисту інформації), то функція включення $M \hookrightarrow A$ ін'єктивна і тому мономорфна. З іншого боку, вільна мономорфна функція $f: U \rightarrowtail B$ визначає підмножину множини $\boldsymbol{B}$, при якій $\mathrm{Im} f = \{f(x): x \in U\}$. Тобто, f індукує бієкцію між U та Im f, далі отримуємо $U \cong \mathrm{Im}\, f$.

Крім того, підмножини системи захисту інформації перебувають, між собою, у взаємозв'язках, які можна описати таким чином:

$$\boldsymbol{U} = \begin{matrix} pr\ t_s^i\left(\langle u_1^1, u_1^2, \dots, u_1^k\rangle\right) = u_1^k; \\ pr\ b_1^w\left(\langle u_2^1, u_2^2, \dots, u_2^k\rangle\right) = u_2^k; \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ pr\ b_2^w\left(\langle u_d^1, u_d^2, \dots, u_d^k\rangle\right) = u_d^k. \end{matrix}$$

$$\boldsymbol{B} = \begin{matrix} pr\ u_1^k(\langle b_1^1, b_1^2, \dots, b_1^w\rangle) = b_1^w; \\ pr\ u_2^k(\langle b_2^1, b_2^2, \dots, b_2^w\rangle) = b_2^w; \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ pr\ u_d^k\left(\langle b_d^1, b_d^2, \dots, b_d^k\rangle\right) = b_d^w. \end{matrix}$$

$$\boldsymbol{H} = \begin{matrix} u_1^k b_1^w \\ u_2^k b_2^w \\ \dots\ \dots \\ u_d^k b_d^w \end{matrix}.$$

Таким чином, область визначення мономорфної функції $\boldsymbol{B}$ ізоморфна деякій підмножині області значень цієї функції $\boldsymbol{U}$. Іншою мовою, область визначення–підмножина u є, з точністю до ізоморфізма, підмножиною області значень – множини b, тобто $f: u \rightarrowtail b$.

У загальному випадку представимо процес захисту інформації, зображений на рис. 6, 7, 8, отримуємо декартовий квадрат, який показано на рис. 9.

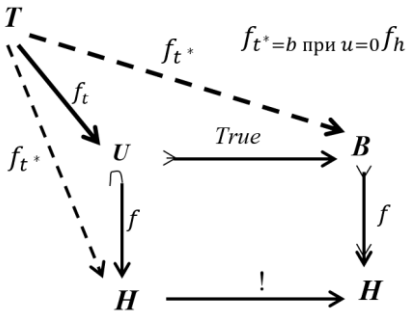


Рис. 9. Комутативна діаграма декартового квадрата

Дійсно, якщо уявити зовнішній "квадрат", як комутативний, тоді, якщо

$$t \in T \text{ і } f\left(f(t)\right) = \mathrm{true}\left(!\,(H)\right) = U,$$
$$\text{то } f(b) \in H, f(u) \in H.$$

Тому при $f_t^*: T \to H, B$, яке визначено рівнянням $f_t(T) = f_{t^*}(T)$, уся діаграма буде комутативною, але при одному f_t. Відповідно, якщо $U \subseteq B$, то квадрат, зображений на рис. 12, декартовий.

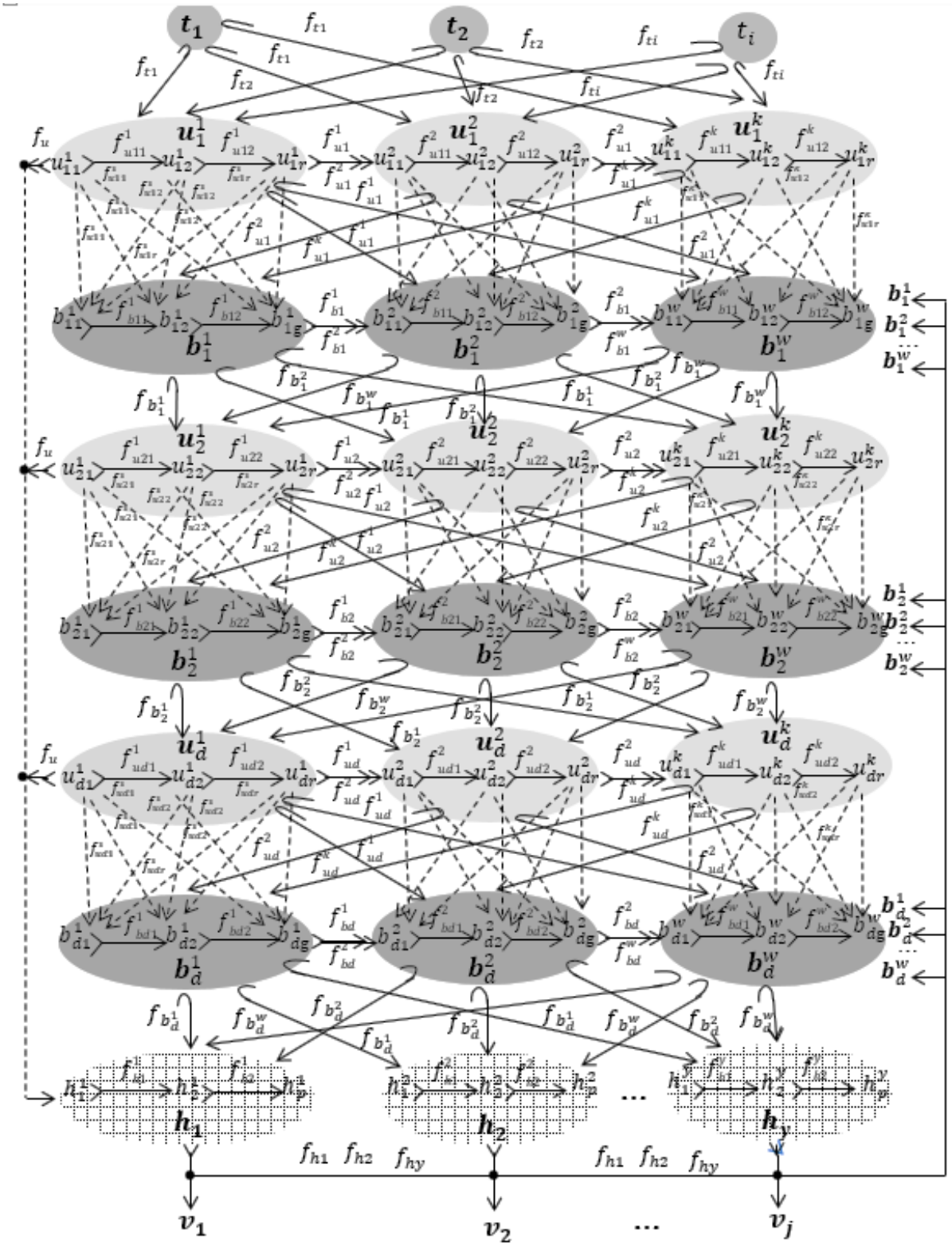


Рис. 8. Проєктна математична модель взаємовідносин множин загроз $t_1, t_2, \dots, t_i$ та множин системи захисту інформації: $u_1, u_2, \dots, u_d$ – уразливостей механізмів захисту, $b_1, b_2, \dots, b_d$ – бар'єрів захисту (фільтрів), $h_1, h_2, \dots, h_y$ – множини підсистеми аналізу загроз, $v_1, v_2, \dots, v_j$ – множини областей захисту інформаційної системи

Відношення еквівалентності на множині $\boldsymbol{H}$ по визначенню – відношення $R \subseteq \boldsymbol{H} \times A$ – має такі властивості:

• рефлективності, тобто aRa для кожного $a \in A$;

• транзитивності, тобто, якщо aRb і bRc, то aRc для будь-яких a, b, c з A;

• симетричності, тобто, якщо aRb, то bRa для будь-яких a і b з A.

Процес ототожнення еквівалентних множин упроваджується в об'єднання цих множин в одну множину у разі поєднання їх одна з одною відношенням еквівалентності. Сукупності, які виникають, розглядаються тут як нові відношення. Формально для $a \in A$ визначається клас R-еквівалентності як множина: $[a] = \{b: aRb\}$ усіх елементів з A, які перебувають у R-відношенні до a.

Одна і та сама множина може бути класом еквівалентності різних елементів. У загальному випадку:

• $[a] = [b]$ тоді і тільки тоді, коли aRb. Тобто два еквівалентні елементи перебувають у відношенні R з однією і тією самою множиною елементів;

• якщо $[a] \neq [b]$, то $[a] \cap [b] = \emptyset$. Тобто два різні класи еквівалентності не мають загальних елементів;

• $a \in [a]$. Тобто кожна $a \in A$ є елементом одного і того самого класу R-еквівалентності.

Процес ототожнення полягає у переході від цієї множини до нової, елементами якої є класи R-еквівалентності, тобто розглядається перехід від множини A до множини

$$A/_R = \{[a]: a \in A\}. \quad (9)$$

Цей перехід виконується за допомогою природного відображення $f_R: A \to A/_R$, де $f_R(a) = [a]$, для $a \in A$.

Якщо aRb, то $f_R(a) = f_R(b)$, тобто функція f_R ототожнює R-еквівалентні елементи.

Функція f_R є коприрівнювачем пари $f, g: R \rightrightarrows A$ функцій проєктування з R до A, тобто тих, які задаються рівняннями

$$f(\langle a, b\rangle) = a \text{ і } g(\langle a, b\rangle) = b. \quad (10)$$

4. ВИСНОВОК

Математична модель проєктних відносин загроз і множин системи захисту інформації дозволяє на рівні математичних множин прогнозувати порядок побудови тих або інших множин або підмножин систем захисту інформації, проводити аналіз правильності побудови цих множин. Запропонований математичний апарат дозволяє з кращим урахуванням практичного застосування визначати загальний порядок побудови структури систем захисту інформації на етапі ескізного проєктування. Це є вхідні дані для системи автоматичного проєктування побудови систем захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі. (2020, 16 червня). У В. В. Литвинов та ін. *Математичні машини і системи.* К., ІПММС НАН України, 2018. 1 (с. 31–40).

[2] Колодчак, О. М. (2012). Сучасні методи виявлення аномалій в системах виявлення вторгнень, *Вісник Національного ун-ту "Львівська політехніка". Комп'ютерні системи та мережі,* 745, 98–104.

[3] Даниленко, Д. О., Смірнов, О. А., Мелешко Є. В. (2012). Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі. *Системи озброєння і військова техніка.* Х., Харківський нац. ун-т Повітряних Сил ім. І. Кожедуба, 1, 92–100.

[4] Al-Sakib Khan Pathan (2014). *The State of the Art in Intrusion Prevention and Detection*. New York, Auerbach Public.

[5] Amrit Pal Singh, Manik Deep Singh (2014). Analysis of Host-Based and Network-Based Intrusion Detection System India. *J. Computer Network and Information Security*, 8, 41–47.

[6] Завада, А. А., Самчишин, О. В., Охрімчук В. В. (2012). Аналіз сучасних систем виявлення атак і запобігання вторгненням. *Інформаційні системи*, Житомир: зб. наук. пр. ЖВІ НАУ, т. 6, № 12, 97–106.

[7] Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas (2012). An implementation of intrusion detection system using genetic algorithm. *International Journal of Network Security & Its Applications (IJNSA)*, Sylhet, vol. 4, no. 2, 109–120.

[8] Lawal, O. B. (2013). Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware. *African Journal of Computing & ICT*, Ibadan, vol. 6, no. 2, 169–184.

[9] Довбешко, С. В., Толюпа, С. В., Шестак, Я. В. (2019). Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації: наук.-техн. журн.*, 1, 56–62.

[10] Toliupa, S., Nakonechnyi, V., Uspenskyi O. (2020). Signature and statistical analyzers in the cyber attack detection system, Information technology and security. *Ukrainian research papers collection*, vol. 7, issue 1(12), 69–79.

[11] Толюпа, С., Штаненко, С., Берестовенко, Г. (2018). Класифікаційні ознаки систем виявлення атак та напрямки їх побудови: зб. наук. пр. Військового ін-ту телекомунікацій та інформатизації ім. Героїв Крут, вип. 3, 56–66.

[12] Toliupa, S., Druzhynin, V., Parkhomenko, I. Signature and statistical analyzers in the cyber attack detection system. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 3(02), 47–53.

[13] Павлов, І. М., Хорошко В. О. (2013). Функторність та граничність відображень об'єктів множин в системах захисту інформації. *Інформаційна безпека*. К., 1(9),107–116.

[14] Павлов І. М. (2013). Альмагами, повнота діаграм та підоб'єкти множин в системах захисту інформації. *Інформатика та математичні методи в моделюванні*. ОНПІ, т. 3. № 1, 50–60.

REFERENCES

[1] Analysis of systems and methods for detecting unauthorized intrusions into computer networks. Retrieved June 16, 2020. In V. V. Litvinov [et al.], *Mathematical machines and systems.* K. IPMMS of the National Academy of Sciences of Ukraine, 2018. 1, 31–40 [in Ukrainian].

[2] Kolodchak, O. M. (2012). Modern methods of detecting anomalies in intrusion detection systems. *Bulletin of the Lviv Polytechnic National University. Computer systems and networks*, 745, 98–104 [in Ukrainian].

[3] Danylenko, D. O., Smirnov, O. A., Meleshko, E. V. (2012). Investigation of methods of detecting intrusions into telecommunication systems and networks. *Armament systems and military equipment.* H.: Hark. national Air Force University named after I. Kozheduba, 1, 92–100 [in Ukrainian].

[4] Al-Sakib Khan Pathan (2014). *The State of the Art in Intrusion Prevention and Detection*. New York, Auerbach Publications.

[5] Amrit Pal Singh, Manik Deep Singh (2014). Analysis of Host-Based and Network-Based Intrusion Detection System India. *J. Computer Network and Information Security*, vol. 8, 41–47.

[6] Zavada, A. A., Samchyshyn, O. V., Okhrimchuk, V. V. (2012). Analysis of modern systems for detecting attacks and preventing intrusions. *Information systems*, Zhytomyr: Collection of scientific works of ZhVI NAU, vol. 6, no. 12, 97–106 [in Ukrainian].

[7] Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas (2012). An implementation of intrusion detection system using genetic algorithm. *International Journal of Network Security & Its Applications (IJNSA)*, Sylhet, vol. 4, no. 2, 109–120.

[8] Lawal, O. B. (2013). Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware. *African Journal of Computing & ICT*, Ibadan, vol. 6, no. 2, 169–184.

[9] Dovbeshko, S. V., Toliupa, S. V., Shestak, Y.V. (2019). Application of intelligent data analysis methods for building attack detection systems. *Scientific and Technical Journal "Modern Information Protection"*, no. 1, 56–62 [in Ukrainian].

[10] Toliupa, S., Nakonechnyi, V., Uspenskyi, O. (2020). Signature and statistical analyzers in the cyber attack detection system, Information technology and security. *Ukrainian research papers collection*, vol. 7, issue 1(12), 69–79.

[11] Toliupa, S., Shtanenko, S., Berestovenko, G. (2018). Classification features of attack detection systems and directions of their construction: Collection of scientific works of the Military Institute of Telecommunications and Informatization named after Heroes Krut, issue 3, 56–66 [in Ukrainian].

[12] Toliupa, S., Druzhynin, V., Parkhomenko, I. Signature and statistical analyzers in the cyber attack detection system. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 3(02), 47–53.

[13] Pavlov, I. M., Khoroshko, V. O. (2013). Functority and finiteness of mappings of set objects in information protection systems. *Information Security*. K., 1(9), 107–116 [in Ukrainian].

[14] Pavlov, I. M. (2013). Almagrams, completeness of diagrams and subobjects of sets in information protection systems. *Informatics and mathematical methods in modeling*. ONPI, vol. 3, no. 1, 50–60 [in Ukrainian].

Стаття надійшла до редколегії 08.03.2023

Mathematical model of system relationships management of information security

An effective solution to the problems of analysis and synthesis of information security management systems can not be provided by simple ways of simply describing their behavior in different conditions - systems engineering solves problems that require quantitative evaluation of characteristics. Such data, obtained experimentally or by mathematical modeling, should reveal the properties of information security management systems. The main one is efficiency, which means the degree of compliance of the results of information protection to the goal. The latter, depending on the resources available, the knowledge of developers and other factors, can be achieved to one degree or another, and there are alternative ways to implement it. In a number of publications the authors propose the basics of the categorical apparatus of set theory, which allows to explain the relationship between sets of threats and sets of information protection system, which allows to build different mathematical models to analyze information exchange systems in critical application systems. At present, the creation of information security management systems is not possible without research and generalization of world experience in building information systems and their constituent subsystems, one of the key of which are information protection and intrusion prevention systems. Components of the process of attacking the mechanisms of protection and blocking or destruction of cyber threats themselves are components of the mathematical support of such systems. The basis of such models is the mathematical apparatus, which should ensure the adequacy of modeling of information security processes for any conditions of cyber threats. When defining the mathematical apparatus, it is necessary to clearly understand how certain sets of cyber threats are built, and how the sets of cyber threat sets, sets of security system elements and sets of cyber attack detection systems, which should control the correctness of the information security process. The article analyzes various options for building models of information security management system and creates a mathematical model that takes into account the internal relationships of different subsets of components of the information security system under the influence of cyber threats.

Keywords: *graph, diagrams, cyber threats, sets, models, functions, subsets, design, information protection system, information security management.*

Сергій Толюпа,
д-р техн. наук, проф.,
Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Serhii Toliupa,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Сергій Штаненко,
канд. техн. наук, доц.
Доцент кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Київ, Україна.

Serhii Shtanenko,
PhD (Engin.), Associate Prof.
Associate Professor of the Department construction of military telecommunication systems. Institute of Telecommunications and Informatization named after Heroes Krut. Kyiv, Ukraine

УДК 004.94:351
DOI 10.17721/ISTS.2023.1.37-42

Сергій Толюпа, orcid.org/0000-0002-1919-9174,
tolupa@i.ua
Лада Сліпачук, orcid.org/0000-0001-9855-0729,
lada.knu@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ФОРМУВАННЯ СИСТЕМИ КІБЕРЗАХИСТУ ДЛЯ ІНТЕГРОВАНОЇ ГАЛУЗЕВОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ УКРАЇНИ СЕКТОРУ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ

Розкрито та висвітлено передбачений склад, структуру заходів і засобів, які увійдуть до комплексної системи захисту інтегрованої галузевої інформаційної системи України (ІГІСУ) сектору національної кібербезпеки. Описано специфіку і стратегічну цінність залучених ресурсів, якими оперуватиме створена система кіберзахисту. Зазначено, що система кіберзахисту ІГІСУ передбачає задіяти комплекс взаємопов'язаних засобів і заходів, виконання яких необхідне й достатнє для повноцінного захисту ІГІСУ, для протистояння зовнішнім несанкціонованим системам доступу (НСД) тощо. Акцентовано увагу на відповідності передбаченої системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для країн НАТО, зокрема і кібербезпековому стандарту міністерства оборони США (TCSEC – "Помаранчева книга"); міжнародним критеріям і стандартам захисту подібних керівних систем інших провідних країн світу, зокрема, міжнародному технічному стандарту ISO/IEC 15408 "Загальні критерії оцінювання безпеки ІТ", який ратифікувало багато країн; настановам і рекомендаціям міжнародної організації NCSS (National Cyber Security Strategies) для країн – партнерів НАТО, що передбачені Стратегією національної кібербезпеки та розроблені міжнародними експертами з питань національної кібербезпеки, науковцями та європейськими радниками з міжнародної кібербезпеки в контексті проєкту Програма НАТО SPS "Наука заради миру та безпеки"; національним технічним стандартам України. У межах цієї статті детально показано повний асортимент загальнообов'язкових ресурсів та інструментів, які передбачені для забезпечення кібербезпеки спроєктованої ІГІСУ сектору національної кібербезпеки, та які включають п'ять рівнів кіберзахисту (організаційний, програмний, апаратно-технічний, інженерно-технічний, додатковий фізичний).

Ключові слова: *система кіберзахисту ІГІСУ сектору національної кібербезпеки; особливість системи кіберзахисту; складові системи кіберзахисту; відповідність системи кіберзахисту.*

1. ВСТУП

Сучасний рівень розвитку технологічного прогресу вимагає від кожної держави, аби автоматизовані керівні системи були дієвими, максимально захищеними та відповідали не лише глобальним викликам, потенційним зовнішнім ризикам цифрового світу та сучасному рівню розвитку ІТ як предметної області, але й задовольняли нагальні потреби сектора національної кібербезпеки як проблемної галузі.

Адже нині сектор національної кібербезпеки являє собою стратегічно важливу для держави макрогалузь, проблематика якої полягає у тому, що назріла нагальна потреба держави у забезпеченні високого рівня керованості сектором національної кібербезпеки, особливо в екстремальних умовах наявності кіберінцидентів. Таку потребу задовольнить спроєктована ІГІСУ сектору національної кібербезпеки, яка, у свою чергу, для безпечного функціонування потребує створення комплексної системи кіберзахисту.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проведений аналіз вітчизняних наукових публікацій, присвячених питанням створення систем захисту керівних систем засвідчив, що вказаний тематичний напрям перебуває у фокусі предмет-

ної уваги таких сучасних вчених: Ю. В. Землянко, О. А. Замула, О. О. Ткач, Н. І. Литвинова, Я. А. Пересічанська, В. В. Домарев, С. В. Ленков, Д. А. Перегудов, В. А. Хорошков, В. А. Герасименко, М. С. Вєртузаєв, О. М. Юрченко [1–5].

3. ПОСТАНОВКА ПРОБЛЕМИ В ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ АКТУАЛЬНІСТЬ

Для забезпечення високого рівня керованості стратегічно важливим для держави сектором національної кібербезпеки синтезовано ІГІСУ сектору національної кібербезпеки, котра, у свою чергу, згідно із чинними державними вимогами, потребує комплексної системи захисту.

Тому така потреба у забезпеченні комплексного кіберзахисту ІГІСУ сектором національної кібербезпеки зумовила вибір теми статті. Саме сформована комплексна система кіберзахисту ІГІСУ сектором національної кібербезпеки і стала фундаментальним ядром і предметом цього дослідження.

4. МЕТА СТАТТІ

Окреслені вище проблеми обумовили мету нашої наукової розвідки, яка передбачає визначення та розроблення комплексної системи для забезпечення захисту ІГІСУ сектору національної кібербезпеки.

5. МЕТОДОЛОГІЧНИЙ АПАРАТ ДОСЛІДЖЕННЯ

Фундаментальним базисом цього дослідження стали структурно-функціональний і системний загальнонаукові підходи.

Додатково використано нормативно-правовий підхід.

6. КОРОТКИЙ ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

ІГІСУ, як і будь-яка вперше запроєктована керівна система державного значення, що містить ІзОД, в обов'язковому порядку, підлягає захисту.

Система кіберберзахисту ІГІСУ сектору національної кібербезпеки має носити комплексний характер.

Причому до складу комплексної системи захисту ІГІСУ сектору національної кібербезпеки передбачено задіяти таку кількість чітко впорядкованих, взаємопов'язаних, сучасних інструментів захисту, сукупність яких:

1) є необхідною та достатньою для повноцінного захисту ІГІСУ як керівної системи, а також для протистояння зовнішнім НСД.

2) дозволить забезпечити максимально високий рівень захисту цілісності, конфіденційності та доступності інформації, яка оброблятиметься в ІГІСУ сектору національної кібербезпеки.

Перелік таких засобів захисту визначався:

1) специфікою та цінністю для держави даних, якими оперує керівна система, що підлягає захисту;

2) відповідністю обраної системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для країн НАТО, зокрема, TCSEC ("Оранжева книга"). Це кібербезпековий стандарт США:

- у ньому прописано критерії, які в обов'язковому порядку використовує міністерство оборони США;
- він установлює базові вимоги щодо контролю комп'ютерної безпеки, убудованої в комп'ютерну систему;
- його використовують для класифікації та оцінювання керівних систем, у яких обробляється закрита інформація [6];

3) відповідністю обраної системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для інших провідних країн світу, зокрема і міжнародному технічному стандарту ISO/IEC 15408 "Загальні критерії оцінки безпеки ІТ", який ратифікувало більшість провідних країн [7];

4) відповідністю обраної системи кіберзахисту настановам і рекомендаціям міжнародної організації NCSS (National Cyber Security Strategies) для країн-партнерів НАТО, що розроблені міжнародними експертами з питань національної кібербезпеки, науковцями та європейськими радниками з міжнародної кібербезпеки в контексті проєкту Програма НАТО SPS "Наука заради миру та безпеки" [8, С. 51–58].

