БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 1 (5) 2021 **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.

INFORMATION SYSTEMS AND TECHNOLOGIES SECURITY

№ 1 (5) 2021 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.

Editorial board address	**Bohdan Hawrylyshyn str. 24, UA-04116, Kyiv, Ukraine ☎ fax (+38044) 481 44 07, e-mail: fit@univ.net.ua**
Confirmed	**Academic Council of the Faculty of Information Technology of Taras Shevchenko National University of Kyiv 29.06.21 (протокол № 20)**
Registered	**Ministery of Information of Ukraine. State registration certificate КВ № 23831-13671Р from 15.03.2019**
Foundator and Publisher	**Taras Shevchenko National University of Kyiv, Publishing and Polygraphic Center "Kyiv University". The certificate is added to registry ДК № 1103 from 31.10.02**
Publisher's address	**Publishing and Polygraphic Center "Kyiv University" 14, Taras Shevchenko blvd., Kyiv, 01601, Ukraine ☎ (38044) 239 3172, 239 32 22; fax 239 31 28**

ЗМІСТ

КОМП'ЮТЕРНІ НАУКИ Й ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

CONTENTS

COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES

INFORMATION AND CYBER SECURITY

INFORMATION AND COMMUNICATION SYSTEMS

Наукове видання

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

№ 1 (5) 2021

Оригінал-макет виготовлено Видавничо-поліграфічним центром "Київський університет"
Виконавець *В. Гаркуша*

**Формат 60x84$^{1/16}$. Ум. друк. арк. 8,1. Наклад 100. Зам. № 221-10349.
Гарнітура Arial. Папір офсетний. Друк офсетний. Вид. № Іт2.
Підписано до друку 29.12.2021**

**Видавець і виготовлювач
ВПЦ "Київський університет",
б-р Тараса Шевченка, 14, м. Київ, 01601, Україна
☎ (38044) 239 32 22; (38044) 239 31 72; тел./факс (38044) 239 31 28
e-mail: vpc_div.chief@univ.net.ua; redaktor@univ.net.ua
http: vpc.knu.ua
Свідоцтво суб'єкта видавничої справи ДК № 1103 від 31.10.02**

КОМП'ЮТЕРНІ НАУКИ Й ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.413.5
DOI https://doi.org/10.17721/ISTS.2021.1.3-8

Ю. Є. Добришин, orcid.org/0000-0003-2473-9507,
dobr@krok.edu.ua
ВНЗ "Університет "КРОК"", Київ, Україна,
О. Є. Іларіонов, orcid.org/0000-0002-7435-3533,
oleg.ilarionov@knu.ua
П. М. Сорока, orcid.org/0000-0002-4864-904X**,**
p_soroka@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛЬ СТРУКТУРНО-ТЕХНОЛОГІЧНИХ ВЗАЄМОЗВ'ЯЗКІВ ОПЕРАЦІЙ З АДМІНІСТРУВАННЯ ТА ВІДНОВЛЕННЯ РОБОТИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Під час експлуатації програмного забезпечення суттєвою проблемою є визначення переліку операцій, які необхідні для створення належних умов роботи загальносистемного, прикладного програмного забезпечення, а саме призначення операцій/проведення заходів з адміністрування програмного забезпечення і швидкого його відновлення після аварій та уражень/пошкоджень комп'ютерним вірусом.

Розглянуто питання застосування логіко-математичного апарату щодо формалізації процесів обслуговування, адміністрування та відновлення роботи програмного забезпечення під час експлуатації автоматизованих інформаційно-телекомунікаційних систем і комплексів. Показано, що дослідники під час розгляду проблем експлуатації програмного забезпечення в основному зупиняються на питаннях удосконалення обслуговування, супроводження та реінженерії програмного забезпечення, зокрема й на описі послідовності виконання взаємопов'язаних процесів, методів і засобів обслуговування програмного забезпечення, питаннях експлуатації програмного забезпечення у розрізі його надійності, потреби у методах і засобах ідентифікації дефектів проєктування, а також прогнозування кількості помилок на етапі експлуатації інформаційних систем тощо. Наведено логічну схему процесу обслуговування програмного забезпечення, яка відображає логіку розв'язання задач і, у своїй основі, представляє сукупність логічних упорядкованих проєктних процедур у вигляді систем множин і відношень.

Для формального представлення технологічного процесу обслуговування програмного забезпечення автоматизованих інформаційно-телекомунікаційних систем і комплексів використовується його декомпозиція. Проєктування технологічного процесу супроводження програмного забезпечення виражається через морфологічну, інформаційну та математичну моделі. Сформульовано відношення слідування, еквівалентності, сумісності та взаємодії, які дозволяють установити та формалізувати взаємозв'язки між технологічними об'єктами, які беруть участь у процесі призначення (проєктування) технологічних операцій з адміністрування програмного забезпечення автоматизованих інформаційно-телекомунікаційних систем і створюють передумови щодо розроблення формалізованих умов синтезу проєктних рішень. За допомогою математичного апарату на базі логіки предикатів наведено приклади різних проєктних рішень, які дозволяють здійснювати проєктування операцій з обслуговування програмного забезпечення засобами комп'ютерної техніки.

Ключові слова: *реінженерія ПЗ; автоматизація обслуговування ПЗ; декомпозиція технологічного процесу.*

1. ВСТУП

Експлуатація автоматизованих інформаційно-телекомунікаційних систем і комплексів (далі АІС) передбачає проведення технологічних операцій з адміністрування, що застосовуються на місцях роботи АІС, та виконання заходів із відновлювання роботи програмного забезпечення в разі його пошкодження або виходу з ладу.

Суттєвою проблемою під час експлуатації програмного забезпечення є визначення переліку операцій, які необхідні для подальшого забезпечення належних умов роботи загальносистемного, прикладного програмного забезпечення, а саме призначення операцій/проведення заходів з адміністрування програмного забезпечення і швидкого його відновлення після аварій та уражень/пошкоджень комп'ютерним вірусом.

Практика розроблення й експлуатації програмного забезпечення складає основу методології обслуговування та подальшого супроводження програмного забезпечення, на базі якої можливо розробити формалізовані методики розв'язання окремих задач щодо призначення технологічних операцій з адміністрування програмних компонентів автоматизованих інформаційно-телекомунікаційних систем, а також визначити їхнє внутрішнє наповнення та взаємозв'язки між ними. Розв'язання такого типу задач потребує побудови математичної моделі у вигляді систем множин і відношень. Така модель дозволить класифікувати та проаналізувати властивості та відношення між технологічними операціями з обслуговування програмного забезпечення АІС, зможе виявити якісні зв'язки між операціями та формалізувати технологію їхнього призначення.

Математичний апарат повинен включати розроблення математичних виразів, що описують проєктні рішення, правила їхнього виведення відповідно з положеннями, прийнятими в математичній логіці. Тобто, під час призначення технологічних операцій з обслуговування програмного забезпечення АІС необхідно добитися заміни словесного виведення математичним виразом.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Вітчизняні та зарубіжні дослідники під час розгляду проблем експлуатації програмного забезпечення зупиняються в основному на питаннях удосконалення обслуговування, супроводження та реінженерії програмного забезпечення [1–14].

У наукових працях [1, 2] надано опис моделі супроводження інформаційних систем на етапах його життєвого циклу. На думку авторів, інформаційна система виступає пасивною категорією, як у процесі досліджень, так і у процесі проєктування. Функціонування інформаційної системи описується моделями розроблення, функціонування та розвитку. Автори визначають, що модель супроводження програмного забезпечення, як частина життєвого циклу інформаційної системи, складається з послідовності виконання взаємопов'язаних процесів, дій і завдань, опис яких можна подати у вигляді систем множин і відношень.

Інтерес представляють наукові роботи [3–5], в яких автор на підставі розгляду великих розподілених комп'ютеризованих інформаційних систем описує методи та засоби обслуговування програмного забезпечення.

Окремими авторами [6–8] питання експлуатації програмного забезпечення розглянуто у розрізі його надійності. У цих наукових працях описано основні підходи до аналізу надійності програмного забезпечення та обґрунтованого вибору необхідної моделі, що дозволяє в умовах реальної експлуатації інформаційних систем правильно визначити операції з їхнього супроводження.

Автори робіт [9–11] стверджують, що для автоматизації процесів обслуговування програмного забезпечення АІС потрібні методи і засоби ідентифікації дефектів проєктування, а також прогнозування кількості помилок на етапі експлуатації інформаційних систем. У цих же публікаціях розглянуто питання щодо аналізу дефектів у роботі програмного забезпечення, їхньої класифікації, закономірності появи та шляхи усунення.

Теоретичні дослідження стратегії обслуговування та супроводження програмного забезпечення АІС відображаються в роботах [12–14].

Таким чином, проблема автоматизації технологічних процесів обслуговування програмного забезпечення залишається актуальною та потребує подальшого вивчення та дослідження.

Певною базою, здатною вирішувати автоматизацію зазначених процесів, а саме, призначення технологічних операцій з адміністрування та відновлення роботи програмного забезпечення під час обслуговування АІС, може виступати формалізована теорія, яка передбачає опис предметної області шляхом визначення множини технологічних об'єктів і знаходження зв'язків між ними з подальшим формуванням певного математичного апарату.

Автоматизація технологічних процесів обслуговування програмного забезпечення АІС у подальшому може служити базою для створення систем автоматизованого управління процесами адміністрування та відновлення програмного забезпечення різних автоматизованих систем і комплексів.

3. МЕТА ДОСЛІДЖЕННЯ

Метою цієї роботи є розроблення моделі структурно-технологічних взаємозв'язків операцій з адміністрування та відновлення роботи програмного забезпечення, які застосовують під

час технологічного обслуговування автоматизованих інформаційно-телекомунікаційних систем.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Математичне моделювання базується на системному підході, який є концептуальним відносно структури проєктування процесу обслуговування програмного забезпечення АІС та визначає методику його розроблення в цілому та в багатьох зв'язках.

Під структурою проєктування процесу обслуговування програмного забезпечення розуміють установлені певні розподілені рішення, визначення яких реалізується за рахунок відповідних взаємозв'язків предметів, що беруть участь у логічній схемі призначення операцій з адміністрування та відновлення програмного забезпечення. Ця логічна схема відображає логіку розв'язання задач і у своїй основі представляє сукупність логічних упорядкованих проєктних процедур, формалізований опис яких спрощує їхнє математичне оброблення та дозволяє здійснювати проєктування операцій з обслуговування та супроводження програмного забезпечення за допомогою комп'ютерної техніки.

Для формального представлення технологічного процесу обслуговування програмного забезпечення АІС необхідно виконати його декомпозицію.

Така укрупнена декомпозиція з урахуванням операцій з адміністрування та відновлення показана на рис. 1. За її результатами можна визначити декілька окремих рівнів із відповідними задачами *Zi*.

Уведемо відношення, які мають місце між задачами різних рівнів і задачами одного рівня, позначивши їх відповідно *HiBj*. Розв'язання однієї задачі неможливо виконати без попереднього розв'язання іншої задачі. Одночасно кожна задача рівнів декомпозиції може бути представлена системою множин

$$Z\_i=\{V_{ij}, C_{ij}, R_{ij}, K_{ij}, T_{ij}, M_{ij}\}\ , \qquad (1)$$

де V_{ij} – вхідні дані; C_{ij} – обмеження на виконання технологічних операцій; R_{ij} – проєктні рішення; K_{ij} – оцінки проєктних рішень; T_{ij} – процедура розв'язання задачі; M_{ij} – модель задачі.

Таким чином, отримані в результаті проєктування розв'язання кожної конкретної задачі можуть бути описані у вигляді такого виразу:

$$T_ij = \{A_{ij}, C_{ij}, K_{ij}\} \overset{M_{ij}}{\longrightarrow} R_{ij}\ . \qquad (2)$$

На рівнях декомпозиції логічної схеми автоматизованого проєктування операцій з адміністрування та відновлення частина задач може виконуватися паралельно або у певному порядку.

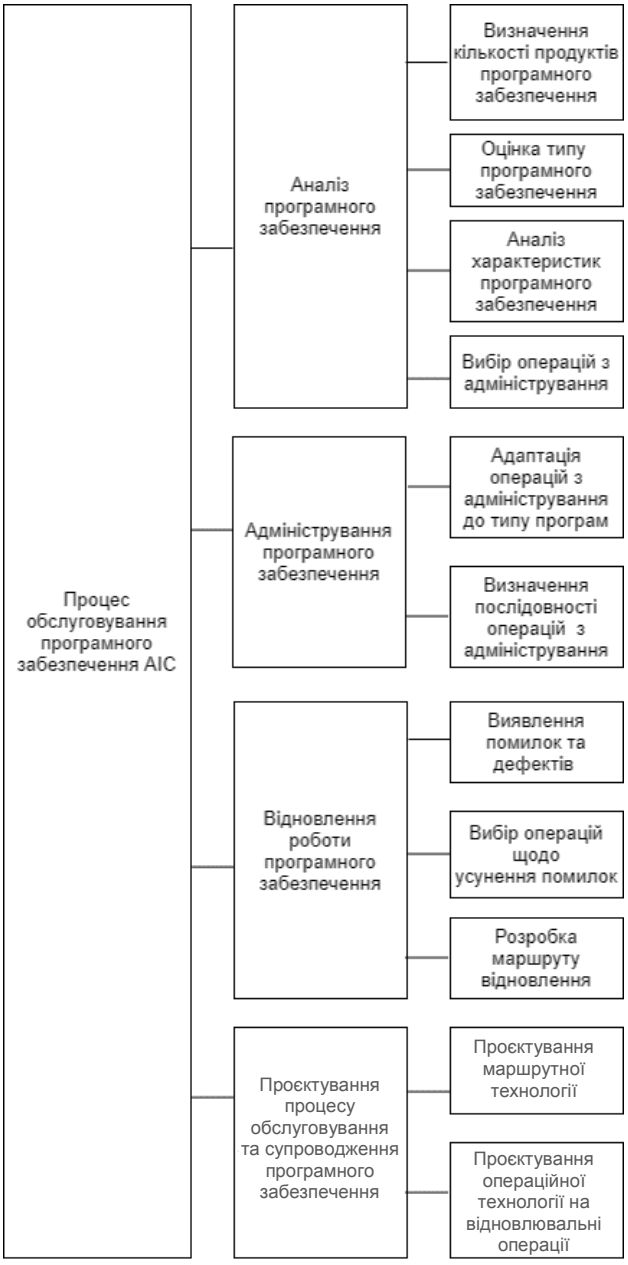


Рис. 1. Декомпозиція технологічного процесу обслуговування програмного забезпечення АІС

Причому під час призначення зазначених операцій необхідно вибрати технологічні об'єкти, які є предметом вивчення та які мають певні параметри (властивості).

Очевидно, що між технологічними об'єктами та властивостями існують певні відношення, які визначаються предикатом *Pt(x)*, де *x* є областю зміни технологічних об'єктів.

Проєктування технологічного процесу супроводження програмного забезпечення може бути

виражено через морфологічну, інформаційну та математичну моделі.

Морфологічна модель L_1 будується шляхом декомпозиції задачі проєктування з урахуванням того, що розв'язання певного кола задач можливе шляхом використання математичних моделей, які адекватно відображають процес призначення операцій.

Інформаційна модель L_2 відображає процес циркуляції інформації між задачами. Масиви інформації, що обробляються, складаються з постійної та змінної частин. Інформаційні зв'язки вказують напрямок передавання інформації між окремими блоками технологічного процесу супроводження.

Кожна задача під час проєктування технологічного процесу супроводження програмного забезпечення розв'язується за допомогою математичної моделі.

Математична модель може бути позначена як L_3. Причому основним моментом є те, що для кожної задачі обирається математичний метод, що забезпечує розв'язання задачі, і на основі якого отримуємо алгоритмічне представлення інформації.

Таким чином, процедуру побудови логічної схеми супроводження програмного забезпечення можна представити такою послідовністю:

$$L_1 \rightarrow L_2 \rightarrow L_3. \qquad (3)$$

У процесі створення технологічного процесу супроводження програмного забезпечення головними технологічними об'єктами проєктування виступає загальносистемне програмне забезпечення (операційна система), прикладне програмне забезпечення (база даних), спеціалізоване програмне забезпечення (прикладні додатки, драйвери, службові програми, програмне забезпечення мережі тощо), дефекти програмного забезпечення та способи їхнього усунення.

З урахуванням цього предметом дослідження на рівні логічної схеми будуть відношення між зазначеними технологічними об'єктами (множинами) та виявлення аналітичних взаємозв'язків, які піддаються математичній інтерпретації.

Розглядаючи множину можливих взаємопов'язаних елементів логічної схеми супроводження програмного забезпечення сформулюємо такі відношення:

Правило 1. Відношення слідування

Всі технологічні об'єкти можуть бути упорядковані під час виконання операцій з адміністрування програмного забезпечення. Наприклад, два технологічних об'єкти слідують один за одним під час призначення технологічних операцій з адміністрування, якщо їхні властивості розглядаються в певній послідовності. Зокрема, першими операціями з адміністрування виступають операції з моніторингу роботи системних журналів операційної системи, завантаженості оперативної пам'яті, перевірки системних журналів і журналів транзакцій. Під час адміністрування прикладного програмного забезпечення (баз даних) спочатку виконують операції з перевірки вільного простору у файлах даних (вільного місця у таблицях) і тільки після цього операції з резервного копіювання та копіювання архівних журналів транзакцій.

Відношення слідування будемо позначати символом ⇨ . У математичному вигляді зазначене відношення можна записати так:

$$\forall O_i\ \forall A_i\ \forall A_j\ \forall A_f\ \ \exists S_i\ \exists S_j\ \exists S_f\ \exists P$$
$$\{(A_i[S_i] \sim A_j[S_j]) \wedge (A_j[S_j] \sim A_f[S_f])\} \Rightarrow$$
$$(A_i[S_i] \sim A_f[S_f]), \qquad (4)$$

де O_i – об'єкт супроводження; $A_i,\ A_j,\ A_f$ – операції з адміністрування програмного забезпечення; $S_i,\ S_j,\ S_f$ – властивості операцій з адміністрування програмного забезпечення.

Правило 2. Відношення еквівалентності

Під відношенням еквівалентності мається на увазі символічне вираження технологічних можливостей і властивостей технологічних об'єктів. Наприклад, якщо існують дві або декілька операцій з адміністрування програмного забезпечення, які можуть бути застосовані, то можна стверджувати, що вони еквівалентні по своїх технологічних можливостях.

Відношення еквівалентності може бути застосовано до різного програмного забезпечення, для якого призначаються однакові операції з адміністрування або застосовуються однотипні способи відновлення роботи програмного забезпечення. Наприклад, це операції з моніторингу роботи програмного забезпечення, операції з обслуговування індексів і таблиць бази даних, створення архівів журналів транзакцій бази даних тощо.

Відношення еквівалентності позначимо символом ≡. Тоді у символічному вигляді вказане відношення описується виразом

$$\forall P_i \forall P_f\ \forall A_i \forall A_j\ \exists S_i\ \exists S_j\ \exists P$$
$$\{(A_i[S_i] = A_j[S_j]) \wedge (P_i[S_i] \neq P_j[S_j])\} \Rightarrow$$
$$(A_i[S_i] \equiv A_j[S_j]), \qquad (5)$$

де P_i, P_j – програмне забезпечення;
$A_i,\ A_j,\ A_f$ – операції з адміністрування програм-

ного забезпечення; $S_i, S_j\ S_f$ – властивості операцій з адміністрування програмного забезпечення.

Правило 3. Відношення сумісності

Якщо декілька технологічних об'єктів можуть бути визначені однаковими властивостями певного складу, то ці технологічні об'єкти мають відношення сумісності. Тобто, для кожного технологічного об'єкта знайдеться інший, який сумісний із першим. Позначимо таке відношення символом ↔.

Відношення сумісності може бути застосоване до різних пар технологічних об'єктів, а саме: операційна система – база даних; операційна система – прикладне програмне забезпечення; операційна система – спеціалізоване програмне забезпечення, що забезпечує роботу драйверів, допоміжного обладнання; дефект програмного забезпечення – спосіб відновлення, тощо.

У символічному вигляді зазначене відношення сумісності записують як

$$\forall O_i\ \forall P_f\ \forall A_j\ \exists S_i\ \exists S_f\ \exists S_j\ \exists P\ \{(O_i[S_i] = = P_f[S_f]) \wedge (P_f[S_f] = A_j[S_j])\} \Rightarrow (O_i[S_i]\ \leftrightarrow A_j[S_j]), \quad (6)$$

де O_i – об'єкт супроводження; P_f – програмне забезпечення; A_j – операція з адміністрування програмного забезпечення; S_i, S_f, S_j – властивості об'єкта супроводження, програмного забезпечення, операції з адміністрування.

Правило 4. Відношення взаємодії

Якщо два або більше технологічних об'єктів діють сумісно, але мають однакові властивості під час реалізації операцій з адміністрування, то вони є у взаємодії. Позначимо вказане відношення взаємодії через ≻—≺. Дійсно, більша частина технологічних об'єктів взаємодіють один з одним під час виконання своїх функцій. Наприклад, програмне забезпечення бази даних і прикладне програмне забезпечення перебувають у взаємодії під час вибору операцій з адміністрування.

Відношення взаємодії можна записати так:

$$\forall O_i\ \forall P_f\ \forall A_j\ \exists S_i\ \exists S_f\ \exists S_j\ \exists P\ \{(O_i[S_i] = P_f[S_f] = A_j[S_j])\} \Rightarrow (O_i[S_i]\ \succ\!\!-\!\!\prec P_f[S_f] \succ\!\!-\!\!\prec A_j[S_j]). \quad (7)$$

Отже, наведені вище відношення дозволяють установити та формалізувати взаємозв'язки між технологічними об'єктами, які беруть участь у процесі призначення (проєктування) технологічних операцій з адміністрування програмного забезпечення автоматизованих інформаційно-телекомунікаційних систем і створюють передумови щодо розроблення формалізованих умов синтезу проєктних рішень.

5. ВИСНОВКИ

Аналізуючи технологію застосування програмного забезпечення АІС у частині визначення операцій з адміністрування, необхідно зазначити, що їхнє призначення може бути здійснено шляхом розроблення логічної схеми процесу обслуговування програмного забезпечення.

У результаті декомпозиції задачі технологічного процесу обслуговування програмного забезпечення стало можливим таке.

1. Розробити математичну модель структурно-технологічних взаємозв'язків елементів програмного забезпечення, яка дозволила виокремити основні відношення між технологічними об'єктами та розкрити їхню формальну структуру з використанням логіко-математичного апарату.

2. Сформулювати відношення слідування, еквівалентності, сумісності та взаємодії між технологічними об'єктами, які беруть участь в обслуговуванні програмного забезпечення, що дозволяє створити формалізовані умови автоматизованого проєктування різних проєктних рішень під час розроблення операцій з адміністрування.

У подальшому автори планують розробити методику проєктування окремих проєктних процедур, що належать до складових технологічного процесу обслуговування, та представити їх за допомогою логіко-математичного апарату з метою подальшого застосування засобами комп'ютерної техніки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Yu Lisetcky, "Models of support for enterprise information systems by stages of the life cycle". *Software & Systems*, 2018, Issue 3, pp.455–460.