5) відповідністю обраної системи кіберзахисту Директивам NIS для країн ЄС, котрі:

- закладають єдині правила та вимоги у сфері кібербезпеки для всіх країн ЄС, але залишають за кожною країною-членом право вжити власних заходів щодо імплементації норм цієї Директиви;
- вимагають запровадити практику управління ризиками та зобов'язати сповіщення про кіберінциденти;
- рекомендують здійснювати аналіз проблем у сфері національної кібербезпеки та пошук шляхів їхнього вирішення;
- стверджують, що побудова ефективної державної політики щодо кібербезпеки можлива лише за наявності єдиного центру управління, за умови створення належної інфраструктури кібербезпеки, за умови розвитку індустрії кібербезпеки (шляхом забезпечення умов для плідної

співпраці всіх українських і міжнародних стейкхолдерів, а також чіткої узгодженої програми дій із стейкхолдерами з метою підвищення рівня довіри між основними стейкхолдерами з питань кібербезпеки) [9];

6) відповідністю обраної системи кіберзахисту національним технічним стандартам України, які вимагають наявності певних кібербезпекових складових, злагоджене функціонування яких підтримуватиме належний захист керівної системи від НСД [10–13].

Загалом, саме така сукупність обраних інструментів і процедур для захисту ІГІСУ сектору національної кібербезпеки:

1) має захищати керівну систему:

• від витікання даних технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні й інші канали;

• від несанкціонованих дій та несанкціонованого доступу до інформації, що 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 тощо;

• від спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів із метою порушення цілісності інформації або руйнування системи захисту тощо.

2) має забезпечувати керівну систему:

• здатністю протистояти шкідливим зовнішнім впливам;

• здатністю адаптуватися до нових непередбачуваних ситуацій, виконуючи свою цільову функцію за рахунок відповідної зміни структури і поведінки системи;

• готовністю адаптуватися до нових непередбачуваних ситуацій (атак, ушкоджень, аварій), виконуючи свою цільову функцію за рахунок відповідної зміни поведінки системи;

• готовністю до технічних відмов системи в заданих межах;

• спроможністю швидко відновлюватися до штатного режиму роботи системи після збоїв;

• спроможністю протистояти зовнішнім деструктивним впливам;

• здатністю убезпечувати та захищати інформацію від несанкціонованого посягання.

У цьому випадку кібербезпека керівної системи:

1) не залежить від архітектурного чи її функціонального наповнення;

2) досягається стандартним шляхом, який є однаковим для всіх ІСУ, який є законодавчо врегульованим і чітко регламентованим, за рахунок обов'язкової наявності:

а) додаткових загальнообов'язкових зовнішніх стандартних модулів для захисту державних інформаційних ресурсів, таких як:

• додаткова система адміністрування кібербезпеки КСЗІ, за встановлення, сертифікацію та функціонування якої відповідає СБУ та ДССЗЗІ (згідно із чинним законодавством, оскільки сектор національної кібербезпеки належить до державних структур стратегічно важливого значення);

• додатковий зовнішній модуль адміністрування інтернет-безпеки ЗВІД (КУПОЛ) як додатковий зовнішній програмно-апаратний блок-модуль та частина зовнішньої державної системи кібербезпеки від інтернет-загроз;

б) додаткових зовнішніх стандартних модулів, що забезпечують готовність керівної системи до перевантаження напруги у мережах;

в) сформованих алгоритмів налаштувань параметрів автоматизованого регулятора залежно від;

• змін параметрів об'єкта управління;

• властивостей і готовності автоматизованого регулятора до можливих автоматичних збурень.

Розглянемо детальніше повний асортимент загальнообов'язкових ресурсів та інструментів, які включають п'ять рівнів кіберзахисту.

Перша група *передбачає застосування всіх можливих організаційних заходів кіберзахисту ІГІСУ сектору національної кібербезпеки та включає:*

1) наявність, знання та дотримання вимог нормативних документів, таких як:

• система забезпечення кібербезпеки;

• політика кібербезпеки у роботі з ІГІСУ сектору національної кібербезпеки;

• принципи кібербезпеки;

• настанови й інструктивні матеріали для адміністраторів і користувачів ІГІСУ сектору національної кібербезпеки;

• регламенти дій на випадок настання кіберінциденту;

2) застосування організаційних процедур розмежування (відповідно до законодавства щодо особливостей поводження з ІзОД), таких як:

• розмежування доступу користувачів та адміністраторів (згідно із законодавчо передбаченою ієрархією категорій і рівнів доступу);

• розмежування допуску користувачів та адміністраторів (згідно із законодавчо передбаченою ієрархією категорій і рівнів допуску);

• розподіл обов'язків адміністраторів;

3) дотримання встановлених рівнів конфіденційності:

• довірча конфіденційність (мінімальна, базова, повна, абсолютна);

• адміністративна конфіденційність (згідно з ієрархією апарату керування сектором національної кібербезпеки);

• аналіз наявності прихованих каналів (виявлення, контроль, перекриття);

• рівні конфіденційності під час трансакційного обміну (експорт-імпорт) інформацією, яка має критерії (мінімальна, базова, повна, абсолютна);

4) належна реєстрація та повноцінне документування будь-яких наглядових процедур:

• перевірки середовища функціонування на об'єкті автоматизації;

• випробувань (краш-тестів тощо);

• перевірок (планових, поточних, позапланових);

• виявлених порушень у паперовому журналі та вчасної сигналізації національної кібербезпеки;

5) забезпечення цілісності системи:

• адміністративної цілісності (мінімальна, базова, повна, абсолютна);

• довірчої цілісності (мінімальна, базова, повна, абсолютна);

• функціональної цілісності шляхом забезпечення належного технічного комплектування та можливості повернення до початкового рівня захисту (повні чи обмежені);

• цілісності інформації у разі обміну (мінімальна, базова, повна);

• цілісності з функціями диспетчера доступу;

6) застосування процедури профілактичного тестування засобів захисту ІГІСУ сектору національної кібербезпеки:

а) періодичне самотестування в реальних умовах функціонування (за потреби, при старті, у будь-який час);

б) тестування:

• на стійкість до відмов (з установленням обмежень);

• профілактичне чи поточне за запитом (із частковою заміною компонентів або повною модернізацією);

• на швидке відновлення після збоїв (ручне, автоматизоване, повне, часткове);

• доступність до необхідного державного ресурсного забезпечення за потреби (пріоритетність таких систем на використання ресурсів);

7) застосування процедур упереджувального технічного нагляду (моніторингу та контролю) рівня кіберзахисту керівної системи:

• перевірка вузлів і даних;

• перевірка достовірності каналу надходження поточних даних (одно- чи двонаправлений);

• перевірка цілісності комплексу засобів захисту;

• експертний нагляд за кібербезпекою та поточне супроводження кіберзахисту ІГІСУ сектору національної кібербезпеки;

• нагляд за дотриманням умов експлуатації;

• нагляд за використанням паролей безпеки.

Друга група *передбачає застосування всіх можливих програмних засобів забезпечення кібербезпеки ІГІСУ сектору національної кібербезпеки* – це спеціальні програмні засоби, що включаються до складу програмного забезпечення комплексних систем (КС) винятково для виконання захисних функцій керівної системи:

а) основні програмні засоби захисту:

• програми ідентифікації та аутентифікації користувачів КС;

• антивірусні програми;

• програми розмежування доступу користувачів до ресурсів КС;

• програми шифрування інформації (криптоключі, шифрувально-дешифрувальні програми, паролі, шифро-алгоритми);

• програми захисту інформаційних ресурсів (системного й прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання тощо) від несанкціонованої зміни, використання й копіювання.

б) допоміжні програмні засоби захисту:

• програми знищення залишкової інформації (у блоках оперативної пам'яті, тимчасових файлах тощо);

• програми аудиту з реєстрацією в журналі факту подій;

• програми тестового контролю рівня захищеності КС тощо.

Третя група *передбачає застосування всіх можливих апаратно-технічних засобів забезпечення захисту керівної системи* – це електронні й електронно-механічні апаратно-технічні пристрої, що включаються до складу технічних засобів КС та виконують (самостійно або в єдиному комплексі із іншими програмними засобами) деякі функції забезпечення інформаційної безпеки:

а) основні апаратні засоби:

• ключі доступу, системи сигналізації, засоби блокування;

• пристрої для ідентифікації користувача (магнітні та пластикові карти, відбитки пальців тощо);

• пристрої для шифрування інформації;

• пристрої для перешкоджання несанкціонованому включенню робочих станцій і серверів (електронні замки і блокатори);

б) допоміжні апаратні засоби:

• пристрої виявлення та знищення інформації на магнітних носіях;

• пристрої сигналізації про спроби несанкціонованих дій користувачів КС;

в) допоміжне апаратно-технічне обладнання, на зразок, апаратно-технічного комплексу КУПОЛ (ЗВІД), яке застосовується для захисту:

• комп'ютерної системи від несанкціонованих Інтернет втручань;

• зовнішніх мережевих каналів передачі інформації.

Четверта група *передбачає застосування усіх можливих додаткових засобів забезпечення кіберзахисту ІГІСУ сектору національної кібербезпеки та включає:*

а) застосування інженерно-технічних засобів зовнішнього поточного відеоконтролю (відеонагляду, відеоспостереження) таких як:

• інженерно-технічний відеозахист зовнішнього периметру території на якій знаходиться об'єкт автоматизації ІГІСУ;

• інженерно-технічний відеозахист зовнішнього інфраструктури об'єкта автоматизації ІГІСУ;

• інженерно-технічний відеозахист внутрішньо-будинкової інфраструктури об'єкта автоматизації ІГІСУ;

• інженерно-технічний захист (зсередини) конкретного приміщення об'єкту автоматизації, де знаходиться сама ІГІСУ сектору національної кібербезпеки;

б) застосування інженерно-технічних пристроїв:

• технічного обладнання;

• пристроїв зовнішнього екранування;

• захисних конструкцій (споруд).

П'ята група *передбачає застосування всіх можливих додаткових засобів, таких як фізична охорона підрозділами безпеки середовища функціонування ІГІСУ сектору національної кібербезпеки:*

• фізична охорона (по периметру) зовнішньої прибудинкової території навколо об'єкта автоматизації ІГІСУ;

• фізична охорона входів-виходів та внутрішньобудинкової інфраструктури, обладнання, систем об'єкта автоматизації ІГІСУ.

7. ОТРИМАНИЙ НАУКОВИЙ РЕЗУЛЬТАТ І ЙОГО ПРИКЛАДНА ЦІННІСТЬ

Результатом дослідження стало представлення ключових аспектів і специфічних особливостей комплексної системи:

• яка спеціально створена для забезпечення кіберзахисту ІГІСУ сектору національної кібербезпеки;

• яка виступає фундаментальним ядром і предметом цього дослідження;

• структурні складові та прикладна цінність якої глибоко пояснюються у межах цього дослідження.

8. ВИСНОВКИ

Із усього вище зазначеного випливає логічний висновок стосовно того, що, найбільшої уваги з-поміж інших заслуговує:

• не лише розроблення сучасної автоматизованої ІГІСУ сектору національної кібербезпеки;

• але й система її кіберзахисту, яка забезпечить безперебійну роботу зазначеної керівної системи в умовах сучасних потенційних ризиків і зовнішніх кіберзагроз.

9. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подальші дослідження доцільно присвятити питанням розроблення, упровадження, а також процедурі ліцензування описаної вище системи кіберзахисту ІГІСУ сектору національної кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Землянко, Ю. В., Замула, О. А., Ткач, О. О., Литвинова, Н. І., & Пересічанська, Я. А. (2010). Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. *Прикладная радиоэлектроника*, т. 9, № 3. 460–469.

[2] Лєнков, С. В., Перегудов, Д. А., & Хорошко В. О. (2008). Методи та засоби захисту інформації. *Несанкціоноване отримання інформації* (Т. 1). К., 464.

[3] Вєртузаєв М. С., Юрченко О. М. (2001). Захист інформації в комп'ютерних системах від несанкціонованого доступу, К., 201 с.

[4] Міжнародний стандарт ISO/IEC 15408. Загальні критерії оцінки безпеки ІТ (Міжнародний стандарт Міністерства оборони США TCSEC – "Помаранчева книга").

[5] A. Klimburg (Ed.) (2012, January 10), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 253. https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

[6] Кольцов, М., Приходько, О., & Аушев, Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Директиви NIS для ЄС). https://pdf.usaid.gov/pdf_docs/PA00XC84.pdf

[7] НД ТЗІ 2.5.004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затв. нак. № 806 ДСТСЗІ СБУ від 28.12.2012.

[8] НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від НСД. Затв. нак. № 22 ДСТСЗІ СБУ від 28.04.1999.

[9] Дежстандарт України. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (Ч. 4). Вибір засобів захисту: ДСТУ ISO/IEC TR 133354:2005 (ISO/IEC TR 13335-4:2000, IDT), [Чинний від 2006-01-07]. К., 2005, 30 с.

[10] НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затв. нак. № 806 ДСТСЗІ СБУ від 28.12.2012.

REFERENCES

[1] Zemlyanko, Y. V., Zamula, O. A., Tkach, O. O., Lytvynova, N. I., & Ya. A. Peresichanska (2010). Principles and order of development of complex information protection systems in information and telecommunication systems. *Applied radio electronics*, vol. 9, no. 3, p. 460–469 [in Ukrainian].

[2] Lenkov, S. V., Peregudov, D. A., & Khoroshko V. O. (2008). Methods and means of information protection, vol. I. *Unauthorized obtaining of information*, K., 464 [in Ukrainian].

[3] Vertuzaev, M. S., Yurchenko, M. S. (2001). Protection of information in computer systems against unauthorized access, K., 201 [in Ukrainian].

[4] International standard ISO/IEC 15408. General criteria for evaluating IT security (International standard of the US Department of Defense TCSEC – "Orange Book") [in Ukrainian].

[5] A. Klimburg (Ed.) (2012, January 10), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 253. https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf.

[6] Koltsov, M., Prykhodko, O., & Aushev, E. Policy Proposals for Reform Policy Proposals for Cybersecurity Reform in Ukraine (NIS Directives for the EU), retrieved January 10 from https://pdf.usaid.gov/pdf_docs/PA00XC84.pdf [in Ukrainian]

[7] ND TZI 2.5.004-99. Criteria for evaluating the security of information in computer systems against unauthorized access. Approval on no. 806 DSTSZI SBU 28.12.2012 [in Ukrainian].

[8] ND TZI 1.1-002-99. General provisions on the protection of information in computer systems from NSD. Approval on DSTSZI SBU No. 22 of April 28, 1999 [in Ukrainian].

[9] Dezhstandard of Ukraine Information technologies. Information technology security management guidelines. Part 4. Selection of means of protection: DSTU ISO/IES TR 133354:2005 (ISO/IES TR 13335-4:2000, IDT), [Valid from 2006-01-07], Kyiv, 2005, 30 p. [in Ukrainian].

[10] ND TZI 3.7-003-2005. The procedure for carrying out work on the creation of a comprehensive system of information protection in the information and telecommunications system of the enterprise. on DSTSZI SB U no. 806 dated 12.28.2012 [in Ukrainian].

Стаття надійшла до редколегії 16.03.2023

Formation of the cyber protection system for the integrated industry information system of Ukraine of the national cyber security sector

This The article is devoted to the disclosure and elucidation of the envisaged composition, structure of measures and tools that will be part of a comprehensive system of protection of industry-integrated MIS in the national cybersecurity sector. The article also describes the specifics and strategic value of the involved resources, which will be operated by the established system of cybersecurity. It is noted that the industry-integrated cyber defense MIS envisages the use of a set of interconnected means and measures, the implementation of which is necessary and sufficient for the full protection of industry-integrated MIS to counter external unauthorized access, etc. Emphasis is placed on the compliance of the envisaged cybersecurity system with international criteria and standards of protection of such control systems for NATO countries, in particular, the US Department of Defense cybersecurity standard (TCSEC also known as "Orange Book"); with international criteria and standards for the protection of similar control systems for other leading countries, in particular, the international technical standard ISO/IEC 15408 "General criteria for assessing IT security", which has been ratified by most leading countries; with guidelines and recommendations of the International Organization NCSS (National Cyber Security Strategies) for NATO Partner countries, as set out in the National Cyber Security Strategy and developed by international national cybersecurity experts, scholars and European international cybersecurity advisers in the context of NATO's "Science for Peace and Security (SPS) Programme"; with national technical standards of Ukraine. The article also presents in detail the full range of mandatory resources and tools for the cybersecurity of designed industry-integrated MIS in the national cybersecurity sector, which include five levels of cybersecurity (organization, software, hardware, engineering, additional physical level).

Keywords: *IGIS cyber protection system; the sector of national cyber security; feature of the cyber protection system; components of cyber protection systems; compliance of the cyber protection system.*

Сергій Толюпа,
д-р техн. наук, проф.
Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Serhii Toliupa,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Лада Сліпачук,
аспірантка кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Lada Slipachuk,
PhD Student of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

КОМП'ЮТЕРНІ НАУКИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.415.056.5
DOI 10.17721/ISTS.2023.1.43-50

Володимир Наконечний, orcid.org/0000-0002-0247-5400,
nvc2006@i.ua
Володимир Сайко, orcid.org/0000-0002-3059-6787,
vgsaiko@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна,
Теодор Наритник, orcid.org/0000-0002-4118-0226,
director@mitris.com
Інститут електроніки та зв'язку Академії наук України, Київ, Україна

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КЕРУВАННЯ ЕНЕРГЕТИЧНИМ ПОТЕНЦІАЛОМ ЗАХИЩЕНИХ РАДІОЛІНІЙ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Зростання великих обсягів інформаційних потоків спонукає до розроблення передавально-приймальних систем у діапазоні вкрай високих частот, для забезпечення ефективного керування радіолініями IR-UWB-сигналів терагерцового діапазону на базі алгоритмів машинного навчання та нейронних мереж з урахуванням енергозбереження. Для цього у статті запропоновано алгоритм стеження за багатопроменевим сигналом системи прийому сигналів від просторово рознесених малопотужних передавачів, особливістю яких є уточнення у процесі стеження часових позицій компонентів та їхньої кількості. Особливістю розробленого алгоритму є застосування вейвлет-оброблення для отримання вхідного образу нейромережі. Запропоновано структурно-функціональну модель побудови приймальної системи IR-UWB-сигналів у діапазоні вкрай високих частот з елементами інтелектуального керування, яка базується на відокремленні площин керування та фізичної інфраструктури для автоматичного й оперативного керування процесом спільного використання ресурсів фізичної інфраструктури і методів штучного інтелекту. На відміну від існуючих моделей приймальних систем IR-UWB-сигналів терагерцових діапазонів, вона забезпечує протокольно й інфраструктурно збір даних для інтелектуальних алгоритмів. Представлена фізична інфраструктура має модуль навчання й оптимізації, який передбачає використання наявної імітаційної моделі радіолінії терагерцового діапазону від 0,11 до 0,17 терагерц для тестування інтелектуальних алгоритмів керування енергетичним потенціалом радіоліній IR-UWB-сигналів. Розроблений алгоритм збору даних передбачає відслідковувати стан блоків приймального комплексу для раціонального збору даних із використанням зміни значень як метрик евклідових відстаней, так і метрик функціональних технічних параметрів, відносно кількості кластерів.

Ключові слова: *захист інформації; система безпеки; теорія ігор; оптимальна стратегія; система порушника; прийняття рішення.*

1. ВСТУП

Розвиток мереж п'ятого покоління (5G) і подальше збільшення щільності малих стільників і точок доступу веде до необхідності приділення суттєвої уваги каналу радіозв'язку між точкою доступу і мережею інтернет. Досить часто використання дротового з'єднання для організації подібного каналу зв'язку недоцільне з багатьох економічних причин.

У цих умовах бездротове з'єднання, що працює в терагерцовому (ТГц) діапазоні частот є приваб-

ливим ресурсом для побудови високошвидкісних бездротових мереж зв'язку. Причому національними регуляторами багатьох країн визначено терагерцові діапазони частот і встановлено обмеження на спектральну потужність випромінювання надширокосмугових (НШС) сигналів для їхнього неліцензованого використання.

У силу обмежень на спектральну щільність дальність випромінювання НШС-пристроїв зв'язку становить 10–50 м, тому основні області застосування НШС зв'язку – це бездротові мережі та бездротові сенсорні мережі зв'язку малого радіуса дії (локальні й персональні мережі).

Для розширення сфери застосування технології НШС терагерцового діапазону, необхідно збільшити дальність дії приймально-передавальних пристроїв у режимі "точка–точка".

2. ПОСТАНОВКА ПРОБЛЕМИ

Неухильне зростання різноманітності й обсягів інформаційних потоків у телекомунікаційних радіомережах спонукають до розв'язання науково-практичного завдання – розроблення інфраструктури передавально-приймальних систем у діапазоні вкрай високих частот для забезпечення ефективного керування радіолініями IR-UWB-сигналів ТГц-діапазону на базі алгоритмів машинного навчання і нейронних мереж з урахуванням параметра енергозбереження.

Для розв'язування поставленої задачі представляє інтерес комбіноване застосування:

- методів прийому багатопроменевого сигналу;
- принципів побудови алгоритмів формування й оброблення сигналів у багатопозиційних системах зв'язку;
- методів штучного інтелекту та машинного навчання.

Розроблення інноваційних методів підвищення ефективності керування використанням енергетичного потенціалу радіоліній терагерцового діапазону для підвищення завадостійкості й дальності дії низькоорбітальної системи зв'язку є новим науковим напрямом [1, 2].

Сучасні підходи до розв'язання подібних науково-технічних задач не дозволяють отримати очікувані результати. З урахуванням висвітленої проблеми метою цієї статті є розроблення методу підвищення ефективності керування та використання енергетичного потенціалу радіоліній на основі просторово рознесених пристроїв [3], в яких застосовують терагерцовий діапазон частот із метою забезпечення підвищення завадостійкості та дальності дії каналів зв'язку систем зв'язку на основі висотних аероплатформ.

Відомий спосіб прийому багатопроменевого сигналу [4], який полягає в тому, що у ході прийому періодично визначають числові й часові затримки компонентів багатопроменевого сигналу, для чого визначають часову область багатопроменевості, проводять пошук сигналу в області багатопроменевості і визначають оцінку пошуку числа і часових затримок компонентів багатопроменевого сигналу. Після цього формують оновлені числа і часові затримки компонентів багатопроменевого сигналу, знаходять часові затримки компонентів багатопроменевого сигналу поточного періоду, постійно уточнюючи оновлені часові затримки компонентів багатопроменевого сигналу. У результаті цього, з використанням указаних часових затримок, формують відповідні рішення про інформаційні символи.

Проте недоліком такого способу є те, що вибір порога h, який використовується для виявлення кластерів променів, ґрунтується на первинній оцінці імпульсної характеристики каналу. Оцінки отримують з аналізу прийнятого тестового сигналу і тому, практично у всіх способах з'являється серйозна інженерна проблема вибору порога прийняття рішення, яка або не вказується, або їй приділяється недостатньо уваги.

У [4] як поріг h обирається поріг, пропорційний потужності шуму. Таким чином, ці способи є малоефективними, тому що знижують інформаційну швидкість, і до того ж частково не доведені до конструктивних інженерних алгоритмів. Тому потрібно знайти ефективніше розв'язання цього завдання.

Крім того, реалізація вказаного способу не враховує факт спотворення часової форми імпульсів приймальної системи IR-UWB-сигналів ТГц-діапазонів [5, 6]. Хоча результати дослідження з передачі UWB-сигналу пікосекундної тривалості через ідеалізовану модель радіоканалу терагерцового каналу 0,11–0,14 ТГц показують, що основним видом спотворення часової форми імпульсу є його розширення від початкової тривалості 140 пс до 250 пс, яка обумовлена в першу чергу обмеженням смуги пропускання у фільтрах нижньої частоти та смуг пропускних фільтрів передавального та приймального трактів [7].

Зауважимо, що розширення імпульсів призводить до зменшеня їхньої амплітуди, а це знижує ефективність селекції імпульсів на тлі шумів і завад. Це обумовлено тим, що у разі неперіодичної послідовності імпульсів середня шпаруватість $\bar{Q}$, як відношення тривалості сигналу T_c до сумарного часу тривалості імпульсів у сигналі, буде така:

$$\bar{Q} = \frac{T_c}{\tau n} = \frac{1}{V \tau n}, \qquad (1)$$

де V – швидкість передачі; n – кількість імпульсів у сигналі; τ – тривалість імпульсу.

І відповідно середня шпаруватість сигналу повинна бути якомога більше 1. В іншому випадку кожен із сигналів буде представляти собою щільний потік імпульсів, що унеможливить кодове розділення сигналів у мережі, де одночасно працює безліч терміналів.

Середня шпаруватість сигналів, по суті, визначає можливість забезпечення їхньої ортогональності, тобто можливість поділу сигналів.

Зауважимо також, що значення середньої шпаруватості Q^{-} визначає середню потужність сигналу P^{-}, що передається, якщо відома пікова потужність імпульсів P_i за такою формулою:

$$\bar{P} = {P_i}/{\bar{Q}}\,. \qquad (2)$$

Тому єдиним шляхом підвищення потужності сигналу при обмеженнях на тривалість і кількість імпульсів є підвищення амплітуди (пікової потужності) переданих імпульсів.

Автори в роботі [4] не запропонували механізм моніторингу й керування тривалістю UWB-сигналу та відповідно модель ефективного керування використанням енергетичного потенціалу радіоліній.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

3.1. Загальна архітектура інноваційного рішення

Авторами пропонується (рис. 1) використання інтелектуальних алгоритмів на базі тренованих моделей штучного інтелекту, які використовуватимуться на фізичному рівні запропонованої архітектури приймальної системи IR-UWB-сигналів ТГц-діапазонів із використанням алгоритмів на базі штучного інтелекту, а також на рівні площини керування комплексом.

Роботу цих алгоритмів зосереджено на керуванні використанням енергетики радіоліній з IR-UWB-сигналів і, як результат, оптимізації використання ресурсів їхнього енергетичного потенціалу.

Наприклад, використання алгоритмів на базі нейронних мереж для реалізації вейвлет-перетворення дозволяє уникнути великої кількості обчислень і набагато прискорити пошук коефіцієнтів вейвлет-розкладання для ефективнішого використання спектральних ресурсів каналу зв'язку.

Інтелектуальні алгоритми керування на SDN-контролері можуть здійснювати оптимізацію на рівні цілого комплексу. Проте для таких алгоритмів, які працюють на рівнях фізичному й керування, повинні мати відповідну інфраструктуру для збору даних, тренування, тестування й оновлення відповідних тренованих моделей.

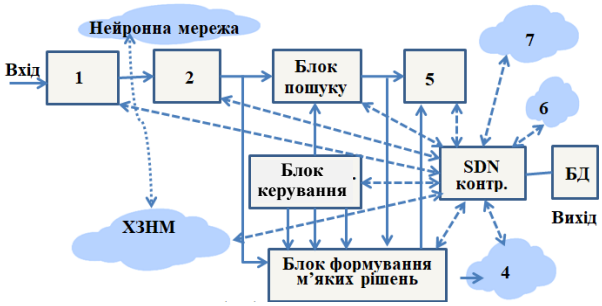


Рис. 1. Структурна схема запропонованої архітектури приймальної системи ТГц-діапазону з використанням алгоритмів на базі штучного інтелекту:

1. Блок ВО – вейвлет-оброблення;
2. Блок АФ – блок адаптивної фільтрації;
3. ХЗНМ – хмара зберігання нейронних мереж;
4. ХЗСП FE – хмара зберігання статистичних параметрів FE;
5. БОКБС – блок оновлення компонент багатопроменевого сигналу;
6. ML алгоритми Н та Т – ML навчання та тренування;
7. ML алгоритми М та О – ML моніторингу й оптимізації

На рис. 2 показано інфраструктуру нейронної мережі розробленого інноваційного рішення. Її складовими є такі модулі: 1 – роботи алгоритмів ML на SDN-контролері; 2 – тренування нейронної мережі; 3 – навчання й оптимізації нейронної мережі; 4 – канали зв'язку для оновлення нейронної мережі та відповідного програмного забезпечення; 5 – модуль роботи алгоритмів із використанням нейронної мережі на блоках інноваційного рішення.

Підтримка такої інфраструктури повинна вартувати менше, ніж переваги, які вона має надати. У багатьох роботах представлено використання поодиноких алгоритмів на базі нейронних мереж, які здійснюють оптимізацію конкретного процесу чи частини пристрою [8].

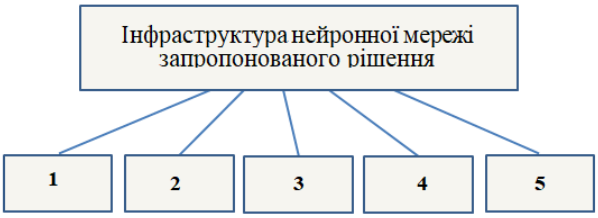


Рис. 2. Інфраструктура нейронної мережі розробленого інноваційного рішення

Проте в них не показано, яким чином відбувається збір даних, тренування нейронних мереж, а також оновлення відповідного програмного забезпечення. Тобто не представлено, яким чином повинна працювати повна інфраструктура із зворотним зв'язком для алгоритмів, які здійснюють

оптимізацію роботи приймального комплексу IR-UWB-сигналів ТГц-діапазону з використанням нейронних мереж.

3.2. Модель попереднього оброблення сигналу із застосуванням вейвлет-оброблення

Існуючі методи [8], які використовують фільтрацію сигналів за допомогою вейвлет-перетворення в нейромережних системах класифікації образів, не можуть бути безпосередньо застосовані до моделей та алгоритмів ефективного керування використанням енергетичного потенціалу радіоліній. Тому важливим напрямом подальших досліджень є адаптація відомих нині методів штучного інтелекту до особливостей моніторингу й оптимізації функціонування багатопозиційних систем на основі малопотужних приймально-передавальних пристроїв для побудови міжсупутникових каналів зв'язку терагерцового діапазону низькоорбітальних супутникових систем з архітектурою розподіленого супутника.

У складі блоку пошук (див. рис. 1) є пристрій, який визначає значення вирішальної функції для заданих дискретних часових затримок області багатопроменевості, порівнює значення сформованої вирішальної функції із заданим порогом h і формує оцінки пошуку часових затримок компонентів багатопроменевого сигналу з перевищення порога h.

Як відомо, у ході прийому широкосмугових багатопроменевих сигналів виконується також процедура пошуку, яка, як правило, являє собою сканування області невизначеності з виявленням сигналу в кожній її точці.

Недоліком відомих підходів оброблення багатопроменевих сигналів на основі застосування процедури пошуку є те, що під час проведення цієї процедури пошуку сигналів променів не враховується вплив компонентів багатопроменевого сигналу один на одного. Унаслідок цього зростає ймовірність помилкового виявлення сигналів променів. Крім того, не здійснюється оптимізація числових сигналів променів, які використовують для отримання м'яких рішень про інформаційні символи, що призводить до завищених вимог до апаратурної реалізації без збільшення якості виділеної інформації.

Із цього погляду, доцільним є введення процедури відстеження й ідентифікація зміни властивостей нестаціонарних процесів в алгоритмі пошуку сигналів, а також адаптація до зміни рівня шуму.

Блок-схема роботи системи попереднього оброблення сигналу із застосуванням вейвлет-оброблення для отримання вхідного образу нейромережі запропонованого підходу зображена на рис. 3.

Особливістю запропонованого підходу є те, що з метою адаптації цифрового оброблення сигналу до змінного в часі шуму, при розв'язанні задачі розпізнавання наявності або відсутності сигналу на заданому інтервалі, запропоновано спосіб на основі вейвлет-перетворення і нейронної мережі.

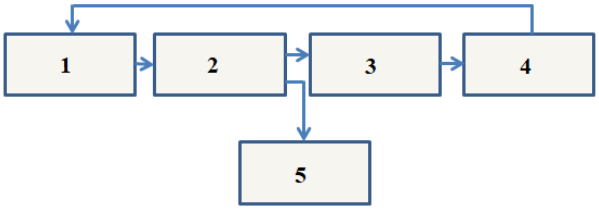


Рис. 3. Блок-схема роботи запропонованої системи попереднього оброблення багатопроменевого сигналу:

1. Багатопроменевий сигнал;
2. Блок вейвлет-перетворення;
3. Нейронна мережа;
4. Результат попереднього оброблення сигналу;
5. Надлишкова інформація

Вейвлет-перетворення дозволяє більш точно локалізувати частотні властивості сигналу в часі та не призводить до збільшення обсягу даних у процесі переходу від часового подання сигналу до його подання у вейвлет-області. Причому найкраще частотне розділення забезпечує фільтр із найбільшою крутизною амплітуди частотних хвиль (АЧХ). Така риса властива вейвлетам Добеши.

Зі збільшенням порядку фільтра Добеши його АЧХ прагне до ідеальної. Але необхідно враховувати те, що застосування фільтра з довгою імпульсною характеристикою призводить до вельми помітного спотворення. З урахуванням цього найдоцільнішим є використання фільтра Добеші 4, кофлета 2 і сіммлета. Біортогональні вейвлети Добеши дозволяють також зменшити обсяг обчислень під час розкладання за рахунок використання коротких фільтрів [9, 10].

Запропонований алгоритм поділу інтервалів наявності або відсутності сигналу побудовано з урахуванням особливостей розповсюдження багатопроменевого сигналу, які описуються персептуальною моделлю. Модель розділяє спектр багатопроменевого сигналу на частотні смуги, на так звані критичні інтервали.

У розробленому алгоритмі використано вейвлет – перетворення багатопроменевого сигналу по біортогональному базису Добеши, а для прийняття рішення про типи інтервалу (сегмента) сигналу – нейронну мережу на багатошаровому персептроні.

Порівняно з традиційними спектральними методами вейвлет-перетворення дає більш точну локалізацію сигналу за часом і за частотою (у субсмугах розкладання), має швидкий алгоритм

реалізації. Біортогональний базис зберігає фазові співвідношення частотних компонентів сигналу після його відновлення зворотним вейвлет-перетворенням. Подальше поліпшення запропонованого способу досягнуто зменшенням розмірності вхідного вектора персептрона, яке дозволило зменшити число навчальної вибірки і прискорити процес навчання. Зниження розмірності вхідних векторів у ході навчання нейронної мережі засновано на алгоритмі головних компонентів.

Результати дослідження залежності ймовірності помилки розпізнавання від розмірності вектора ознак після виконання перетворення методом головних компонентів показано на рис. 4.

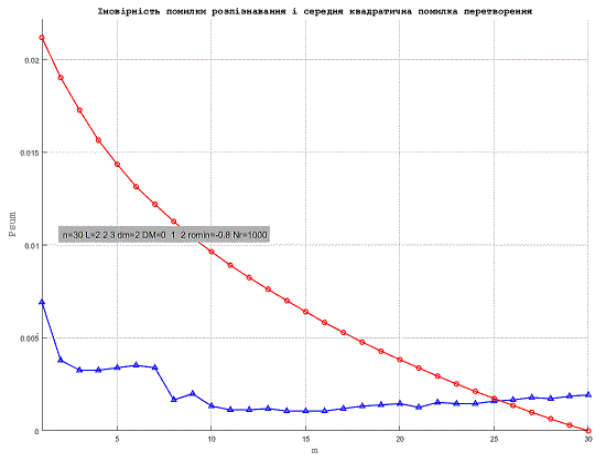


Рис. 4. Залежності для сумарної імовірності помилки і СКП перетворення від розмірності вектора ознак після виконання перетворення алгоритмом головних компонентів

Представлені результати показують, що залежності для сумарної імовірності помилки розпізнавання (крива зверху) і середньоквадратичної помилки (СКП) перетворення мають практично монотонно спадний характер, причому виділення головних компонентів і зниження на цій основі розмірності простору ознак дає суттєвіший ефект у разі збільшення ступеня кореляції вихідних ознак.

Для навчання багатошарового персептрона використано алгоритм Левенберга – Марквардта (Levenberg – Marquardt Algorithm, LMA), який є найпоширенішим алгоритмом для мінімізації квадратичних відхилень. Його перевагами, порівняно з методом градієнтного спуску, є велика швидкість обчислення.

3.3. Система моніторингу й оптимізації роботи запропонованого рішення

У розробленій архітектурі запропоновано застосовувати модуль навчання та тестування, який дозволяє підлагоджувати інтелектуальні алгоритми керування, а саме процеси підготовки, тестування й оцінювання перед їхнім розгортанням у інноваційному рішенні.

Для навчання або тестування таких алгоритмів можна використовувати змодельовані дані або дані з реальної приймальної системи IR-UWB сигналів ТГц-діапазонів. Указаний підхід дозволяє якісніше підготуватись до запуску таких алгоритмів на реальних мережах і зменшити відповідні ризики (див. рис. 1).

4. РЕЗУЛЬТАТИ

Для оцінювання таких алгоритмів слід увести певні функціональні метрики розробленої системи, на базі яких будуть здійснювати оцінку даних алгоритмів. Модуль навчання та тестування включає імітаційну модель бездротової телекомунікаційної системи терагерцового діапазону на основі використання IR-UWB багатопроменевих сигналів пікосекундної тривалості з відповідними складовими для максимального наближення до роботи реального розробленого приймального пристрою.

Як середовище імітаційного моделювання обрано програмний NI Multisim 13.0 [11]. Це пов'язано з тим, що у САПР Microwave Office відсутня можливість підключення до приймального тракту ТГц-діапазону активної моделі приймача IR-UWB-сигналів, що зібрана з окремих елементів.

Особливістю моделювання приймача IR-UWB-сигналів є те, що у першу чергу необхідно зібрати імітаційну модель, що відповідає передавальній частині, в якій саме й відбувається формування IR-UWB-сигналу.

Ідеалізовану імітаційну модель радіолінії ТГц-діапазону будуватимемо на базі параметрів і структурної схеми діючого макета приймача-передавача ТГц-діапазону [7].

Метрики розробленої системи оцінювання роботи нейронної мережі повинні мати звичні функціональні параметри цього рішення: співвідношення сигнал/шум, тривалість імпульсу UWB-сигналу, ефективність використання спектральних ресурсів каналів зв'язку тощо.

Якщо перетренована модель для певного алгоритму призвела до погіршення функціональних параметрів, то дана модель повинна бути повернена або має бути видалена з модуля зберігання даних.

Щоб інтелектуальні алгоритми керування видавали правильний результат, необхідно зібрати достатній набір даних, під яким розуміють оптимальну кількість даних, при якій тренування моделей вважається завершеним і не спосте-

рігається так званий процес оверфітингу. Для збору функціональних даних використовують SDN-контролер, який безпосередньо здійснює процес збору відповідних даних із блоків приймальної системи IR-UWB-сигналів ТГц-діапазону. Кожен блок приймальної системи є як джерелом інформації для ML-алгоритмів, так може бути і метою їхнього застосування. Основне оброблення даних перед тренуванням нейронних мереж здійснюється на SDN-контролері. Усі зібрані функціональні параметри, які необхідні для тренування нейронних мереж, зберігаються у хмарі FE. Доступ до цих параметрів мають лише інтелектуальні алгоритми на SDN-контролері.

Якщо відбулася зміна стану приймальної системи IR-UWB-сигналів у діапазоні на вкрай високих частотах, яка вимагає перетренування відповідних моделей, то відповідні алгоритми здійснюють необхідну процедуру перетренування їх на базі нових параметрів FE. Після цього відбувається заміна відповідних натренованих моделей у хмарі. Коли з'явилась нова версія моделі для відповідного блоку, блок завантажує відповідну оновлену версію моделі.

У роботі використано кластерний підхід визначення станів приймальної системи IR-UWB-сигналів у діапазоні вкрай високих частот із навчанням без нагляду з використанням ML-алгоритмів *k*-means (*k* – середніх) та *c*-means (*c* – середніх) для розробленого алгоритму збору даних [12, 13]. Цей підхід дозволяє визначити на базі певного проміжку часу необхідні стани запропонованого пристрою або появу нових станів. Крім того, такий підхід дозволяє враховувати більшу кількість функціональних технічних параметрів із мінімальною зміною програмного забезпечення. Важливою складовою інтелектуальних алгоритмів керування є збір безпосередньо даних для навчання.

Однією з особливостей використання даних алгоритмів у телекомунікаційних радіомережах ТГц-діапазону є змінність станів у комплексі, а також поява нових і зникнення поточних станів, що вимагає додаткового збору даних і перетренування нейронних мереж.

У роботах [8, 9] представлено використання алгоритмів на базі нейронних мереж для реалізації вейвлет-перетворення у приймальних системах. Але в цих роботах не показано, яким чином здійснюється збір певних функціональних технічних даних. Тому розроблення алгоритму раціонального збору даних для нейронних мереж із відповідних блоків приймальної системи є досі актуальним.

Розроблений алгоритм збору даних передбачає відстежування стану блоків приймального комплексу для раціонального збору даних фактично з використанням зміни значень як метрик евклідових відстаней, так і метрик функціональних технічних параметрів, відносно кількості кластерів. Новизна цього підходу полягає у відмінності від класичної реалізації у тому, що введено метрики співвідношення сигнал/шум і тривалість імпульсу UWB-сигналу, замість метрики евклідової відстані, що дає змогу враховувати просторові характеристики поширення сигналу у процесі самооптимізації розробленої приймальної структури та відповідно підвищити її технічну ефективність.

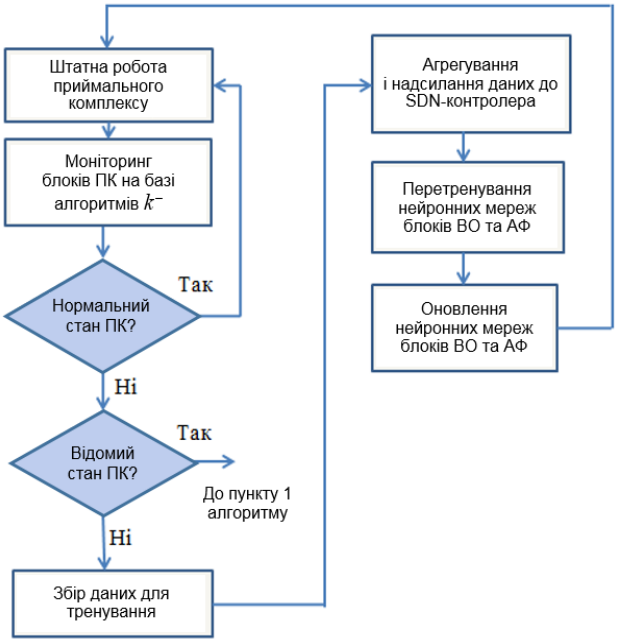


Рис. 5. Блок-схема алгоритму відстежування стану приймального комплексу для збору і перетренування відповідних нейронних мереж

5. ВИСНОВКИ

1. Розроблено алгоритм стеження за багатопроменевим сигналом системи прийому сигналів від просторово рознесених малопотужних передавачів, особливістю якого є уточнення у процесі стеження не тільки часових позицій компонентів, але також і їхнього числа. Відмінною особливістю розробленого алгоритму є те, що він побудований із застосуванням вейвлет-оброблення для отримання вхідного образу нейромережі.

2. Запропоновано структурно-функціональну модель побудови приймальної системи IR-UWB-сигналів ТГц-діапазонів з елементами інтелектуального керування приймальним комплексом на фізичному рівні та керування комплексом. На відміну від існуючих інфраструктур приймальної

системи IR-UWB-сигналів ТГц-діапазонів, ці радіомережі не здатні забезпечити протокольно й інфраструктурно збір необхідних даних для інтелектуальних алгоритмів. Запропонована інфраструктура має модуль навчання й оптимізації, який передбачає використання існуючої імітаційної моделі радіолінії ТГц-діапазону від 0,11 до 0,17 ТГц для тестування інтелектуальних алгоритмів керування енергетичним потенціалом радіоліній IR-UWB-сигналів ТГц-діапазону.

3. Подальше наукове дослідження направлено на проведення моделювання й дослідження ефективності запропонованих рішень на основі розробленої імітаційної моделі керування енергетичним потенціалом радіоліній IR-UWB-сигналів ТГц-діапазону, а також розроблення вебзастосунку, який відображатиме реальний стан розробленого приймального пристрою і дозволить змінювати необхідні функціональні параметри для одержання необхідних результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Saiko, V., Nakonechnyi, V., Narytnyk, T., Brailovskyi, M., & Toliupa, S. (2020). Increasing Noise Immunity between LEO Satellite Radio Channels. In *Proceedings – 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, TCSET 2020, pp. 442–446.

[2] Saiko, V., Nakonechnyi, V., Narytnyk, T., Brailovskyi, M., & Lukova-Chuiko, N. (2020). Terahertz Range Interconnecting Line for LEO-System. In *Proceedings – 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, TCSET 2020, pp. 425–429.

[3] Сайко В. Г. (2020, 22–24 бер.). Алгоритм обробки сигналів багатопозиційної системи, що використовує принцип просторово-розподіленого випромінювання. *The 3th International scientific and practical conference, Eurasian scientific congress*‖*, Barca Academy Publishing*, Barcelona, Spain, pp. 155–160.

[4] Narytnik, T., Saiko, V., Bilous, O., & Fisun, A. (2019). Energy calculation of the terahertz radio link Telecommunications and Radio Engineering. *English translation of Elektrosvyaz and Radiotekhnika*, 78(6), 537–557.

[5] Avdeenko, G., Narytnik, T., Korsun, V., & Saiko, V. (2019). Simulation of a terahertz band wireless telecommunication system based on the use of IR-UWB signals. *In Telecommunications and Radio Engineering, English translation of Elektrosvyaz and Radiotekhnika*, 78(10), 901–919.

[6] Наритник Т. М., Авдєєнко Г. Л., Сайко В. Г., & Корсун В. І. (2018). Дослідження передавання модульованих IR-UWB сигналів системою радіозв'язку терагерцового діапазону. *Цифрові технології*, 24, 17–32.

REFERENCES

[1] Saiko, V., Nakonechnyi, V., Narytnyk, T., Brailovskyi, M., & Toliupa, S. (2020). Increasing Noise Immunity between LEO Satellite Radio Channels. *In Proceedings – 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, TCSET 2020, pp. 442–446.

[2] Saiko, V., Nakonechnyi, V., Narytnyk, T., Brailovskyi, M., & Lukova-Chuiko, N. (2020). Terahertz Range Interconnecting Line for LEO-System. In Proceedings – 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2020, pp. 425–429.

[3] Saiko V. G. (March 22–24, 2020). Algorithm for processing signals of a multi-position system using the principle of spatially distributed radiation. *The 3th International scientific and practical conference, Eurasian scientific congress*‖*, Barca Academy Publishing*, Barcelona, Spain., pp. 155–160 [in Ukrainian].

[4] Narytnik, T., Saiko, V., Bilous, O., & Fisun, A. (2019). Energy calculation of the terahertz radio link Telecommunications and Radio Engineering. *English translation of Elektrosvyaz and Radiotekhnika*, 78(6), 537–557.

[5] Avdeenko, G., Narytnik, T., Korsun, V., & Saiko, V. (2019). Simulation of a terahertz band wireless telecommunication system based on the use of IR-UWB signals. *In Telecommunications and Radio Engineering, English translation of Elektrosvyaz and Radiotekhnika*, 78(10), 901–919.

[6] Narytnyk, T. M., Avdeyenko, G. L., Saiko, V. G., & Korsun, V. I. (2018). Study of the transmission of modulated IR-UWB signals by a radio communication system of the terahertz range. *Digital technologies*, 24, 17–32 [in Ukrainian].

Стаття надійшла до редколегії 27.02.2023

The method of increasing the efficiency of management of the energy potential of protected radio lines in the terahertz range using artificial intelligence

The growth of large volumes of information flows encourages the development of transmission and reception systems in the very high frequency range to ensure effective control of IR-UWB radio links of terahertz signals based on machine learning algorithms and neural networks, taking into account energy saving. For this purpose, the article proposes an algorithm for tracking a multipath signal of a system for receiving signals from spatially separated low-power transmitters, a feature of which is the refinement in the process of tracking the time positions of the components and their number. A feature of the developed algorithm is the use of the wavelet transform to obtain the input image of the neural network. A structural and functional model for constructing a receiving system for IR-UWB signals in the very high frequency range with intelligent control elements is proposed, which is based on separate control planes and physical infrastructure for automatic and operational control of the process of sharing physical infrastructure resources and artificial intelligence methods. Unlike existing models of IR-UWB receiving systems for terahertz signals, it provides protocol and infrastructure data collection for intelligent algorithms. The presented physical infrastructure has a training and optimization module that involves the use of an existing simulation model of a radio link in the terahertz range from 0.11 to 0.17 terahertz to test intelligent algorithms for controlling the energy potential of IR-UWB radio links. The developed data collection algorithm involves monitoring the state of the blocks of the receiving complex for rational data collection using the change in the values of both the Euclidean distance metrics and the metrics of functional technical parameters in relation to the number of clusters.