[2] Yu Lisetcky, V. Snytyuk "Formal presentation of a corporate integrated system in the form of a set of mathematical models" in *17-th Intern. Conf. "System Analysis and Information Technologies SAIT 2015"*, Kyiv, 2015. pp. 80–81.

[3] M. Sidorov "Methods for establishing and supervising software security for great computerized information systems" *Software engineering*, 2014. Issue 4, pp.30–37.

[4] E. Sidorov "Reverse engineering software for aviation simulators" *Information technology and computer engineering*, 2013, Issue 2, pp. 33–38.

[5] M. Lytsky, M. Sidorov, Yu. Ryabokin "Support the suitability and continued operation of aircraft software" *Programming problems*, 2010, Issue 3, pp. 229–236.

[6] V. Yukovyna, V. Smirnov, An overview of the main approaches to software reliability analysis" Lviv Polytechnic National University, Department of Software engineering, 2011, Issue 2. pp. 278–282.

[7]. L. Sakovy`ch, V.Pavlov, S.Livencev, Ya Nebesna. "Comparative analysis of special communication software reliability models" *Information Technology and Security*, 2012, Issue 2. pp. 61–69.

[8] D. Maevsky, S. Yaremchuk, "Analysis of software reliability models of guaranteed information systems", Electrical engineering and electrical equipment, 2010, Vol. 76, pp. 68–79.

[9] O. Nechaj, M. Sidorov, "Methods and means of detecting defects in the design of object-oriented software", Bulletin of NAU, 2009, Issue 3, pp.200–205.

[10] S. Antoshhuk, D. Maevsky`j, S. Yaremchuk, "Forecasting the number of errors at the stage of operation of adaptable accounting information systems", Electronic and computer systems, 2010, Issue 6, pp. 204–210.

[11] O. Shherbakov, Evaluation of the effectiveness of software testing based on the analysis of the number and criticality of the found defects", *Information processing systems*, 2011, Issue 3, pp.88–92.

[12] S.Cyucyura, O.Kryvoruchko, M. Cyucyura. "Energy management project reengineering project management strategy", Project management and production development, 2014, Issue 2, pp.70–76.

[13] V. Kuliamin, "Component architecture of model-based testing environment" *Journal of Programming and Computer Software*, 2010, Vol. 36, Issue 5, pp. 289–305.

[14] Ya. Volyans`ka, O. Mazur, T. Obnyavko, O. Ony`shhenko, "Method of selection of organizations for maintenance and repair of multi-purpose dual-purpose vessels" *Project management and production development*, 2018, Issue 2, pp.5–17.

[15] M. Barnett M., M. Fahndrich, P.de Halleux, F. Logozzo, N. Tillmann N. *Exploiting the Synergy between Automated-Test-Generation and Programming-by-Contract* in Proceeding of ICSE 2009, Vancouver, Canada, May 2009.

[16] I.V. Guchenko, "Usability management in the context of software architecture" *Software engineering*, 2014, Issue 2, pp. 20–25.

Стаття надійшла до редколегії 27.04.2021

Model of structural and technological interrelationships of software administration and recovery operations

During the operation of the software, a significant problem is to determine the list of operations that are necessary to ensure proper operating conditions of system-wide, application software, namely the appointment of operations/measures for software administration and rapid recovery after accidents and damage/damage by computer virus.

The article considers the application of the logical-mathematical apparatus for the formalization of maintenance, administration and restoration of software during the operation of automated information and telecommunications systems and complexes. It is shown that researchers when considering the problems of software operation mainly focus on improving the maintenance, maintenance and reengineering of software, in particular on the description of the sequence of interconnected processes, methods and tools of software maintenance, software operation in terms of its reliability, the need for methods and means of identifying design defects, as well as forecasting the number of errors during operation of information systems The paper presents a logical scheme of the software maintenance process, which reflects the logic of solving problems and, in its basis, represents a set of logically ordered design procedures in the form of systems of sets and relations.

For the formal presentation of the technological process of software maintenance of automated information and telecommunication systems and complexes, its decomposition is used. The design of the technological process of software support is expressed through morphological, informational and mathematical models. The paper formulates the relationship of following, equivalence, compatibility and interaction, which allow to establish and formalize the relationship between technological objects involved in the process of appointment (design) of

technological operations for the administration of software for automated information and telecommunications systems and create prerequisites for development of formalized conditions for the synthesis of design solutions. With the help of a mathematical apparatus based on the logic of predicates, examples of various design solutions are given, which allow to design software maintenance operations by means of computer equipment.

Keywords: *software reengineering; software maintenance automation; decomposition of the technological process.*

Юрій Добришин,
кандидат технічних наук, доцент кафедри комп'ютерних наук Навчально-наукового інституту інформаційних та комунікаційних технологій Вищого навчального закладу "Університет "КРОК".

Yuriy Dobryshyn,
Candidate of Technical Sciences, Associate Professor of the Department of Computer Science of the Educational and Scientific Institute of Information and Communication Technologies of the Higher Educational Institution "KROK University".

Олег Іларіонов,
кандидат технічних наук, доцент, завідувач кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Oleg Ilarionov,
Candidate of Technical Sciences, Associate Professor, Head of the Department of Intellectual Technologies, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv.

Петро Сорока,
кандидат фізико-математичних наук, доцент кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Petro Soroka,
Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Intellectual Technologies, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv.

УДК 005.8:316.422
DOI https://doi.org/10.17721/ISTS.2021.1.9-18

В. В. Морозов, orcid.org/0000-0001-7946-0832,
knumvv@gmail.com
А. С. Коломієць, orcid.org/0000-0003-4252-5975,
kolomietsa@fit.knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

РОЗРОБЛЕННЯ МОДЕЛЕЙ УПРАВЛІННЯ РИЗИКАМИ У ПРОЄКТАХ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ НЕЧІТКОЇ ЛОГІКИ

Статтю присвячено аналізу умов реалізації стартап-проєктів у галузі кібербезпеки, які сьогодні реалізуються та фінансуються державою за допомогою сучасних інформаційних технологій. У цій галузі з'являється багато різноманітних стартап-проєктів, пов'язаних із бурхливим розвитком інформаційних технологій і технологій захисту інформації. Однак можливості державного фінансування та залученого приватного фінансування таких проєктів є обмеженими, що певним чином стримує можливості подальшого розвитку. Отже, постає задача відбору для реалізації кращих стартап-проєктів у галузі кібербезпеки, що у свою чергу вимагає розроблення необхідних моделей і методів моделювання. Досліджено та проведено аналіз інформаційних джерел, які показують, що питання оцінювання ефективності IT-стартапів опрацьоване недостатньо, особливо для використання продуктів таких проєктів у питаннях кібербезпеки. Це накладає додаткові вимоги й обмеження на IT-продукти таких проєктів і на самі процеси управління вказаними проєктами. Крім того, майбутнє стартапів із кібербезпеки пов'язано з багатьма параметрами, які на початкових стадіях розгляду проєкту є вельми умовними та мають прогнозований характер. Тому для прийняття проєкту до розгляду доцільно використовувати методи нечіткого моделювання. За допомогою методу нечітких множин є можливість використовувати нечіткі змінні, які відображають невизначеність деяких параметрів таких проєктів. Запропонована методика досліджень базується на аналізі ефективності проєктів і використанні методів нечітких множин. Проводячи дослідження для оцінювання показників проєкту, користувалися нечіткими параметрами. Для цього побудовано функції належності, які встановлюють ступінь належності нечіткої множини. Як тип функції обрано модель трапеції та задано параметри, які відповідають песимістичному, базовому й оптимістичному сценаріям. Новизною роботи є визначення показника ступеня ризику стартап-проєкту, який залежить від критерію ефективності проєкту. Доведено залежність показника ступеня ризику проєкту з кібербезпеки від значення критерію ефективності проєкту. Запропонований підхід показав свою доцільність і може бути використаний для аналізу стартап-проєктів науковцями, проєктними менеджерами, підприємцями та інвесторами, фахівцями з кібербезпеки.

Ключові слова: *стартап, кіберпростір, проєкти з кібербезпеки, інформаційні технології, ризики, IT-продукти, нечіткі множини.*

1. ВСТУП

Сучасний розвиток інформаційних систем ґрунтується на подальшому використанні та вдосконаленні методів кібербезпеки та захисту інформації. Аналіз тенденцій кіберзлочинності, що є загрозою інформаційній безпеці країни, указує на нові руйнівні практики, що розвиваються в кіберпросторі, включаючи злочинне використання інтернету (кіберзлочинність), шпигунство з політичною або економічною метою, а також напади на критичну інфраструктуру (транспорт, енергетика, зв'язок та ін.) з метою саботажу [1] тощо.

З огляду на це, кібератаки на інформаційну інфраструктуру стали реальною загрозою і є однією з пріоритетних проблем національної безпеки й управління ризиками. Таким чином, з наукової точки зору слід приділяти значну увагу розвитку методів управління ризиками, які дозволяють моделювати майбутню поведінку складних інформаційних систем у разі різного роду атак і відмов [2].

Разом із тим, достатньо ефективним у дослідженнях такого спрямування є використання методів і технологій управління ІТ-проєктами [3]. Більше того, управління ризиками є однією зі складових галузей знань в управлінні проєктами [4].

Однак достатня конструктивна і технологічна складність побудови програм розроблення складних ІТ-продуктів вимагає використання не тільки проєктного підходу [5], а ще спеціального апарату, який здатний керувати ризиками в умовах недостатньої інформації та невизначеності. Найбільш придатним у цих умовах є апарат нечітких множин і нечіткої логіки [6].

Досвід показує, що для аналітичного оброблення значних обсягів інформації про взаємодію клієнтів з ІТ-системою, використання інноваційних підходів і нечіткої логіки матиме значний вплив на ефективність створення програм розвитку (проєктів) у галузі кібербезпеки.

2. АНАЛІЗ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ ТА ПУБЛІКАЦІЙ

Питаннями дослідження інноваційного розвитку через проєкти займались такі вчені: Стівен Бланк [7], Бред Фелд, Джейсон Мендельсон [8]. Серед українських учених у галузі управління проєктами, дослідження, пов'язані з використанням ціннісного підходу для інноваційних проєктів, проводили: Виленський П. Л. [9], Бушуєв С. Д., Ярошенко Ф. А. [10], Ципес Г. Л. [11] та ін. Причому ефективність проєктів вивчалася в публікаціях українських і зарубіжних учених, таких як Колеснікова К. В. [12], Кононенко І. В. [13], Морозов В. В. [14], Білощицький А. О. [15], Тімінський О. Г. [16], та іноземними вченими – Нонака І., Такеучи Х. [17], Тернер Р. [18], Мілошевич Д. [19], Том ДеМарко [20] та ін.

Аналіз інформаційних джерел показав, що нині питання оцінювання ефективності стартапів у галузі кібербезпеки опрацьоване недостатньо, не завжди можна використовувати класичні аналітичні методи, особливо для задач із невизначеністю.

Також проблеми реалізації інноваційного співробітництва з точки зору максимізації прибутку всіх зацікавлених сторін щодо збільшення їхньої ціннісної зацікавленості є ще недостатньо досліджені й потребують нових розроблень і удосконалень.

Мета статті. Метою статті є розроблення методики оцінювання безпекових ризиків в ІТ-проєктах розроблення систем із кібербезпеки у формі стартапів на основі теорії нечітких множин.

3. ЗАПРОПОНОВАНА МОДЕЛЬ І МЕТОД МОДЕЛЮВАННЯ

Як зазначено вище, наукові дослідження з розроблення економіко-математичних моделей аналізу ефективності стартапів із кібербезпеки потребують певного вдосконалення. Однак такі моделі й відповідне моделювання часто пов'язані з відсутністю необхідної інформації. Це певним чином впливатиме на ризикові події, які можуть трапитися у майбутньому з такими проєктами і будуть впливати не тільки на успіх реалізації проєкту, але й на безпеку не лише замовників і виконавців проєкту, а й на його оточення. Тому в цьому випадку доцільно використовувати нечітке моделювання. За допомогою методу нечітких множин будуються нечіткі змінні, які відображають невизначеність [8, 21, 22].

Основна ідея застосування цього апарату полягає в тому, що будь-який економічний показник трактується як інтервальний, задається не конкретним числом, а деяким проміжком, у вигляді нечіткої множини. Це відповідає ситуації, коли досить точно відомі лише межі значень показника, в яких він може змінюватися, але відсутня будь-яка кількісна або якісна інформація про можливості або ймовірності реалізації різних його значень усередині заданого інтервалу. Моделям, побудованим на нечіткій логіці, властива можливість адаптації до мінливих умов застосування інформаційних систем, як продуктів безпекових стартап-проєктів [22, 23].

Реалізацію математичної моделі розглянемо на конкретному прикладі. Нехай початкові інвестиції для певного ІТ-стартапу з кібербезпеки становлять близько 7–10 млн грн. Дослідження проєкту проведемо на основі приведеної вартості і внутрішньої прибутковості [23]. Визначимо цінність стартап-проєкту з кібербезпеки (СПКБ) як $\boldsymbol{P}$ – різниця між грошовими доходами і величиною початкових витрат:

$$P = -I_0 + \sum_{k=1}^{n} \frac{V_k}{(1+r)^k}, \qquad (1)$$

де $\boldsymbol{I_0}$ – обсяг первинних інвестицій для створення стартапу; V_k – надходження та платежі (прибуток) у $\boldsymbol{k}$-му періоді; $\boldsymbol{n}$ – число періодів; $\boldsymbol{r}$ – ставка дисконтування в $\boldsymbol{k}$-му періоді.

Задаємо показники СПКБ, як нечіткі параметри. Для цього побудуємо для них функції належності, які встановлюють ступінь належності нечіткій множині. З урахуванням виразу (1) визначимо змінні, які представимо в нечіткій формі. Це початкова інвестиція у реалізацію СПКБ – $\boldsymbol{I_0}$, прибуток – $\boldsymbol{V}$, ставка дисконтування – $\boldsymbol{r}$.

Виберемо межі змін досліджуваних показників. Задамо для них функції належності у вигляді трапецієвидної функції. Створимо множини $\boldsymbol{\alpha}$-рівня. Будуючи множини $\boldsymbol{\alpha}$-рівня, отримуємо наближене розкладання нечіткої множини (рис. 1).

Використовуючи операції над $\boldsymbol{\alpha}$-рівнями, знайдемо $\boldsymbol{P}$ і отримаємо наближене розкладання

нечіткої множини $\boldsymbol{P_\alpha}$ за рівнями **α**. Фактично побудуємо функцію належності для $\boldsymbol{P_\alpha}$, яку будемо досліджувати.

Трапецієвидне нечітке число записується у вигляді A= ($a_{\min}$,a_2,a_3,$a_{\max}$). Елементи множини A однозначно містяться у діапазоні [$a_{\min}$,$a_{\max}$], а діапазон [a_2, a_3] – це відрізок толерантності (інтервал стійкості), тобто елементи множини A приблизно дорівнюють будь-якому числу з цього відрізка.

Аргументи $a_{\min}$,a_2,a_3,$a_{\max}$ називають значущими точками нечіткого числа ***A***. Описуючи математичну модель за допомогою трапецієвидних нечітких чисел, значущі точки можна інтерпретувати як песимістичний, найбільш імовірний на відрізку, й оптимістичний сценарії розвитку ситуації.

Передбачається, що початкова інвестиція у СПКБ становить 7–10 млн грн., задаємо множину $\boldsymbol{I_0}$ числовими параметрами I_0= (7; 8; 9; 10).

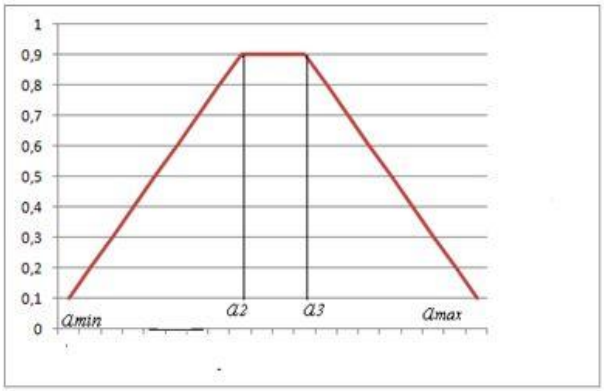


Рис. 1. Графік функцій належності трапецієвидної форми

Задаємо множину прибутку числовими параметрами V = (4; 4.5; 5.5; 6). Для ставок дисконтування r < 21,5 % реалізація СПКБ є прибутковим, оскільки його прибуткова вартість $\boldsymbol{P}$>0. Для ставки дисконтування r= 21,5 %, доходи від реалізації СПКБ дорівнюють інвестиційним витратам. Це максимально можлива ставка дисконту, при якій можна інвестувати кошти без втрат. Виберемо ставку дисконтування r у межах від 12 % до 21 % із вірогідним значенням 17 %. Задаємо множину числовими параметрами r = (0.12; 0.14; 0.18; 0.21). Трапецієвидна функція належності в загальному випадку може бути задана аналітично виразом (2).

Аналогічно побудовано функції належності для I_0, R. Далі будуємо наближене розкладання нечітких множин I_0, V , r по **α**-рівнях. Розраховуємо межі множин I_0, V , r при заданому значенні **α** – інтервали достовірності.

Обираємо 10 рівнів **α** на відрізку [0,1]:

$$\alpha \in \{0; 0{,}1; 0{,}2; 0{,}3; 0{,}4; 0{,}5; 0{,}6; 0{,}7; 0{,}8; 0{,}9; 1\}.$$

$$f_T(x; a_{\min}; a_2; a_3; a_{\max}) = \begin{cases} 0, & x < a_{\min} \\ \dfrac{x - a_{\min}}{a_2 - a_{\min}}, & a_{\min} \le x \le a_2 \\ 1 & a_2 \ge x \ge a_3 \\ \dfrac{a_{\max} - x}{a_{\max} - a_3}, & a_3 \le x \le a_{\max} \\ 0, & a_{\max} \le x \end{cases}, \quad (2)$$

де $a_{\min}; a_2; a_3; a_{\max}$ – деякі числові параметри, які набувають довільні дійсні значення.

Для розрахунку інтервалів достовірності при заданому значенні α_i і розв'язуються рівняння вигляду

$$I(x)_i = \alpha_i,\ V(x)_i = \alpha_i,\ r(x)_i = \alpha_i.$$

Інтервали достовірності представляються у вигляді матриць з елементами

$$I\alpha_{ij},\ V\alpha_{ij},\ V\alpha_{ij},\ R\alpha_{ij} (i = 1...10;\ j = 1,2).$$

Використовуючи матриці інтервалів достовірності $I\alpha$,$V\alpha$,$r\alpha$, знайдемо функцію

$P\alpha(I\alpha, V\alpha, r\alpha)$ за формулою (3):

$$P\alpha(I\alpha, V\alpha, r\alpha) = -I\alpha + \sum_{k=1}^{n} \frac{V\alpha}{(1 + r\alpha)^k}. \quad (3)$$

Результати розрахунків записуємо у таблицю.

Функція P має трапецієвидний вигляд, причому $P_{\min}$ = 0,571, $P_{\max}$ = 0,958, $P_{2,3}$ = 0,9. $P_3 = P_{\min}$ – песимістичний сценарій, $P_{\max}$ – оптимістичний сценарій. P_2, P_3 – базове значення. Отримані розрахунки значень P , показано на рис. 2.

Нечіткі числа є досить зручним способом моделювання стартап-проєктів із неоднозначними, імовірнісними характеристиками. Під час використання нечітких множин формула розрахунку P трансформується таким чином:

$$[P_{\min}, P_2, P_3, P_{\max}] = -[I_{\min}, I_2, I_3, I_{\max}] + \sum_{k=1}^{n} \left(\frac{[V_{\min}, V_2, V_3, V_{\max}]}{(1 + [R_{\min}, R_2 R_3, R_{\max}])^k} \right). \quad (4)$$

Унаслідок розрахунків ми отримуємо трапецієвидне нечітке значення показника $P = (P_{\min}, P_2, P_3, P_{\max})$.

Проєкт СПКБ має позитивну цінність, якщо P буде більше заданого інвесторами критерію W. Де W – оцінювання ризику інвестицій – визначення критеріїв, за яких результуюче значення інвестиційного процесу P буде нижче встановленого граничного рівня.

Таблиця

Матриці $I\alpha, V\alpha, r\alpha$

	rL	*IR*	*VL*	*VR*	*rL*	*rR*
0	4	10	4	6	0,12	0,21
1	4,15	9,85	4,1	5,9	0,125	0,206
2	7,3	9,7	4,2	5,8	0,13	0,202
3	7,45	9,55	4,3	5,7	0,135	0,198
4	7,6	9,4	4,4	5,6	0,14	0,194
5	7,75	9,25	4,5	5,5	0,145	0,19
6	7,9	9,1	4,6	5,4	0,15	0,186
7	8,05	8,95	4,7	5,3	0,155	0,182
8	8,2	8,8	4,8	5,2	0,16	0,178
9	8,35	8,65	4,9	5,1	0,165	0,174
10	8,5	8,5	5	5	0,17	0,17

Нехай W– вибране граничне значення. У цій задачі з нечіткими змінними оцінимо можливість події $P < W$, що визначає ризик того, що проєкт виявиться неефективним.

Оскільки результатом розрахунку P є нечітке число, то можливі такі варіанти його співвідношення з критерієм ефективності W (рис. 3).

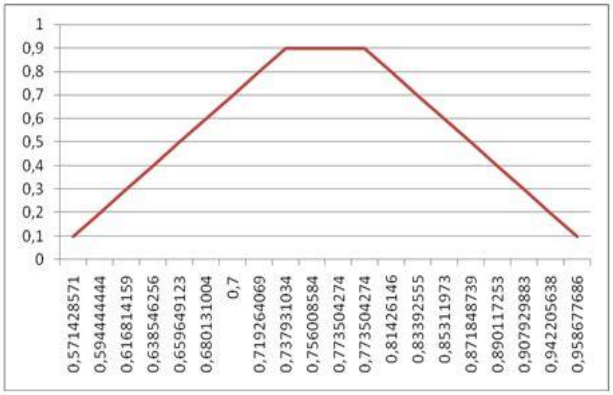


Рис. 2. Графік функцій P

Зазначені площі фігур можуть бути знайдені різними шляхами. У найзагальнішому вигляді площа фігури на інтервалі $[a_{\min}, W]$ являє собою певний інтеграл від функції, що обмежує фігуру зверху:

$$S_{(a_2, a_{\min})} = \int_{a_{\min}}^{W} \mu_{lef}\, dx, \qquad (5)$$

де μ_{lef} – функція, що дає опис *лівої частини* функції належності трапецієвидного нечіткого числа P.