Keywords: *information protection; security system; game theory; optimal strategy; system of the violator; making a decision.*

Володимир Наконечний,
д-р техн. наук, проф.
Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Volodymyr Nakonecnii,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Cyber Security and Information Protection of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Володимир Сайко,
д-р техн. наук, проф.
Професор кафедри прикладних інфор - маційних систем Київського національного університету імені Тараса Шевченка. Київ, Україна.

Volodymyr Saiko,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Applied Information Systems of Taras Shevchenko Kyiv National University. Kyiv, Ukraine

Теодор Наритник,
канд. техн. наук, проф.
Директор Інституту електроніки та зв'язку Української академії наук. Київ, Україна.

Teodor Narytnyk,
PhD (Engin.), Prof.
Director of the Institute of Electronics and Communication of the Ukrainian Academy of Sciences. Kyiv, Ukraine.

УДК 004-26
DOI 10.17721/ISTS.2023.1.51-60

Сергій Зибін, orcid.org/0000-0002-2670-2823,
zysv@ukr.net
Яна Бєлозьорова, orcid.org/0000-0002-0688-3436,
bryuhanova.ya@gmail.com
Національний авіаційний університет, Київ, Україна

МЕТОД ВИЗНАЧЕННЯ ФОРМАНТНИХ ЧАСТОТ ІЗ ВИКОРИСТАННЯМ СПЕКТРАЛЬНОГО РОЗКЛАДАННЯ МОВНОГО СИГНАЛУ

Форманти є одним з основних компонентів систем ідентифікації мовця, а точність визначення формант – це основа ефективності систем ідентифікації мовця. Поліпшення існуючих систем розпізнавання мови дозволить істотно спростити взаємодію людини з комп'ютером у тому випадку, коли використання класичних інтерфейсів неможливо, а також зробити подібну роботу комфортнішою та ефективною.

Необхідність досліджень із цієї тематики пояснюється незадовільними результатами наявних систем при низькому співвідношенні сигнал/шум, залежністю результату від людини, а також невисокою швидкістю роботи подібного виду систем.

Для порівняння із запропонованим методом використовували такі чотири основні формант-трекери: PRAAT, SNACK, ASSP та DEEP. Існує багато досліджень, що стосуються порівняння формант-трекерів, однак серед них не можна виокремити такий, що має найкращу ефективність.

Виокремлення формант супроводжує цілий ряд проблем, пов'язаних з їхньою динамічної зміною у процесі мовлення. Складність також викликають проблеми, пов'язані з близьким розташуванням піків під час аналізу спектрограм і проблеми правильного визначення піків максимумів формант на спектрограмі. Розташування формант на спектрограмах мовного сигналу достатньо легко визначає людина, але автоматизація цього процесу викликає деякі труднощі.

Виокремлення формантних частот запропоновано виконувати у декілька етапів. Результатом проведеного огляду підходів до визначення формантних частот став алгоритм, що складається з дев'ятьох таких етапів. Сегментація мовного сигналу на вокалізовані фрагменти та паузи виконується методом оцінювання змін фрактальної розмірності. Отримання спектра мовного сигналу виконувалось із використанням комплексного вейвлету Морле на основі віконної функції Гаусса. Для дослідження розглядалися формант-трекери PRAAT, SNACK, ASSP і DEEP. Налаштування кожного з них здійснювали на основі набору параметрів за замовчуванням, що закладено розробниками цих трекерів. Набір налаштувань для кожного з трекерів використовували для порівняння. У дослідженні трекери самостійно виконували сегментацію на вокалізовані фрагменти і паузи, застосовуючи датасет VTR-TIMIT. Проведений порівняльний аналіз показав достатньо високу точність визначення формантних частот порівняно з існуючими формант-трекерами.

Ключові слова: *мовний сигнал (МС); формантні частоти; спектральна декомпозиція; обчислювальний алгоритм; вейвлет-аналіз.*

1. ВСТУП

У сучасному світі все більше значення приділяють інтерфейсам, які використовують мовне введення і виведення для взаємодії між користувачем і комп'ютером. Тому розробник систем мовної інформації має надавати увагу все більшій кількості налаштувань і параметрів у підсистемах, що реалізують акустичний інтерфейс.

Задача розпізнавання мови (у багатьох своїх проявах: від сегментації промови до верифікації та ідентифікації особи) нині є вкрай актуальною. Свідченням цього є зростаюча кількість публікацій і конференцій із цієї тематики [1], а також відкриття в транснаціональних корпораціях департаментів, що орієнтовані на дослідження в мовній інформації.

Поліпшення існуючих систем розпізнавання мови дозволить істотно спростити взаємодію людини з комп'ютером у тому випадку, коли використання класичних інтерфейсів неможливо (наприклад, під час керування автомобілем або для людей з обмеженими фізичними можливостями), а також зробити подібну роботу більш комфортною та ефективною.

Необхідність досліджень із цієї тематики пояснюється незадовільними результатами існуючих систем при низькому співвідношенні сигнал/шум, залежностями результату від людини, а також невисокою швидкістю роботи подібного роду систем [2].

Дослідження методів визначення формант та розроблення нових точніших методів дозволить знизити похибку визначення та підвищити точність роботи систем ідентифікації мовної інформації.

2. ДОСЛІДЖЕННЯ ХАРАКТЕРНИХ ОСОБЛИВОСТЕЙ МОВНИХ СИГНАЛІВ

У системах ідентифікації мовного сигналу отримання характерних ознак мови особи, є однією з основних запорук успіху роботи системи ідентифікації мовної інформації. У завданнях аналізу мовного сигналу з метою визначення найважливіших характеристик, як правило, використовують методи його частотно-часового або спектрального уявлення, одними з найбільш ефективних є методи вейвлет-перетворення мовного сигналу. Найважливішим параметром, що характеризує спектр (розподіл енергії або амплітуди по частотах) мовного сигналу є форманти [3], які визначають як концентрацію енергії в обмеженій частотній області. Форманта характеризується частотою, шириною частотної смуги й амплітудою. Зважаючи на складність визначення й опису формантної частотної смуги, часто в дослідженнях під частотою форманти мають на увазі частоту максимальної амплітуди в межах форманти. Тому часто можна зустріти визначення форманти, як амплітудний сплеск на графіку спектра [4], що має частоту, відповідну до частоти піку цього сплеску. Форманти прийнято позначати F0-F6. Форманта F0 називається також частотою основного тону мовного сигналу. Форманти F1-F6 визначають концентрацію енергії мовного сигналу по частоті і характеризують вокалізовані (як правило, голосні) звуки.

Існує безліч методів виявлення формант [5–7], основними з яких є кепстральний аналіз і метод лінійного передбачення. Кепстральний аналіз є математичною основою нелінійних методів виділення сигналів. Кепстр – це математичне перетворення, що полягає в тому, що спектральному перетворенню піддається спектр функції. Якщо взяти спектр від спектра, то вийде сама початкова функція. Природно, що для отримання більш гладкої функції в результаті спектрального перетворення необхідно згладити початковий спектр. Для цього найчастіше використовують логарифмування початкового спектра або його модуля. Такий варіант перетворення прийнято називати кепстр. В отриманому кепстрі виявляються гармонійні складові [8].

Метод лінійного передбачення (метод, який використовує LPC-коефіцієнти) полягає в пошуку комплексних коренів полінома з LPC-коефіцієнтами (коефіцієнти фільтра мовного тракту) і надалі їхні наступні перетворення. Вважається, що метод лінійного передбачення [9] забезпечує високу обчислювальну швидкість, незначну складність і максимальну точність оцінювання формант.

Зазвичай використовують ефективний метод обчислення коефіцієнтів лінійного передбачення, заснований на автокореляції, що застосовує алгоритм Левінсона – Дарбина. У задачі розпізнавання мови часто застосовують коефіцієнти лінійного передбачення, обчислені на основі статичного закону людського слуху [10, 11]. Відмінності від простого обчислення коефіцієнтів лінійного передбачення полягають у такому. По-перше, застосовується шкала Баркова і логарифмічна компресія амплітуди до застосування алгоритму Левінсона – Дарбина. По-друге, для відповідності законам людського слуху потужність спектральних компонент зводиться до ступеня 0,33. Ця модифікація застосовується в частотної області, що призводить до того, що автокореляційні коефіцієнти не можуть бути обчислені безпосередньо, отже, необхідним є додаткове перетворення Фур'є [12].

Описані методи використовують у різних комбінаціях в чотирьох основних формант-трекерах PRAAT [13], SNACK [14], ASSP [15] і DEEP [16].

PRAAT [13] виділяє форманти таким чином: для кожного фрагмента, що аналізується, застосовується вікно, подібне до вікна Гаусса. Обчислюються коефіцієнти LPC за алгоритмам Бурга [17]. Кількість максимумів, яку обчислює цей алгоритм, удвічі перевищує максимальну кількість формант, тому рекомендується встановлювати максимальну кількість формант кратну 0,5. Спочатку алгоритм знаходить максимальну кількість формант у всьому діапазоні від 0 Гц і вище. Тому знайдені форманти можуть мати аномально низькі або високі частоти, що пов'язано з артефактами алгоритму LPC.

SNACK [14] застосовує той самий підхід, що і PRAAT. Цей метод використовує відбір формантів за мінімальними значеннями вагових коефіцієнтів, в основі яких лежать відмінності між фрагментами, частота та ширина форманти. На відміну від PRAAT використовується лише один параметр, пов'язаний із відстеженням функції. Цей параметр дозволяє визначити значення першої форманти, вищі форманти знаходять на основі заданого значення для першої форманти F1. Таким чином метод вважає, що всі інші форманти пов'язані з F1 коефіцієнтами прямого зв'язку. Цей метод не дає можливості змінити поведінку обчислення або вагові коефіцієнти для інших формант.

У методі ASSP [15] значення формант отримують шляхом визначення резонансних частот за рахунок розв'язання коренів полінома LPC, використовуючи метод автокореляції на основі алгоритму Спліт – Левінсона (SLA) [18]. Потім виконується класифікація резонансних частот як формант із використанням частоти Писаренко [19] та встановлення границі діапазону частот формант, що визначаються з номінальної частоти першої форманти F1. У методі вказується, що форманті частоти необхідно збільшити на 12 % для точнішого обчислення формант жіночих голосів.

DEEP [16] використовує нейронні мережі для визначення формант. Вхідними даними є отримання на основі LPC-методу кепстральних коефіцієнтів, які корегуються частотою основного тону, отриманою зі спектрограми. Навчання нейронної мережі виконувалось на основі тестової частини мовного датасету VTR-TIMIT [20]. VTR-TIMIT є відкритим датасетом із 516 видами записів від 186 осіб, що є носіями англійської мови. У датасеті виконана ручна корекція та маркування формант спеціальної групою експертів, тому саме цей датасет найчастіше використовується для оцінювання точності роботи формант-трекерів.

Є ряд досліджень, що стосуються порівняння формант-трекерів, однак серед них не можна виділити такий, що має найкращу ефективність [21, 22].

На основі викладеного можна зробити висновок про деяку складність, а частково, навіть про відсутність фізичної аргументації механізмів визначення формант, а також відсутність достатньої точності формант-трекерів, що потребує побудови методу визначення формант, який має достатнє фізичне обґрунтування та достатню точність порівняно з аналогами.

3. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Форманти є одними з основних елементів ідентифікації особи в мовному сигналі тому, що природа їхнього походження пов'язана з порожнинами людського мовного тракту. Зважаючи на індивідуальність подібних компонентів для кожної людини, можна дійти висновку, що визначення формантних частот є важливим компонентом побудови системи ідентифікації мовної інформації.

Дослідження формантних атрибутів найчастіше виконується шляхом:

- порівняння спектра формант однакових фонемічних елементів (ударних голосних, голосних у кінці або на початку слів тощо);
- порівняння спектрів формант для зрізів спектрограм (кожного елемента спектрограми або всередині слів, складів та ін.);
- порівняння динамічних змін частот формант уздовж усього МС чи у важливих його компонентах.

Виокремлення формант супроводжує ряд проблем, пов'язаних з їхньою динамічною зміною у процесі мовлення. Навіть однакові голосні змінюють формантний набір залежно від свого розташування у складі слів, складів тощо. Труднощі також визивають проблеми, пов'язані з близьким розташуванням піків під час аналізу спектрограм і проблемами правильного визначення піків максимумів формант на спектрограмі. Визначення розташування формант на спектрограмах МС достатньо легко виконується людиною, але автоматизація цього процесу визиває деякі труднощі. Типове представлення спектрограми з розміченими людиною розташуваннями формант представлено на рис. 1, що відповідає зонам розташування формант, причому характеризується не тільки середньою частотою форманти, а також її шириною.

Проведення подібного розмічення є досить складною задачею, зважаючи не велику кількість конкуруючих частотних піків. Трудомісткість подібного роду маркування формант досить висока, тому в експериментальних дослідженнях використовують заздалегідь розмічені данні, що можна знайти в різних типах мовних датасетів. В наступному дослідженні будемо використовувати датасет VTR-TIMIT, що має підготовлений набір розмічених даних подібного типу.

Крім того, під час проголошення окремих видів звуків на положення формант можуть впливати безліч факторів, що може приводити до коливань формантних частот, а на окремих фрагментах навіть відсутності деяких із них.

Існує декілька підходів для визначення положень формант на частотній шкалі, але всі вони базуються на аналізі та перетвореннях спектрограми мовного сигналу. При виділенні формантних частот першим етапом дослідження завжди є побудова спектрограми за визначеними дослідником критеріями. Серед них є ширина фрейму, тип вейвлет-базису, частотний діапазон та ін.

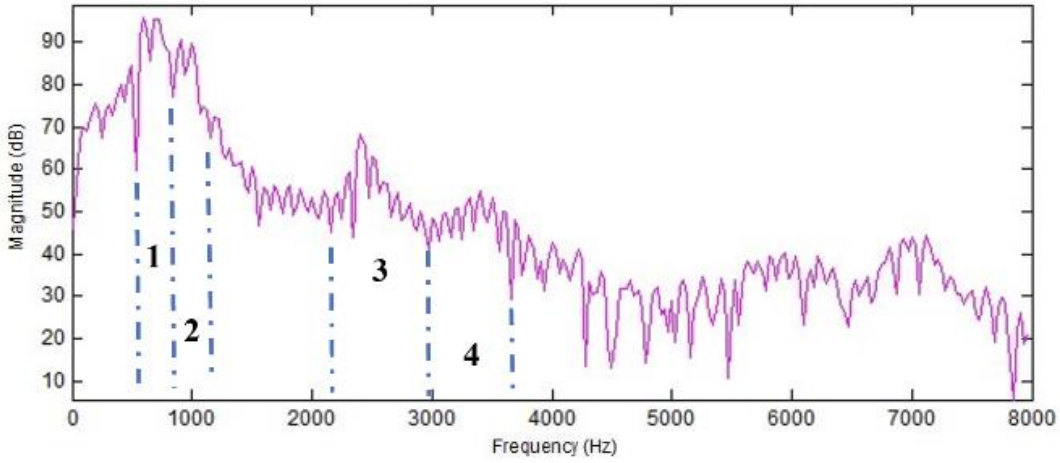


Рис. 1. Визначення формант людиною

Наступним етапом є таке представлення спектрограми, що дозволить провести сегментацію формантних частот на основі різних математичних методів, найчастіше всі вони базуються на алгоритмах кластеризації або на побудові обвідної спектра. Найвідомішими з алгоритмів, що використовують обвідну спектра, є:

- метод лінійного передбачення – коли обвідна спектра будується на алгоритмі LPC [23];
- апроксимації спектра кубічними сплайнами або іншими видами функцій [24].

Однак згідно з дослідженнями обидва алгоритми мають практично однакову точність при різній обчислювальній складності [25].

Приклад обвідної на основі алгоритму лінійного передбачення виділеного спектра для стандартного фрагмента дослідження (20 мс) зображено на рис. 2. На основі цього рисунка виділяють локальні максимуми обвідної для спектра мовного сигналу, які розглядають як центри формантних частот.

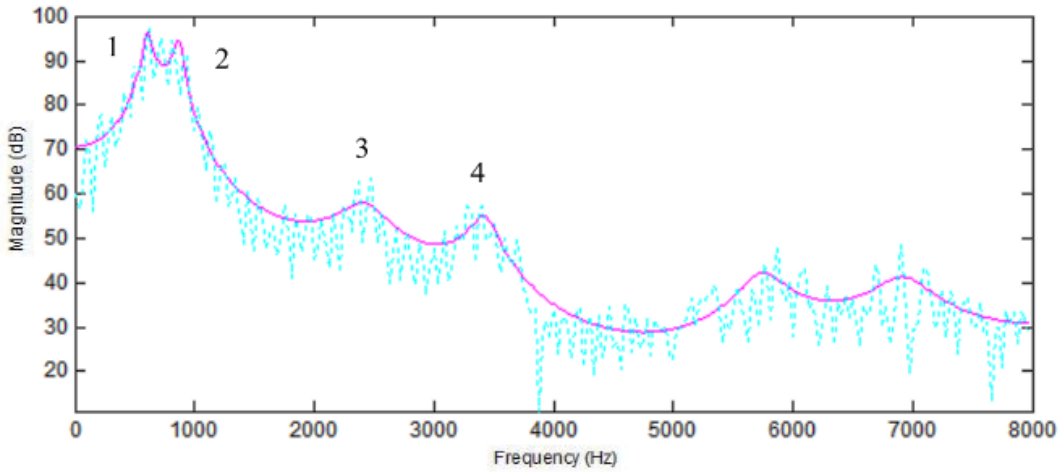


Рис. 2. Побудова обвідної для спектра мовного сигналу (числами зображено формантні діапазони 1–4)

Проведені попередні дослідження вказують на відповідність розподілу частот відносно голосних звуків, які вносять найбільшу вагу в формування формант в мовному сигналі. Установлено, що

частина голосних звуків у більшості мов розташована в частотному діапазоні 200–500 Гц, а інша частина голосних звуків у діапазоні від 500 до 1500 Гц. Зважаючи на це, раціональним є окремий розгляд цих частотних діапазонів, під час формування характерних ознак мовного сигналу, що дозволяє підвищити кількість параметрів, та набирати більшу статистику при визначенні максимумів формантних частот.

Результатом проведеного огляду підходів до визначення формантних частот став алгоритм (рис. 3), що складається з таких етапів.

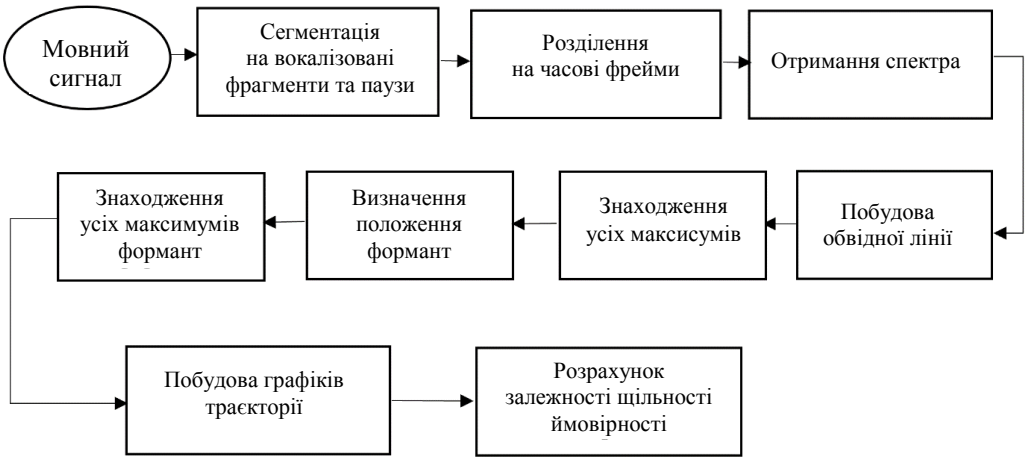


Рис. 3. Алгоритм визначення формантних частот

1. Сегментація мовного сигналу на вокалізовані фрагменти та паузи.
2. Розбиття вокалізованих фрагментів МС на часові фрейми.
3. Для кожного фрагмента отримання спектра на основі вейвлет-перетворення.
4. Побудова обвідної лінії.
5. Знаходження всіх максимумів.
6. Визначення положень формантних діапазонів.
7. Отримання максимумів формантних діапазонів.
8. Побудова графіків траєкторії положення формант (рис. 4).

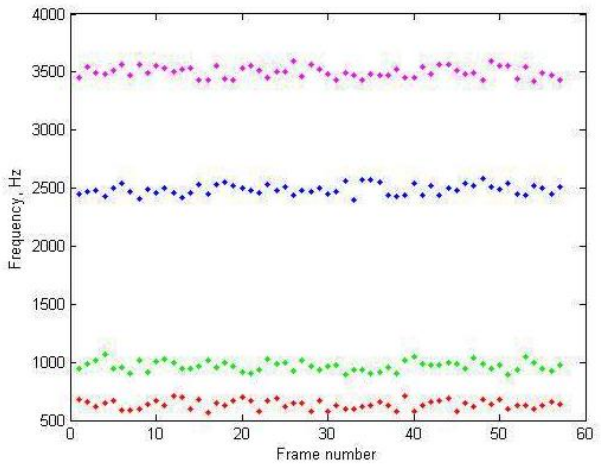


Рис. 4. Траєкторія положення формант за номерами фреймів

9. Розрахунок залежності щільності ймовірності розподілу кожної із чотирьох формантних частот (максимумів формантних частот).

Сегментація МС на вокалізовані фрагменти й паузи виконується методом оцінювання змін фрактальної розмірності [26]. У роботі визначено, що фрактальна розмірність D для невокалізованих фрагментів у 99 % випадків перебуває в межах $1{,}04 \leq D \leq 1{,}45$, а фрактальна розмірність вокалізованих фрагментів не спостерігалася менше $D = 1{,}55$ для часового вікна розміром 20 мс.

Операцію розбиття виділених вокалізованих фрагментів МС на часові фрейми виконувалась фреймами 10–20 мс для тестування робочої спроможності методу.

Отримання спектра мовного сигналу виконувалося з використанням комплексного вейвлету Морле на основі віконної функції Гаусса.

Відповідно до розглянутого підходу до визначення формантних частот необхідно побудувати обвідну спектра для кожного з фрагментів МС. Проведені в багатьох роботах дослідження при побудові обвідної пропонують використання безлічі підходів, але у разі визначення форматних частот саме кубічні сплайни дозволяють найточніше визначити вид цієї функції обвідної за заданими значеннями спектра МС. Фактично побудова функції обвідної представляє собою задачу інтерполяції. Визначимо, як ця задача розв'язується у нашому випадку.

Розглянемо спектр МС, як функцію, визначену в точках $x_0, x_1, x_2, \dots, x_N$, де відомі значення деякої функції $f(x)$, а саме $y_0, y_1, y_2, \dots, y_N$.

Інтерполюємо графік функції $f(x)$ побудовою функції $F(x)$ такої, що набуває в зазначених точках ті ж значення, тобто $F(x_0) = y_0, F(x_1) = = y_1, \dots, F(x_N) = y_N$.

З геометричної точки зору стоїть задача пошуку певного типу кривої $y = F(x)$, що проходить через набір представлених точок. Подібна задача може мати багато розв'язків чи розв'язки можуть бути відсутні. У процесі використання кубічного сплайну наша функція $F(x)$ представляє набір фрагментів, що визначені на кожному інтервалі $[x_{k-1}; x_k]$, та може мати вигляд

$$F_k(x) = a_k + b_k(x - x_k) + c_k(x - x_k)^2 + d_k(x - x_k)^3 \quad (1)$$

$F = F_1$ для $[x_0; x_1]$

…

$F = F_N$ для $[x_{N-1}; x_N]$ де N – кількість точок, за якими проводиться інтерполяція.

Звичайно, що коефіцієнти полінома a_k, b_k, c_k, d_k будуть відрізнятися для кожного з відрізків $[x_{k-1}; x_k]$.

Для визначення коефіцієнтів накладається ряд умов, серед яких такі:

Рівність других похідних функції на кінцях відрізка $[x_0; x_N]$:

$$F''(x_0) = 0, F''(x_N) = 0. \quad (2)$$

Безперервності першої і другої похідної функції $F(x)$, а також:

$$\begin{gathered} F_{k-1}(x_{k-1}) = F_k(x_{k-1}), \\ F'_{k-1}(x_{k-1}) = F'_k(x_{k-1}), \\ F''_{k-1}(x_{k-1}) = F''_k(x_{k-1}), \\ \text{при } k = 2,3, \dots, N \end{gathered} \quad (3)$$

Запишемо похідні функції F_k у вигляді

$$\begin{gathered} F'_k(x) = b_k + 2c_k(x - x_k) + 3d_k(x - x_k)^2, \\ F''_k(x) = 2c_k + 6d_k(x - x_k). \end{gathered} \quad (4)$$

Зважаючи на описані вище умови, отримуємо таку систему рівнянь:

$$\begin{gathered} a_1 - b_1h_1 + c_1h_1^2 - d_1h_1^3 = y_0, \\ a_k = y_k, k = 1,2, \dots, N, \\ a_{k-1} = a_k - b_kh_k + c_kh_k^2 - d_kh_k^3, \\ k = 2,3, \dots, N, \\ b_{k-1} = b_k - 2c_kh_k + 3d_kh_k^2, \\ k = 2,3, \dots, N, \\ c_{k-1} = c_k - 3d_kh_k, \ k = 2,3, \dots, N, \\ c_1 - 3d_1h_1 = 0, \\ c_N = 0, \end{gathered} \quad (5)$$

де $h_k = x_k - x_{k-1}, \ k = 1,2, \dots, N,$

$l_k = (y_k - y_{k-1})/h_k, \ c_0 = 0.$

Існує досить багато варіантів розв'язання представленої системи рівнянь. Для розв'язання будемо використовувати метод прогонки.

В основі методу лежить застосування коефіцієнтів, що будуть корегуватися у процесі налаштування. Визначимо коефіцієнти у вигляді

$$\begin{gathered} \delta_1 = -h_2/(2(h_1 + h_2)), \\ \lambda_1 = 3(l_2 - l_1)/(2(h_1 + h_2)), \\ \delta_{k-1} = -\frac{h_k}{2h_{k-1} + 2h_k + h_{k-1}\delta_{k-2}}, \\ k = 3,4, \dots, N, \end{gathered} \quad (6)$$

$$\lambda_{k-1} = \frac{(3l_k - 3l_{k-1} - h_{k-1}\lambda_{k-2})}{(2h_{k-1} + 2h_k + h_{k-1}\delta_{k-2})}. \quad (7)$$

На основі коефіцієнтів прогону отримуємо c_k за алгоритмом зворотного прогону:

$$\begin{gathered} c_{k-1} = \delta_{k-1}c_k + \lambda_{k-1}, \\ k = N, N-1, N-2, \dots, 2. \end{gathered} \quad (8)$$

Усе це дає можливість визначити коефіцієнти b_k і d_k за формулами

$$\begin{gathered} b_k = l_k + \frac{2c_kh_k + h_kc_{k-1}}{3}, \ k = 1,2, \dots, N \\ d_k = (c_k - c_{k-1})/(3h_k), \ k = 1,2, \dots, N. \end{gathered} \quad (9)$$

Таким чином, результатом описаного алгоритму будуть коефіцієнти b_k, c_k, d_k для кожного з розглянутих інтервалів графіка спектра МС.

Результатом розрахунку обвідної буде графік спектра МС у заданому фрагменті та обвідної спектра для цього ж інтервалу (рис. 5).

Визначаючи максимуми обвідної спектра (рис. 5), отримуємо максимуми чотирьох перших формант. Набір формант для кожного фрейму зображено на графіку відповідно до частоти форманти та номера фрейму, з якого вона була отримана (рис. 4). Аналіз цього графіка показує достатньо високу стабільність визначення формантних частот для розглянутого у попередньому дослідженні мовного сигналу.

З метою оцінювання та порівняння запропонованого методу з методами, що використовуються у відомих формант-трекерах, виконано наступне дослідження.

Для дослідження розглядались формант-трекери PRAAT, SNACK, ASSP і DEEP. Налаштування кожного з них здійснювалося на основі набору параметрів за замовчуванням, що

було закладено розробниками цих трекерів. Набір налаштувань для кожного з трекерів представлено у табл. 1. Основні параметри налаштувань відомих трекерів визначено на основі [21]. Необхідно також зазначити, що кожен із цих відомих трекерів має особливості використання відповідно до статі особи, так: PRAAT оптимізовано для мовних сигналів жінок, SNACK та ASSP оптимізовано під мовні сигнали чоловіків. DEEP, як описано у розробника, оптимізувався на наборі даних 67 жінок на 95 чоловіків, тому, можливо, він буде точніше працювати з мовними сигналами чоловіків.

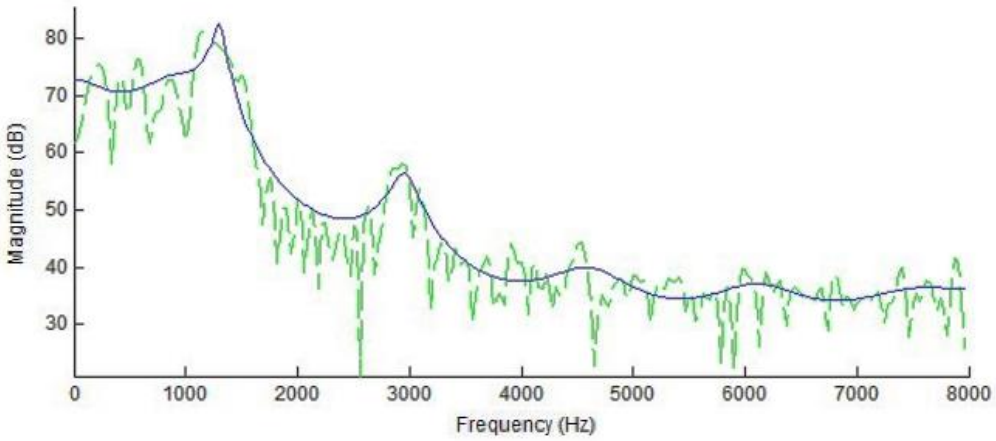


Рис. 5. Обвідна спектра МС

***Таблиця* 1**

Налаштування формант-трекерів, використаних у дослідженні

Параметр	PRAAT	SNACK	ASSP	DEEP	Пропонований метод
formants	5	4	4	4	4
LPC	10	12	18	n/a	n/a
preemph	50 Hz/oct	0,7	0.96	unk	–
window	gauss	cos4	blackman	unk	gauss
w.length, ms	25	25	25	unk	25
stepsize, ms	10	10	10	10	10

Налаштування часових інтервалів власного методу має відповідати розміру подібних інтервалів для інших формант-трекерів для коректного порівняння, тому використовують розмір вікна 25 ms із кроком 10 ms.

У дослідженні трекери самостійно виконували сегментацію на вокалізовані фрагменти і паузи, застосовуючи датасет VTR-TIMIT, у випадку некоректної сегментації (невокалізований фрагмент вважався вокалізованим) помилкові результати сегментації вилучалися з розгляду.

Як параметри порівняння використовували середньоквадратичне відхилення формант між еталонною розміткою мовних сигналів та результатами формант-трекерів (табл. 2).

***Таблиця* 2**

Середньоквадратичне відхилення визначення формант (Гц)

Formant	Female/Male	PRAAT	SNACK	ASSP	DEEP	Proposed Method
F1	f	97	104	82	61	78
	m	161	92	71	53	70
F2	f	185	197	172	99	89
	m	215	209	109	84	91
F3	f	194	183	215	156	167
	m	247	261	113	171	144

Розгляд саме трьох формант, замість чотирьох, пов'язаний із тим, що в датасеті VTR-TIMIT розмічені експертами лише три форманти. Крім того, проведений аналіз цього датасету [27] показав середнє відхилення частоти максимуму для 1–3 формант відповідно 78, 100, 111 Гц, тому отримані значення достатньою мірою відповідають раніше проведеним дослідженням.

Порівняльний аналіз показує достатньо високу точність визначення формантних частот порів-

няно з існуючими формант-трекерами. Виняток стосується DEEP, але зважаючи не те, що він натренований на саме цьому датасеті, можна вважати, що метод достатньо добре показує себе порівняно з іншими. Поряд із цим, необхідно зазначити простоту реалізації, низьку обчислювальну складність, швидкість і відповідність методу наявним фізичним процесам.

4. ВИСНОВКИ

На основі огляду існуючих підходів до алгоритму визначення формантних частот установлено наявність складності їхньої реалізації та часткову відсутність фізичного обґрунтування операцій, що входять до їхнього складу. Запропоновано метод визначення формантних частот, що як вхід використовує спектральне розкладання мовного сигналу на два діапазони, що відповідають частотним межам голосних звуків. Представлено алгоритм обчислення обвідної, а також опис методу визначення параметрів формантних частот до побудови функції щільності ймовірності, що може бути використана під час безпосереднього порівняння в задачі прийняття рішення щодо мовної ідентифікації особи. Порівняння методу з іншими подібними методами показало задовільну точність. Використання запропонованого методу разом із методологією сегментації мовного сигналу дозволять знизити похибку під час виділення формант, що приведе до підвищення точності прийняття рішення у процесі побудови систем ідентифікації мовного сигналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Yegnanarayana, B., Veldhuis, R. N. J. (1998). Extraction of vocaltract system characteristics from speech signals, IEEE Trans. Speech Audio Process, 6 (4), 313–327.

[2] Kim, C., Seo, K., & Sung, W. A Robust (2006). Formant Extraction Algorithm Combining Spectral Peak Picking and Root Polishing. *EURASIP Journal on Applied Signal Processing*, 1–16.

[3] Wet, F. D., Weber, K., Boves, L., Cranen, B., Bengio, S., & Bourlard, H. (2004). Evaluation of Formant-Like Features for Automatic Speech Recognition. *Journal of the Acoustical Society of America*, 116, 1781–1791.

[4] Mallat, S. (1999.) A Wavelet Tour of Signal Processing. *Academic Press.*

[5] Yan, Q., Vaseghi, S., Zavarehei, E., Milner, B., Darch, J., White, P., & Andrianakis, I. (Jul. 2007). Formant Tracking Linear Prediction Model using HMMs and Kalman Filters for Noisy Speech Processing. *Computer Speech and Language*, vol. 21, pp. 543–561.

[6] Messaoud, Z. B., Gargouri, D., Zribi, S., & Hamida, A. B. (2009). Formant Tracking Linear Prediction Model using HMMs for Noisy Speech Processing. *International Journal of Signal Processing*, vol. 5, pp. 291–296.

[7] Cooke, M., Barker, J., Cunningham, S., & X. Shao (2006). An audio-visual corpus for speech perception and automatic speech recognition. *Journal of the Acoustical Society of America*, vol. 120.

[8] Acero, A. Formant Analysis and Synthesis using Hidden Markov Models (1999). In *Proc. of the Eurospeech Conference.* Budapest.

[9] Veldhuis, R. (1997). A computationally e$cient alternative for the LF model and its perceptual evaluation. *J. Acoust. Soc.*, 103 (1), 566–571.

[10] Bazzi, I., Acero, A., & Deng, L. (2003). An expectation maximization approach for formant tracking using a parameter-free non-linear predictor. In *Proc. ICASSP*, vol. 1, 464–467.

[11] Ali, J. A. M. A., Spiegel, J. V. D., & Mueller P. (2002). Robust Auditory-based Processing using the Average Localized Synchrony Detection. In *IEEE Transaction Speech and Audio Processing*.

[12] Vakman, D. (1996). On the analytic signal, the Teager-Kaiser energy algorithm, and other methods for defining amplitude and frequency. *IEEE Trans. Signal Process*, SP-44, 791–797.

[13] Boersma, P., & D. Weenink, (2017). Praat: doing phonetics by computer [Computer program]. Version 6.0.23, retrieved 2021-05-17. http://www.praat.org/

[14] Kåre Sjölander(2020) The Snack Sound Toolkit [Computer program]. https://www.speech.kth.se/snack/

[15] Scheffer, M. (2017). Available: Advanced Speech Signal Processor (libassp), retrieved 2021-05-17. http://www.sourceforge.net/projects/libassp.

[16] Keshet, J. (2017). DeepFormant, retrieved 2021-05-25. https://github.com/MLSpeech.

[17] Gray, A., & Wong, D. (1980, Dec.). The Burg algorithm for LPC speech analysis/Synthesis. *In IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 28, no. 6, pp. 609–615.

[18] Krishna, H., & Wang, Y. (1993). The Split Levinson Algorithm is Weakly Stable. *SIAM Journal on Numerical Analysis*, 30(5), 1498–1508., http://www.jstor.org/stable/2158249

[19] So, H. C., & Chan, K. W. (2004). Reformulation of Pisarenko Harmonic Decomposition Method for Single-Tone Frequency Estimation. *Signal Processing, IEEE Transactions* on. 52. 1128–1135. 10.1109/TSP.2004.823473.

[20] VTR Formants Database. http://www.ee.ucla.edu/~spapl/VTRFormants.rar

[21] Nearey, T. & Assmann, P. & Hillenbrand, J. (2002). Evaluation of a strategy for automatic formant tracking. *The Journal of the Acoustical Society of America*. 112. 2323. 10.1121/1.4779372.

[22] Schiel, Florian & Zitzelsberger. Thomas (2018). Evaluation of Automatic Formant Trackers. *Proceedings of the Eleventh International Conference on Language Resources and Evaluation {LREC}*, Miyazaki, Japan.

[23] Markel, J. E. & Gray, A. H. (1982). *Linear Prediction of Speech.* New York, NY: Springer.

[24] Sun, Don X. (1995). Robust estimation of spectral center-of-gravity trajectories using mixture spline models. In *EUROSPEECH-1995*, 749–752.

[25] Schalk-Schupp, Ingo. (2012). Improved Noise Reduction for Hands-Free Communication in Automobile Environments. 10.13140/2.1.4068.6724.

[26] Бєлозьорова, Я. А. (2017). Ідентифікація диктора на основі кратномасштабного аналізу. Інженерія програмного забезпечення: наук. журн., 1(29). 15–25.

[27] Deng, L., Cui, X., Pruvenok, R., Huang, J., Momen, S., Chen, Y. N., & Alwan, A. (2006). A Database of Vocal Tract Resonance Trajectories for Research in Speech Processing. In Proc. of the Int. Conf. on Acoustics, Speech, and Signal Processing.

REFERENCES

[1] Yegnanarayana, B., Veldhuis, R. N. J. (1998). Extraction of vocaltract system characteristics from speech signals, IEEE Trans. Speech Audio Process, 6 (4), 313–327.

[2] Kim, C., Seo, K., & Sung, W. A Robust (2006). Formant Extraction Algorithm Combining Spectral Peak Picking and Root Polishing. *EURASIP Journal on Applied Signal Processing*, 1–16.

[3] Wet, F. D., Weber, K., Boves, L., Cranen, B., Bengio, S., & Bourlard, H. (2004). Evaluation of Formant-Like Features for Automatic Speech Recognition. *Journal of the Acoustical Society of America*, 116, 1781–1791.

[4] Mallat, S. (1999.) A Wavelet Tour of Signal Processing. *Academic Press.*

[5] Yan, Q., Vaseghi, S., Zavarehei, E., Milner, B., Darch, J., White, P., & Andrianakis, I. (Jul. 2007). Formant Tracking Linear Prediction Model using HMMs and Kalman Filters for Noisy Speech Processing. *Computer Speech and Language*, vol. 21, pp. 543–561.

[6] Messaoud, Z. B., Gargouri, D., Zribi, S., & Hamida, A. B. (2009). Formant Tracking Linear Prediction Model using HMMs for Noisy Speech Processing. *International Journal of Signal Processing*, vol. 5, pp. 291–296.

[7] Cooke, M., Barker, J., Cunningham, S., & X. Shao (2006). An audio-visual corpus for speech perception and automatic speech recognition. *Journal of the Acoustical Society of America*, vol. 120.

[8] Acero, A. Formant Analysis and Synthesis using Hidden Markov Models (1999). In *Proc. of the Eurospeech Conference.* Budapest.

[9] Veldhuis, R. (1997). A computationally e$cient alternative for the LF model and its perceptual evaluation. *J. Acoust. Soc.*, 103 (1), 566–571.

[10] Bazzi, I., Acero, A., & Deng, L. (2003). An expectation maximization approach for formant tracking using a parameter-free non-linear predictor. In *Proc. ICASSP*, vol. 1, 464–467.

[11] Ali, J. A. M. A., Spiegel, J. V. D., & Mueller P. (2002). Robust Auditory-based Processing using the Average Localized Synchrony Detection. In *IEEE Transaction Speech and Audio Processing*.

[12] Vakman, D. (1996). On the analytic signal, the Teager-Kaiser energy algorithm, and other methods for defining amplitude and frequency. *IEEE Trans. Signal Process*, SP-44, 791–797.

[13] Boersma, P. & Weenink, D. (2017). Praat: doing phonetics by computer [Computer program]. [Online]. Available: Version 6.0.23, retrieved 2022-05-17 from http://www.praat.org/

[14] Kåre Sjölander (2020) The Snack Sound Toolkit [Computer program]. [Online]. Available: https://www.speech.kth.se/snack/

[15] Scheffer, M. (2017). [Online]. Available: Advanced Speech Signal Processor (libassp), retrieved 2022-05-17 from http://www.sourceforge.net/projects/libassp.

[16] Keshet, J. (2017). [Online]. Available: DeepFormant, retrieved 2022-05-25 from https://github.com/MLSpeech.

[17] Gray, A., & Wong, D. (1980, Dec.). The Burg algorithm for LPC speech analysis/Synthesis. *In IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 28, no. 6, pp. 609–615.

[18] Krishna, H., & Wang, Y. (1993). The Split Levinson Algorithm is Weakly Stable. SIAM Journal on Numerical Analysis, 30(5), 1498–1508. [Online]. Available: Retrieved Juny 11, 2021, from http://www.jstor.org/stable/2158249

[19] So, H.C. & Chan, K.W. (2004). Reformulation of Pisarenko Harmonic Decomposition Method for Single-Tone Frequency Estimation. Signal Processing, IEEE Transactions on. 52. 1128–1135. 10.1109/TSP.2004.823473.

[20] VTR Formants Database. [Online]. Available: http://www.ee.ucla.edu/~spapl/VTRFormants.rar

[21] Nearey, Terrance & Assmann, Peter & Hillenbrand, James. (2002). Evaluation of a strategy for automatic formant tracking. The Journal of the Acoustical Society of America. 112. 2323. 10.1121/1.4779372.

[22] Schiel, Florian and Zitzelsberger, Thomas. "Evaluation of Automatic Formant Trackers", Proceedings of the Eleventh International Conference on Language Resources and Evaluation {LREC} 2018, Miyazaki, Japan.

[23] Markel, J.E. & Gray, A.H. (1982). Linear Prediction of Speech. New York, NY: Springer.

[24] Sun, Don X. (1995): "Robust estimation of spectral center-of-gravity trajectories using mixture spline models", In EUROSPEECH-1995, 749–752.

[25] Schalk-Schupp, Ingo. (2012). Improved Noise Reduction for Hands-Free Communication in Automobile Environments. 10.13140/2.1.4068.6724.

[26] Belozyorova Y. A. (2017). Speaker identification based on multiple-scale analysis. Scientific journal. Software engineering, 1(29), 15–25 [in Ukrainian].

[27] Deng, L., Cui, X., Pruvenok, R., Huang, J., Momen, S., Chen, Y. N. & Alwan, A. (2006). A Database of Vocal Tract Resonance Trajectories for Research in Speech Processing. In Proc. of the Int. Conf. on Acoustics, Speech, and Signal Processing.

Стаття надійшла до редколегії 21.03.2023

Method of determining formant frequencies using spectral decomposition of speech signal

Formants are one of the main components of speaker identification systems and the accuracy of formant determination is the basis for the efficiency of speaker identification systems. Improving existing speech recognition systems will significantly simplify human-computer interaction when the use of classic interfaces is not possible, as well as make such work more comfortable and efficient.

The necessity for research on this topic is due to unsatisfactory results of existing systems with low signal-to-noise ratio, the dependence of the result on humans, as well as low speed of such systems.

The following four main formant trackers were used for comparison with the proposed method: PRAAT, SNACK, ASSP and DEEP. There are a number of studies concerning the comparison of formant trackers, but among them it is impossible to single out the one that has the best efficiency.

The selection of formants is accompanied by a number of problems associated with their dynamic change in the language process. The complexity is also caused by a number of problems related to the close location of the peaks in the analysis of spectrograms and the problems of correctly determining the peaks of the formant maxima on the spectrogram. Determining the location of the formant on the spectrograms of the vocal signal is quite easy to perform by man, but the automation of this process causes some difficulties.

The selection of frequency formants was proposed to be performed in several stages. The result of the review of approaches to the determination of formant frequencies has been the algorithm consisting of the following nine stages. The segmentation of vocal signal into vocalized fragments and pauses is performed by estimating changes in fractal dimension. Obtaining the spectrum of the vocal signal has been performed using a complex Morlet wavelet based on the Gaussian window function. PRAAT, SNACK, ASSP and DEEP formant trackers have been considered for the study. Each of them has been configured on the basis of a set of default parameters set by the developers of these trackers. A set of settings for each of the trackers has been used for comparison. In the study, trackers independently have been performed segmentation into vocalized fragments and pauses using the VTR-TIMIT dataset.

The comparative analysis has been showed a fairly high accuracy in determining the formant frequencies in comparison with existing formant trackers.

Keywords: *speech signal; formant frequencies; spectral decomposition; computational algorithm; wavelet analysis.*

Сергій Зибін,
д-р техн. наук, проф.
Завідувач кафедри інженерії програмного забезпечення Національного авіаційного університету. Київ, Україна.

Serhii Zybin,
Dr. Sci. (Engin.), Prof.
Head of the Software Engineering Department of the National Aviation University. Kyiv, Ukraine.

Яна Бєлозьорова,
канд. техн. наук, доц.
Доцент кафедри інженерії програмного забезпечення Національного авіаційного університету. Київ, Україна.

Yana Belozyorova,
PhD (Engin.), Associate Prof.
Associate Professor of the Department of Software Engineering of the National Aviation University. Kyiv, Ukraine.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

УДК 004.645.34
DOI 10.17721/ISTS.2023.1.61-69

Тетяна Бабенко, orcid.org/0000-0003-1184-9483,
babenko.tetiana.v@gm
Андрій Бігдан, orcid.org/0000-0002-2940-6085,
abigdan@gmail.com
Лариса Мирутенко, orcid.org/0000-0003-1686-261X,
myrutenko.lara@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ІНТЕЛЕКТУАЛЬНА МОДЕЛЬ КЛАСИФІКАЦІЇ МЕРЕЖНИХ ПОДІЙ ІЗ КІБЕРБЕЗПЕКИ

Через збільшену складність сучасних комп'ютерних атак, виникає потреба у фахівцях із безпеки не тільки для виявлення шкідливої активності, але і для визначення відповідних кроків, які проходитиме зловмисник у ході виконання атаки. Незважаючи на те, що виявлення експлойтів і вразливостей зростає з кожним днем, розроблення методів захисту просувається помітно повільніше за розроблення методів нападу. Саме тому це все ще залишається відкритою дослідницькою проблемою. У цій статті представляємо дослідження у галузі ідентифікації мережних атак із використанням нейронних мереж, зокрема багатошарового персептрона Румельхарта, для виявлення та прогнозування майбутніх подій мережної безпеки на основі попередніх спостережень. Для забезпечення якості процесу навчання й отримання бажаного узагальнення моделі використано 4 млн записів, накопичених протягом 7 днів Канадським інститутом кібербезпеки. Наш результат демонструє, що моделі нейронних мереж, що базуються на багатошаровому персептроні, можуть використовуватися після уточнення для виявлення та прогнозування подій мережної безпеки.

Ключові слова: *безпека інформаційних систем; нейронна мережа; мережна безпека; прогнозування.*

1. ВСТУП

Щороку до загальної кількості програмного коду додається 111 трильйонів рядків, причому кожен рядок потенційно може бути новою вразливістю і, як наслідок, може бути реалізована атака нульового дня. Зазначимо, що технології, які використовуються зловмисниками для атак на комп'ютерні системи та мережі, стають усе складнішими та досконалішими [1]. Вивчають багато шляхів розв'язання цієї проблеми, зокрема і технології, що дозволяють створювати захищене програмне забезпечення [2]. Із цією метою для автоматизації процесів контролю подій безпеки в інформаційних системах традиційно використовують системи виявлення вторгнень (IDS/IPS – Intrusion Detection/Protection System), основним завданням яких є автоматизація процесу виявлення атак або неправомірного застосування [3–6]. Ці системи залежно від технології, що використовується для виявлення атак, прийнято розділяти на дві основні групи: системи виявлення зловмисної поведінки користувачів; системи виявлення аномальної поведінки комп'ютерної системи. У першому випадку порівнюється шаблон атаки з потоком подій, у другому – порівнюється шаблон нормальної поведінки системи з потоком подій. Прийнято вважати, що завдання виявлення вторгнень у мережі TCP/IP зводиться до розпізнавання задач [7–9]:

- структурні ознаки (сигнатури) відомих видів атак;
- інваріантні ознаки структури правильних обчислювальних процесів;
- кореляційні ознаки нормального функціонування розподілених обчислювальних систем.