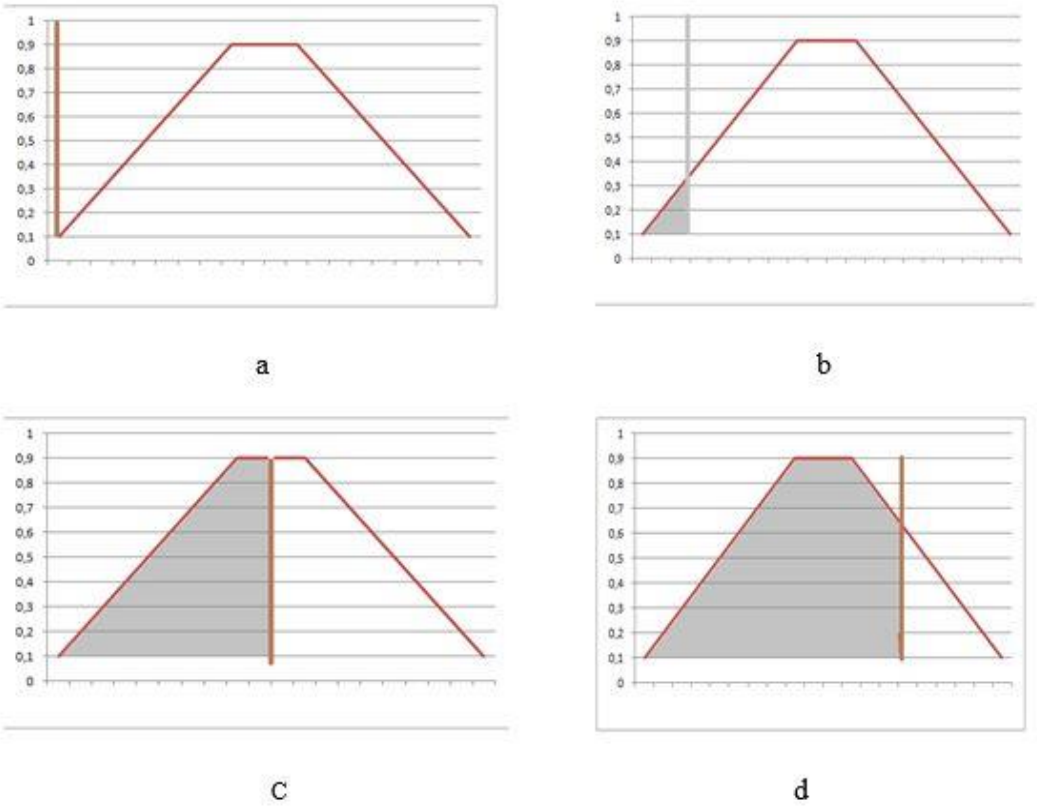


Рис. 3. Визначення ступеня ризику проєкту з кібербезпеки

Оскільки графіком функції належності трапецієвидного нечіткого числа є трапеція, то для отримання рівняння функції μ_{lef} скористаємося формулою прямої, що проходить через дві точки:

$$\frac{\mu_{lef}-\mu_2}{\mu_2-\mu_{\min}}=\frac{x-a_2}{a_2-a_{\min}}.$$

Знаючи, що $\mu_{lef}=0$ в точці $x=a_{\min}$ і $\mu_{lef}=1$ при $x=a_2$, ми можемо отримати таке рівняння графіка функції μ_{lef}:

$$\mu_{lef}=\frac{x-a_2}{a_2-a_{\min}}. \quad (6)$$

Тепер, знаючи функцію, ми можемо обчислити площу фігури:

$$S_{(a_{\min},W)}=\int_{a_{\min}}^{W}\mu_{lef}dx=\frac{(W-a_{\min})}{2(a_2-a_{\min})}. \quad (7)$$

Площу всієї області можливих значень P обчислимо значно простіше, якщо згадати, що графік функції власності є трапеція:

$$S_{(a_{\min},a_{\max})}=\frac{(a_{\max}-a_2)+(a_3-a_2)}{2}. \quad (8)$$

Отже тепер можемо отримати розрахункову формулу показника ризику при $a_{\min}<W\le a_2$:

$$R=\frac{(W-a_{\min})}{(a_2-a_{\min})(a_{\max}-a_{\min})(a_2-a_2)}. \quad (9)$$

У випадку $a_2<W\le a_3$ ступінь ризику R буде визначатися по аналогії з попереднім випадком (рис. 3, c):

$$R=\frac{S_{(a_{\min},a_2)}+S_{(a_2,W)}}{S_{(a_{\min},a_{\max})}},$$

де R – показник ступеня ризику проєкту,

$S_{(a_{\min},a_2)}+S_{(a_2,W)}$ – площа області неефективних інвестицій,

$S_{(a_{\min},a_{\max})}$ – площа області можливих значень P.

$$S_{(a_{\min},a_2)}=\frac{a_2-a_{\min}}{2}. \quad (10)$$

Формула показника ризику для $a_2<W\le a_3$:

$$R=\frac{(2W)-a_2-a_{\min}}{(a_{\max}-a_{\min})+(a_3-a_2)}. \quad (11)$$

Якщо $a_3<W\le a_{\max}$, то ступінь ризику R буде визначатися по аналогії з попереднім випадком (рис. 3, d):

$$R=\frac{S_{(a_{\min},a_2)}+S_{(a_2,a_3)}+S_{(a_2,W)}}{S_{(a_{\min},a_{\max})}}, \quad (12)$$

де R – показник ступеня ризику проєкту,

$S_{(a_{\min},a_2)}+S_{(a_2,a_3)}+S_{(a_2,W)}$ – площа області неефективних інвестицій,

$S_{(a_{\min},a_{\max})}$ – площа області можливих значень P.

У випадку $a_{\max}\le W$, увесь отриманий діапазон значень P однозначно менше оцінного критерію W, це говорить про те, що ризик такого проєкту становить 100 %, тобто R=1.

У підсумку для всіх описаних випадків ми можемо записати таку систему рішень, яка значною мірою спрощує механізм розрахунку ризиків інвестиційних стартап-проєктів:

$$R=\begin{cases}0, & W\le a_{\min},\\ \dfrac{(W-a_{\min})^2}{(a_2-a_{\min})((a_{\max}-a_{\min})+(a_3-a_2))}, & a_{\min}<W\le a_3,\\ \dfrac{(2W)-a_2-a_{\min}}{(a_{\max}-a_{\min})+(a_3-a_2)}, & a_2<W\le a_3,\\ 1-\dfrac{(a_{\max}-W)^2}{(a_{\max}-a_3)((a_{\max}-a_{\min})+(a_3-a_2))}, & a_3<W\le a_{\max},\\ 1, & a_{\max}\le W,\end{cases} \quad (13)$$

де $a_{\min}$ – нижня межа інтервалу значень P,

a_2 – крайня ліва межа інтервалу стійкості (толерантності) значень P,

a_3 – крайня права межа інтервалу стійкості (толерантності) значень P,

$a_{\max}$ – верхня межа інтервалу значень P,

W – критерій ефективності реалізації стартап-проєкту.

Таким чином, отримуємо модель, за допомогою якої можна розрахувати ризики інвесторів під час вкладення коштів у стартап-проєкти з кібербезпеки. Варто зазначити, що ця модель розраховує оцінки ризику інвестування в стартап-проєкти для інвестора (держави) залежно від критерію ефективності стартапу (рис. 4).

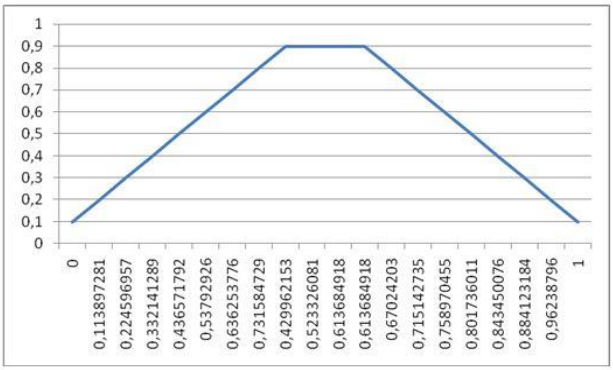


Рис. 4. Розрахунок ефективності СПКБ для інвесторів

Розраховано показник ефективності ризику, Якщо значення ефективності ризику,буде нижче за значення цього показника, то проєкт вважатиметься невигідним для фінансування (інвестора або держави).

4. ВИСНОВКИ

У роботі розроблено математичну модель розрахунку безпекових ризиків стартап-проєкту на основі теорії нечітких множин.

Доведено, що теорія нечітких множин є однією з найефективніших математичних теорій, спрямованих на оброблення невизначеної інформації, яка інтегрує відомі підходи і методи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Хлапонін Ю. Кондакова С. та інші Аналіз стану кібербезпеки в провідних країнах світу, https://www.csecurity.kubg.edu.ua/index.
php/journal/article/view/72

[2] Cybersecurity strategy (2018). Retrieved from: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

[3] Morozov V., Kalnichenko O., Liubyma Iu., "Proactive Project Management for Development of Distributed Information Systems". Proceedings of the 4th International Scientific and Practical Conference "Problems of Infocommunications. Science and Technology" (PIC S&T-2017), Kharkiv, Ukraine.

[4] A Guide to the Project Management Body of Knowledge (PMBOK®). 6-th ed. Project Management Institute Four Campus Boulevard. Delaware, Pennsylvania, USA, 2017, 586 p.

[6] Proactive Project Management. [Online]. Available: http://www.itexpert.ru/rus/ITEMS/200810062247 /, last accessed 2019/01/02.

[7] Blank, S., Dorf B.(2012). The Startup Owner's Manual: The Step-By-Step Guide for Building a Great Company (DI-ATEINO) Paperback – pp. 608. [in English].

[8] Feld B., Mendelson J. (2016).Venture Deals: Be Smarter Than Your Lawyer and Venture Capitalist 3rd Edition. – pp.304.

[9] Виленский П.Л., Лившиц В.Н., Смоляк С.А. Оценка эффективности инвестиционных проєктов: Теория и практика: Учеб.-практ. пособие. М.: Дело, 2001. – 888 с.

[10] Bushuiev S. D., Bushuiev D. A., Yaroshenko R. F. Deformatsiia polia kompetentsij v innovatsijnykh proektakh [Deformation of the field of competence in innovative projects]. Visnyk NTU "KhPI". Seriia: Stratehichne upravlinnia, upravlinnia portfeliamy, prohramamy ta proektamy. Kharkiv: NTU "KhPI". 2017. № 2 (1224). pp. 3–7.

[11] Tsypes H. L. Upravlenye ynnovatsyonnymy proektamy [Management of innovative projects]. URL:https://www.coursera.org/learn/innovacionnye-proekty (accessed 10.12.2019).

[12] Kolesnikova K., Olekh T. & other. Development of the Markovian model for the life cycle of a project's benefits. Eastern-European journal of enterprise technologies. 2018. 5/ 4(95), pp.30–39.

[13] Kononenko I. V., Aghaee A. Model and Method for Synthesis of Project Management Methodology With Fuzzy Input Data. Bulletin of NTU "KhPI". Ser.: Strategic Management, Portfolio, Program and Project Management. 2016. №1 (1173). pp. 9–13. doi: 10.20998/2413-3000.2016.1173.2.

[14] Morozov V., Mezentseva O., Proskurin M., Application of Game Theory for Decisions Making on the Development of IT Products. In Shpringer e-book "Lecture Notes in Computational Intelligence and Decision Making". Proceedings of the International Scientific Conference "Intellectual Systems of Decision Making and Problems of Computational Intelligence" (ISDMCI'2020), 2020, pp.377–394.

[15] Biloshchytskyi A., Kuchansky, Andrashko Yu., Biloshchytska S. A method for the identification of scientists' research areas based on a cluster analysis of scientific publications. Eastern-European Journal of Enterprise Technologies. 2017 № 5/2 (89), pp. 4–10.

[16] Timinsky O., Voitenko O., Achkasov I. Competence-based knowledge management in project oriented organisations in bi-adaptive context. Proceedings of the IEEE 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies (17-20 September, Lviv). Lviv, 2019, pp. 111–115.

[17] Nonaka I., Takeuchi H. The Knowledge-creating Company: How Japanese Companies Create the Dynamics of Innovation. Oxford University Press, 2011. 304 p.

[18] Turner R., "Guide to project-based management", tran. from English, Moskow: Grebennikov Publishing House, 2007. 552 p.

[19] Milosevic D. Z. A set of tools for project management / Trans. from English Mamontova E. V. Moscow: IT Co.; DMK Press, 2006. 729 p.

[20] DeMarco T., Lister T. Waltzing with bears. Risk management in software development projects. Moscow: Izd."Company p.m.Office", 2005.196 p.

[21] Damodaran A. (2012). Investment Valuation: Tools and Techniques for Determining the Value of Any Asset Hardcover –Wiley. Publ.– pp. 999.

[22] Levin, J,(2001) Information and the market of lemons. The RAND Journal of Economics. 32(4),pp.657–666.

[20] Недосекин А.О. Применение теории нечетких множеств к задачам управления финансами // Аудит и финансовый анализ. 2000. № 2. С.3–59.

[21] Цеслів О.В., Коломієць А.С. Оцінка інноваційної активності ІТ-підприємства.// V Міжнародна науково-практична конференція Інформаційні технології та взаємодії 20-21 листопада 2018, С.63–66.

[22] Цеслів О.В., Козюра А. О. Побудова економіко-математичної моделі взаємодії засновника стартапу із інвестором // Науковий вісник Херсонського державного університету. Сер. : Економічні науки. – 2018. – Вип. 30(2). – С. 160–162.

[23] Morozov V., Kolomiiets A., Investigation of Optimization Models in Decisions Making on Integration of Innovative Projects. In Springer e-book "Lecture Notes in Computational Intelligence and Decision Making". Proceedings of the International Scientific Conference "Intellectual Systems of Decision Making and Problems of Computational Intelligence" (ISDMCI'2020), 2020, pp. 51–64.

Стаття надійшла до редколегії 10.05.2021

Development of risk management models in projects cyber security using fuzzy logic

This article is devoted to the analysis of the conditions for the implementation of startup projects in the field of cybersecurity, which are currently implemented and funded by the state through the use of modern information technology. There are many different startup projects in this field, related to the rapid development of information technology and information security technology. However, the opportunities for public funding and attracted private funding for such projects are limited, which in some way hinders opportunities for further development. Thus, there is a task of selecting the best startup projects in the field of cybersecurity, which in turn requires the development of the necessary models and modeling methods. This paper investigates and analyzes information sources that show that the issue of evaluating the effectiveness of IT startups is not sufficiently addressed, especially for the use of products of such projects in cybersecurity. This imposes additional requirements and restrictions on the IT products of such projects and on the management processes of such projects. In addition, the future of cybersecurity startups is associated with many parameters that are highly conditional and predictable in the early stages of project review. Therefore, to accept the project for consideration, it is advisable to use fuzzy modeling methods. By using the fuzzy set method, it is possible to use fuzzy variables that reflect the uncertainty of some parameters of such projects. The proposed research methodology is based on the analysis of project efficiency and the use of fuzzy set methods. For this purpose, membership functions are constructed, which establish the degree of belonging of a fuzzy set. The trapezoid model is chosen as the function type and the parameters corresponding to the pessimistic, basic and optimistic scenarios are set. The novelty of the work is to determine the degree of risk of a startup project, which depends on the criterion of project effectiveness. The paper proves the dependence of the cybersecurity project risk indicator on the value of the project effectiveness criterion. The proposed approach has shown its feasibility and can be used to analyze startup projects by scientists, project managers, entrepreneurs and investors, cybersecurity professionals.

Keywords: *startup, cyberspace, cybersecurity projects, information technology, risks, IT products, fuzzy sets.*

Віктор Морозов,
кандидат технічних наук, професор, завідувач кафедри технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Victor Morozov,
Candidate of Technical Sciences, Professor, Head of the Department of Management Technology, Faculty of Information Technology, Taras Shevchenko National University of Kyiv.

Анна Коломієць,
кандидат економічних наук (економічна кібернетика), доцент кафедри технологій управління факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Anna Kolomiets,
Candidate of Economic Sciences (Economic Cybernetics), Associate Professor of the Department of Technology Management, Faculty of Information Technology, Taras Shevchenko National University of Kyiv.

ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА БЕЗПЕКА

УДК 005.8:316.422
DOI https://doi.org/10.17721/ISTS.2021.1.17-24

Н. В. Лукова-Чуйко, orcid.org/0000-0003-3224-4061,
lukova@ukr.net
С. В. Толюпа, orcid.org/0000-0002-1919-9174,
tolupa@i.ua
І. І. Пархоменко, orcid.org/0000-0001-6889-9284,
parkh08@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У СУЧАСНИХ СИСТЕМАХ IDS

Нині гостро стоїть проблема захисту інформаційно-комунікаційних систем і ресурсів кібернетичного простору. Швидкий розвиток інформаційної сфери приводить і до модернізації та ускладнення методів проведення атак на об'єкти кібернетичного простору. Кожного року зростає статистика вдалих атак на комп'ютеризовані системи різних організацій, включаючи і державні установи. Із цього можна зробити висновок, що навіть найнадійніші системи захисту не дають стовідсоткової гарантії захисту. Однією з можливих причин такого стану речей може бути саме використання більшістю систем безпеки стандартних механізмів і способів захисту. До таких механізмів належать – розмежування доступу, яке базується на правах суб'єкта доступу, шифрування й ідентифікація, і аутентифікація. Традиційні способи не можуть захисти від власних користувачів, які мають злочинні наміри. Крім того, цей підхід не вирішує проблеми чіткого поділу наявних суб'єктів системи на предмет авторизованого використання глобалізованих ресурсів, можливості підбору паролів із застосуванням спеціалізованого програмного забезпечення, а також залишається проблема обмеження доступу до ресурсів інформаційної системи, що може мати як наслідок зменшення продуктивності й ускладнення проходження транзакцій між компонентами вказаної системи. Виникає потреба застосовувати механізми, які б не відкидали переваги традиційних, але і доповнювали б їх. А саме, щоб ці механізми виявляли спроби неавторизованого, несанкціонованого доступу, надавали інформацію про такі спроби, і крім того, могли реагувати у відповідь. Одним із ключових факторів використання таких систем захисту є їхня здатність запобігати атакам зловмисників, які були аутентифіковані й авторизовані з додержанням усіх процедур і правил доступу й отримали необхідні права на певні дії. Звичайно неможливо передбачити повний набір сценаріїв подій у системі з авторизованим користувачем, який має зловмисні наміри, але необхідно зробити детальний опис можливих "зловмисних" сценаріїв, або піти від зворотного й описати так звані "нормальні" сценарії. Опис "нормальних сценаріїв" дасть можливість виявити небезпечну активність, адже ця активність буде мати відхилення від так званого "нормального" сценарію поведінки в системі навіть авторизованим користувачем. Отже дослідження можливостей використання механізмів, які спрямовані на виявлення аномалій у системі або на пошук зловживань, можуть допомогти реалізувати ефективні рішення для систем виявлення та попередження вторгнень.

Ключові слова: *система виявлення вторгнень, виявлення статистичних аномалій, виявлення на основі сигнатур, безпека інформаційних технологій.*

1. ВСТУП

У сучасних системах виявлення та попередження вторгнень як правило використовують методи, які зорієнтовані на два напрямки, а саме: перший напрямок спрямований на виявлення аномалій у системі, а інший – на пошук зловживань [1]. У переважній більшості систем попередження та виявлення вторгнень використовують поєднання різних рішень на базі синтезу відповідних методів. Це зумовлено тим, що два зазначені напрямки мають як переваги, так і недоліки.

Методи, які використовують для виявлення аномалій, ідентифікують процес, що викликав підозрілі відхилення чи зміни в роботі системи. Реалізація цієї ідеї дозволяє виявляти дії зловмисника, що має авторизовані права доступу в системі.

У цьому контексті існують дві групи методів, а саме: методи з контрольованим навчанням та з неконтрольованим навчанням. Характерною ознакою методів контрольованого навчання є те, що вказані методи використовують фіксований набір параметрів оцінки й апріорні відомості про значення параметрів оцінки, а також фіксований час навчання.

Що стосується неконтрольованого навчання, то в цьому випадку всі параметри оцінки можуть змінюватися із часом, крім того, сам процес навчання відбувається неперервно.

Методи, які належать до іншого напрямку, а саме виявлення зловживань, використовують механізми пошуку певних послідовностей подій, що визначаються як етапи реалізації вторгнень. І в цьому випадку застосовують контрольоване навчання.

Методи, які реалізовані в системах виявлення та попередження вторгнень, засновані на загальних уявленнях теорії розпізнавання образів. У цьому випадку для виявлення аномалій формується образ нормального функціонування системи, який базується на експертних оцінках. Указаний образ є певною сукупністю значень параметрів оцінки. І якщо відбувається зміна цього образу, то це трактується як аномальний стан системи.

Коли аномалії виявлені і проведена оцінка, то визначається природа цих змін, а саме: чи це просто допустиме відхилення, чи це результат вторгнення. Зазначені вище функції виконують системи виявлення та попередження вторгнень.

2. СТАН ПРОБЛЕМИ

Якщо атаку на інформаційну систему реалізує зловмисник високої кваліфікації, то це буде як правило багатокроковий процес. Тому одним із найпростіших способів злому системи або виведення її з дієздатного стану є використання сформованих модулів, які реалізують усі етапи атаки. Такі модулі мають назву "експлойти" і їх можна легко завантажити через інтернет.

Як відомо, системи виявлення та попередження вторгнень (Intrusion Detection System – IDS) мають два типи – це системи виявлення зловживань (Misuse Detection Systems – MDS) та системи виявлення аномалій (Anomaly Detection Systems – ADS).

Щодо систем MDS, то їхня робота ґрунтується на формуванні шаблонів атак. Рівень абстракції цих шаблонів атак може бути достатньо простим, якщо оперують інформацією про певні значення заголовків мережного пакета або послідовності певних команд у файлі аудиту, або достатньо складним. Якщо враховувати траєкторії системи у просторі станів під час проходження певних небезпечних станів, то в цьому разі система захисту може мати досить високу ефективність в тому випадку, коли буде відома схема атак. Але якщо вказана схема не буде відома, або атаки будуть мати непередбачувані відхилення від цієї схеми, тоді виникають проблеми. Тому звичайно в цьому випадку необхідно постійно актуалізувати базу даних кожної атаки та її можливих варіацій.

Можна зазначити, що в системах ADS певні дії, які є відмінними від поведінки в нормальному стані, ідентифікуються як аномальні. І це дає можливість реєструвати невідомі атаки в атакованій системі.

Системи ADS перед початком використання мають накопичити необхідну інформацію і скласти певну концепцію нормальної активності системи, чи окремих користувачів, або процесів. Ця концепція стає еталоном для оцінювання наступних дій і даних. У цьому випадку має бути визначена оптимальна сукупність факторів для спостереження. З одного боку їхня кількість не повинна знизити загальну продуктивність системи, а з іншого – для побудови профілю нормальної поведінки треба мати вичерпні характеристики цієї сукупності факторів.

Звичайно системи ADS не застраховані від помилок, які є двох видів:

а) користувач помилково приймається за зловмисника, або нормальна поведінка сприймається як зловмисні дії (англ. false positives);

б) за нормальну активність приймаються зловмисні дії чи спроба зловмисного проникнення в систему (англ. false negatives).

Друга помилка є небезпечніша за першу, і тому необхідно визначати умови, за яких ситуація може сприйматися як аномальна [2, 17].

Більшість спроб побудови ADS є концептуальними моделями, що перевіряють можливість застосування математичної моделі. А от реальних продуктів реалізації IDS мало і зазвичай це MDS.

З літературних джерел можна визначити типи методів виявлення аномалій, а саме:

а) частотні,

б) нейромережні,

в) на базі скінченних автоматів,

г) на базі зберігання прикладів поведінки,

д) спеціальні.

Отже як основне завдання можна визначити пошук найоптимальніших методів побудови ADS.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Формування образу нормального функціонування на базі сукупності певних параметрів для систем IDS характерно для методів виявлення аномалій, які саме і спрямовані на запобігання невідомим атакам і вторгненням.

Існує декілька способів формування образу нормального функціонування, а саме:

- для кожного параметра оцінки акумулюють характерну статистичну інформацію;
- нейронні мережі навчаються значенням параметрів оцінки;
- застосовують подієве подання.

У цьому випадку, як видно з переліку, у процесі виявлення сукупність параметрів відіграє ключову роль. Отже, головним завданням у цьому є визначення оптимальної множини, а також формування загального показника аномальності.

Для системи, яка підлягає захисту, у задачі вибору оптимальної сукупності ознак можна використати евристичний вибір сукупності параметрів вимірювань системи. Застосовуючи цей метод, можна досягти достатньо ефективного і точного розпізнавання вторгнень. Але треба брати до уваги той факт, що складові підмножини залежать від типів виявлених атак, тому для всього різновиду атак певний набір параметрів не підходить.

Кожна система має свій унікальний комплекс апаратно-програмних засобів і тому існує вірогідність, що IDS пропускає специфічні для даної системи вторгнення, які застосовують ідентичний набір параметрів.

Отже, визначати необхідні параметри оцінки доцільно у процесі роботи. Звичайно існують труднощі за динамічного формування параметрів оцінки. Ці труднощі пов'язані з тим, що області пошуку по експоненті залежать від потужності початкового набору параметрів.

Візьмемо певний початковий список з N параметрів, які є актуальними при передбаченні вторгнень. З урахуванням цього кількість підмножин даного списку буде становити 2^N. Ми бачимо, що в цьому випадку не є можливим для знаходження оптимальної множини використовувати алгоритми перебору. Тому одним із рішень може бути використання генетичних алгоритмів [3].

Треба зазначити, що оцінка аномальності має визначатися з розрахунку множини її параметрів. Для формування цієї загальної оцінки можливо використовувати метод, який базується на статистиці Баєса, або метод, заснований на використанні коваріантних матриць.

Використовуючи методи статистики Баєса зазначаємо, що A_1 ... A_n – це n вимірів. Ці виміри використовують для визначення в будь-який момент часу факту вторгнення. Оцінку різних аспектів системи, таких як кількість порушень пам'яті чи подій вводу-виводу, позначимо A_i.

Позначимо, що A_i може мати значення 1 – аномальне вимірювання, 0 – неаномальне вимірювання. У цьому випадку I беремо як гіпотезу того, що в системі є процес вторгнення.

Показники достовірності й чутливості кожного виміру визначають таким чином:

$$P(A_i = 1 \mid I) \text{ и } P(A_i = 1 \mid \neg I). \quad (1)$$

Далі за теоремою Баєса ймовірність обчислюється як

$$P(I \mid A_1, A_2, \dots, A_n) = \\ = P(A_1, A_2, \dots, A_n \mid I) \frac{P(I)}{P(A_1, A_2, \dots, A_n)}. \quad (2)$$

Для будь-якої комбінації множини вимірів треба обчислити умовну ймовірність для подій I.

Припускаємо, що кожне з вимірювань A_i залежить тільки від I і також умовно від інших вимірів не залежить, а саме A_j, де $i \neq j$.

Враховуючи зазначене вище, напишемо такі співвідношення:

$$P(A_1, A_2, \dots, A_n \mid I) = \prod_{i=1}^{n} P(A_i \mid I) \quad (3)$$

і

$$P(A_1, A_2, \dots, A_n \mid -I) = \prod_{i=1}^{n} P(A_i \mid \neg I), \quad (4)$$

тому

$$\frac{P(A_1, A_2, \dots, A_k \mid I)}{P(A_1, A_2, \dots, A_k \mid I)} = \frac{P(I) \prod_{i=1}^{n} P(A_i \mid I)}{P(I) \prod_{i=1}^{n} P(A_i \mid I)}. \quad (5)$$

Для визначення ймовірностей вторгнень використовують значення вимірювань аномалій, а також значення ймовірності появи кожного з вимірів аномальності, що були зафіксовані раніше, та ймовірність вторгнення.

Треба зазначити, що для більш реалістичної оцінки P ($I|A_1 \dots A_n$) треба врахувати вплив певних вимірювань A_i один на одного.

Ще один із методів, який допоможе враховувати зв'язки між вимірами, є коваріантні матриці. У цьому випадку, якщо виміри A_1 ... A_n являють собою вектор A, то

$$A^T C^{-1} A. \quad (6)$$

У цій формулі C є коваріантною матрицею, яка представляє залежність між кожною парою вимірів аномалій.

Далі розглянемо так звані мережі довіри чи мережі Баєса. Зазначимо, що вказані мережі – це графові моделі ймовірнісних і причинно-наслідкових зв'язків між змінними в статистичному інформаційному моделюванні. У цьому

випадку має місце поєднання емпіричних частот появи різних значень змінних, суб'єктивних оцінок "очікувань" і теоретичних уявлень про математичні ймовірності інших наслідків з апріорної інформації [4].

У цьому разі накопичені в певній спеціальній структурі вимірювання значень параметрів оцінки формують образ нормальної поведінки системи. Саме ця структура і називається профайлом. До структури профайла є ряд вимог. До головних можна віднести вимогу мінімального кінцевого розміру та вимогу до операції оновлення, яка повинна виконуватися як можна швидше.

Зазвичай застосовують статистичні методи оцінювання у разі виявлення можливих аномалій із використанням профайла. У цьому випадку в процесі виявлення відбувається порівняння поточних значень вимірювань профайла із збереженими значеннями. Таким чином визначається показник аномальності при вимірюванні.

Слід зазначити, що загальний показник аномальності в деякому простому випадку може обчислюватися з використанням загальної функції, враховуючи значення показника аномалії в кожному з вимірювань профайла. Як приклад можемо використати M_1, M_2 ... M_n, – вимірювання профайла, а S_1, S_2 .... S_n відповідно – значення аномалії кожного з вимірювань. І треба врахувати те, що чим більше число S_i, тим більше аномалій в i-му показнику.

Отже в цьому випадку об'єднувальна функція може бути вагою сум їхніх квадратів:

$$a_1 s_1^2 + a_2 s_2^2 + \ldots + a_n s_n^2 > 0, \qquad (7)$$

де a_i показує відносну вагу метрики M_i.

А якщо припустити, що параметри M_1, M_2 ... M_n, залежать один від одного, то в цьому випадку для їхнього об'єднання може знадобитися складніша функція.

Основна перевага такого підходу ґрунтується на застосуванні відомих статистичних методів.

Ще один спосіб формування образу нормальної поведінки – це використання нейронних мереж для навчання значенням параметрів оцінки.

Що стосується навчання нейронної мережі, то в цьому випадку застосовують послідовність команд, і будь-яка із цих команд може бути на більш абстрактному рівні, ніж використовувані параметри оцінки.

Нейронною мережею обробляють вхідні дані, які складаються з поточних команд і минулих W команд, які ще мають назву розміру вікна. Мережа являтиме собою образ нормальної поведінки, тільки після того, як дана нейронна мережа буде навчена множиною послідовних команд системи або хоча б однієї з її підсистем.

Фактично виявляється відмінність у поведінці об'єкта і передбачається визначення показника неправильно передбачених команд. І саме це є процесом виявлення аномалій.

На рисунку стрілки на рівні рецептора показують вхідні дані останніх W команд, які виконані користувачем.

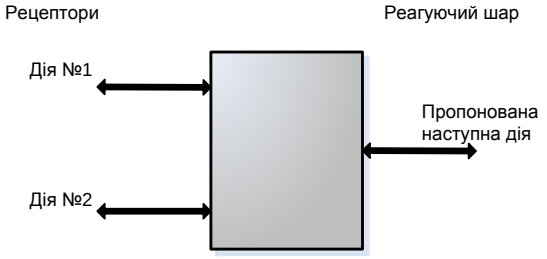


Рисунок. Концептуальна схема нейроних мереж IDS

У цьому випадку кілька значень або рівнів задає вхідний параметр. У свою чергу кожен із цих рівнів чи значень унікально визначає команду. А вихідний реагуючий багаторівневий шар передбачає наступну можливу команду користувача [5].

Щодо переваг указаного методу, то слід заначити, що нейронні мережі достатньо легко справляються з викривленими даними і крім того, враховують зв’язки між різними вимірюваннями, що впливають на результат оцінювання, причому роблять це автоматично. Підкреслимо, що успіх цього підходу не залежить від природи вихідних даних.

Звичайно, крім переваг метод має і недоліки, а саме: величезне значення має величина розміру вікна IDS та визначення топології мережі і ваги вузлів, що реалізуються після великої кількості спроб і помилок.

Далі розглянемо генерацію патернів. У цьому випадку представлення образу базується на певному припущенні про те, що можна пов’язати з поточним станом системи поточні параметри оцінювання. З урахуванням цього припущення функціонування можна подати у вигляді послідовності подій і станів.

У роботі [6] запропоновано певні тимчасові правила, які характеризують сукупності значень патерну (параметрів оцінювання) нормальної роботи. Крім того, ці правила можуть динамічно змінюватися на кращі правила у процесі навчання і їхнє формування відбувається індуктивно. Що стосується кращих правил, або так званих "хороших правил", то тут можна розуміти такі правила, які мають більшу ймовірність їхньої появи і крім того мають великий рівень унікальності для системи захисту.

Із сказаного вище можемо для прикладу записати таке правило:

$$E_1 \geq E_2 \geq E_3 \Rightarrow (E_4 = 95\%, E_5 = 5\%), \quad (8)$$

де $E_1 \ldots E_5$ – подія з безпеки.

З урахуванням зазначеного твердження доходимо висновку, що встановилася певна залежність для послідовності патернів, а саме: якщо маємо E_1, а далі E_2 та E_3, то після цього вірогідність прояву E_4 відповідно має 95 % , а E_5 усього 5 %.

Указані правила під час спостереження роботи користувача створюються індуктивно.

Якщо маємо таку ситуацію, що спостережувана послідовність подій відповідає лівій частині правила, виведеного раніше, а події, які відбулися в системі після цього, значно відрізняються від тих, які мали настати за правилом, то в такому випадку аномалія реєструється.

Отже стосовно переваг цього методу, можна зазначити, що він може ефективно визначати вторгнення з урахуванням залежності між подіями та їхньою послідовністю. Крім того, ураховуючи, що правила у вказаному методі містять у собі семантику процесів, то він має кращу чутливість до виявлення порушень. Також цей метод має кращу обробку користувачів, які мають чітку послідовність патернів, хоча можуть містити великі коливання поведінки. І безумовно перевагою такого методу є те, що він акцентує увагу не на всю підозрілу сесію, а на певні важливі події.

Треба звичайно зазначити і недолік указаного підходу, який пов’язаний із тим, що певні невпізнані патерни поведінки можуть бути не прийняті за аномальні тому, що вони не мають відповідності жодному з правил.

Звичайно використання методів виявлення аномалій не дає абсолютної гарантії з виявлення всіх вторгнень, тому системи IDS використовують окрім технології виявлення аномалій і технологію розпізнавання зловживань. У цій технології процес виявлення вторгнень базується на прогнозі з визначення можливих атак, і далі відбувається спостереження за їхньою появою [1, 13].

Під час застосування технології розпізнавання зловживань на відміну від технології виявлення аномалій образ є необхідним для подання несанкціонованих дій зловмисника і він не буде моделлю нормальної поведінки системи. Отже такий образ має назву сигнатура вторгнень. І ця сигнатура формується на значеннях параметрів оцінювання, а саме на основі тих же вхідних даних, що і в разі виявлення аномалій.

Слід зазначити, що ці сигнатури вторгнень визначають умови та спорідненість між подіями, які можуть призвести до певних зловживань. Крім того, дані сигнатури є корисними у виявленні спроб вчинення незаконних дій. Важливий аспект полягає в тому, що за наявності часточкового збігу сигнатур можна ідентифікувати спробу вторгнення.

Отже, для визначення можливих зловживань необхідно розрахувати умовну ймовірність. Позначимо так: *P (Вторгнення | Патерн подій).*

У цьому випадку використовуємо формулу Баєса для визначення ймовірності того, що якась множина подій є діями зловмисника:

$$P(I \mid A_1, A_2, \ldots, A_n) = \\ = P(A_1, A_2, \ldots, A_n \mid I) \frac{P(I)}{P(A_1, A_2, \ldots, A_n)}, \quad (9)$$

де I – вторгнення, а $A_1 \ldots A_n$ – послідовність подій.

Саме сукупність параметрів системи і є певною подією.

Для розв'язання задач із виявлення вторгнень також застосовують продукційні системи, перевагою яких є можливість поділу причин і рішень виниклих проблем.

Ця система, використовуючи правила if (якщо), причина then (то), рішення кодує інформацію про вторгнення. А саме у частині (if) правила кодують умови (причини), необхідні для атаки, і коли всі умови виконано, то виконується дія (рішення), задана у правій частині [7, 12].

Що стосується проблем, які можуть виникати під час використання певних додатків, які ґрунтуються на вказаному методі, то слід зазначити їхню недостатню ефективність у роботі з великими обсягами даних і складність у врахуванні залежної природи даних параметрів оцінки. Крім того, є проблеми з тим, що відсутня вбудована або природна обробка порядку послідовностей в аналізованих даних. Також прийнятність вбудованої експертизи залежить від того, чи певні модельовані навички адміністратора безпеки не є суперечливими.

Слід також зазначити, що під час використання продукційних систем об'єднання різних вимірів вторгнень і створення пов'язаної картини вторгнення призводить до того, що деякі причини стають невизначеними. Але все-таки за допомогою наявних даних можна встановити символічний прояв вторгнення. Хоч у вказаних системах виявляються лише відомі вразливості.

Ще один метод, а саме метод аналізу станів, був описаний у публікації [8] і його реалізація наведена в публікації [9]. У цьому випадку сигнатура вторгнень представляється послідовністю переходів між станами системи. А також патерни атаки пов’язані з певним станом системи і звичайно пов’язані із цим станом певною логічною

функцією. Можна вважати, що система вже перебуває в певному стані, якщо функція виконується. Необхідними подіями для наступних переходів є певні стани, які з'єднані з поточним лініями і при цьому певні типи подій, які можуть відбутися, є вбудованими в модель і як правило відповідають за принципом один до одного значенням параметрів оцінки.

Але слід зазначити, що певні патерни атак тільки задають послідовність подій і тому складніші способи визначення подій не можливі. Отже в цьому випадку використовується проста вбудована логічна функція.

Ще одна технологія, яка використовується для виявлення вторгнень – технологія спостереження за натисканням клавіш. У цій технології відбувається моніторинг натискань на клавіатурі певним користувачем для того, щоб ідентифікувати атаки. Отже в цьому випадку послідовність таких натискань користувачем є патерном атаки.

Проте на жаль під час використання такого підходу є проблема з надійністю механізму перехоплення роботи з клавіатурою, особливо коли відсутня підтримка операційної системи. Крім того, може бути велика кількість варіантів представлення ідентичних атак.

Ще одним слабким місцем цієї технології є те, що різного роду псевдоніми команд без використання семантичного аналізатора натискань просто зруйнують дану технологію. Причому досить складно буде виявити автоматизовані атаки, які є результатом виконання програм зловмисника [10, 14].

Ще одну групу методів для виявлення вторгнень, які застосовуються в IDS-системах, засновано на моделюванні поведінки зловмисника. У цьому випадку для виявлення зловживань можна використовувати метод об'єднання моделі зловживання з очевидними причинами, який використовує базу даних певних сценаріїв атак із послідовністю поведінок, що характерні для атаки.

Звичайно існує можливість, що кожна з підмножин у сценарії атак може бути присутня в системі. Результатом пошуку певної інформації в записах аудиту про наявність цих сценаріїв атак є певна кількість фактів, яка або підтверджує, або спростовує гіпотези.

Процес, в якому виконується перевірка, має назву антисепатор, і вказаний процес формує певну множину поведінок, базуючись на активній моделі, яка функціонує в поточний момент часу. Ця наступна можлива множина поведінок має бути перевірена у записах аудиту і тільки після цього буде передана планувальнику. Саме планувальник має визначити, яким чином має відобразитись у записах аудиту ця передбачена множина поведінок і сформувати певний системний вираз, який залежить від аудиту. Дані вирази повинні мати достатньо високу ймовірність того, що вони з’явилися б у записах аудиту, і крім того, такі структури, мають давати можливість легкого їх знаходження.

Отже, якщо у деяких сценаріїв підстави підозр збільшуються, а в інших сценаріїв зменшуються, то в цьому випадку йде мінімізація списку моделей активностей. Крім того, у такому списку може відбуватися оновлення ймовірностей появи сценаріїв атак за рахунок убудованого в систему обчислення причин [11, 16].

Що стосується переваг цього методу, то варто зазначити, що для одного запису аудиту є можливість мінімізувати кількість обробок, тобто більш явні події спочатку спостерігаються пасивно, а далі відбувається їхнє уточнення у разі підозри на загрозу. Також важливим моментом є те, що присутня незалежність у поданні даних аудиту в певній формі, і ця можливість забезпечується планувальником.

Відносно недоліків указаного методу, звичайно необхідно розробнику формувати точні кількісні характеристики для різних частин графічного представлення моделі, і це є суттєве додаткове навантаження. Зауважимо, що безумовно цей підхід тільки доповнює підсистему виявлення аномалій, а не змінює її. Крім того, не існує програмного прототипу, який би демонстрував ефективність цього підходу.

4. ВИСНОВКИ

Сучасні системи виявлення та запобігання вторгнень мають дві групи недоліків, а саме: недоліки, які пов’язані зі структурою систем, і недоліки, які пов’язані реалізованим методом виявлення вторгнень.

Що стосується недоліків, які пов’язані зі структурою системи виявлення вторгнень та запобігання їм, то можна зазначити деякі з них:

- загальна методологія побудови відсутня [26];
- прив’язка до конкретного обладнання систем IDS;
- складність установки IDS;
- складність оновлення IDS новими технологіями виявлення;
- виявлення методами системи зрозумілих атак може призводити до ряду незадовільних наслідків;
- оцінювання продуктивності в реальних умовах для IDS є складною задачею.

Також можна зазначити недоліки методів виявлення, які є в системах виявлення вторгнень та запобігання їм:

- наявність пропусків атак і помилкових спрацьовувань;
- складності в ідентифікації атакуючого та цілей атаки;
- складність виявлення вторгнень у реальному часі;
- складності у виявленні нових атак;
- низький рівень виявлення вторгнень на початкових етапах;
- відсутність критеріїв ефективності результатів роботи;
- відсутність можливості виявляти вже відомі атаки з модифікованими або новими стратегіями;
- складність в автоматичному виявленні координованих складних атак;
- перевантаження системи.

Отже можна дійти висновку, що для вдосконалення систем IDS необхідно акцентувати увагу на напрямках, які пов’язані з використанням методів теорії аналізу та синтезу інформаційних систем та апарату теорії розпізнавання образів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] J. Allen, A. Christie, W. Fithen, J. McHuge, J. Pickel, E. Stoner, "State of Practice of intrusion detection technologies", Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute, 2000.

[2] Amrit Pal Singh, Manik Deep Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System", India: Computer Network and Information Security, Vol. 8. pp.41–47, 2014.

[3] R. Heady, G. Luger, A. Maccabe, M. Servilla, "The Architecture of a Network Level Intrusion Detection System", Technical report, Department of computer since, University of New Mexico, August 1990.

[4] B. Balajinath, S. Raghavan "Intrusion detection through learning behavior model", Computer Communications, vol. 24, no. 12, pp. 1202–1212, 2001.

[5] H. Debar, M. Becker, D. Siboni. "A neural network component for intrusion detection systems", In proceeding of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 240–250, Oakland, CA, USA, May 1992.

[6] K. Cheng. "An Inductive engine for the Acquisition of temporal knowledge", Ph. D. Thesis, Department of computer science, university of Illinois at Urbana-Champain 1988.

[7] P. Porras, P. Neumann, "EMERLAND: Event Monitoring Enabling Response to Anomalous Live Disturbance", Proceeding of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1997.

[8] K. Ilgun, R. Kemmerer, P. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection System", IEEE Trans. Software Eng. vol. 21, no. 3, Mar. 1995.

[9] K. Ilgun, "USTAT: A Real-time Intrusion Detection System for UNIX", Proceeding of the IEEE Symposium on Research in Security and Privacy.

[10] T. Heberlein, G Dias, K. Levitt, B. Mukherjee, J. Wood. "A network security monitor", In Proceeding of the 1990 IEEE Symposium on Research in Security and Privacy, pp. 296–304.

[11] T. Garvey, T. Lunt, "Model-based Intrusion Detection", Proceeding of the 14 th Nation computer security conference, Baltimore, MD, October 1991.

[12] S. Toliupa, I. Parkhomenko "The development of a process planning model of rational modular composition of the information protection systems" 2016 3rd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2016 – Proceedings, 2017, pp. 159–162, 7905367

[13] Z. Bankovic, D. Stepanovich, S. Bojanic, O. Nieto-Taladris, "Improving network security using genetic algorithm approach", Computers and Electrical Engineering, vol. 33, no. 5-6, pp. 438–451, 2007.

[14] S. Toliupa, M. Brailovskyi, and I. Parkhomenko, "Building intrusion detection systems based on the basis of methods of intellectual analysis of data", IAPGOS, vol. 8, no. 4, pp. 28-31, Dec. 2018.

[15] Z. Bankovic "Improving network security using genetic algorithm approach", Computers and Electrical Engineering, vol. 33, no. 5-6., pp. 438–451, 2007.

[16] J. Anderson, "Computer Security Threat Monitoring and Surveillance", Developer Works, IBM, 19 Mart 2013

[17] A. Tajbakhsh, M. Rahmati, A. Mirzaei, "Intrusion detection using fuzzy association rules", Applied Soft Computing, vol. 9, no. 2, pp.462–469, 2009.

Стаття надійшла до редколегії 15.05.2021

Intrusion detection methods in modern IDS systems

Currently, the problem of protection of information and communication systems and resources of cyberspace is acute. The rapid development of the information sphere also leads to the modernization and complexity of methods of attacking cyberspace objects. The statistics of successful attacks on computer systems of various organizations, including government agencies, are growing every year. From this we can conclude that even the most reliable protection systems do not give a 100% guarantee of protection. One of the possible reasons for this state of affairs may be the use of standard security mechanisms and methods by most security systems. Such mechanisms include access delimitation based on the rights of the access subject, encryption and identification and authentication. Traditional methods cannot protect against their own users who have criminal intent. In addition, this approach does not solve the problem of clear division of existing system entities for authorized use of globalized resources, the ability to select passwords using specialized software, and the problem of limiting access to information system resources, which can result in reduced performance and complexity passing transactions between components of this system. Thus, there is a need to use mechanisms that would not reject the advantages of traditional ones, but also complement them. Namely, that these mechanisms detect attempts at unauthorized, unauthorized access, provide information about these attempts, and also be able to respond. One of the key factors in the use of such protection systems is their ability to prevent attacks by attackers who have been authenticated and authorized in accordance with all procedures and access rules and have obtained the necessary rights to certain actions. Of course, it is impossible to predict a complete set of event scenarios in a system with an authorized user who has malicious intent, but it is necessary to make a detailed description of possible "malicious" scenarios, or go back and describe the so-called "normal" scenarios. The description of normal scenarios will make it possible to detect dangerous activity, because this activity will deviate from the so-called "normal" scenario of behavior in the system, even by an authorized user. Thus, exploring the possibility of using mechanisms that are aimed at detecting anomalies in the system, or to search for abuses can help implement effective solutions for intrusion detection and prevention systems.