У разі проблеми з розпізнаванням мережних аномалій виникають деякі труднощі, які в основ-

ному пов'язані зі зростаючим попитом на виявлення раніше невідомих атак і деструктивних впливів, що у свою чергу потребує:

• побудови еталонних множин нормального (семантично правильного) профілю поведінки системи в умовах невизначеності впливів зовнішнього середовища;

• визначення необхідних і достатніх інформативних ознак;

• побудови правил визначення аномалій.

Як правило, виявлення мережних аномалій здійснюється за схемою, в якій виокремлюють такі функціональні блоки [10]:

• аналіз інформації, що міститься в заголовках IP-дейтаграм;

• побудова прогнозування;

• пошук та оцінювання аномалій;

• реакція на аномалію;

• наповнення та/або редагування базових правил IDS/IPS.

Зібрану статистичну інформацію використовують для побудови математичної моделі прогнозування трафіка на основі циклічного аналізу часових рядів. Ця модель дозволяє прогнозувати завантаження мережі на основі пошуку частот у мережному трафіку.

У всіх випадках IDS не зможе виявити вторгнення, тому що не зможе відрізнити його від фонового білого шуму, який існує в будь-якій системі через слабкість інструменту аналізу пакетів або відсутність сигнатури відповідної атаки тощо.

Отже, більшість типових способів виявлення атак і протидії їм мають низьку точність і швидкість і не дозволяють ефективно протидіяти як відомим атакам, так і атакам нульового дня. Тому розробляється велика кількість різних технологій захисту комп'ютерних систем та мереж, заснованих на технологіях перевірки даних із використанням штучного інтелекту із застосуванням нейронних мереж [11–15]. Це пов'язано зі здатністю нейромережної структури розв'язувати завдання, що важко формалізуються, а також з її здатністю до навчання, самоорганізації та узагальнення. Такий підхід дозволяє отримувати моделі, здатні швидко адаптуватися до навколишнього середовища та прогнозувати розвиток процесу на основі якості узагальнення [16, 17].

Штучний інтелект – термін у широкому сенсі – спирається за допомогою комп'ютерів на імітації можливостей людини: почуття, розуміння, реагування.

Машинне навчання – область штучного інтелекту у розділі комп'ютерних наук, де часто використовують статистичні методи, щоб дати комп'ютерам можливість "навчатись" (наприклад, поступово підвищувати продуктивність у конкретній задачі) [18].

Розглядаючи науку про дані, зазначимо, що для виконання (використання) алгоритмів машинного навчання необхідне визначення наборів даних, вибір відповідних змінних та метрик, а також виконання різних інформаційно-інженерних завдань: пошук прихованих залежностей, збір даних, навчання, інтеграція, візуалізація, визначення продуктивності алгоритмів тощо.

Кожна модель навчання має ґрунтуватися на певному алгоритмі. Зокрема, до них належать класифікація, кластеризація, асоціативні правила, поглиблене навчання, регресія, зіставлення із зразком. Вибір алгоритму залежить від кінцевої мети, яку потрібно досягти. Модель ідентифікації подій кібербезпеки, що розглядається в цьому дослідженні, заснована на навчанні з учителем та на алгоритмах класифікації нейронних мереж.

2. МАТЕРІАЛ І МЕТОДИ

У ході розв'язання завдання класифікації подій, що відбуваються у процесі мережної взаємодії, виникають проблеми, в основному пов'язані з необхідністю обліку невідомих атак і деструктивних впливів, що у свою чергу вимагає: системи в умовах невизначеності впливів зовнішнього середовища, визначення необхідних і достатніх інформативних ознак та побудови правил виявлення аномалій [19, 20].

Аналогічне і менш складне завдання виконано для атак із застосуванням (ін'єкції) SQL (Structured Query Language) [21]. SQL-ін'єкція – це атака, що реалізується шляхом модифікації запитів до бази даних за рахунок експлуатації вразливостей, що містяться у вебдодатках. Успішна реалізація атаки дає зловмиснику можливість отримати конфіденційну інформацію, змінити або знищити її.

Для синтезу й аналізу моделі ідентифікації атак SQL-ін'єкцій були підготовлені набори даних попереднього навчання, контролю та тестування. Навчальний набір даних містив параметри навчання; вибір параметрів був евристично заснований на аналізі основних ознак атаки, які можуть містити URL-адресу.

Штучні нейронні мережі – це математичні моделі та їхні програмні чи апаратні реалізації. Цей термін з'являється під час вивчення процесів, що відбуваються в мозку, та за спроби змоделювати ці процеси. Основними принципами є інтерпретація сенсорних даних за допомогою свого роду машинного сприйняття, маркування або угруповання

даних, що надходять. Образи, що розпізнаються, є числовими і містяться у векторах, в які транслюються будь-які інші дані [22].

Кожен вузол має один або кілька входів і один вихід. Нейрон має два режими роботи: режим навчання та режим використання або тестування. У режимі навчання нейрон навчається реагувати на певний вхідний шаблон. У робочому режимі нейрон реагує на вхідний шаблон і пов'язує вихід. Якщо нейрон отримує на вхід нетиповий набір параметрів, він сам визначає, активувати себе чи ні.

Кожен вхідний сигнал має відповідну вагу, яка розраховується на основі вхідних даних. Якщо це число перевищить поріг, нейрон спрацює.

Активація будь-якого нейрона регулюється його активаційною функцією.

Нейронні моделі працюють виключно з числовими даними, представленими в деякому числовому діапазоні, тому на першому етапі дослідження розроблено класифікатор URL. Це програмний модуль, який перетворює URL-адресу на двійковий формат і встановлює логічний ідентифікатор "true (1)", якщо адреса відноситься до атаки, і "false (0)" – в іншому випадку. Таким чином, для кожної з URL-адрес було згенеровано вхідний вектор, тобто вихідний вектор може бути представлений у форматі

$$X^{\mathrm{T}} = [x_1 x_2 \cdots x_n],$$

де n – кількість параметрів запиту, що використовується у шаблонах SQL.

На основі цього підходу нейромережна модель матиме на вході n нейронів. Кожен вектор характеризується параметром: доброякісний (0) – не відноситься до нападу, та ін'єкційний (1) – відноситься до нападу. Достатньо мати на виході лише один нейрон, що розділяє вхідні вектори на два класи 0 та 1.

У результаті відносна похибка синтезованої моделі на контрольному та дослідному зразках не перевищує 5 %. Таким чином, можемо застосувати такий підхід для ширшого спектра подій безпеки й атак.

Метою цього дослідження є вивчення можливостей використання штучних нейронних мереж, зокрема персептрона Румельхарта (окремий випадок персептрона Розенблатта) для виявлення мережних атак і прогнозування подій, пов'язаних із мережною безпекою [23, 24]. Для забезпечення якості процесу навчання й отримання бажаного узагальнення властивостей моделі необхідно мати значну кількість прикладів реалізації відповідних атак. В експериментальних цілях зібрано 4 млн записів, які протягом 7 днів накопичив Канадський інститут кібербезпеки. Мережна інфраструктура зловмисника складалася з 50 машин. Організація-жертва містила 5 відділів, і кожен з них використовував 420 користувацьких вузлів і 30 серверів. Набір даних містить інформацію про перехоплений мережний трафік і системні журнали кожної машини організації-жертви. Схему оброблення даних показано на рис. 1. Для аналізу набору даних використовували профільні поняття: B-профіль і M-профіль.

B-профіль (Benign – доброякісний) – інкапсуляція поведінки користувача з використанням різних методів машинного навчання та статистичного аналізу (таких як, K-Means, Random Forest, SVM і J48).

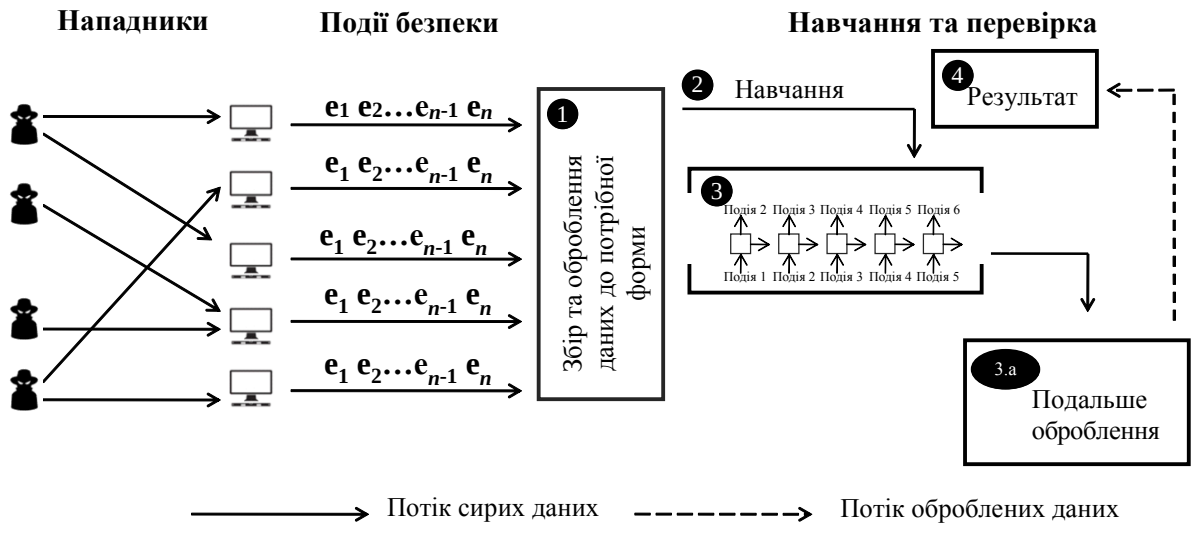


Рис. 1. Схема оброблення даних

Інкапсульовані функції – це розподіл пакетів протоколу за розміром, кількістю пакетів у потоці, певною структурою корисного навантаження, розміром корисного навантаження та запитом тимчасового поділу для протоколу.

Модель складається з таких кроків:

1. Збір даних про мережну активність із системних журналів і журналів подій.

2. Оброблення попередніх даних і зведення їх до потрібного вигляду.

3. Навчання та тестування нейронної мережі.

4. Аналіз результатів.

У моделюванні використовували такі протоколи: HTTPS, HTTP, SMTP, POP3, IMAP, SSH та FTP. За результатами частотного аналізу даних зроблено висновок, що основна маса трафіка представлена HTTP- та HTTPS-пакетами. M-профіль (Malignant – зловмисний) – спроба однозначно описати сценарій атаки. У найпростішому випадку люди можуть інтерпретувати ці профілі, а потім їх виконувати. В ідеалі для інтерпретації та виконання цих сценаріїв використовуватимуться автономні агенти разом із компіляторами. Було розглянуто різні сценарії реалізації атак:

• мережне проникнення: у цьому сценарії зловмисний файл надіслано жертві електронною поштою. Після успішної експлуатації вразливості на комп'ютері жертви запускався бекдор, після чого комп'ютер жертви використовувався для сканування внутрішньої мережі та пошуку нових поштових скриньок;

• відмова в обслуговуванні HTTP: у цьому сценарії як основні інструменти використовувалися Slowloris і LOIC (Low Orbit Ion Cannon – додаток для стрес-тестування й атаки типу "відмова в обслуговуванні" (DoS або DDoS) із відкритим вихідним кодом, написаний на C#), які, як відомо, роблять вебсервери повністю недоступними через одну атакуючу систему. Атака за допомогою Slowloris починається з повного з'єднання TCP із віддаленим сервером. Інструмент підтримує з'єднання відкритим, відправляючи дійсні неповні HTTP-запити на сервер через певні проміжки часу, щоб уникнути закриття сокетів. Оскільки будь-який вебсервер може обслуговувати обмежену кількість можливих підключень, вичерпання всіх сокетів буде лише питанням часу, і в результаті жодних інших підключень не буде прийнято;

• атака на вебпрограми: у цьому сценарії використовувався вразливий вебдодаток (DVWA – Damn Vulnerable Web App), який спеціально розроблено, щоб допомогти фахівцям із безпеки перевірити свої навички в аналізі безпеки. Першим кроком є сканування вебсайту за допомогою сканера вразливостей вебзастосунків, а потім виконання різних типів вебатак на вебсайт, включаючи SQL-ін'єкції, ін'єкції системних команд і можливість завантаження незахищених файлів.

До способів виявлення вразливостей програмного забезпечення для SQL-ін'єкцій належать: функціональне тестування (чорна/біла скринька); фазинг (техніка автоматизованого тестування програмного забезпечення, яка полягає в тому, що на вхід програми подають недійсні, невідповідні або випадково згенеровані дані); статичний, динамічний, ручний аналізи вихідного коду. Також слід зазначити, що паралельно з пошуком вразливостей у програмованих програмах зазвичай використовується широкий спектр WAF (Web Application Firewall – брандмауер вебдодатків). Як правило, вони засновані на двох моделях безпеки: на основі підпису та на основі правил. Кожна із цих моделей має свої переваги й недоліки, але їхнім загальним недоліком є неможливість виявлення загроз "нульового дня", і зауважимо, що використання WAF може лише частково перекрити вектор атак [25–28].

Таким чином, більшість типових підходів до забезпечення безпеки від атак SQL-ін'єкцій не дозволяють отримати достатній рівень безпеки через низьку точність ідентифікації та швидкість роботи. Тому нині з'явилася велика кількість різних технологій захисту комп'ютерних систем і мереж, які ґрунтуються на технологіях інтелектуального аналізу даних, зокрема і на використанні нейронних мереж, що дозволяє ефективно протидіяти вже відомим атакам та атакам "нульового дня". Розроблено такі атаки:

• атака грубою силою: в основному спрямована на підбір комбінації імені користувача та пароля для отримання доступу до облікового запису користувача. Для цієї атаки існує безліч інструментів, таких як модулі Hydra, Medusa, Ncrack, Metasploit та Nmap NSE. Крім того, є деякі інструменти, такі як hashcat і hashpump для злому хеш-паролів. Але одним з найповніших багатопотокових інструментів є Patator, який написаний на Python і є більш гнучким, ніж інші. Він також може зберігати кожну відповідь в окремому файлі журналу для подальшого перегляду та оброблення. Для переліку паролів ми використали словник із 90 млн слів;

• атаки на останнє оновлення: атаки, засновані на деяких відомих вразливостях, які можуть бути реалізовані протягом певного періоду часу (це екстраординарні вразливості, які іноді зачіпають мільйони серверів або жертв, і зазвичай

потрібно кілька місяців, щоб виправити весь вразливий програмний код), одна з найвідоміших в останні роки – Heartbleed.

Детальну інформацію про виявлені атаки та засоби, використані для їхньої реалізації, представлено в табл. 1.

***Таблиця* 1**

Атаки на цільові системи

Тип атаки	Застосовані інструменти
Атака грубої сили (Brute-force)	FTP – Patator SSH – Patator
Атака на відмову в обслуговуванні (DoS)	Hulk, GoldenEye, Slowloris, SlowHTTPtest, Heartleech
Вебатака	Damn Vulnerable Web App (DVWA), власний Selenium Framework (XSS та Brute force)
Інфільтраційна атака	Перший рівень: завантаження Dropbox на комп'ютері з Windows. Другий рівень: Nmap і PortScan
Атака ботнету	Ares (розробка Python): віддалена оболонка (remote shell), завантаження/вивантаження файлів, захоплення знімків екрана та запис клавіш, що натискаються
DDoS разом із PortScan	Low Orbit Ion Canon (LOIC) для UDP, TCP або HTTP запитів

3. РЕЗУЛЬТАТИ

Існує два підходи до аналізу мережних атак: один ґрунтується на аналізі мережної активності, інший – на аналізі вмісту пакетів. У цьому дослідженні ми зосередилися на підході, заснованому на аналізі мережної активності. Аналіз активності мережі проводився за допомогою спеціалізованого програмного забезпечення CICFlowMeter, яке генерує двонаправлені потоки, де відправлення першого пакета визначає шлях до джерела призначення та назад до вихідної системи, і дозволяє отримати більше 80 статистичних атрибутів мережного трафіка. Для цілей моделювання визначено 67 параметрів мережного трафіка у кожному потоці.

Під час підготовки даних було додано новий атрибут Label, який ідентифікує потік як конкретну атаку чи нормальну роботу інформаційних служб. Таким чином, усі дані були позначені відповідно до таких значень: Benign, FTP-BruteForce, SSH-Bruteforce, DoS-GoldenEye, DoS-Slowloris, DoS-SlowHTTPTest, DoS-Hulk, DDoS attacks-LOIC-HTTP, DDoS-LOIC-UDP, DDOS-HOIC, Brute Force–Web, Brute Force – XSS, Infiltration, Bot.

Синтез нейромережної моделі (рис. 2) виконано на основі багатошарового персептрона Румельхарта. Багатошаровий персептрон Румельхарта є окремим випадком персептрона Розенблатта, в якому вагові коефіцієнти нейрона коригують за допомогою алгоритму зворотного розповсюдження похибки. Особливістю нейронної мережі є більше одного шару (зазвичай двох чи трьох шарів) [22]. Отже нейронна мережа у вигляді персептрона Розенблатта ділить вхідні вектори на два класи 0 і 1. Навчальна послідовність формується з двох масивів: вхідного масиву X і масиву цілей Y, який привласнює кожному зі вхідних векторів одного з двох класів.

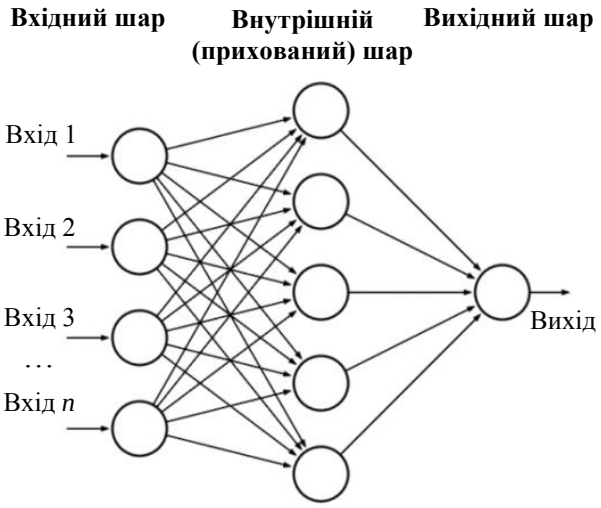


Рис. 2. Модель нейронної мережі

У дослідженні використовувалися три шари: вхідний, вихідний і один прихований. Операції нейронних мереж зворотного поширення похибки можна розділити на два етапи: пряме і зворотне поширення. На етапі прямого поширення вхідний шаблон застосовується до вхідного шару, і його ефект поширюється шар за шаром по мережі до отримання результату. Фактичне вихідне значення мережі порівнюється з очікуваним виходом, і для кожного з вихідних вузлів обчислюється сигнал помилки. Оскільки всі приховані вузли певною мірою сприяли виявленню помилок у вихідному шарі, помилки вихідних сигналів поширюються назад від вихідного шару до кожного вузла прихованого (внутрішнього) шару, що впливає на вихідний шар. Потім цей процес повторюється шар за

шаром, поки кожен вузол мережі не отримає повідомлення про помилку, що описує його відносний внесок у загальну помилку.

Після визначення сигналу помилки для кожного вузла дані про помилки будуть використовуватися для оновлення значень ваги кожного з'єднання, доки мережа не ввійде у стан, що дозволяє закодувати всі схеми навчання. Алгоритм зворотного розповсюдження помилки шукає мінімальне значення функції помилки у просторі вагових значень, використовуючи техніку, яка називається дельта-правилом або градієнтним спуском. Шкали, які мінімізують функцію помилок, вважаються розв'язанням проблеми навчання [11, 12].

У той час, як певний шаблон передається вхідному шару у процесі навчання, зважена сума входу j-го вузла у прихованому шарі обчислюється за формулою

$$Net_j = \sum w_{ij} x_j + \theta_j. \quad (1)$$

Рівняння (1) використовують для розрахунку загального входу до нейрона θ_j, який є зваженим вузлом зміщення, що завжди має вихідне значення 1. Вузол зміщення вважається "псевдовходом" для кожного нейрона у прихованому та вихідному шарі і використовується для розв'язання проблем у ситуаціях, коли значення вхідного шаблона дорівнює нулю. Якщо будь-який вхідний шаблон містить нульові значення, нейронна мережа може бути навчена без вузла зміщення.

Щоб вирішити, чи активувати нейрон, значення потенціалу Net_j дії передається у відповідну функцію активації. Результуюче значення функції активації визначає вихід нейрона та стає вхідним значенням для нейронів у наступних шарах, які з ним пов'язані.

Оскільки однією з вимог до алгоритму зворотного поширення помилки є те, що функція активації має бути диференційована, типовою функцією є сигмоїдальне рівняння:

$$O_j = x_k = \frac{1}{1+ e^{-Net_j}}. \quad (2)$$

Слід зазначити, що можуть використовуватися інші типи функцій, наприклад, гіперболічні. Рівняння (1) та (2) застосовують для визначення вихідного значення вузла k у вихідному шарі.

Синтез моделі ґрунтувався на створенні власного програмного забезпечення, що реалізує навчання та тестування моделі. Основні математичні алгоритми, використані для нормалізації даних і навчання моделі, виконувались із використанням Weka API (інтерфейс прикладного програмування). Weka – це програмне забезпечення з відкритим вихідним кодом, випущене під GNU General Public License, що містить набір алгоритмів машинного навчання для задач інтелектуального аналізу даних. Він містить інструменти для підготовки даних, класифікації, регресії, кластеризації, правил вилучення асоціацій і візуалізації. Weka містить API, який написаний на Java та реалізує існуючі алгоритми навчання з мінімальними налаштуваннями. Остаточний модуль навчання та перевірки написано мовою програмування Java.

Для ідентифікації події із заданою точністю потрібно, щоб відносна помилка не перевищувала 4 %. Через великий обсяг навчальних даних він був розбитий на кілька блоків за типом атаки і прийнято рішення синтезувати окрему нейромережну модель для ідентифікації кожного типу атаки.

Для класифікації атак із використанням синтезованої моделі створено спеціальну процедуру з таким алгоритмом.

1. Завантаження тренувальних даних.

2. Визначення номінальних значень із числових. Нейронна мережа представляє числові значення в певному відношенні, ваги коригуються від значення величини. Під час процесу нормалізації даних залежності між певними атрибутами можуть бути неправильно інтерпретовані і заплутати процес навчання. Для критичних числових атрибутів, таких як порт (1-65565), необхідно змінити представлення. Для розв'язання цієї проблеми використовують форматування числових значень до номінальних.

3. Нормалізація даних. Нормалізація даних у нейронних мережах – це процес оптимізації значень набору даних для числових типів з великого діапазону в діапазон значень від 0 до 1 із збереженням пропорційності. Нормовані значення значно збільшують швидкість навчання моделі та не порушують правильність її навчання.

4. Класифікатор узгоджує вихідне значення нейронної мережі з типом виявленої атаки.

5. Валідатори описують вихідні класи мережі, які використовуються для відображення значення класифікації користувача.

6. Відбувається класифікація шаблонів на основі отриманої відповіді від нейромережі.

7. Визначення помилки мережі. Якщо дані, що передаються у класифікатор, містять шаблони збігів, можна обчислити відносну помилку мережі.

Ми суворо вимагаємо, щоб дані навчання, перевірки та тестування були отримані з різних машин, щоб вони могли ідентифікувати можливості в кінцевих точках, які не є частиною даних навчання. Зокрема, ми навчаємо модель для 100 епох,

перевіряємо продуктивність моделі після кожної епохи та вибираємо модель, що забезпечує найкращу продуктивність для даних перевірки. Детальна інформація про оцінку адекватності отриманої моделі для представлення тестової підмножини даних наведена в табл. 2. Ця вибірка відображає різні типи атак та їхню відносну похибку ідентифікації у разі застосування синтезованої моделі.