Keywords: *startup, cyberspace, cybersecurity projects, information technology, risks, IT products, fuzzy sets.*

Наталія Лукова-Чуйко,
доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Natalia Lukova-Chuiko,
Doctor of Technical Sciences, Professor, Head of the Department of Cybersecurity and Information Protection of the Kyiv National Taras Shevchenko University.

Сергій Толюпа,
доктор технічних наук, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Serhii Toliupa,
Doctor of Technical Sciences, Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

Іван Пархоменко,
кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Ivan Parkhomenko,
Candidate of Technical Sciences, Associate Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

UDC 621.391
DOI https://doi.org/10.17721/ISTS.2021.1.25-34

R. S. Odarchenko, orcid.org/0000-0002-7130-1375, **odarchenko@ukr.net**
National Aviation University, Kyiv, Ukraine,
S. Y. Dakov, orcid.org/0000-0001-9413-3709, **dacov@ukr.net**
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
L. V. Dakova, orcid.org/0000-0001-6104-8217, **dacova@ukr.net**
State University of Telecommunications, Kyiv, Ukraine

RESEARCH OF CYBER SECURITY MECHANISMS IN MODERN 5G CELLULAR NETWORKS

The main feature of the 5G network is Network slicing. This concept enables network resource efficiency, deployment flexibility, and support for rapid growth in over the top (OTT) applications and services. Network Slicing involves splitting the 5G physical architecture into multiple virtual networks or layers. Each network layer (slice) includes control layer functions, user traffic level functions, and a radio access network.

Slice isolation is an important requirement that allows the basic concept of Network slicing to be applied to the simultaneous coexistence of multiple fragments in a single infrastructure. This property is achieved by the fact that the performance of each slice should not affect the performance of the other. The architecture of network fragments expands in two main aspects: slice protection (cyber attacks or malfunctions affect only the target slice and have a limited impact on the life cycle of other existing ones) and slice privacy (private information about each slice, such as user statistics) does not exchange between other slices).

In 5G, the interaction of the user's equipment with the data networks is established using PDU sessions. Multiple PDU sessions can be active at the same time to connect to different networks. In this case, different sessions can be created using different network functions following the concept of Network Slicing.

The concept of "network architecture", which is developed on hardware solutions, is losing its relevance. It will be more appropriate to call 5G a system, or a platform because it is implemented using software solutions.

5G functions are implemented in VNF virtual software functions running in the network virtualization infrastructure, which, in turn, is implemented in the physical infrastructure of data centers, based on standard commercial COTS equipment, which includes only three types of standard devices - server, switch and a storage system.

For the correct operation of a network, it is necessary to provide constant monitoring of parameters which are described above. Monitoring is a specially organized, periodic observation of the state of objects, phenomena, processes for their assessment, control, or forecasting. The monitoring system collects and processes information that can be used to improve the work process, as well as to inform about the presence of deviations.

There is a lot of network monitoring software available today, but given that 5G is implemented on virtual elements, it is advisable to use the System Center Operations Manager component to monitor network settings and performance and to resolve deviations on time.

The Operations Manager reports which objects are out of order sends alerts when problems are detected and provides information to help determine the cause of the problem and possible solutions.

So, for the 5G network, it is extremely important to constantly monitor its parameters for the timely elimination of deviations, as it can impair the performance and interaction of smart devices, as well as the quality of communication and services provided. System Center Operations Manager provides many opportunities for this.

The purpose and objectives of the work. The work aims to analyze the main mechanisms of cybersecurity in 5G cellular networks.

Keywords: *5G; network; monitoring; virtual software.*

1. INTRODUCTION

The modern world is impossible to imagine without the Internet, smartphones, and other gadgets that have become an integral part of our lives. With the development of information technology, the needs of users are growing rapidly, which cannot always meet the 4th generation mobile networks. That is why it is necessary to develop and implement a 5G network.

5G will allow the active development of IoT technologies, which will ensure the emergence of smart cities, smart vehicles, and other IoT technologies. Base stations will be able to communicate with objects that move at high speeds, up to 500 km / h.

5G is a qualitative development of technologies, not just an increase in network bandwidth. Enhanced security, increased connection stability, increased number of devices connected to the network at the same time, the ability to work with IoT in real-time - these are the opportunities that can provide 5G.

In general, the 5G network absorbs not only mobile but also fixed communication services, high-speed low-speed Internet access, and specialized corporate networks for industries.

The 5G network platform provides operators with significant benefits, primarily in terms of functionality, increased network bandwidth, and increased user satisfaction.

5G network security features

The security concept of mobile communication networks of the fifth generation is based on the reuse of the corresponding technologies adopted in the 4G-LTE standard [26]. Figure 1 shows the general architecture for building the core of a 5G network. Functional objects that implement security mechanisms are highlighted in dark color [27]:

Security Anchor Function (SEAF) - security anchor function.

Authentication Server Function (AUSF) is an authentication server function.

Authentication Credential Repository and Processing Function (ARPF) is a function of storing and processing authentication credentials.

Security Context Management Function (SCMF) is a security context management function.

Security Policy Control Function (SPCF) is a security policy management function.

Subscription Identifier De-concealing Function (SIDF) - a function to retrieve user ID Fig. 1.

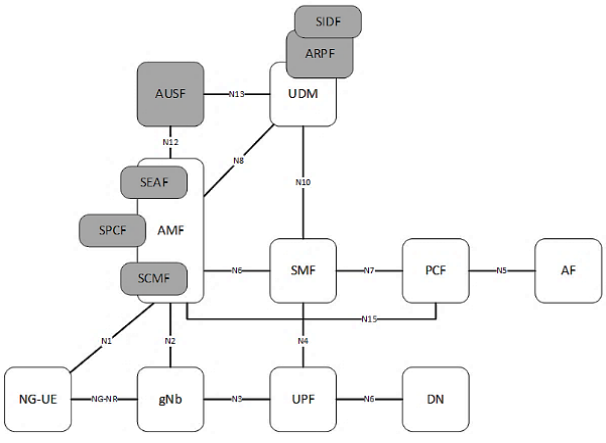


Fig. 1. 5G backbone architecture

During the first phase, the SEAF, SCMF, and SPCF are expected to be combined with the Access and Mobility Management (AMF) module of the ARPF and SIDF with the Unified Database (UDM).

Safety anchor function (SEAF). In cooperation with the AUSF, it provides authentication of the user of the terminal (UE) upon registration in the network (attach) for any access technology.

Authentication function (AUSF.). Acts as an authentication server, terminating requests from SEAF and translating them into ARPF. Can be combined with the Authentication Credentials Repository (ARPF).

Authentication Credential Repository (ARPF). Provides storage of personal secret keys (KI) and parameters of cryptographic algorithms, as well as generation of authentication vectors following 5G-AKA or EAP-AKA algorithms. It is in a home network protected from external physical influences of the data center and, as a rule, is integrated with a unified database (UDM).

Security Context Management Function (SCMF). Provides 5G security context lifecycle management.

Security Policy Management Module (SPCF). Ensures the negotiation and enforcement of security policies for specific user terminals (UE). This considers network capabilities, UE capabilities, and specific service requirements. Application of security policies includes a selection of AUSF, selection of authentication algorithm, selection of data encryption and integrity control algorithms, determination of the length and life cycle of keys.

User ID Delete Function (SIDF). Provides extraction of the permanent subscriber subscription identifier (5G SUPI) from the hidden identifier (SUCI) obtained as part of the "Auth Info Req" authentication procedure request.

Overall, the 5G network security concept includes:

User authentication from the network.

User side authentication of the network.

Negotiation of cryptographic keys between the network and the user terminal.

RRC signaling traffic encryption and integrity control (between UE and gNb).

Encryption and integrity control of signaling traffic at the NAS layer (between UE and AMF).

Encryption and integrity control of user traffic (between UE and gNb).

User ID protection.

Protection of interfaces between different network elements following the concept of a network security domain described in the recommendation 3GPP TS 33.310, incl. protection of interfaces N2, N3, and Xn.

Isolating the different layers of the Network slicing architecture and defining its security levels for each layer.

Protection of signaling and user traffic between 4G-LTE eNb and 5G gNb in the "Option 3" 4G to 5G migration scenario, including cryptographic key negotiation, encryption, and integrity control.

User authentication and traffic protection at the end service level (IMS, V2X – Vehicle to Everything, IoT).

Authentication and Key Agreement Procedure

The purpose of the Authentication and Key Agreement (AKA) procedure is to perform mutual authentication between the user terminal and the network, as well as generate the security function key KSEAF (see Fig. 2). Once generated, the KSEAF key can be used to form several security contexts, incl. for 3GPP and non-3GPP access.

Release 15 3GPP defines two mandatory methods for authentication and key agreement - EPS-AKA "and 5G-AKA, which will be discussed below.

Within both methods, a derivation function (KDF) is called, which, based on the control character string, converts the cryptographic key. The control character string may include the name of the serving subscriber of the guest network (Serving Network Name - SN-name). In particular, SN-name is used when calculating:

- security function key KSEAF;
- Authentication revocation (RES * XRES *)
- intermediate keys CK "and IK".

The SN-name is constructed by combining a service code (service code = "5G") and a guest network identifier, user authentication (network identifier or SN Id). SN Id is calculated based on Mobile Country Code (MCC) and Mobile Network Code (MNC) – see Fig. 2.

	7	6	5	4	3	2	1	0
1	MCC digit 2				MCC digit 1			
2	MNC digit 3				MCC digit 3			
3	MNC digit 2				MNC digit 1			

Fig. 2. Network identifier or SN Id

Using the name of the serving network (SN-name) allows you to unambiguously bind the results of cryptographic algorithms in a specific guest network.

Initiation and selection of authentication method

In accordance with the operator's security policy, SEAF can initiate user authentication of the terminal (UE) in any procedure involving the establishment of a signaling connection with the UE, for example, when registering with the network (attach) or updating the tracking area (tracking area update). To "go on the air", the UE must use either the hidden SUCI code (when first registering with the network) or 5G-GUTI (otherwise).

To authenticate the terminal user, SEAF uses a previously created and not yet used authentication vector, or sends an "Authentication Initiation Request" (5G-AIR) to the AUSF, setting the user ID to SUCI (upon initial registration in the network) or SUPI (upon receipt from the UE valid 5G-GUTI). The authentication request (5G-AIR), in addition to the user ID, must also include the access type (3GPP or non-3GPP), as well as the serving network name (SN-name).

Next, the AUSF verifies the legality of using the serving network name (SN-name) and, upon successful verification, translates the received request to the unified database (UDM) block, where (if necessary) the user identifier retrieval functional module (SIDF) decrypts the hidden user identifier (SUCI), after which the Authentication Credential Repository (ARPF) selects the appropriate authentication algorithm - 5G-AKA, or EAP-AKA. "

EAP-AKA Authentication Method '

The EAP-AKA authentication method is a further development of the EAP-AKA and introduces a new derivation function that binds cryptographic keys to the access network name. The "EAP-AKA" method described in RFC 5448 is triggered by UDM / ARPF when it receives a user authentication request from AUSF (Authentication Information Request - Auth Info-Req message) Fig. 3 shows a diagram including the following steps.

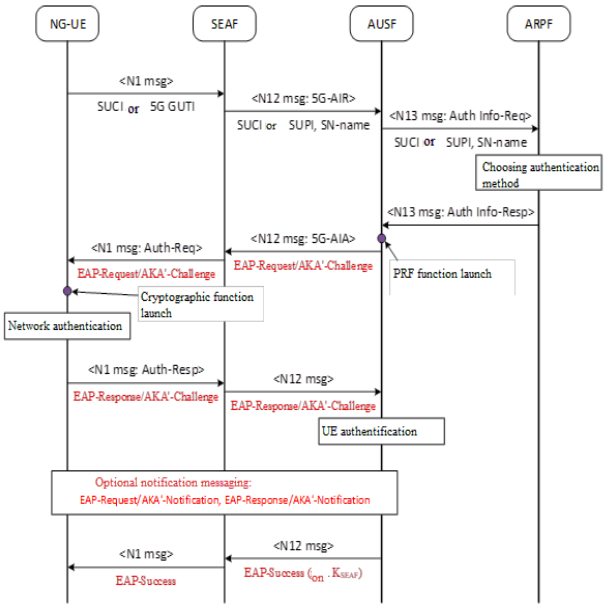


Fig. 3. EPS-AKA Authentication Method

The user credential storage and processing module (UDM / ARPF) generates an authentication vector including RAND, AUTN, XRES, CK, IK. To calculate the authentication vector, five one-way functions f1-f5 are used, implemented based on the MILEAGE block cipher (following 3GPP TS 33.102 – see Fig. 4) with the AMF bit set to "1". When calculating f1-f5, a 128-bit operator-variant algorithm configuration field (OP) is used. OP allows you to make a unique (secret) implementation of the algorithm for each operator. The OP value (or OPC, calculated from OP and KI via the block cipher function) must be stored in the ARPF and on the user's USIM.

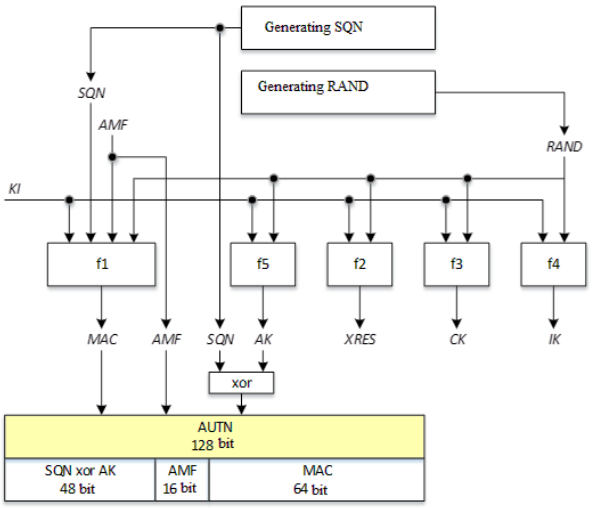


Fig. 4. Authentication vector

2. UDM / ARPF using the derivation function and using the service network name (SN-name) calculates the "bound" value CK ", IK 'and transmits the vector (RAND, AUTN, XRES, CK", IK') of the authentication server (AUSF) from which the request was received.

3. AUSF launches the cryptographic function PRF of the EAP-AKA method "described in RFC5448. The input parameters of the function are the keys CK" and IK ", as well as the name of the serving network (SN-name). The following fields are obtained at the output of the function:

- K_encr – key (128 bit) used to encrypt individual attributes of EAP-AKA messages "(in accordance with the operator's security policy);
- K_aut – key (256 bit) used to calculate the message integrity control codes EAP-AKA "(MAC - Message Authentication Code)
- K_re – key (256 bits) used for re-authentication;
- MSK (Master Session Key) – master key (512 bit)
- EMSK (Extended Master Session Key) – extended master key (512 bits).

4. The AUSF sends an EAP-Request / AKA'-Challenge to the Security Anchor Function (SEAF), which is then transparently broadcast to the terminal user in the NAS message. EAP-Request / AKA'-Challenge contains the following attributes:

- AT_RAND (random number)
- AT_AUTN (authentication token)
- AT_KDF (identifier of the used derivation function, where 1 corresponds to using the default derivation function)
- AT_KDF_INPUT (serving network name – SN-name)
- AT_MAC (Message Authentication Code).

5. User terminal:

- calculates the value of XMAC, RES, CK "and IK
- starts the cryptographic function PRF of the EAP-AKA algorithm "(similar to the function performed by the authentication server)
- checks the correctness of the message integrity control code (AT_MAC attribute)
- checks if the AMF bit of the AT_AUTN attribute is set to "1";
- performs network authentication by comparing the calculated and received AUTN values;
- sends an EAP-Response / AKA'-Challenge with the attributes AT_RES and AT_MAC to the security anchor function (SEAF), which is then transparently broadcast by the authentication server (AUSF).

6. AUSF validates the message integrity check code (AT_MAC attribute) and authenticates the terminal user by comparing the RES and XRES values received from the UE and ARPF / UDM, respectively.

7. If successful, the AUSF sends an EAP-Success Feedback to the UE via the Security Anchor Function (SEAF). If the operator's security policy provides for the transmission of an encrypted EAP-Success – "protected successful result indications", notification messages are first exchanged. Also (if necessary), through the SIDF function call, the hidden identifier (SUCI) decryption and 5G SUPI extraction are performed.

8. At the final stage, ARPF / UDM generates an authentication function key KAUSF, which is used as the first 256 bits of the extended master key (EMSK). Further, based on KAUSF, encryption and integrity control keys are calculated according to the hierarchy of cryptographic keys shown in Fig. 7.

2. 5G-AKA AUTHENTICATION METHOD

The 5G-AKA authentication method is a further development of the EPS-AKA described in 3GPP TS 33.401 and is applied on 4G-LTE networks. The 5G-AKA method is triggered by UDM / ARPF when it

receives a user authentication request from AUSF (Authentication Information Request message – Auth Info-Req). In fig. 6 is a diagram that includes such steps.

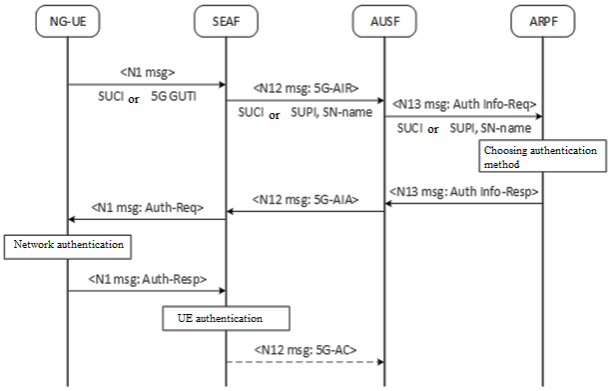


Fig. 5. 5G-AKA Authentication Method

1. By analogy with the EAP-AKA algorithm "the user credentials repository and processing module (UDM / ARPF), based on the MILENAGE block cipher, generates an authentication vector that includes RAND, AUTN, XRES, CK, IK (the AMF bit must be set to unit).

2. UDM / ARPF using the derivation function and using the serving network name (SN-name) calculates:

- the value of the expected response XRES * is bound
- the key value of the authentication function KAUSF,
- generates the vector "5G not the AV" (Home Environment Authentication Vector), including RAND, AUTN, XRES * KAUSF and sends it to the authentication server (AUSF).

3. AUSF calculates:

- the HXRES * value, which is a hash truncated to 128 bits from the concatenation of the expected XRES * authentication response and a random number RAND: HXRES * num lower 128 bits from SHA-256 [RAND || XRES *];
- the value of the key of the security function KSEAF.

The AUSF then generates 5G AV (5G Authentication Vector) including RAND, AUTN, HXRES * KSEAF and sends it to the Security Anchor Function (SEAF) using a 5G-AIA (Authentication Initiation Answer) message. If the authentication request (5G-AIR) contained a hidden user code (SUCI), the AUSF receives the 5G SUPI through the SIDF function call and adds it to the 5G-AIA.

4. SEAF monitors the received vector lifetime timer and sends an Auth-Req message to the NAS terminal user with the RAND and AUTN parameters enabled.

5. User terminal:

- calculates the value of RES, AUTN, CK, IK by calling the corresponding functions of the USIM module;
- performs network authentication by comparing the calculated and received AUTN values;
- calculates the values of the keys KAUSF and KSEAF;
- computes the bound values of the RES * authentication response;
- sends an Auth-Resp message containing RES * to the safety anchor function (SEAF).

6. SEAF calculates the hash HRES * (similar to AUSF) and authenticates the terminal user by comparing HRES * and HXRES *.

7. Upon successful authentication, SEAF sends a 5G-AC (Authentication Confirmation) message to the AUSF, including the RES * response values received from the UE. This step is optional and may not be used when registering a user on a home network.

8. AUSF checks the lifetime timer of the authentication vector, compares the value of the calculated (XRES *) and received (RES *) feedback, and then completes the authentication procedure.

3GPP recommends that only one vector be generated and used per authentication procedure. This will allow a confirmation message to complete each authentication procedure.

Hierarchy of cryptographic keys

The following are the keys, variables, and cryptographic functions that are used in 5G security procedures:

1. The user's secret key KI – 128 (or 256) bits. Stored in read-protected ARPF and USIM memory of the module.

2. Random number RAND (RANDom challenge) – 128 bits;

3. Rejection of authentication RES (authentication RESponse) – 128 bits. Generated by a user terminal (UE) and used in the UE's network authentication procedure.

4. The expected revocation of XRES authentication (eXpected RESponse) is 128 bits. An ARPF is generated and used in a terminal (UE) user authentication procedure by the network.

5. Pegged Authentication Revocation (pending authentication revocation) (X) RES * – 128 bits. Represents (X) RES modified by the derivation function.

6. Shortened hash of the bound (expected bound) authentication response and the random number H (X) RES * – 128 bits.

7. Sequence number SQN (SeQuence Numbers) – 48 bits.

8. Anonymous key AK (Anonymity Key) – 48 bits. Used to protect the sequence number (SQN).

9. AMF (Authentication Management Field) – 16 bits. Specifies the type of authentication vector generated by ARPF (UMTS or EPS / 5G).

10. Message Authentication Code (MAC) – 64 bits. An ARPF is generated and used in the UE's network authentication procedure.

11. The expected eXpected Message Authentication Code (XMAC) is 64 bits. Generated by a user terminal (UE) and used in the UE's network authentication procedure.

12. Authentication token AUTN (authentication token) – 128 bits. Includes an Authentication Message Code (expected Authentication Message Code) – (X) MAC and an Authentication Control Field (AMF).

13. Keys CK (Cipher Key) and IK (Key Integrity) – 128 bits each. They are located at the top of the tree of the hierarchy of cryptographic keys and underlie the calculation of encryption keys and control the integrity of signaling and user traffic.

14. Is the second ancestor of the KAUSF authentication function key.

15. Key for authentication function KAUSF.

16. Security function key KSEAF.

17. KAMF access and mobility management function key. When performing a handover with changing the access and mobility control module to the target Fig. 6.