***Таблиця* 2**

Результати випробувань моделі

Назва атаки	Відносна помилка, %
FTP- Bruteforce	0,15
SSH- Bruteforce	0,10
Dos attack GoldenEye	97,50
Dos attack Slowloris	98,96
Dos attack LOIC-UDP	100,00
Dos attack HOIC	0,00
Dos attack HULK	0,00
HTTP Benign	80,40
Infiltration	100,00
Botnet	0,004
Inf-Bot Benign	0,00

4. ВИСНОВКИ

Аналіз отриманих результатів показує, що відносна помилка ідентифікації у процесі представлення тестових зразків до синтезованої моделі суттєво відрізняється для різних типів мережних атак. Як видно з табл. 2, модель не може ідентифікувати такі типи DoS-атак, як GoldenEye, Slowloris, LOIC-UDP та HTTP Benign. Проте загалом подальші дослідження можливості використання цього типу нейронних мереж на розв'язання завдань ідентифікації мережних атак дуже перспективні. Під час досягнення прийнятних результатів точність моделі ідентифікації дозволить не тільки виявляти мережні атаки, а й виконувати прогноз подій мережної безпеки на основі ретроспективних даних, накопичених в інформаційній системі за період і переданих нейромережною моделлю для навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Chen, P., Desmet, L, & Huygens, C. (2014). A study on advanced persistent threats in *IFIP International Conference on Communications and Multimedia Security*. Aveiro, Portugal, pp. 63–72.

[2] Stringhini, G., & Thonnard, O. (2015). That ain't you: Blocking spearphishing through behavioural modelling in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*.

[3] SPECTRUM.IEEE.ORG INTERNATIONAL. (2019, Feb.). *01 The WhiteHat Hacking Machine*, pp. 30–35.

[4] Denning, Dorothy E. (1986, May), An Intrusion Detection Model in *Proceedings of the Seventh IEEE Symposium on Security and Privacy*, pp. 119–131.

[5] Scarfone, K, & Mell, P. (2007, Feb.). Guide to Intrusion Detection and Prevention Systems (IDPS). *NIST Special Publication on Computer security*, pp. 58–69.

[6] Daş, R., Karabade, A. & Tuna, G. (2015, 16–19 May). Common Network Attack Types and Defense Mechanisms in *Signal Processing and Communications Applications Conference (SIU)*, pp. 2658–2666.

[7] Bellovin, S. M., AT & T. Lab Res., USA. (2004, 6–10 Dec.). A look back at security problems in the *TCP/IP protocol suite 20th Annual Computer Security Applications Conference*. USA, pp. 268–286.

[8] Borkar, A., Donode, A., & Kumari, A. (2017, 23–24 Nov.). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS in *International Conference on Inventive Computing and Informatics (ICICI)*. Coimbatore, India, pp. 878–880.

[9] Azhagiri, M., Rajesh, A., & Karthik, S. (2015). Intrusion detection and prevention system: technologies and challenges. *International Journal of Applied Engineering Research*. India, ISSN 0973-4562, vol. 10, no. 87, pp. 1–11.

[10] Daş, R., & Baykara, M. (2015, October). A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems, *in International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 5, pp. 203–208.

[11] Linh Van Ma Van Quan Nguyen; Jin-young Kim; Kwangki Kim; & Jinsul Kim (2018). Applications of Anomaly Detection Using Deep Learning on Time Series Data in *16th Intl Conf on Dependable, Autonomic and Secure Computing*, pp. 393–396.

[12] Usage of Machine Learning for Intrusion Detection in a Network. *International Journal of Computer Networks and Applications (IJCNA)*, vol. 3, Issue 6, (2016, November–December) Prachi Department of CSE & IT, The NorthCap University. India, pp. 139–145.

[13] Shen, Y., Mariconti, E., Vervier, P. A., & Stringhini, G. (2018). "Tiresias", in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security – CCS '18*, pp. 592–605.

[14] Lianbing, Z. (2016). Study on Applying the Neural Network in Computer Network Security Assessment in *Eighth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, pp. 639–642.

[15] Li J., & Dong, C. (2010). Research on Network Security Situation Prediction-Oriented Adaptive Learning Neuron in *Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, pp. 483–485.

[16] Shin, E. C. R., Song, D., & Moazzezi, R. (2015, 12–14 August). Recognizing Functions in Binaries with Neural Networks in *USENIX Security Symposium Washington*, pp. 611–626.

[17] Kuznetsov, A. A., Smirnov, A. A., Danilenko, D. A., & Berezovsky, A. (2015).The statistical analysis of network traffic for the intrusion detection and prevention systems. *Telecommunications and Radio Engineering*, vol. 74, Issue 1, pp. 61–78.

[18] Menshawy, A. (2018). *Deep Learning By Example: A Hands-on Guide to Implementing Advanced Machine Learning Algorithms and Neural Networks*. Pact Publishing Ltd. 442 p.

[19] Naumenko, N. I., Stasev, Yu. V., & Kuznetsov, A. A. (2007, May), Methods of synthesis of signals with prescribed properties. *Cybernetics and Systems Analysis*, vol. 43, Issue 3, pp. 321–326.

[20] Duman, S., Kalkan-Cakmakci, K, Egele, M., William K. Robertson, K., & Kirda, E. (2016, 10–14 June). EmailProfiler: Spearphishing Filtering with Header and Stylometric Features of Emails in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, USA, pp. 121–126.

[21] Hubskyi, O., Babenko, T., Myrutenko, L., & Oksiiuk, O. (2021). Detection of SQL injection attack using neural networks. *Advances in Intelligent Systems and Computing*, 1265 AISC, pp. 277–286.

[22] Haykin, S. (2010). *Neural Networks and Learning Machines: International Edition. 3rd edn.* Pearson Education. 936 p.

[23] Stringhini, G., Holz, T., Stone-Gross, B., Kruegel, C., & Vigna, G. (2011, 8–12 August). *BotMagnifier: Locating Spambots on the Internet" in Proceedings of the 2011 USENIX Security Symposium San Francisco*. CA, pp. 427–443.

[24] Toliupa, S., Babenko, T., & Trush, A. (2017). The building of a security strategy based on the model of game management in *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T*. Kharkiv, Ukraine, pp. 103–108.

[25] Multiple Buffer Format String Vulnerabilities in SQL Server. http://www.microsoft.com/technet/security/bulletin/MS01-060.asp, last accessed 2020/03/11.

[26] Taking the monkey work out of pentesting, http://pentestmonkey.net/

[27] The Web Application Security Consortium / SQL Injection. http://projects.webappsec.org/SQL-Injection

[28] Microsoft SQL Server extended stored procedure vulnerability (technical explanation and exploit code) SecuriTeam, https://securiteam.com/windowsntfocus/6n0010u0kw/

REFERENCES

[1] Chen, P., Desmet, L, & Huygens, C. (2014). A study on advanced persistent threats in *IFIP International Conference on Communications and Multimedia Security*. Aveiro, Portugal, pp. 63–72.

[2] Stringhini, G., & Thonnard, O. (2015). That ain't you: Blocking spearphishing through behavioural modelling in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*.

[3] SPECTRUM.IEEE.ORG INTERNATIONAL. (2019, Feb.). *01 The WhiteHat Hacking Machine*, pp. 30–35.

[4] Denning, Dorothy E. (1986, May), An Intrusion Detection Model in *Proceedings of the Seventh IEEE Symposium on Security and Privacy*, pp. 119–131.

[5] Scarfone, K, & Mell, P. (2007, Feb.). Guide to Intrusion Detection and Prevention Systems (IDPS). *NIST Special Publication on Computer security*, pp. 58–69.

[6] Daş, R., Karabade, A. & Tuna, G. (2015, 16–19 May). Common Network Attack Types and Defense Mechanisms in *Signal Processing and Communications Applications Conference (SIU)*, pp. 2658–2666.

[7] Bellovin, S. M., AT & T. Lab Res., USA. (2004, 6–10 Dec.). A look back at security problems in the *TCP/IP protocol suite 20th Annual Computer Security Applications Conference.* USA, pp. 268–286.

[8] Borkar, A., Donode, A., & Kumari, A. (2017, 23–24 Nov.). A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS in *International Conference on Inventive Computing and Informatics (ICICI)*. Coimbatore, India, pp. 878–880.

[9] Azhagiri, M., Rajesh, A., & Karthik, S. (2015). Intrusion detection and prevention system: technologies and challenges. *International Journal of Applied Engineering Research*. India, ISSN 0973-4562, vol. 10, no. 87, pp. 1–11.

[10] Daş, R., & Baykara, M. (2015, October). A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems, *in International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 5, pp. 203–208.

[11] Linh Van Ma Van Quan Nguyen; Jin-young Kim; Kwangki Kim; & Jinsul Kim (2018). Applications of Anomaly Detection Using Deep Learning on Time Series Data in *16th Intl Conf on Dependable, Autonomic and Secure Computing*, pp. 393–396.

[12] Usage of Machine Learning for Intrusion Detection in a Network. *International Journal of Computer Networks and Applications (IJCNA)*, vol. 3, Issue 6, (2016, November–December) Prachi Department of CSE & IT, The NorthCap University. India, pp. 139–145.

[13] Shen, Y., Mariconti, E., Vervier, P. A., & Stringhini, G. (2018). "Tiresias", in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security – CCS '18*, pp. 592–605.

[14] Lianbing, Z. (2016). Study on Applying the Neural Network in Computer Network Security Assessment in *Eighth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, pp. 639–642.

[15] Li J., & Dong, C. (2010). Research on Network Security Situation Prediction-Oriented Adaptive Learning Neuron in *Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, pp. 483–485.

[16] Shin, E. C. R., Song, D., & Moazzezi, R. (2015, 12–14 August). Recognizing Functions in Binaries with Neural Networks in *USENIX Security Symposium Washington*, pp. 611–626.

[17] Kuznetsov, A. A., Smirnov, A. A., Danilenko, D. A., & Berezovsky, A. (2015).The statistical analysis of network traffic for the intrusion detection and prevention systems. *Telecommunications and Radio Engineering*, vol. 74, Issue 1, pp. 61–78.

[18] Menshawy, A. (2018). *Deep Learning By Example: A Hands-on Guide to Implementing Advanced Machine Learning Algorithms and Neural Networks*. Pact Publishing Ltd. 442 p.

[19] Naumenko, N. I., Stasev, Yu. V., & Kuznetsov, A. A. (2007, May), Methods of synthesis of signals with prescribed properties. *Cybernetics and Systems Analysis*, vol. 43, Issue 3, pp. 321–326.

[20] Duman, S., Kalkan-Cakmakci, K, Egele, M., William K. Robertson, K., & Kirda, E. (2016, 10–14 June). EmailProfiler: Spearphishing Filtering with Header and Stylometric Features of Emails in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, USA, pp. 121–126.

[21] Hubskyi, O., Babenko, T., Myrutenko, L., & Oksiiuk, O. (2021). Detection of SQL injection attack using neural networks. *Advances in Intelligent Systems and Computing*, 1265 AISC, pp. 277–286.

[22] Haykin, S. (2010). *Neural Networks and Learning Machines: International Edition. 3rd edn.* Pearson Education. 936 p.

[23] Stringhini, G., Holz, T., Stone-Gross, B., Kruegel, C., & Vigna, G. (2011, 8–12 August). *BotMagnifier: Locating Spambots on the Internet" in Proceedings of the 2011 USENIX Security Symposium San Francisco*. CA, pp. 427–443.

[24] Toliupa, S., Babenko, T., & Trush, A. (2017). The building of a security strategy based on the model of game management in *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T*. Kharkiv, Ukraine, pp. 103–108.

[25] Multiple Buffer Format String Vulnerabilities in SQL Server. http://www.microsoft.com/technet/security/bulletin/MS01-060.asp, last accessed 2020/03/11.

[26] Taking the monkey work out of pentesting, http://pentestmonkey.net/

[27] The Web Application Security Consortium / SQL Injection. http://projects.webappsec.org/SQL-Injection

[28] Microsoft SQL Server extended stored procedure vulnerability (technical explanation and exploit code) SecuriTeam, https://securiteam.com/windowsntfocus/6n0010u0kw/

Стаття надійшла до редколегії 20.02.2023

Intelligent model of classification of network cyber security events

Due to the increased complexity of modern computer attacks, there is a need for security professionals not only to detect harmful activity but also to determine the appropriate steps that an attacker will go through when performing an attack. Even though the detection of exploits and vulnerabilities is growing every day, the development of protection methods is progressing much more slowly than attack methods. Therefore, this remains an open research problem. In this article, we present our research in network attack identification using neural networks, in particular Rumelhart's multilayer perceptron, to identify and predict future network security events based on previous observations. To ensure the quality of the training process and obtain the desired generalization of the model, 4 million records accumulated over 7 days by the Canadian Cybersecurity Institute were used. Our result shows that neural network models based on a multilayer perceptron can be used after refinement to detect and predict network security events.

Keywords: *security of information systems; neural network; network security; prognostication.*

Тетяна Бабенко,
д-р техн. наук, проф.
Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Tetyana Babenko,
Dr. Sci. (Engin.), Prof.
Professor of the Department of Cyber Security and Information Protection, Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Андрій Бігдан,
Асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Київ, Україна.

Andrii Bigdan,
Assistant of the Department of Cyber Security and Information Protection, Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Лариса Мирутенко,
канд. техн. наук, доц.
Доцент кафедри кібербезпеки та захисту інформації, Київського національного університету імені Тараса Шевченка. Київ, Україна.

Larisa Myrutenko,
PhD (Engin.), Associate Prof.
Associate Professor of the Department of Cyber Security and Information Protection, Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

УДК 004.7:519.87(043.3):621.391
DOI 10.17721/ISTS.2023.1.70-77

Олександр Торошанко, orcid.org/0000-0002-2354-0187,
toroshanko@gmail.com
Юрій Щебланін, orcid.org/0000-0002-3231-6750,
y.shcheblanin@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ СХЕМ ВИЯВЛЕННЯ ПЕРЕВАНТАЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Розглянуто схему виявлення перевантажень і регулювання вхідного потоку даних на основі аналізу функції чутливості продуктивності телекомунікаційної мережі. Градієнт функції чутливості характеризує швидкість зміни цієї функції і надає оптимальний напрямок для налаштування швидкості джерела даних. Для визначення функції чутливості запропоновано використання простої нейронної мережної моделі динамічної системи. Визначення градієнта за поточним значенням знаку функції чутливості показника продуктивності здійснюють на основі алгоритму адитивного збільшення/множинного зменшення. Указаний алгоритм є альтернативою системи прогнозування перевантаження і керування потоком, заснованої на контролі поточного значення величини черги порівняно із заданим порогом. Розглянуто нейронну модель для багатокрокового передбачення стану черги з боку приймача телекомунікаційної мережі. Запропоновано й обґрунтовано схему багатокрокового передбачення стану черги. Для передбачення та завчасного виявлення перевантаження використано апарат загальної теорії чутливості з непрямим зворотним зв'язком та керуванням активністю джерел повідомлень. Результати цієї теорії застосовано для побудови системи керування з непрямим зворотним зв'язком, що дозволяє економити канальний та обчислювальний ресурси. Представлено результати порівняльного аналізу способів контролю перевантаження на підставі аналізу довжини черги і на основі аналізу показника чутливості з 1-кроковим та 3-кроковим горизонтами передбачення стану мережі. Дослідження проведено для синусоїдальної функції вузького місця черги. Показано, що ключові показники ефективності для схеми на основі функції чутливості кращі, ніж для схеми на основі аналізу довжини черги. Схема на основі аналізу розміру черги чутливіша до змін у швидкості обслуговування черги, а коливання швидкості джерела даних менші для схеми на основі чутливості. Для систем на основі аналізу функції чутливості схема з 3-кроковим горизонтом передбачення стану забезпечує кращу продуктивність і меншу величину черги на обслуговування ніж схема з 1-кроковим горизонтом.

Ключові слова: *телекомунікаційна мережа; прогнозування перевантаження; функція чутливості; градієнт; нейронна система;керування чергою; горизонт передбачення.*

1. ВСТУП

Ключові показники ефективності функціонування телекомунікаційної мережі значною мірою визначаються способами й алгоритмами керування потоками даних і маршрутизації. Саме ці два напрямки пов'язані з розв'язанням ключової задачі інформаційного обміну – прогнозування і запобігання перевантаженням.

Головна вимога до використовуваних методів маршрутизації – статичних чи динамічних, локальних чи децентралізованих тощо – це спрямувати повідомлення від джерела до місця призначення таким чином, щоб затримка даних у мережі була мінімальною, а керування трафіком даних мало б забезпечити уникнення чи мінімізацію появи перевантаження [1–3].

Телекомунікаційна мережа представляє собою сукупність ресурсів, що використовуються конкуруючими користувачами. Ресурси телекомунікаційної мережі (буферна пам'ять, смуга пропускання, процесорний час, простір імен, логічні канали) мають обмежені (скінченні) можливості, які спричиняють виникнення конфліктів між користувачами. Це може призвести до суттєвого зниження продуктивності системи до такого моменту, що система стає "засміченою" внаслідок

багатократного дублювання даних і різкого збільшення технологічної керівної інформації. Унаслідок цього пропускна здатність суттєво зменшується, можливо і до нульової позначки. Це є типова поведінка "конкуруючих" систем [3–6]. Така ситуація може призвести до колапсу мережі.

Існує декілька визначень перевантаження, які, однак, не суперечать одне одному. Будемо користуватись таким визначенням [7–9]: "перевантаження – це втрата даних користувачем, спричинена збільшенням навантаження в мережі". Тоді керування перевантаженням можна визначити як набір механізмів, що запобігають таким негативним для користувача наслідкам або зменшують їх. Якщо мережа не здатна запобігти втраті даних користувача, тоді потрібно спробувати максимально обмежити втрати, і в подальшому спробувати, щоб система була справедливою до всіх постраждалих користувачів.

Перевантаження має значний вплив на ключові показники ефективності телекомунікаційної мережі і якість обслуговування користувачів. Сказане вище обумовлює актуальність і необхідність проведення досліджень у цьому напрямку.

2. ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

Одним із способів запобігання перевантаженню є збільшення об'єму пам'яті вхідних буферів [4]. Однак зі зростанням об'єму буферної пам'яті (розбухання буфера – Bufferbloat) збільшується кількість необроблених пакетів, а головне – збільшується час очікування їхнього оброблення. Це може привести до перевищення допустимих норм тривалості тайм-ауту, що призводить до подальшого зниження корисної пропускної здатності мережі і може спричинити виникнення лавинного процесу: переповнення буфера призводить до втрати пакетів, які доведеться передавати повторно або навіть кілька разів. Таким чином, обчислювальний вузол маршрутизатора-відправника отримує надлишкове паразитне завантаження, що може призвести до збільшення негативних наслідків, пов'язаних із перевантаженням.

У роботах [10–12] запропоновано розгорнуту класифікацію способів і алгоритмів боротьби з перевантаженнями, які використовують нині, розглянуто алгоритми RED, TCP Veno, Tail Drop, WRED (weighted random early detection) тощо. Однак згадані роботи [10–12] носять, певною мірою, оглядовий характер, не приводяться кількісні порівняльні оцінки ефективності і складності розглянутих методів, зокрема. Причиною цього, очевидно, є неможливість детального аналізу внаслідок відсутності статистики достатньо великого об'єму.

Важливу роль у системах керування потоками даних і прогнозуванні перевантаження відіграють показники чутливості складних систем. У фундаментальній роботі [13] визначено категорію чутливості складної системи як математичного показника та запропоновано логарифмічні функції чутливості.

У [14] розглянуто способи і методи визначення чутливості вихідних характеристик телекомунікаційних мереж як систем масового обслуговування. В основу цих способів покладено моделі керування чергою для адаптації регульованого доступу зовнішнього трафіка в систему з метою отримання очікуваної межі продуктивності.

Однак асимптотичні характеристики функцій чутливості в роботі остаточно не визначено, не отримано аналітичні вирази для функціонального зв'язку параметрів функцій чутливості та відповідних параметрів системи керування чергами.

Метою цього дослідження є вдосконалення і розроблення способу контролю і прогнозування перевантаження в телекомунікаційній мережі з використанням явного зворотного зв'язку за знаком функції чутливості продуктивності мережі, а також виконання порівняльного аналізу відомих і запропонованих рішень.

3. КОНТРОЛЬ ПЕРЕВАНТАЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ АНАЛІЗУ ФУНКЦІЇ ЧУТЛИВОСТІ

У [15] розглянуто схему контролю перевантажень із використанням зворотного зв'язку за знаком функції чутливості продуктивності телекомунікаційної мережі. Для визначення цієї функції запропоновано використання простої нейронної мережної моделі динамічної системи. Запропонований алгоритм адитивного збільшення/множинного зменшення визначає зміну швидкості джерела даних залежно від знаку функції чутливості показника продуктивності. Указаний алгоритм є альтернативою системи прогнозування перевантаження і керування потоком, заснованої на пороговому заповненні черги, тобто контролю перевантаження за показником довжини черги.

Алгоритм і правило регулювання адитивного збільшення/множинного зменшення швидкості джерела визначає аналітичний вираз вигляду

$$\Delta J(t) = \frac{\partial J}{\partial R(t)} = -E(t + i\tau)\frac{\partial \hat{G}(t + i\tau)}{\partial R(t)}, \quad (1)$$
$$i = 1, 2, ..., L.$$

Тут $J(t)$ – оціночні дані про наявність чи загрозу перевантаження; $\Delta J(t)$ – градієнт системи оці-

нювання перевантаження в момент часу t; $G(t)$ – довжина черги або затримки обслуговування в момент часу t; $\hat{G}(t+i\tau)$ – прогнозована довжина черги або затримки обслуговування в момент часу $t+i\tau$, вихід нейронної мережі; $R(t)$ – миттєва швидкість черги на вході в момент часу t; $E(t)$ – функція відхилення параметра, що відслідковується (помилка); τ – період часових відліків, період тактової частоти системи; L – горизонт передбачення.

Зауважимо, що похідна $\partial\hat{G}(t+i\tau)/\partial R(t)$ у нашому випадку представляє собою параметр чутливості мережі – градієнт показника ефективності системи [7].

На основі виразу (1) визначається параметр R_{qs} – швидкість обслуговування черги (queue service).

Визначимо функцію вартості (cost function), як цільову функцію наявності перевантаження, таким чином:

$$J=\frac{1}{2}e^2(t+i\tau)=\frac{1}{2}\left[Q-\hat{G}(t+i\tau)\right]^2,\ i=1,2,...,L. \quad (2)$$

Тут Q – заздалегідь установлена характеристика системи, у нашому випадку максимально допустиме значення довжини черги.

Керівний сигнал в (1) для $R(t)$ (швидкість джерела даних) повинен бути обраний так, щоб мінімізувати J. У дискретному випадку керівна змінна оновлюється відповідно до такого правила градієнтного спуску [16]:

$$R(t+\tau)=R(t)+\Delta R(t)=R(t)-\eta\frac{\partial J}{\partial R(t)}. \quad (3)$$

Індикатор перевантаження $B(t)$ формується залежно від градієнта системи $\Delta J(t)$ у момент часу t [15]:

$$\begin{cases} B(t)=0 & \text{if} \quad \Delta J(n)<0, \\ B(t)=1 & \text{if} \quad \Delta J(n)\geq 0. \end{cases} \quad (4)$$

На рис. 1 показано схему регулювання вхідного потоку (РВП) від джерел даних $D_1 \ldots D_s$ на основі аналізу показника чутливості [15]. Однак вона не дає повного уявлення щодо гарантованого прогнозування перевантаження на основі аналізу показника чутливості.

Необхідно пояснити, у чому полягає різниця між задачами запобігання перевантаженню і керування потоком. Запобігання перевантаженню гарантує, що мережа справиться із запропонованим їй трафіком. Для розв'язання цього питання необхідно аналізувати поведінку всіх хостів і маршрутизаторів, процесів зберігання і пересилання даних, а також ураховувати багато інших чинників, що знижують пропускну спроможність мережі [17, 18].