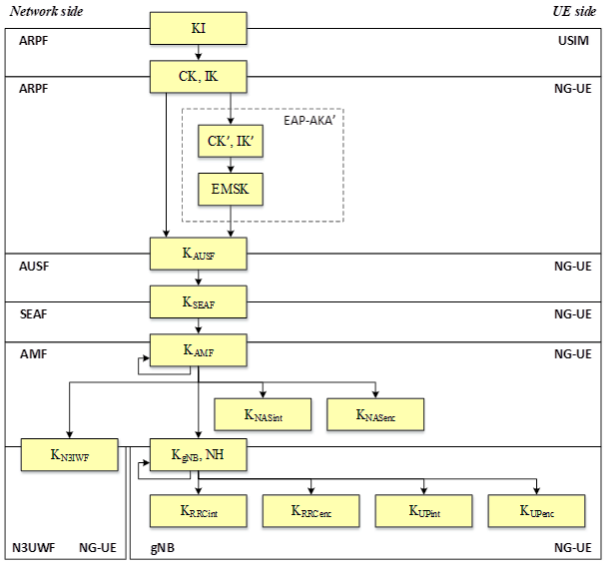


Fig. 6. Key hierarchy

Security contexts

One of the fundamental concepts of traffic protection in 5G networks is the concept of a security context (5G security context) – a block of information that includes keys, parameters, variables that ensure the functioning of encryption and data integrity control mechanisms. Symmetric copies of the "5G security context" are stored in the user terminal and on the network elements. 3GPP defines three types of "5G security context":

- "full native" – a context created within the 5G authentication and key agreement (EAP-AKA "or 5G-AKA) for which NAS traffic security mechanisms (NAS-SMC) were successfully activated
- "partial native" – a security context created within the 5G authentication and key agreement (EAP-AKA "or 5G-AKA) for which the NAS traffic security mechanisms (NAS-SMC) have not yet been activated.
- "mapped" – a security context created when a user transitions from a network of one communication standard to a network of another, by converting UMTS (or EPS) keys into a 5G key.

The security context can be in one of two possible states – "current" – the current (last activated security context) and "non-current". The "current" state can be a context of the "full native" or "mapped" type, the "non-current" state – "fully native" or "partial native". At the same time, in the "non-current" state, the context has no 5G AS data.

The 5G security context includes the following sections:

1) 5G NAS security context – parameters and variables to ensure the security of NAS alarm, including:

- the key of the KAMF access and mobility management function,
- a list of NAS security algorithms supported by the user terminal (UE),
- identifiers of selected algorithms for NAS encryption and integrity control,
- the value of NAS COUNT counters for downstream and upstream traffic,
- keys for NAS encryption and KNASint and KNASenc integrity control.

2) 5G AS security context – parameters and variables to ensure the security of RRC signaling and user traffic, including:

- base station key KgNB,
- a list of security AS algorithms supported by the user terminal (UE),
- identifiers of selected algorithms for RRC / UP encryption and integrity control,
- the value of the RRC / COUNT UP counters for downstream and upstream traffic,
- key for RRC / UP encryption and integrity control KRRCint, KRRCenc, KUPint, KUPenc,
- NH (Next Hop parameter) and NCC (Next Hop Chaining Counter parameter) parameters are used for key derivation.

3) 5G AS security context for non-3GPP access - parameters and variables to ensure user security and signaling traffic for non-3GPP access (Wi-Fi, etc.).

The mechanisms for using this context are not defined at the time of this writing.

When the user turns off the terminal, the AMF and UE store copies of the current NAS security context (current 5G NAS security context) and all unused authentication vectors, which allows the next time the terminal is turned on, on the one hand, to minimize its registration time, on the other hand, to ensure the required level of security. On the UE side, a copy of the current security context can be stored either by the USIM (if the module contains the appropriate files for storing the network connection parameters) or in the non-volatile memory of the UE.

Securing NAS Traffic

Securing NAS traffic includes encryption parameters and integrity control of NAS signaling messages transmitted between the user terminal (UE) and the access and mobility control module (AMF) via the N1 interface (see Fig. 1).

Security mechanisms for NAS traffic are activated as part of the NAS Security Mode Command - NAS-SMC procedure (see Fig. 10). The choice of encryption and integrity control algorithms is performed by AMF based on the priorities set by the operator, as well as following the priorities received from the UE security capabilities. If the user terminal (UE) does not have an up-to-date security context, then the primary NAS message should be sent in an open (unencrypted form and contain only the user ID and "security capabilities". In this case, the integrity of the NAS messages signaling is provided starting with "NAS Security Mode Command encryption – with" NAS Security Mode Complete. "If the UE has an up-to-date security context, then the attributes of the primary NAS message MUST be encrypted except for the already mentioned user ID and" security capabilities ".

Using a man-in-the-middle attack, an attacker can change the value of the "security capabilities" field of the primary unsecured NAS message and thereby reduce the security level of the NAS conversation as a whole. To detect this, the AMF sends a copy of "security capabilities" to the UE and has integrity protection to the "NAS Security Mode Command", allowing the UE to detect an attack. For the same purpose, the AMF, by setting the Request Initial Message Flag, may invite the UE to send a copy of the primary NAS message as part of the NAS Security Mode Complete secure revocation.

Securing AS Traffic

Securing AS traffic includes parameter encryption and integrity control of RRC signaling messages, as well as user data packets transmitted between the UE and the base station (gNb) via the NG-NR interface (Fig. 7).

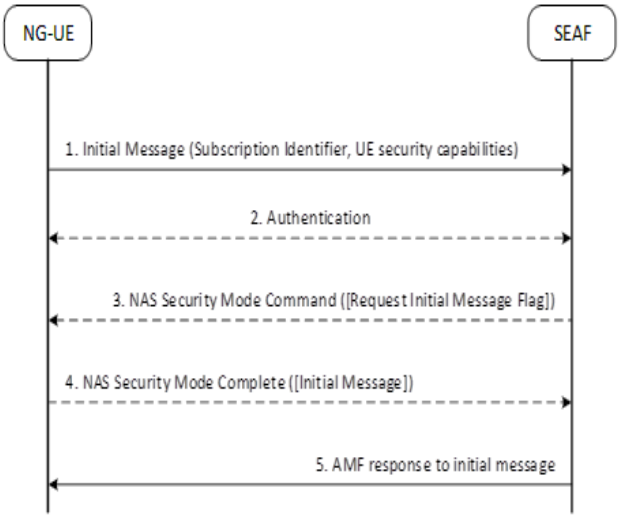


Fig. 7. NAS Security Mode Command Procedure

The activation of security mechanisms for AS traffic is carried out as part of the AS Security Mode Command (AS-CMS) procedure, which includes the exchange of AS Security Mode Command and AS Security Mode Complete messages (the integrity of these messages must be protected). The choice of encryption and integrity control algorithms is performed by gNb based on the priorities set by the operator, as well as following the security capabilities received from the UE.

Integrity control is provided starting from the RRC message "AS Security Mode Command", encryption – from the "AS Security Mode Complete".

When the handover is performed, the source base station transmits encryption and integrity control algorithms and capabilities for the terminal user in the handover request message to the target base station. Based on the received data, the target gNb, on the one hand, can read the "RRCReestablishmentComplete" message from the UE, and on the other hand, can select and broadcast new algorithms to the UE.

As part of the handover procedure, a new KgNB * key is generated at the target base station. The key is generated either on the basis of the pre-key KgNB (horizontal derivation) or on the basis of NH (vertical derivation). This mechanism is called "AS key refresh" in 3GPP terminology.

3. USER IDs

Many identifiers have been defined for 5G users, detailed in 3GPP TS 23.003. Below is a brief description of them:

1. International permanent subscriber subscription identifier – 5G SUPI (Subscription Permanent Identifier). Assigned to each subscriber of the 5G network and stored in the unified UDM and USIM database of

user modules. The SUPI identifier can be an international mobile subscriber identifier - IMSI (International Mobile Subscriber Identity), or a network access identifier – NAI (Network Access Identifier), the format of which is defined by RFC 4282.

2. Hidden user identifier – SUCI (Subscription Concealed Identifier). It is an encrypted copy of the international permanent subscriber subscription identifier (5G SUPI) and avoids the transmission of 5G SUPI over the network in the clear, even when the terminal user is initially registered in the network (Initial attach).

SUPI is protected using an Elliptic Curve Integrated Encryption Scheme (ECIES). The public key used for SUPI encryption must be stored in the secure memory of the USIM card; the private key is in the User ID Withdrawal Functional (SIDF). In this case, the SUPI part containing the mobile country code (MCC) and mobile network code (MNC) and is used for routing signaling traffic is not encrypted. 3GPP allows SUPI encryption in the user terminal (default option) and USIM modules. The operator's network and user terminal must also support the so-called null-scheme, in which the public user ID is not protected.

The 5G Globally Unique Temporary Identifier (5G Globally Unique Temporary Identifier) is assigned by the Access and Mobility Management (AMF) module regardless of the type of access network (3GPP, non-3GPP). When "going on the air", the user terminal must use exactly 5G-GUTI (except for initial registration in the network – initial attach, as well as in other cases when there is no valid 5G-GUTI) The 5G-GUTI format is shown in Fig. 8.

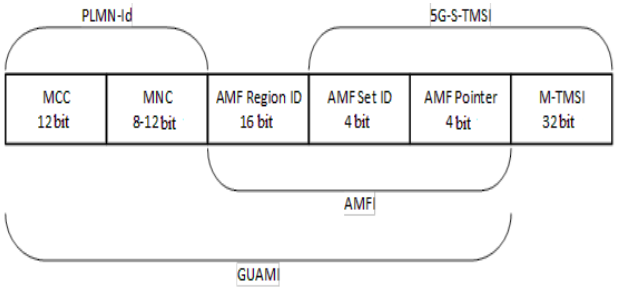


Fig. 8. 5G-GUTI structure

here:

- GUAMI (Globally Unique AMF Identifier) - global (international) identifier of the AMF access and mobility control module;
- MCC - mobile country code;
- MNC - mobile network code;
- AMF Region ID – identifier of the region served by the AMF module;
- AMF Set ID – unique identifier of the group of AMF modules within the region;
- AMF Pointer – unique identifier of the AMF module within the AMF Set ID group;
- AMFI – unique (within the network) AMF identifier;
- 5G-TMSI (5G Temporary Mobile Subscription Identifier) – a temporary identifier of a 5G mobile subscriber (unique within AMF)
- 5G-S-TMSI – unique (within the region) temporary identifier of a 5G mobile subscriber.

4. CONCLUSION

Explained to the public understanding of the "monitoring of the fancy". It is centrally organized, systematically changing over the camp of objects, appearances, processes with the mark of evaluating, monitoring or forecasting. Monitoring is a systematic collection and processing of information, as it can be used for polishing the process of taking decisions, as well as for informing loudness and or as a design tool for a star star link tool for measuring. In the Danish hour, the monitoring of the measurement will be added to the number of additional subsystems, for example:

- intrusion detection system – follow the emergence of threats (Intrusion detection system). The whole system, which displays fancy traffic on the subject of suspicion of activity and type of improvement, if such activity is detected. Other quality of service is provided by the administrator or selected centrally for additional systems and security and management of pods. The SIEM system integrates vyhodi with decilkoh dzherel and vikorista methods of filtering trivia, allowing you to identify the malicious activity of pompous trivia.

The intrusion memorization system is an excellent degree to enable the use of the Intrusion Prevention System. Bagato IPS can also react to the threat of a threat, if you do not allow it to be damaged. Smell the vicious methods of reacting, teach the IPS the attack itself, reduce the middle of the bezpeka or change the attack. The system for monitoring the productivity of the net (Network Performance Monitoring, NPM) is a rewiring of the attachment / channel. With the monitoring of the hedgehog, the vison is watching over the hedge in the jokes of the problems that are caused in the robots of the server systems, their attachments or the hedgehogs.

At the connection with the active, growing nature of the development of information technologies, the growth of the foldability of the scale of the systems and the net, in its turn, a special acceleration of the monitoring and forecasting of For such universities, it is not necessary to throw viruses of increased and

security, as well as toxicity.

Boolean view System Center Operations Manager (SCOM). The product of the building consoles information about the function of the new IT-infrastructure components, which is secured in the second consoles.

Vikoristannya Operational manager will lie behind a great number of computers, annexes, services and supplements. Console for dose management to reconsider the rate, productivity, availability of all advanced facilities in the middle, and

Agents view the dzherela on computers pick up the views according to the configuration that controls the server. When I change the status of the object or the visibility of other minds, the agent can change. Tse with the permission of the operator to know, if vimagим їхної respect. I will transfer the data about the status of the post-hosted object to the control server, the agent will send the picture of the pre-delivery status of the annex and all the data

Bulo is proponent of the option of the system and monitoring of parameters in the 5G grid. Merezhi of the fifth generation are implemented on virtual elements, also on the secondary SCOM component for controlling the parameters and correctness of the hedge and the time-consuming operation.

5G functions are implemented in virtual programmable VNF functions, which are implemented in the NFV infrastructure. In its own place, NFV is implemented in the physical infrastructure of the data center on the basis of the standard commercial property of COTS.

The 5G skin element is used for monitoring agents. A data modifier generates various data with preceding variable icons that trigger the actions that result from the action. Server for management of configuration and extended agencies on state-of-the-art computers. All agents send calls to the management server in the group. The cei server is used as the main control server of the agent.

A circuit has been installed in the maybutny can of the vikoristan for the control of parameters in the 5G mesh.cellular networks.

REFERENCES

[1] Tomas Hegr, Leos Bohac, Impact of Nodal Centrality Measures to Robustness in, Software-Defined Networking // Advances in Electrical and Electronic Engineering. 2014;12(4):252-259 DOI 10.15598/aeee.v12i4.1208

[2] R. S. Odarchenko, S. Yu. Dakov, V. V. Polischuk, A. M. Tyrsenko, Modeling of SDN Overlay Networks and Their Main Characteristics Research // Knowledge-based technologies № 3 (31), 2016 с. 284

[3] Odarchenko, R., Abakumova, A., Polihenko, O., Gnatyuk, S., Traffic offload improved method for 4G/5G mobile network operator // 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 – Proceedings 2018-April, pp. 1051-1054

[4] Hung LeHong, Jackie Fenn. Key Trends to Watch in Gartner. Emerging Technologies Hype Cycle / Hung LeHong, Jackie Fenn, 2012.

[5] Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

[6] Intrusion Prevention System (IPS) URL: https://www.geeksforgeeks.org/intrusion-prevention-system-ips/.

[7] Reporting Server URL: https://scom.fandom.com/wiki/Reporting_Server.

[8] Data Warehouse URL: https://scom.fandom.com/wiki/Data_WarehouseACS Database URL https://scom.fandom.com/wiki/ACS_Database.

[9] Operational Database URL: https://scom.fandom.com/wiki/Operational_Database.

[10] Operations Console URL https://scom.fandom.com/wiki/Operations_Console.

[11] Web Console URL https://scom.fandom.com/wiki/Web_Console.

Стаття надійшла до редколегії 11.05.2021

Дослідження механізмів кібербезпеки стільникової мережі 5G

Основною особливістю мережі 5G є розділення мережі. Ця концепція забезпечує ефективність використання мережних ресурсів, гнучкість розгортання та підтримку швидкого зростання топових (OTT) програм і служб. Зрізування мережі передбачає поділ фізичної архітектури 5G на кілька віртуальних мереж або шарів. Кожен мережний рівень (зріз) включає функції рівня керування, функції рівня трафіка користувача та мережу радіодоступу. Ізоляція фрагментів є важливою вимогою, яка дозволяє застосувати основну концепцію зрізу мережі до одночасного співіснування кількох фрагментів в одній інфраструктурі. Ця властивість досягається тим, що продуктивність кожного зрізу не повинна впливати на продуктивність іншого. Архітектура мережних фрагментів розширюється за такими основними аспектами: захист фрагментів (кібератаки або збої в роботі зачіпають лише цільовий фрагмент і мають обмежений вплив на життєвий цикл інших існуючих) і конфіденційність фрагмента (приватна інформація про кожен фрагмент, наприклад, користувача), статистика (не обмінюється з іншими фрагментами). У 5G взаємодія обладнання користувача з мережами передачі даних встановлюється за допомогою сеансів PDU. Декілька сеансів PDU можуть бути активними одночасно для підключення до різних мереж. У цьому випадку можна створити різні сеанси за допомогою різних мережних функцій відповідно до концепції Network Slicing. Поняття "архітектура мережі", яке розроблено на апаратних рішеннях, втрачає свою актуальність. 5G доцільніше буде називати системою, або платформою, оскільки вона реалізована за допомогою програмних рішень.Функції 5G реалізовані у віртуальних програмних функціях VNF, що працюють в інфраструктурі віртуалізації мережі, яка, у свою чергу, реалізована у фізичній інфраструктурі центрів обробки даних, на основі стандартного комерційного обладнання COTS, яке включає лише три типи стандартних пристроїв – сервер, комутатор і система зберігання.

Для правильної роботи мережі необхідно забезпечити постійний моніторинг параметрів, які описані вище. Моніторинг – це спеціально організоване періодичне спостереження за станом об'єктів, явищ, процесів для їх оцінювання, контролю чи прогнозування. Система моніторингу збирає та обробляє інформацію, яка може бути використана для покращення робочого процесу, а також для інформування про наявність відхилень. Сьогодні існує велика кількість програмного забезпечення для моніторингу мережі, але враховуючи те, що 5G реалізовано на віртуальних елементах, доцільно використовувати компонент System Center Operations Manager для моніторингу налаштувань і продуктивності мережі, а також для вчасного усунення відхилень. Менеджер операцій повідомляє, які об'єкти вийшли з ладу, надсилає сповіщення при виявленні проблем і надає інформацію, яка допоможе визначити причину проблеми та можливі рішення. Отже, для мережі 5G надзвичайно важливо постійно контролювати її параметри для своєчасного усунення відхилень, які можуть погіршити продуктивність і взаємодію розумних пристроїв, а також якість зв'язку та наданих послуг. System Center Operations Manager надає багато можливостей для цього. Мета цієї роботи – аналіз основних механізмів кібербезпеки в стільникових мережах 5G.

***Ключові слова**: 5G; мережа; моніторинг; віртуальне програмне забезпечення.*

Roman Odarchenko,
Doctor of Technical Sciences, Associate Professor. Head of the Department of Telecommunication and Radio Electronic Systems of the National Aviation University.

Роман Одарченко,
доктор технічних наук, доцент, завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету.

Serhii Dakov,
Candidate of Technical Sciences, Assistant Department Cybersecurity And Protection Information.
Taras Shevchenko National University of Kyiv.

Сергій Даков,
кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Larisa Dakova,
Candidate of Technical Sciences, Associate Professor of the Department of International Relations of the State University of Telecommunications.

Лариса Дакова,
кандидат технічних наук, доцент кафедри МВТ Державного університету телекомунікацій.

УДК 004.056
DOI https://doi.org/10.17721/ISTS.2021.1.35-43

О. А. Лаптєв, orcid.org/0000-0002-4194-402X,
alaptev64@ukr.net
С. О. Лаптєв, orcid.org/0000-0002-7291-1829,
salaptiev@gmail.com
Т. О. Лаптєва, orcid.org/0000-0002-5223-9078,
tetiana1986@ukr.net
Державний університет телекомунікацій, Київ, Україна

УДОСКОНАЛЕНИЙ МЕТОД ВИЗНАЧЕННЯ ВИПАДКОВИХ РАДІОСИГНАЛІВ ЗА ВІДХИЛЕННЯМ ГОЛОВНИХ ПАРАМЕТРІВ СИГНАЛІВ

Запропоновано вдосконалений метод визначення випадкових радіосигналів, які можуть бути сигналами засобів негласного отримання інформації. Новизна методу полягає у визначенні відхилення головних параметрів сигналів від заданих параметрів. Метод об'єднує методи визначення відхилення амплітуди від амплітуди сигналів засобів, що легально працюють у цьому радіодіапазоні, та метод визначення фаз випадкових сигналів. Сигнали засобів негласного отримання інформації визначають за середньоквадратичним відхиленням (дисперсією) амплітуд та фаз сигналів.

Для визначення засобів негласного отримання інформації пропонується на першому етапі визначати відхилення амплітуди від амплітуди сигналів легально працюючих пристроїв або від амплітуди сигналів файла "зразка", на другому етапі – визначати відхилення фаз сигналів. Таким чином, за двома параметрами відхилення амплітуди та фази можливо з великою ймовірністю визначати сигнали засобів негласного отримання інформації. Шляхом вимірювання параметрів сигналів легально працюючих пристроїв та використання цих параметрів, як параметрів файла "зразка", суттєво збільшується ймовірність визначення випадкових сигналів. Це досягається суттєвим скороченням часу за рахунок виключення відомих сигналів із додаткового програмного аналізу заданого радіодіапазону.

Для підтвердження запропонованого сукупного методу проведено моделювання методу визначення відхилення амплітуди та методу визначення фаз випадкових сигналів, які можливо і є сигналами засобів негласного отримання інформації. Отримано графічні матеріали, які цілком підтверджують можливість визначення сигналів засобів негласного отримання інформації запропонованим методом.

Ключові слова: *метод, порівняння, визначення сигналів, дисперсія, амплітуда, фаза, моделювання.*

1. ВСТУП

Особливістю теперішнього часу є перехід від індустріального суспільства до інформаційного, в якому інформація стає важливішим ресурсом, ніж матеріальні або енергетичні ресурси. Інформація стала найціннішим ресурсом у сучасному світі. Під її впливом наше життя змінюється щохвилини. Боротьба за інформаційні ресурси стала дуже запеклою. Інформація часто стає фактором великомасштабних конфліктів, трагедій і політичних маніпуляцій. Таким чином, існує потреба в забезпеченні конфіденційності, цілісності та надійності даних, що обробляються заради мирного та стабільного тихого життя.

Вартість інформації часто в сотні або тисячі разів перевищує вартість комп'ютерної системи, в якій вона зберігається. Технічна розвідка охоплює всі сфери ринкової економіки. Збиток від економічної розвідки становить сотні мільярдів доларів на рік. Наприклад у Німеччині збиток оцінюються у 50 млрд євро на рік, у США вже у 150 млрд доларів на рік. Згідно з дослідженнями зарубіжних фірм 76 % компаній і державних установ стикалися з промисловою розвідкою.

Тому питання інформаційної безпеки сьогодні як ніколи актуальне.

Витік інформації з технічного каналу означає неконтрольоване поширення інформації від носія інформації, який захищений, через фізичне середовище, до технічних засобів, які перехоплюють інформацію. Технічні засоби приймання та передачі інформації є засобами прихованого отримання інформації. Гарантоване виявлення і надійне розпізнавання сигналів цих інструментів – дуже важливе завдання.

Проблема полягає в тому, що важко відрізнити легальний пристрій, що працює за прямим призначенням, від пристрою для негласного отримання інформації, що робить методи виявлення засобів негласного отримання інформації актуальними.

1.1. АНАЛІЗ ЛІТЕРАТУРИ ТА ПОСТАНОВКА ЗАДАЧІ

Значну кількість публікацій присвячено питанням захисту інформації, пошуку і локалізації засобів негласного отримання інформації.

Так, у роботі [1] розглянуто питання пошуку засобів негласного отримання інформації за допомогою пошукових систем і допоміжних пристроїв. Однак для виявлення сигналів засобів негласного отримання інформації використовують, в основному, тільки принципи, викладені у програмному пакеті, і питання виокремлення сигналів для подальшого розпізнавання та ідентифікації не розглядається.

У [2, 4] описано методи пошуку засобів негласного отримання інформації з використанням пошукового обладнання (ручні методи) і пошукових систем (напівавтоматичні методи), а також пошук радіозакладки, за допомогою приладів для вимірювання відстані, до засобів негласного отримання інформації. Але ці методи [2, 4] не дозволяють показувати сам сигнал радіозакладки, пошук проводиться з урахуванням переважно практичного досвіду фахівця та техніко-акустичних характеристик обладнання.