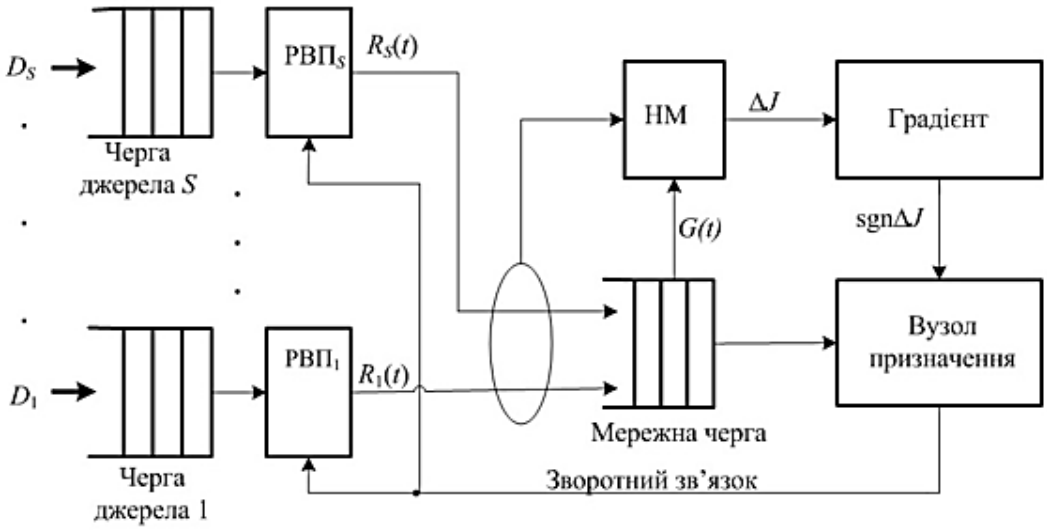


Рис. 1. Схема регулювання вхідного потоку даних

Керування потоком, навпаки, належить до трафіка між двома конкретними станціями – відправником і отримувачем. Завдання керування потоком полягає в узгодженні швидкості передачі відправника зі швидкістю, з якою отримувач здатний приймати потік пакетів.

Керування потоком зазвичай реалізується за допомогою зворотного зв'язку між отримувачем і відправником.

Слід зауважити, що алгоритми боротьби з перевантаженням також використовують зворотний зв'язок у вигляді спеціальних повідомлень

щодо уповільнення темпу передачі даних різними відправниками. Таким чином, хост може отримати повідомлення щодо уповільнення передачі у двох випадках: коли з потоком, що передається, не справляється отримувач, або, коли з ним не справляється вся мережа.

На рис. 2 зображено схему виявлення перевантаження зі зворотним зв'язком по параметру *G(t)* – довжина черги або затримки обслуговування.

Зазначимо, що обчислений нейронною мережею прогнозований параметр $\hat{G}(t)$, у точках формування відхилень враховується з різними знаками.

Аналітичне представлення алгоритму керування адитивним збільшенням/множинним зменшенням швидкості джерела полягає в такому [19]:

$$R(t+\tau)=\begin{cases} R(t)+F, & \Delta J(n-\tau)<0, \\ R(t)-F, & \Delta J(n-\tau)\geq 0. \end{cases} \quad (5)$$

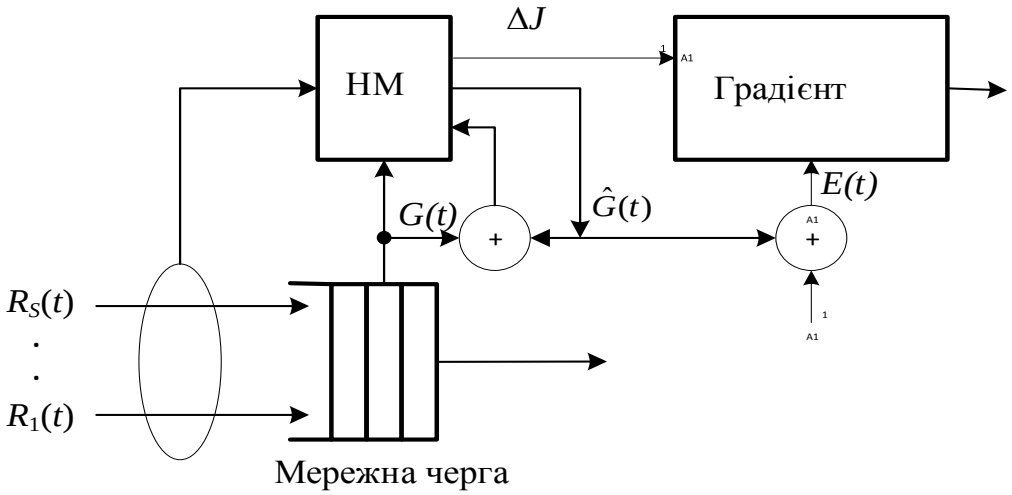


Рис. 2. Схема виявлення перевантаження зі зворотним зв'язком

Значення величин $R_1(t)\ldots R_S(t)$ (швидкості регульованих вхідних потоків від джерел даних $D_1\ldots Ds$) поступають на вхідний шар нейронної мережі НМ. На основі аналізу отриманих даних і поточного значення довжини мережної черги $G(t)$ вихідний шар нейронної мережі відслідковує величину функції J (наявності чи загрози перевантаження) та її відхилення. Знак величини відхилення sgnΔJ враховується вузлом призначення під час формування сигналу зворотного зв'язку.

4. ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ СХЕМ ВИЯВЛЕННЯ ПЕРЕВАНТАЖЕННЯ

Параметри і показники функціонування телекомунікаційної мережі можуть змінюватися із часом, тому в керівній схемі необхідне онлайн навчання нейронної мережі [20].

Алгоритм навчання нейронної мережі і формування ознаки перевантаження детально розглянуто в [15].

Розглянемо одне з'єднання з таким набором параметрів:

- пікова швидкість джерела R_{max}=100 пакетів за одиницю часу;
- мінімальна швидкість R_{min} = 0 пакетів за одиницю часу;
- одиниця часу τ = 0,25 мс;
- поріг перевантаження встановлений при Q = 500 пакетів;
- коефіцієнт адитивного збільшення $F^{+}= R_{max}/16$;
- коефіцієнт мультиплікативного зменшення $F^{-}=15/16$;
- затримка округлення із 6 одиниць часу – 6τ.

Розглядається тришарова нейронна мережа: вхідний, вихідний і прихований шари складаються з 8 нейронних елементів кожен.

Для визначення стану вузького місця черги (bouttleneck queue) досліджують 1- і 3-крокові горизонти передбачення. Числові значення вузького місця визначено синусоїдальною функцією integer[35(1+sin(2$\pi\tau$/*T*))+10] пакетів за одиницю часу (integer – ціла частина числа).

Представимо результати порівняльного аналізу таких способів контролю перевантаження:

а) на основі аналізу довжини черги (рис. 3);

б) на основі аналізу показника чутливості з 1-кроковим передбаченням стану мережі (рис. 4);

в) на основі аналізу показника чутливості з 3-кроковим передбаченням стану мережі (рис. 5).

Спосіб а) реалізується на основі схеми, показаної в [1] на рис. 1. Способи б) і в) реалізуються на основі схем, зображених на рис. 1 і 2 цієї статті.

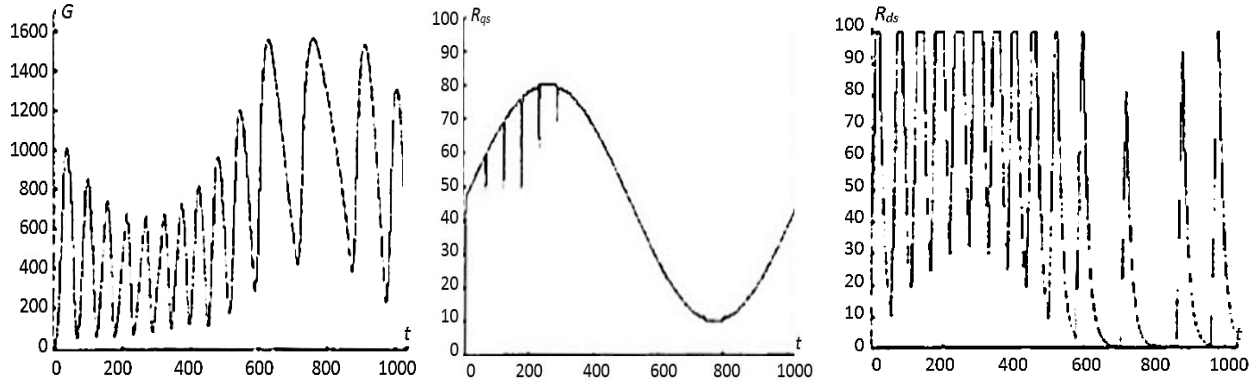
На графіках прийнято такі позначення:

пунктирна лінія – реальні значення параметрів, суцільна – прогнозовані;

G – розмір черги (кількість запитів);

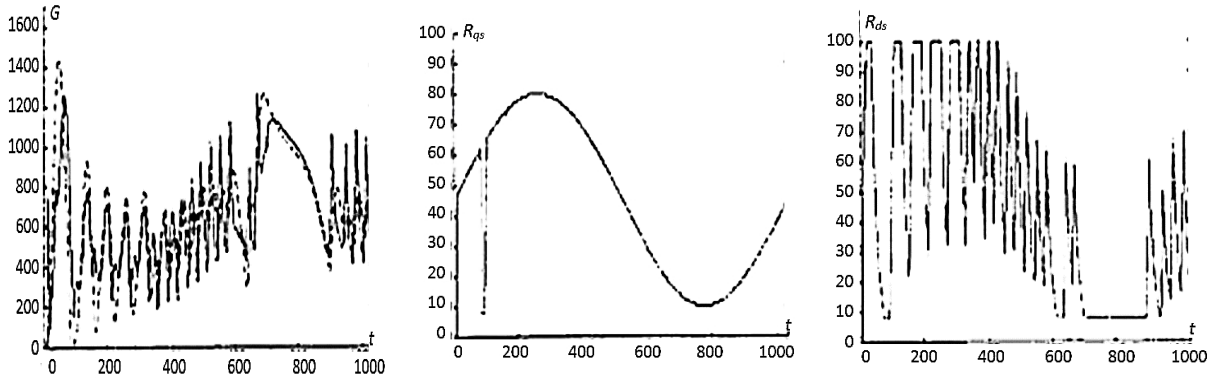
R_{qs} – швидкість обслуговування черги (*queue service*), запитів/с;

R_{ds} – швидкість джерела даних (*data source*), запитів/с.



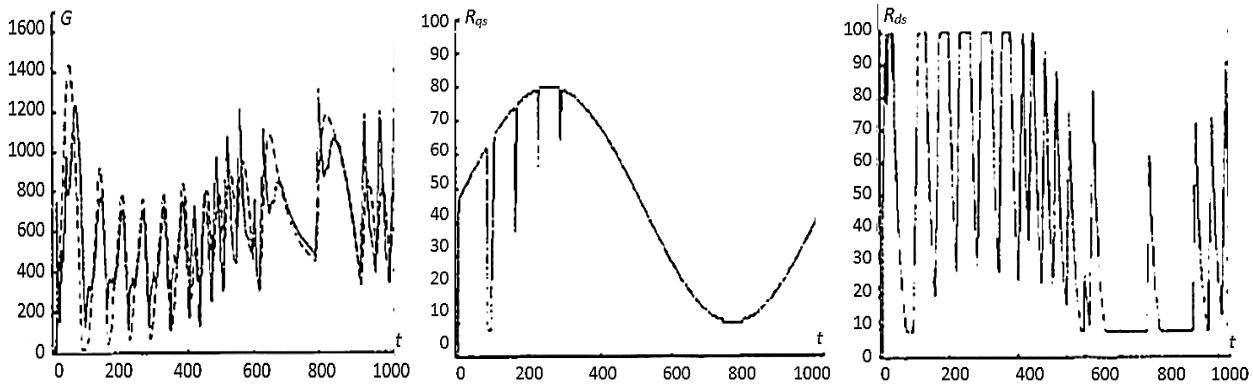
а) **розмір черги *G*** ***б)*** **швидкість обслуговування черги R_{qs}** ***в)*** **швидкість джерела R_{ds}**

Рис. 3. Контроль перевантаження на основі аналізу довжини черги



а) **розмір черги *G*** ***б)*** **швидкість обслуговування черги R_{qs}** ***в)*** **швидкість джерела R_{ds}**

Рис. 4. Контроль перевантаження на основі схеми чутливості з 1-кроковим передбаченням



а) **розмір черги *G*** ***б)*** **швидкість обслуговування черги R_{qs}** ***в)*** **швидкість джерела R_{ds}**

Рис. 5. Контроль перевантаження на основі схеми чутливості з 3-кроковим передбаченням

Визначимо такі показники ефективності для виконання моделювання:

- $G_{\max} = \max\{G(t),\ 0 \le t \le T\}$,

тут максимальне значення $G(t)$ відображає розмір буфера, потрібний вузькому місцю для уникнення втрати пакету, T – час виконання моделювання;

- середній розмір черги і швидкості джерела, визначено як

$$\tilde{f} = \frac{1}{T}\int_0^T f(t)dt;$$

- дисперсію розміру черги і швидкості джерела, визначено як

$$\sigma^2(f) = \frac{1}{T}\int_0^T [f(t) - \tilde{f}]^2 dt.$$

Аналіз зображених графіків свідчить про таке:

1) величини черги G менші для схеми на основі чутливості (рис. 4,*а* і 5,*а*) ніж для схеми на основі черги (рис. 3,*а*). Разом із тим схема на основі чутливості з 3-кроковим передбаченням стану (рис. 5) забезпечує кращу продуктивність, тобто меншу величину черги на обслуговування, ніж відповідна схема з 1-кроковим передбаченням (рис. 4);

2) Схема на основі аналізу розміру черги чутливіша до змін у швидкості обслуговування черги (рис. 3,*б*), ніж схеми на основі чутливості (рис. 4,*б* і 5,*б*). У схемі на основі черги слід зазначити, що за значного зниження швидкості обслуговування розмір черги зростає екстенсивно, раніше спостережуваних значень. Збільшення розміру черги стабільніше за тих самих умов для схем на основі чутливості;

3) коливання швидкості джерела R_{ds} менші для схеми на основі чутливості (рис. 4,*в* і 5,*в*) ніж для схеми на основі черги (рис. 3,*в*). Аналізуючи схеми на основі чутливості, зауважимо, що для 3-крокового передбачення керівні сигнали зворотного зв'язку (тобто, двійковий біт затору), отримані у джерелі даних з мережної черги, несуттєві у віці й відображають ближчі мережні умови порівняно з 1-кроковим передбаченням процесу. У схемах керування затором на основі зворотного зв'язку зі значними затримками поширення керівні сигнали, отримані у джерелах, можуть бути застарілими, і в результаті відповідь керування вступить у силу тільки після деякої затримки. Недоліком передбачення на основі аналізу стану черги є те, що чим із більшою затримкою ми робитимемо передбачення, тим складніше буде отримати передбачення з невеликими помилками.

Короткий перелік результатів моделювання для синусоїдального типу вузького місця наведено в таблиці, де G_{av} і R_{av} позначають середній за часом розмір черги і швидкість джерела.

Таблиця

Перелік результатів моделювання

Підхід	$G_{\max}$	G_{av}	$\sigma^2(G)$	**Інд.** $G_{\max}$	R_{av}	$\sigma^2(R)$
На основі аналізу черги	1556	713,8	179305,5	281	45,7	1211,4
На основі функції чутливості: 1-кроковий горизонт передбачення	1428	653,3	86115,5	48	44,4	1066,9
На основі функції чутливості: 3-кроковий горизонт передбачення	1443	628,7	89936,5	49	44,5	1139,7

У цій роботі, на відміну від традиційних систем контролю перевантаження за змінами стану та параметрів черг, запропонована система працює за оптимальними алгоритмами налаштування вагових параметрів. Завдяки цьому підвищується точність визначення керівних сигналів, зменшується вплив їхньої затримки і, як результат, мінімізуються середні витрати ресурсу.

Розлянута система керування телекомунікаційною мережею по суті представляє собою статичну нейронну мережу, до складу якої вводиться зворотний зв'язок через елемент затримки на один такт [19, 20]. Це припущення для пакетних телекомунікаційних мереж є вельми логічним.

6. ВИСНОВКИ

Проведені дослідження показують, що підхід на основі чутливості здатний зменшити величину коливань черги (як показує значення дисперсії в таблиці), але не може повністю усунути коливання. Використання чутливості функції продуктивності системи дозволяє виявити затор своєчасно, і це веде до своєчасної реакції керування зворотним зв'язком із джерелами даних. Використання нейронної архітектури для реалізації функції чутливості і градієнта цільової функції під час збільшення горизонту передбачення забезпечують прийнятні значення затримки повідомлень зворотного зв'язку і тим самим

покращують точність передбачення і виявлення перевантажень у телекомунікаційних мережах. Розроблено метод керування перевантаженнями телекомунікаційної мережі з використанням нейронної мережі як системи моніторингу та керування. Запропоновано й обгрунтовано схему багатокрокового передбачення стану черги. Для передбачення та завчасного виявлення перевантаження використано апарат загальної теорії чутливості з непрямим зворотним зв'язком і керуванням активністю джерел повідомлень. Результати цієї теорії використано для побудови системи керування з непрямим зворотним зв'язком, що дозволяє економити канальний та обчислювальний ресурси. У результаті перевірки теоретичних результатів шляхом комп'ютерного моделювання отримано кількісні порівняльні оцінки ефективності (точності та потрібного обчислювального ресурсу) розробленого методу та методів, що існували раніше. Можна стверджувати, що з довершеною архітектурою нейромережі, придатною для моделювання динаміки системи, можна отримати уповні задовільну продуктивність телекомунікаційної системи як об'єкта керування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Tanenbaum, A. S., Andrew, S., & David, J. (2011). *Wetherall*. PrenticeHall, Cloth. 960 p.

[2] Stallings, W. (2016). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson Education, Inc., OldTappan*. New Jersey. 544 p.

[3] Mao, G. (2017). *Connectivity of Communication Networks Springer International Publishing AG*. Springer. 435 p.

[4] Виноградов, Н. А., Дрововозов, В. И., Лесная, Н. Н., & Зембицкая, А. С. (2006). Анализ нагрузки на сети передачи данных в системах критичного применения. *Зв'язок*, 1(61), 9–12.

[5] Bonaventure, O. (2018). *Computer Networking: Principles, Protocols and Practices, Release*. cnp3book. 272 p.

[6] Keshav, S. (1991). *Congestion Control in Computer Networks* [PhD Thesis University of California].

[7] Kurose, J. F., & Keith, W. Ross. (2017). *Computer Networking: A Top-Down Approach, 7th ed.* Pearson Education, Inc. 864 p.

[8] Göransson P., Black, C. Culver, T. (2017). *Software Defined Networks: A Comprehensive Approach, 2nd ed*. Morgan Kaufmann, US, 409 p.

[9] Максимов, В. В., & Чмихун, С. О. (2014). Класифікація алгоритмів боротьби з перевантаженнями. *Наукові записки Українського науково-дослідного ін-ту зв'язку*, 5(33), 73–79.

[10] Максимов В. В., & Чмихун, С. О. (2015). Дослідження алгоритму боротьби з перевантаженнями TCP VENO. *Телекомунікаційні та інформаційні технології*, 4, 30–36.

[11] Торошанко, Я. І. (2016). Аналіз чутливості систем масового обслуговування на основі моделі адаптації і регулювання зовнішнього трафіка. *Вісник Хмельницького нац. ун-ту*, 6(243), 171–175.

[12] Vinogradov, N., Stepanov, N., Toroshanko, Y., Cherevyk, V., Savchenko, A., Hladkykh, O., Toroshanko, V., & Uvarova, T. (2019). Development of the method to control telecommunication network congestion based on a neural model. *Eastern European journal of advanced technologies*, 2(9), 67–73.

[13] Zhaoming, L., Pan, Q., & Wang, L. (2016, December 9). Overload Control for Signaling Congestion of Machine Type Communications in 3GPP Networks. *Xiangming WenPLOS ONE*. 11 p.

[14] Гладких, В. М., & Торошанко О. С. (2017). Ієрархічна маршрутизація з балансуванням навантаження в сенсорних мережах. *Вісник Національного ун-ту "Львівська політехніка": Радіоелектроніка та телекомунікації*, 885, 68–75.

[15] Климаш, М. М., Стрихалюк, Б. М., & Кайдан, М. В. (2010). Тензорне подання алгоритмів маршрутизації. *Зв'язок*, 1, 33–35.

REFERENCES

[1] Tanenbaum, A. S., Andrew, S., & David, J. (2011). *Wetherall*. PrenticeHall, Cloth. 960 p.

[2] Stallings, W. (2016). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson Education, Inc., OldTappan*. New Jersey. 544 p.

[3] Mao, G. (2017). *Connectivity of Communication Networks Springer International Publishing AG*. Springer. 435 p.

[4] Vinogradov, N. A, Drovovozov, V. I., Lesnaya, N. N., & Zembytskaya, A. S. (2006). Analysis of the load on data transmission networks in critical application systems. *Communication*, 1 (61), 9–12.

[5] Bonaventure, O. (2018). *Computer Networking: Principles, Protocols and Practices, Release*. cnp3book. 272 p.

[6] Keshav, S. (1991). *Congestion Control in Computer Networks* [PhD Thesis University of California].

[7] Kurose, J. F., & Keith, W. Ross. (2017). *Computer Networking: A Top-Down Approach, 7th ed.* Pearson Education, Inc. 864 p.

[8] Göransson P. Software Defined Networks: A Comprehensive Approach, 2nd ed. / Paul Göransson, Chuck Black, Timothy Culver. – Morgan Kaufmann, US, 2017. – 409 p.

[9] Maksimov, V. V., & Chmyhun, S.O. (2014). Classification of congestion control algorithms. *Scientific Notes of the Ukrainian Research Institute of Communications*, 5(33), 73–79 [in Ukrainian].

[10] Maksimov V. V., & Chmyhun, S.O. (2015). A study of the TCP VENO congestion control algorithm. *Telecommunications and Information Technologies*, 4, 30–36 [in Ukrainian].

[11] Toroshanko, Ya. I. (2016). Sensitivity analysis of mass service systems based on the model of adaptation and regulation of external traffic. *Bulletin of the Khmelnytskyi National University*, 6(243), 171–175 [in Ukrainian].

[12] Vinogradov, N., Stepanov, N., Toroshanko, Y., Cherevyk, V., Savchenko, A., Hladkykh, O., Toroshanko, V., & Uvarova, T. (2019). Development of the method to control telecommunication network congestion based on a neural model. *Eastern European journal of advanced technologies*, 2(9), 67–73.

[13] Zhaoming, L., Pan, Q., & Wang, L. (2016, December 9). Overload Control for Signaling Congestion of Machine Type Communications in 3GPP Networks. *Xiangming WenPLOS ONE*. 11 p.

[14] Hladkykh, V. M., & Toroshanko, O. S. (2017). Hierarchical routing with load balancing in sensor networks. *Bulletin of the Lviv Polytechnic National University: Radioelectronics and Telecommunications*, 885, 68–75 [in Ukrainian].

[15] Klymash, M. M., Strykhalyuk, B. M., & Kaidan, M. V. (2010). Tensor representation of routing algorithms. *Connection*, 1, 33–35 [in Ukrainian].

Стаття надійшла до редколегії 25.03.2023

Comparative analysis of the efficiency of telecommunication network overload detection schemes

The scheme of congestion detection and regulation of input data flow based on the analysis of the sensitivity function of the telecommunication network performance is considered. The gradient of the sensitivity function characterizes the rate of change of this function and provides the optimal direction for adjusting the speed of the data source. To determine the sensitivity function, the use of a simple neural network model of a dynamic system is proposed. Determination of the gradient on the current value of the sign of the sensitivity function of the performance indicator is based on the algorithm of additive increase / multiple decrease. This algorithm is an alternative to the system of overload prediction and flow control, based on the control of the current value of the queue in comparison with a given threshold. The neural model for multi-step prediction of the queue state on the side of the telecommunication network receiver is considered.

The results of comparative analysis of congestion control methods based on queue length analysis and sensitivity analysis with 1-step and 3-step horizons predicting network status are presented. The study was conducted for sinusoidal function of the narrow queue. It is shown that the key performance indicators for the sensitivity function-based scheme are better than for the queue length analysis scheme. The queue size-based scheme is more sensitive to changes in queue maintenance speed, and data source speed fluctuations are less sensitive for the sensitivity-based scheme. For systems based on sensitivity function analysis, a 3-step horizon predictor provides better performance and a smaller maintenance queue than a 1-step horizon scheme.

Keywords: *telecommunication network; congestion forecasting; sensitivity function; gradient; neural system; queue management; prediction horizon.*

Олександр Торошанко,
канд. техн. наук, асист.
Асистент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Oleksandr Toroshanko,
PhD (Engin.), Assistant Prof.
Assistant Professor of the Cyber Security and Information Protection Department of the Faculty of Information Technologies of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Юрій Щебланін,
канд. техн. наук, ст. наук. співроб.
Доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Yury Shcheblanin,
PhD (Engin.), Senior Researcher.
Associate Professor of the Cyber Security and Information Protection Department of the Faculty of Information Technologies of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.