У роботі [3] наведено методи виявлення сигналів засобів негласного отримання інформації та їхнє узагальнення, входження в базу даних із послідовними спектральними й іншими методами аналізу. Однак питання аналізу сигналів із метою поділу реальних і складних радіосигналів не піднімається. У результаті використовують значні математичні та технічні ресурси, що збільшує час пошуку небезпечних сигналів, які можуть бути сигналами засобів негласного отримання інформації.

У [5, 7] розглянуто методи спектрального аналізу, засновані на використанні математичних моделей для опису сигналу, але при їхньому використанні робиться припущення про поведінку сигналу поза інтервалом спостереження. Завдання спектрального аналізу або оцінки в цьому випадку – знайти параметри своєї моделі, яка вибирається на підставі наявної апріорної інформації про досліджуваний процес. Це метод спектрального аналізу, який використовує частину класичного методу Проні. Пропонується визначати не тільки статичні параметри, але і швидкість зміни цих параметрів. Швидкість зміни параметрів дозволяє більш точно визначати небезпечний радіосигнал передачі інформації. Але такий метод дуже складний і вимагає багато часу, що може не дозволити своєчасно виявити засоби негласного отримання інформації, які працюють в імпульсному режимі.

Математичне моделювання у [8] розглянуто на прикладі моделі конкретних параметрів. Але деякі параметри є імовірними, питання взаємозв'язку вхідних параметрів у разі моделювання процесів, глибини їхнього взаємозв'язку в моделі не розглядаються. Ці чинники взаємозв'язку і взаємодії можуть значно спотворити результати моделювання і поставити під сумнів адекватність моделі й отриманих результатів.

У [9] досліджено розрахунок основних параметрів випадкових сигналів методом, заснованим на математичній моделі диференціальних перетворень у межах теорії кореляції. Але немає чітко визначених параметрів для знаходження сигналів засобів негласного отримання інформації.

У роботах [10–13] проаналізовано складність сучасного радіомоніторингу в інтересах забезпечення виявлення радіосигналів засобів негласного отримання інформації. Проблема в тому, що сучасні закладні пристрої з передачею інформації по радіоканалу все частіше використовують ті ж стандарти передачі інформації, що і пристрої, які працюють у дозволених державою смугах частот, та розташовані у приміщеннях, де проводять пошукові роботи. Таким чином, старі методи радіомоніторингу не дозволяють ідентифікувати закладні пристрої, що працюють під виглядом пристроїв, що працюють легально. Необхідно розробити нові науково-методичні методи для пошуку прихованих засобів негласного отримання інформації, які працюють в дозволених державою смугах частот.

Перераховані вище фактори дозволяють зробити висновок про те, що на сучасному етапі розвитку суспільства процес пошуку небезпечних сигналів переходить на якісно інший рівень.

Проблема відмінності легального пристрою, що працює за прямим призначенням, від пристрою, що використовується для негласного отримання інформації, є складною, що свідчить про актуальність розроблення методів виявлення засобів негласного отримання інформації.

1.2. МЕТА СТАТТІ

У процесі захисту інформації виникає завдання виявлення критичних загроз витоку інформації. Засоби негласного отримання інформації – одна з найсерйозніших загроз витоку інформації. Надійне виявлення прихованих засобів отримання інформації є дуже складним завданням. Тому і питання розроблення нових методів і способів виявлення засобів негласного отримання інформації дуже актуальне.

Метою дослідження є вдосконалення методу виявлення сигналів засобів негласного отримання інформації.

2. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У процесі пошуку засобів негласного отримання інформації пропонується використовувати метод оцінювання параметрів випадкового сигналу. Причому у запропонованому методі змінами параметрів відомих сигналів радіомоніторингу можна знехтувати. Точніше, постійними або легальними сигналами, які працюють у цьому радіодіапазоні частот, можна знехтувати [13–15, 19]. У першому наближенні ці сигнали слід ігнорувати. Таким чином, завдання полягає в тому, щоб оцінити змінний параметр, застосовуваний для приймання повністю відомого сигналу на тлі білого шуму. Завдання – виявлення сигналу, який коливається на тлі сигналів, законно працюючих у заданому діапазоні частот. Тоді будемо розглядати такий варіант представлення радіосигналів.

Нехай на вхід приймального пристрою в момент часу надходить додаткова суміш:

$$x(t) = A_0 S_0(t, l_0(t)) + b(t), \qquad (1)$$

де $S(t, l_0(t)) = A_0 S_0(t, l_0(t))$ – корисний сигнал, $b(t)$ – сигнал білого шуму.

Під час оптимального прийняття сигналу пристрій має побудувати логарифм функції вірогідності флуктуючого параметра. Точне розв'язання задачі побудови функції правдоподібності флуктуючого параметра, у загальному вигляді, отримати дуже складно і це вимагає великої кількості апріорних даних [16, 17, 20]. З фундаментальної точки зору апостеріорна щільність імовірності може бути знайдена у двох випадках.

Перший випадок, $l_0(t)$ – параметр є марковським процесом. Другий, якщо параметр $l_0(t)$ – нормальний випадковий процес.

Для отримання наближеного виразу апостеріорної щільності ймовірності в оптимальному прийнятті сигналу на тлі білого шуму можна врахувати, що протягом часу, котрий дорівнює часу кореляції параметра флуктуації, значення оцінюваного параметра залишається незмінним.

У реальних умовах остаточний час інтегрування визначається постійною часу пристрою для порівняння сигналів флуктуацій із постійними допустимими сигналами заданого частотного діапазону та постійною часу згладжувальних фільтрів, розташованих після дискримінаторів.

Тоді отримуємо

$$V_s(l,T) = \int_0^T W(T-t)x(t)s(l,t)dt, \qquad (2)$$

де $W(T-t)$ – ваговий коефіцієнт характеристик пристрою для порівняння сигналів флуктуації з постійними допустимими сигналами заданого частотного діапазону і постійною часу згладжувальних фільтрів.

Наявність вагового коефіцієнта у виразі (2) можна інтерпретувати таким чином. Оскільки оцінка формується у конкретний момент часу через коливання параметра оцінки, інформація про її значення, яка була відома у виразі, що передує часу $T = t$, поступово втрачає свою вагу.

У виразі (2) передбачається, що більш цікаві для нас значення параметра вимірюються в $T = t$. Однак потрібно враховувати, що в деяких випадках рекомендується визначати оцінку вдруге, наприклад $T \geq t_1$. Це положення характерно для сигналів непрямокутної форми, коли із часом $T = t$, значення сигналу падає до мінімуму або до 0.

$$W(T-t) = e^{-\beta(T-t)}, \quad 0 \leq t \leq T, \qquad (3)$$

або

$$W(T-t) = e^{-[\beta(T-t)]^2}, \quad 0 \leq t \leq T, \qquad (4)$$

де β-параметр обчислюється обернено пропорційно часу кореляції флуктуації оцінюваного параметра.

Якщо вимога виконана: час спостереження набагато більший, ніж час кореляції флуктуацій оцінюваного параметра, то нижня межа інтегрування може бути розширена з 0 до $-\infty$.

Тоді вираз (2) набуде вигляду

$$V_s(l,T) = \int_{\infty}^T W(T-t)x(t)s(l,t)dt. \qquad (5)$$

Якщо ваговий параметр залежить від модуля різниці в часі $|t_1 - t_2|$ і t_1 набагато більше, $T - t_1$, ніж час кореляції флуктуацій, тоді оцінюється вираз (2) та набуде вигляду

$$V_s(l,T) = \int_{\infty}^{T} W(|t - t_1|)x(t)s(l,t)dt. \quad (6)$$

Для розрахунку статичних характеристик оцінки – дисперсії – уявімо вихідний сигнал у вигляді сигналу і шуму:

$$V_s(l,T) = S(l,T) + N(l,T), \quad (7)$$

де

$$S(l,T) = \int_{0}^{T} W(T-t)s(l_0,t)s(l,t)dt, \quad (8)$$

$$N(l,T) = \int_{0}^{T} W(T-t)n(t)s(l,t)dt. \quad (9)$$

Щоб визначити параметри оцінки максимального вихідного сигналу пристрою, враховуючи, що інтегрування вагової функції $W(T-t)$ не змінює цілісність сигнальної функції вираження (8) в точці $l = l_0$, можна використовувати вирази для випадкової оцінки параметра та дисперсії випадкової величини.

Вираз для оцінки випадкових параметрів:

$$\Delta l = \left[\frac{\frac{d}{dt}N(t)}{\frac{d^2S(l)}{d^2l}} \right]_{l=l_0}. \quad (10)$$

Вираз для дисперсії оцінки випадкової величини:

$$D(l) = <\Delta l^2> = \left[\frac{\frac{d^2}{dl_1 dl_2} <N(t_1)N(t_2)}{\left|\frac{d^2S(l)}{d^2l}\right|^2} \right]_{l_0}. \quad (11)$$

Дисперсія оцінки флуктуючого параметра сигналу визначається виразом

$$D(l) = \left[\frac{\frac{N_0}{2} \times \int_0^T W^2(T-t)\frac{d^2}{dl_1 dl_2}S(t,l_1)S(t,l_2)dt}{\left|\int_0^T W(T-t)S(t,l_1)\frac{d^2S(t,l)}{d^2l}dt\right|^2} \right]_{l_0=l_1=l_2=l}. \quad (12)$$

Для параметрів, закодованих у фазі радіосигналу, з точністю до швидко осцилюючих членів, справедливе рівняння:

$$\left[\frac{d^2}{dl_1 dl_2}S(t,l_1)S(t,l_2)dt\right]_{l_0} = \left[\frac{d^2}{d^2l}S(t,l_1)S(t,l_2)\frac{dl}{dl_1}\frac{dl}{dl_2}\right]_{l_0} = -S(t,l_0)\frac{d^2}{d^2l}S(t,l_0). \quad (13)$$

Тоді вираз (12) можна представити у вигляді

$$D(l) = -\frac{N_0}{2} \times \frac{\int_0^T W^2(T-t)S(t,l_0)\frac{d^2}{d^2l}S(t,l)dt}{\left[\int_0^T W(T-t)S(t,l_0)\frac{d^2S(t,l)}{d^2l}dt\right]_{l_0}}. \quad (14)$$

Вираз (14) – це вираз для виявлення будь-якого випадкового відхилення від параметрів радіосигналів, які законно діють у заданому діапазоні радіочастот. Тобто це вираз, реалізація якого в автоматизованому програмному комплексі пошуку прихованих засобів негласного отримання інформації дозволить виявляти випадкові сигнали, які, можливо, є сигналами засобів негласного отримання інформації.

Блок-схема вимірювача відхилення випадкового сигналу зображена рис. 1.

Для підтвердження запропонованого методу виконаємо математичне моделювання процесу виявлення параметрів випадкових сигналів. Для цього візьмемо сигнал, який буде імітувати випадковий сигнал, визначимо "сигнали пристроїв, які законно працюють у цьому радіодіапазоні". Сигнали, що законно працюють у цьому радіодіапазоні, визначаємо шляхом сканування вказаного

радіодіапазону. Порівняємо ці сигнали і визначимо параметри відхилення від "сигналів пристроїв, які законно працюють в цьому радіодіапазоні".

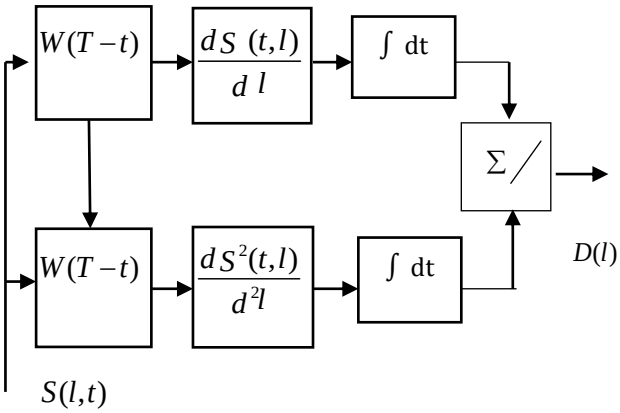


Рис. 1. Блок-схема вимірювача відхилення параметрів випадкового сигналу від "сигналів пристроїв, які законно працюють в цьому радіодіапазоні"

Отримані графічні матеріали моделювання зображено на рис. 2.

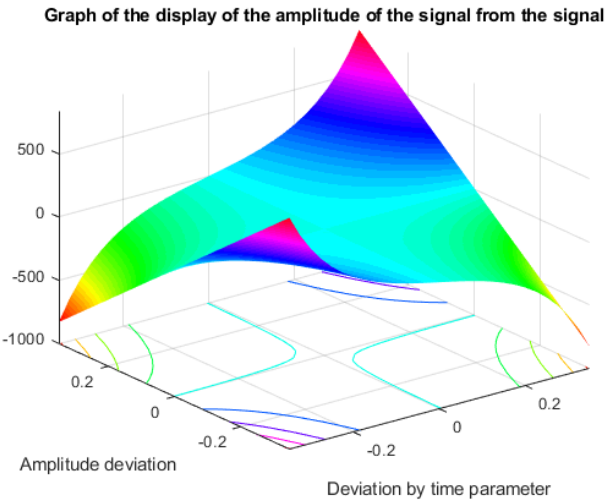


Рис. 2. Графік визначення відхилення амплітуди випадкового сигналу від амплітуди відомих сигналів "сигналів пристроїв, які законно працюють в цьому радіодіапазоні"

Графік на рис. 2 визначає залежність відхилення амплітуди випадкового сигналу, який імітує сигнал засобу негласного отримання інформації, від амплітуд сигналів файла "зразка" або файла параметрів "сигналів пристроїв, які законно працюють у цьому радіодіапазоні".

Бачимо відсутність відхилення амплітуд сигналів, тобто випадковий сигнал відсутній, при довільній зміні інших параметрів відхилення дорівнює нульовому значенню, що відповідає дійсності. У разі виникнення відхилення амплітуди випадкового сигналу від амплітуди відомих сигналів, функція параметра відхилення від зміни параметрів сигналу значно зростає в абсолютному значенні. Причому зростання проходить у сотні разів швидше ніж відхилення амплітуди. Це доводить можливість визначати незначні відхилення амплітуди від амплітуди відомих сигналів або "сигналів пристроїв, які законно працюють в цьому радіодіапазоні". Указане свідчить про надійність запропонованого методу.

Графічні результати, отримані внаслідок математичного моделювання, підтверджують можливість виявлення відхилення амплітуди випадкового сигналу, що імітує сигнал засобу несанкціонованого отримання інформації, від "сигналів пристроїв, які законно працюють у цьому радіодіапазоні". Тобто, запропонованим методом можливе виявлення сигналів засобів негласного отримання інформації.

Для більш точного виявлення сигналів засобів негласного отримання інформації та виключення помилкового прийняття рішення по виявленому сигналу необхідно аналізувати більшу кількість параметрів сигналу. Тому пропонується подальше вдосконалення методу шляхом додаткового аналізу параметрів сигналів. Указаний метод пропонує аналізувати такий параметр, як фаза сигналу і дозволяє визначати відхилення такого параметра, як фаза сигналу.

Для пояснення запропонованого методу розглядатимемо сигнал у вигляді

$$S(t,\varphi_0) = A_0 U_0(t)\cos[\omega_0 t + \psi_0(t) - \varphi_0], \quad 0 < t < T, \tag{15}$$

де $U_0(t)$ – функція амплітудної модуляції, $\psi_0(t)$ – функція фазової модуляції, A_0 – амплітуда сигналу, φ_0 – початкова фаза сигналу.

Корисний сигнал на виході приймача у разі приймання його на фоні "сигналів пристроїв, які законно працюють у цьому радіодіапазоні", має такий вигляд:

$$S(\varphi-\varphi_0) \approx \cos(\varphi-\varphi_0)\frac{A_0^2}{2}\int_0^T U_0(t)F(t)dt = Q_0\cos(\varphi-\varphi_0). \tag{16}$$

Тоді дисперсія оцінки фази з урахуванням другого наближення

$$D(\varphi) = \frac{1}{Q_0}\left(1+\frac{1}{Q_0}\right), \tag{17}$$

де Q_0 – співвідношення сигнал/"сигнал пристроїв, які законно працюють у цьому радіодіапазоні". Тобто подвоєно відношення енергії сигналу до потужності "сигналів пристроїв, які

законно працюють у цьому радіодіапазоні", на одиницю ефективної частоти.

Проведемо математичне моделювання процесу виявлення параметрів випадкових сигналів. Для цього візьмемо сигнал, який буде імітувати випадковий сигнал, визначимо "сигнали пристроїв, які законно працюють у цьому радіодіапазоні". Порівняємо ці сигнали і знайдемо відхилення параметрів від параметрів "сигналів пристроїв, які законно працюють у цьому радіодіапазоні".

Якщо, наприклад, ми візьмемо зважений сигнал у вигляді білого шуму зі спектральною щільністю N_0, то отримаємо вираз

$$Q_0 = \frac{E_0}{N_0} = \frac{A_0^2}{N_0}\int_0^T U_0^2(t)dt. \qquad (18)$$

Із цього прикладу ми можемо бачити, що функція сигналу, а потім і дисперсія оцінки фази не залежать від типу амплітудної та фазової модуляції прийнятого сигналу.

Нормалізована функція сигналу має вигляд

$$G_{N0}(\varphi - \varphi_0) = \frac{1}{Q_0} S(\varphi - \varphi_0). \qquad (19)$$

Ця функція змінюється за гармонійним законом із періодом 2π, тобто у виборі оцінки фази присутня неоднозначність визначення, кратна 2π радіан.

Для пояснення запропонованого методу, розглянемо розв'язання рівняння правдоподібності:

$$\left(\frac{dV_s(\varphi)}{d\varphi}\right)_{\varphi_m} =$$

$$= A_0\int_0^T x(t)F(t)\sin[\omega_0 t + \psi_0(t) - \varphi_m]dt = 0. \qquad (20)$$

Розв'язати це рівняння потрібно, щоб отримати оцінку фази сигналу. Розв'язуючи рівняння (20) щодо оцінки φ_m, отримуємо

$$\varphi_m = arctg\frac{\int_0^T x(t)F(t)\sin[\omega_0 t+\psi_0(t)-\varphi_m]dt}{\int_0^T x(t)F(t)\cos[\omega_0 t+\psi_0(t)-\varphi_m]dt}. \qquad (21)$$

Блок-схему вимірювача девіації фази випадкового сигналу, відповідно до отриманого виразу (21), зображено на рис. 3.

Для підтвердження запропонованого методу виконаємо математичне моделювання процесу виявлення параметрів випадкових сигналів. Для цього візьмемо сигнал, який буде імітувати випадковий сигнал, визначимо "сигнали пристроїв, які законно працюють у цьому радіодіапазоні". Сигнали, які законно працюють у цьому радіодіапазоні, визначаємо шляхом сканування такого радіодіапазону. Порівняємо ці сигнали і визначимо відхилення фази від фази "сигналів пристроїв, які законно працюють у цьому радіодіапазоні".

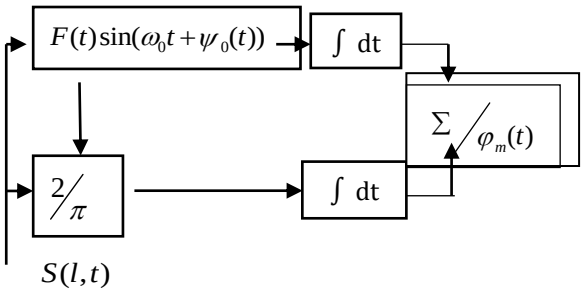


Рис. 3. Блок-схема вимірювача відхилення фази випадкового сигналу від фаз "сигналів пристроїв, які законно працюють у цьому радіодіапазоні"

Отримані графічні матеріали моделювання зображено на рис. 4.

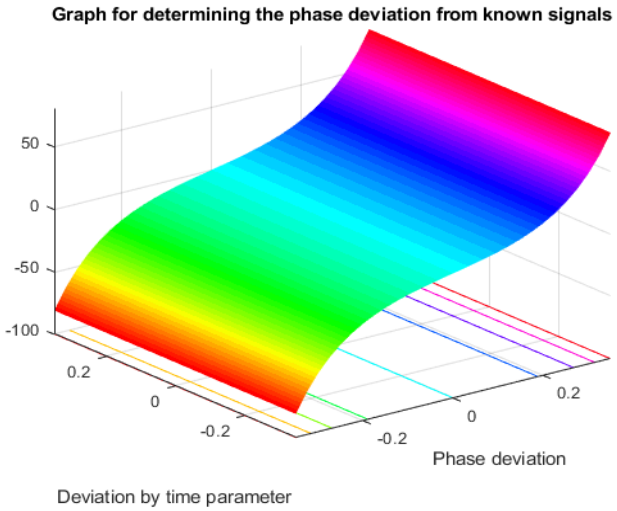


Рис. 4. Графік визначення відхилення фаз від фаз "сигналів пристроїв, які законно працюють у цьому радіодіапазоні"

Графік на рис. 4 визначає залежність відхилення фази випадкового сигналу, який імітує сигнал засобу негласного отримання інформації, від фаз "сигналів пристроїв, які законно працюють у цьому радіодіапазоні". З аналізу отриманого графіка бачимо, що при збіганні фаз відхилення відсутнє, тобто випадковий сигнал відсутній, у разі довільної зміни інших параметрів відхилення дорівнює нульовому

значенню, що відповідає дійсності. Під час виникнення відхилення фази випадкового сигналу від фази відомих сигналів функція відхилення параметра від зміни параметрів сигналу значно зростає в абсолютному значенні. Причому зростання проходить у десятки разів швидше ніж відхилення фази. Це доводить можливість визначати незначні відхилення фази від фаз відомих сигналів, що свідчить про надійність запропонованого методу.

Запропонований метод визначає відхилення фази випадкового сигналу, який можливо, є сигналом засобу негласного отримання інформації, від фаз сигналів пристроїв, легально працюючих у заданому радіодіапазоні.

Тобто, маємо сукупний метод, який складається з двох методів:

- методу визначення відхилення амплітуди випадкових сигналів від амплітуди сигналів файла "зразка";
- методу визначення відхилення фаз випадкових сигналів від фаз сигналів файла "зразка".

Аналіз уже виконується за двома параметрами відхилення сигналів: за амплітудою та фазою, що значно збільшує імовірність виявлення випадкових сигналів, які можуть бути сигналами засобів негласного отримання інформації.

Графічні результати, отримані в результаті математичного моделювання, цілком підтверджують надійність запропонованого сукупного методу визначення відхилення амплітуди та фаз імовірних сигналів від амплітуди та фази відомих сигналів файла "зразка".

Одержані результати моделювання цілком підтверджують запропоновану методику виявлення випадкових сигналів – сигналів засобів негласного отримання інформації. Графічні результати за рахунок збільшеного зростання функції відхилення параметрів підтверджують перевагу запропонованого методу перед іншими "класичними" методами визначення сигналів засобів негласного отримання інформації.

3.ОБГОВОРЕННЯ ЕКСПЕРИМЕНТАЛЬНИХ РЕЗУЛЬТАТІВ

Розроблений метод визначення випадкових радіосигналів, сигналів, які можуть бути сигналами засобів негласного отримання інформації, дозволяє виявляти сигнали пристроїв з більшою ефективністю. Новизна методу полягає у визначенні відхилення головних параметрів сигналів від заданих параметрів. Метод об’єднує методи визначення відхилення амплітуди та метод визначення фаз випадкових сигналів від сигналів засобів, що легально працюють у цьому радіодіапазоні. Самі методи є класичними, але запропоновано загальний метод, який поєднує обидва методи, та додатково вони вдосконалюються засобом визначення відхилення сигналів сторонніх пристроїв. Пропонується визначати сигнали засобів негласного отримання інформації за середньоквадратичним відхиленням (дисперсією) амплітуд і фаз випадкових сигналів.

Для визначення засобів негласного отримання інформації пропонується на першому етапі визначати відхилення амплітуди від амплітуди сигналів, що легально працюють у заданому радіодіапазоні або від амплітуди сигналів файла "зразка", на другому етапі – визначати відхилення фаз сигналів. Таким чином, ефективність методу досягається визначенням двох параметрів відхилення амплітуди та фази, на відміну від класичних методів виявлення засобів негласного отримання інформації. Це дає можливість виявляти випадкові сигналі з великою імовірністю.

Шляхом вимірювання параметрів сигналів пристроїв, що легально працюють у заданому радіодіапазоні, та використання цих параметрів, як параметрів файла "зразка", суттєво збільшується ймовірність визначення випадкових сигналів. Таким чином досягається суттєве скорочення часу шляхом виключення відомих сигналів із додаткового програмного аналізу заданого радіодіапазону. Це ще одна відмінність запропонованого методу.

Для підтвердження запропонованого розробленого методу проведено моделювання методу визначення відхилення амплітуди та методу визначення фаз випадкових сигналів, які можливо і є сигналами засобів негласного отримання інформації. Отримані графічні матеріали, цілком підтверджують можливість визначення сигналів засобів негласного отримання інформації запропонованим методом, доводять переваги розробленого методу над методами та способами, що існують нині.

Подальші шляхи вдосконалення методу можна здійснити шляхом урахування шумів пристроїв і завад із сигналів пошукового радіодіапазону.

4. ВИСНОВКИ

Запропонований метод визначення випадкових сигналів, які можливо є сигналами засобів негласного отримання інформації, складається з двох методів.

Відхилення визначається від амплітуди та фази "сигналів законно працюючих у заданому

радіодіапазоні" або від так званих сигналів файла "зразка".

Цей метод дозволяє визначати випадкові сигнали (сигнали засобів негласного отримання інформації) з імовірністю на 11 % вищій ніж методи "класичного" визначення випадкових сигналів. Це можливо за рахунок значно більшого зростання запропонованої функції відхилення параметрів при незначному відхиленні параметра відхилення амплітуди або фази сигналу.

Запропонований метод дозволяє скоротити час аналізу всіх виявлених випадкових сигналів під час радіомоніторингу на 12–15 % (залежно від завантаженості радіодіапазону) порівняно з існуючими методами. Це забезпечується за рахунок виключення з аналізу "сигналів пристроїв законно працюючих у заданому радіодіапазоні" (сигналів файла "зразка").

Указаний запропонований сукупний метод виявлення засобів негласного отримання інформації дозволить на 11 % підвищити ймовірність виявлення засобів негласного отримання інформації порівняно з існуючими "класичними методами".

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Barabash Oleg, Laptiev Oleksand, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278–3075. pp.4133–4139.

[2] Gromov D. V., Suyakov S. A., Methods for measuring and converting time-frequency parameters of signals. Journal Informatization and Control Systems in Industry. 2013.No. 3 (45).

[3] Khudov H., Khudov R., Khizhnyak I., Loza V., Kravets T., Kibitkin S.Estimation of the Kullback-Leibler Divergence for Canny Edge Detector of Optoelectronic Images Segmentation, International Journal of Emerging Trends in Engineering Research, Vol. 8. № 7, 2020, pp. 3927–3934.

[4] Barabash Oleg, Laptiev Oleksand, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278–3075. pp. 4133–4139

[5] Laptiev Oleksandr, Shuklin German, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 .November – December 2019. Scopus Indexed – ISSN 2278–3091.pp.2840–2846.

[6] Грозовський Р.І., Лаптєв О.А. Аналіз та тенденції розвитку засобів пошуку цифрових радіозакладок.Сучасні інформаційні технології у сфері безпеки та оборони: науковий журнал К.: НУНО України імені Івана Черняховського, (2)35,2019, С 35–41.

[7] Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия . Вопросы кибербезопасности. 2014. №1 (2)., С. 22–27.

[8] Вентцель Е. С., Овчаров Л. А, Теория вероятностей и ее инженерные приложения М. : Наука, 1988. – 480 с.с

[9] Грищук Р.В., Бурячок В.Л., Мамарєв В.М. Науково-технічне обґрун-тування вибору підходу до формування множини інформативних параметрів для систем захисту інформації. Специальные телекоммуникационные системы и защита информации. 2014. № 2 (26). С. 82–86.

[10] Захаров А.В. Требования к перспективному анализатору сетей Wi-Fi [Електронний ресурс] Режим доступу: http://www.analitika.info/ (25.05.2019).

[11] Лукова-Чуйко Н.В. Моделювання оптимальних систем захисту інформації. Науково-технічна конференція "Інформаційна безпека держави": Наукові доповіді учасників науковотехнічної конференції 12–13 березня, Київ, КНУ імені Т. Шевченка, 2015. С. 119–120.

[12] Толюпа С.В., Пархоменко І.І. Побудова комплексних систем захисту складних інформаційних систем на основі структурного підходу. Сучасний захист інформації. 2015. №4. С.62–70.

[13] ХорошкоВ.О.,Хохлачова.Ю.Є.Алгоритм розпізнавання об’єктів у складних умовах. Сучасна спеціальна техніка.2017. №1. С.10.

Стаття надійшла до редколегії 01.06.2021

An improved method of determining random radio signals by deviation of the main parameters of the signals

The article proposes an improved method for determining random radio signals that can be signals of illegan means of obtaining information. The novelty of the method is to determine the deviation of the main parameters of the signals from the specified parameters. The method combines methods for determining the deviation of the amplitude from the amplitude of signals of means legally operating in this radio range and a method for determining the phases of random signals. The signals of the means of illegal obtaining information are determined by the standard deviation (variance) of the amplitudes and phases of the signals.

To determine the means of illegal obtaining information, it is proposed in the first stage to determine the deviation of the amplitude from the amplitude of the signals of legally operating devices or from the amplitude of the signals of the file "sample", in the second stage to determine the deviation of signal phases. Thus,

the two parameters of the deviation of the amplitude and phase can with high probability determine the signals of the means of covert receipt of information. By measuring the signal parameters of legally operating devices and using these parameters as parameters of the "sample" file, the probability of determining random signals is significantly increased. This is achieved by significantly reducing the time by excluding known signals from the additional software analysis of a given radio range.

To confirm the proposed improved method, modeling of the method of determining the deviation of the amplitude and the method of determining the phases of random signals, which are possible and are signals of the means of illegal obtaing information. The obtained graphic materials, which fully confirm the possibility of determining the signal the means of illegal obtaing of information by the proposed method.

Keywords: *method, comparison, signal definition, variance, amplitude, phase, modeling.*

Олександр Лаптєв,
доктор технічних наук, старший науковий співробітник, професор кафедри систем інформаційного та кібернетичного захисту Навчально-наукового інституту захисту інформації.

Alexander Laptev,
Doctor of Technical Sciences, Senior Researcher, Professor of the Department of Information and Cyber Security Systems. Educational and Scientific Institute of Information Protection.

Сергій Лаптєв,
вищу освіту здобув у Київському політехнічному університеті 2009 р.
Сфера наукових інтересів: захист інформаційних ресурсів підприємств, блокування каналів витоку інформації.

Serhii Laptev,
He graduated from Kyiv Polytechnic University in 2009.
Research interests: protection of information resources of enterprises, blocking information leakage channels.

Тетяна Лаптєва,
вищу освіту здобула у Національному авіаційному університеті 2011 р.

Tatiana Lapteva,
She graduated from the National Aviation University in 2011.

УДК 681.3.06
DOI https://doi.org/10.17721/ISTS.2021.1.44-52

С. В. Толюпа, orcid.org/0000-0002-1919-9174, **tolupa@i.ua**
Ю. Я. Самохвалов, orcid.org/0000-0001-5123-1288, **yu1953@ukr.net**
Київський національний університет імені Тараса Шевченка, Київ, Україна,
С. С. Штаненко, orcid.org/0000-0001-9776-4653, **sh_sergei@i.ua**
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АСУ ТП ШЛЯХОМ ЗАСТОСУВАННЯ ПЛІС-ТЕХНОЛОГІЇ

У сучасних умовах питання кібербезпеки переходять із рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави, як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації, у вузькому сенсі цього слова, а й усього кіберпростору. У процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, розробляються нові засоби і методи впливу на інформаційну інфраструктуру потенційного противника, створюються спеціалізовані кібернетичні центри, які реалізуються на високотехнологічних платформах. Нині процедура кіберзахисту не в повному обсязі відображає питання, пов'язані з кібербезпекою автоматизованих систем управління технологічним процесом (АСУ ТП). Це пов'язано з тим, що АСУ ТП спочатку розроблялася з урахуванням ідеології фізичної ізоляції від зовнішніх мереж і суворого розмежування доступу обслуговуючого персоналу, у цьому процесі застосовується специфічне програмне забезпечення, обмін інформацією здійснюється за промисловими комунікаційними протоколами Modbus, Profibus тощо, які часто працюють поверх TCP/IP протоколу. Відповідно в АСУ ТП виникає безліч вразливостей, імовірність використання яких у разі різних кіберінцидентів прямо пропорційна важливості і значимості об'єкта. З огляду на той факт, що АСУ ТП стали невід'ємною частиною нашого існування, відповідно проблема кібербезпеки систем, які розглядаються, нині є актуальним і своєчасним завданням. У статті розглянуто підхід до забезпечення кібербезпеки АСУ ТП шляхом створення інтелектуальних систем кібербезпеки (ІСКб). Передбачено, що в основу побудови запропонованих систем повинно бути покладено поняття "еволюція (розвиток)", тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак), шляхом застосовування технологій із протидії кібератакам протягом усього життєвого циклу. Технічно реалізувати ІСКб запропоновано за рахунок застосування експертної системи і катастрофостійких інформаційних систем (КАІС) характерною особливістю яких, на відміну від відмовостійких систем, є продовження роботи в умовах масових і, можливо, послідовних відмов системи або її підсистем у результаті проведення кібератак. Такими властивостями (катастрофостійкими властивостями) володіють програмовані логічні інтегральні схеми (ПЛІС) – клас мікропроцесорних систем, характерною особливістю яких є можливість реалізації багатопроцесорної структури, здатної протидіяти зовнішнім впливам (кібератакам). Слід зазначити, що сучасні ПЛІС представляють собою інтегральну схему, внутрішню конфігурацію якої задано шляхом програмування за рахунок застосування спеціальних мов опису апаратури.

Ключові слова: *кібербезпека; автоматизована система управління; катастрофостійка система; програмована логічна інтегральна схема; експертна система.*

1. ВСТУП

Нові цифрові технології і глобальні інформаційні мережі, які вчинили справжню революцію у сфері накопичення, обміну й оброблення інформації, поставили нас перед фактом корінної зміни застарілих принципів її захисту в контексті кібербезпеки [1].

У сучасних умовах питання кібербезпеки переходять з рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави, як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації, у вузькому сенсі цього слова, а й усього кіберпростору.

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин,

утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем, і забезпечення електронних комунікацій із використанням інтернету та/або інших глобальних мереж передачі даних [2].

Слід зазначити, що у процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, розробляються нові засоби і методи впливу на інформаційну інфраструктуру потенційного противника, створюються спеціалізовані кібернетичні центри (*SOC – Security Operations Center, CSOC – Cyber Security Operations Center*), які реалізуються на платформах *SIEM* (*Securitu Information and Event Management* – системи управління інформацією про безпеку та подіями інформаційної безпеки), *IRP* (*Incident Response Platform* – платформи реагування на інциденти інформаційної безпеки), *SOAR* (*Security Orchestration, Automation and Respons*e – системи управління, автоматизації та реагування на інциденти), *SGRC* (*Security Governance, Risk-management and Compliance* – системи управління інформаційною безпекою, ризиками і відповідністю законодавству) (рис. 1).

Крім цього, швидкими темпами по всьому світу створюються підрозділи управління і кіберкомандування (*US Cybercom* – США, *NCSC* – Великобританія, *Cybercom* – Франція, командування військ зв'язку та кібербезпеки – Україна), а також кібервійська, основним завданням яких є захист цивільних і військових критично важливих об'єктів інфраструктури (КВОІ), якими є автоматизовані системи управління технологічним процесом (АСУ ТП), а також підготовка і проведення активних деструктивних дій в інформаційних системах супротивника.

Рис. 1. Основні функції SOC

На думку фахівців із кібербезпеки, у технічному плані повний адекватний кіберзахист передбачає побудову та використання таких основних підсистем [3]:

- підсистема захисту (*Protection Capabilities*) забезпечує скритність випромінювань радіоелектронних засобів, систем і засобів зв'язку, комп'ютерну безпеку (*computer security*) та інформаційну безпеку (*Infosec*);
- підсистема виявлення (*Detection Capabilities*) забезпечує розпізнавання аномалій у мережі за рахунок застосування систем їхнього виявлення;
- підсистема реагування на зміни технічних параметрів і обстановки (*Reaction Capabilities*) забезпечує відновлення (реконфігурацію) і виконання інших процесів інформаційних операцій.

Однак розглянута процедура кіберзахисту не в повному обсязі відображає питання, пов'язані з кібербезпекою АСУ ТП. Це викликано тим, що АСУ ПТ спочатку розроблялася з урахуванням ідеології фізичної ізоляції від зовнішніх мереж і суворого розмежування доступу обслуговуючого персоналу, при цьому застосовується специфічне програмне забезпечення, обмін інформацією здійснюється за промисловими комунікаційними протоколами *Modbus, Profibus* тощо, які часто працюють поверх *TCP/IP* протоколу.

Відповідно в АСУ ТП виникає безліч вразливостей, імовірність використання яких у різних кіберінцидентах прямо пропорційна важливості і значимості об'єкта. Про наслідки таких кіберінцидентів важко судити, оскільки дуже багато залежить від конкретних цілей зловмисника, а вони варіюються від крадіжки конфіденційної інформації до порушення технологічних процесів, що може привести до широкого спектра необоротних наслідків, починаючи з негативних явищ в економічному секторі та закінчуючи виникненням загрози життю і здоров'ю громадян. З огляду на те, що АСУ ТП стали невід'ємною частиною нашого існування, відповідно проблема кібербезпеки систем, які розглядаються, є на сьогоднішній день актуальним і своєчасним завданням.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Нині існує багато наукових робіт, присвячених автоматизації управління АСУ ТП та її безпеці. Зокрема, у роботах [4] інтелектуалізацію розглядають як головний напрямок розвитку автоматизації управління, що можливо реалізувати побудовою нечітких лінгвістичних баз даних, підсистем нечіткого виведення. Подальший розвиток АСУ ТП – це інтеграція інтелектуальних систем підтримки прийняття рішень із класичними *SCADA*-системами, з використанням сенсорних мереж, інтелектуальних середовищ.

Одним із перспективних напрямків розвитку АСУ ТП в роботі [5] вважають розроблення екс-

пертних систем (ЕС), тобто використання можливостей штучного інтелекту для підвищення ефективності автоматизації технологічних процесів.

У роботі [6] пропонують застосовувати систему контролю вразливостей – один з ефективних методів протидії промисловим кіберзагрозам, що представляють собою вузькопрофільні програми, розроблені спеціально для промислових систем автоматизації. Вони дозволяють визначити цілісність внутрішнього середовища пристроїв, зафіксувати всі спроби змінити прикладну програму контролера, зміни в конфігурації мережних пристроїв захисту і управління в енергомережах.

3. МЕТА СТАТТІ

Метою статті є створення інтелектуальної системи кібербезпеки, яка спроможна забезпечити захист АСУ ПТ від кібератак, у цьому процесі як технічну реалізацію пропонується застосовувати експертні системи та програмовані логічні інтегральні схеми, які належать до класу катастрофостійких (живучих) систем і здатні протидіяти кібервпливам, кібератакам тощо.

4. ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

Сучасні АСУ ТП представляють собою комплекс апаратно-програмних засобів, а також персоналу, призначений для управління різними процесами в межах технологічного процесу, основним завданням яких є підвищення ефективності управління цими процесами, шляхом мінімізації людського втручання в указані процеси.

Якщо розглядати сучасні АСУ ТП, з точки зору структурної ієрархії, то очевидним стає питання кібербезпеки цих систем. Це пов'язано з тим, що вони є типовими, багаторівневими, розгалуженими людино-машинними системами управління, які представлено на трьох рівнях на рис. 2 [7]:

- верхній рівень реалізується шляхом застосування системи диспетчерського управління та збору даних у режимі реального часу (*SCADA*-система – *Supervisory Control And Data Acquisition*);
- середній рівень реалізується застосуванням програмованих логічних контролерів (*PLC – programmable logic controller*);
- нижній рівень представлено контрольно-вимірювальними приладами, приладами автоматики, виконавчими пристроями управління, пультами сигналізації.

На сьогоднішній день питання, пов'язані з кібербезпекою АСУ ТП, є комплексним завданням. Його розв'язання залежить від виконання правил на всіх рівнях:

- адміністративний – формування керівництвом програми робіт із кібербезпеки;
- процедурний – визначення норм і правил для персоналу, який обслуговує систему;
- програмно-технічний – управління доступом; забезпечення цілісності; забезпечення безпечної міжмережної взаємодії; антивірусний захист; аналіз захищеності; виявлення вторгнень; безперервний моніторинг стану, виявлення інцидентів, реагування.

Рис. 2. Структура АСУ ТП

Проведений аналіз компанією *Positive Technologies* в області кібербезпеки АСУ ТП промислових об'єктів за 2018 рік показав, що загальне число виявлених кіберінцидентів продемонструвало тенденцію до збільшення і склало 257, що на 25 % більше кількості, зафіксованої в попередньому звітному періоді. Найчастіше 2018 року кіберзлочинці націлювалися на обладнання *Schneider Electric* та *Siemens* – 69 і 66 кібератак відповідно, 23 % випадків виявлення вразливостей були пов'язані з промисловим мережним обладнанням, а також із програмним пакетом *SCADA* та людино-машинним інтерфейсом. Крім цього, 21 % вразливостей виявлено у програмованих логічних контролерах. У 18 % і 4 % випадках уразливості знайдено у програмному забезпеченні АСУ ТП і числовому програмному управлінні. Ще 11 % цілей вказано у звіті *Positive Technologies* як "інші" [8].

Win32/*Stuxnet* (мережний черв'як – *network worms*) – це перший відомий комп'ютерний вірус, який зміг перехопити і модифікувати інформаційний потік між програмованими логічними контролерами і робочими станціями *SCADA*-системи іранської атомної електростанції в Бушері. Унікальність шкідливої програми полягала в тому, що вперше в історії кібератак вірус фізично зруйнував інфраструктуру, шляхом поши-

рення по мережі і створення своїх копій, використовуючи мережні протоколи і периферійні пристрої. На думку експертів [9], саме програмовані логічні контролери стали тим "вузьким місцем" у системі автоматизованого управління, які сприяли зміні самого технологічного процесу.

Аналіз існуючих підходів щодо кіберзахисту сучасних технологічних систем показує, що одним із перспективних напрямків забезпечення безпеки АСУ ПТ є створення інтелектуальних систем кібербезпеки. Причому в основу побудови запропонованих систем має бути покладено поняття "еволюція (розвиток)", тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак), шляхом застосовуваних технологій щодо протидії кібератакам протягом всього життєвого циклу [10].

Запропонована інтелектуальна система кібербезпеки АСУ ТП повинна забезпечити не тільки виявлення нових і невідомих кіберзагроз (кібератак) у ході моніторингу (розвідки) кіберпростору, але провести аналіз виявлених кіберзагроз (кібератак) і автоматичний вибір параметрів функціонування АСУ ТП в умовах деструктивних впливів без погіршення її основних характеристик.

Крім цього, у системі кібербезпеки АСУ ТП, також мають бути реалізовані додаткові можливості:

- автоматичної зміни властивостей і параметрів систем і засобів забезпечення кібербезпеки, залежно від зміни стану кіберпростору (виявлення активності потенційних джерел кіберзагроз, виявлення кібератак) і результатів проведених кібератак;
- автоматичного оцінювання зміни рівня захищеності АСУ від кіберзагроз у ході зміни умов функціонування;
- автоматизованої підтримки прийняття рішень щодо протидії кібератакам і автоматичного впливу на джерела кібератак;
- автоматизованої підтримки прийняття рішення про перерозподіл ресурсів систем і засобів кібербезпеки в разі їхнього функціонального ураження в результаті кібератак;
- обліку у процесі забезпечення кібербезпеки всіх взаємопов’язаних, взаємодіючих і змінюваних у часі чинників, що впливають на рівень кібербезпеки АСУ;
- зниження нецільового навантаження на комплекс засобів автоматизації системи кібербезпеки АСУ;
- прогнозування, на основі закладених і накопичених у процесі експлуатації знань, факторів, що впливають на рівень захищеності АСУ від усіх видів кіберзагроз.

Визначаючи завдання боротьби із загрозами кібербезпеки, не можна відкидати розроблення і реалізацію активних способів і методів забезпечення кібербезпеки. Тому в системі кібербезпеки АСУ повинні бути передбачені можливості проведення попереджувальних апаратно-програмних впливів (превентивних ударів) і активних атак на джерела кібератак, які виявлені, інформаційні системи і ресурси протиборчої сторони, а також здатність до дезінформації протиборчої сторони про справжні властивості і параметри АСУ та її системи кібербезпеки.

Однією з умов створення інтелектуальної системи забезпечення кібербезпеки АСУ ТП є застосування апаратної і програмної платформ зі складу довіреного програмно-апаратного середовища. Під довіреністю будемо розуміти сувору, гарантовану відповідність необхідним вимогам у частині інформаційної безпеки, надійності та функціональної стійкості в умовах сучасного інформаційного протиборства за дотримання певних умов технологічної незалежності.

Передбачено, що інтелектуальна система кібербезпеки буде функціонувати на верхньому рівні ієрархії побудови АСУ ТП, шляхом інтеграції в *SCADA*-систему. Як інтелектуальну систему пропонується використовувати ЕС – людино-машинну систему, яка застосовує експертні знання для забезпечення високоефективного розв'язання неформалізованих задач у вузькій предметній області.

Експертні системи дозволяють, використовуючи знання фахівців про деяку конкретну предметну вузькоспеціалізовану область і в межах цієї області, приймати рішення на рівні експерта-професіонала. Найбільшу увагу сьогодні приділяють ЕС, здатним приймати рішення в масштабі часу, близькому до реального (динамічного). Динамічні експертні системи, порівняно зі статистичними, містять додатково такі компоненти: підсистему моделювання зовнішнього світу і підсистему взаємодії із зовнішнім світом, що дозволяє управляти складними технологічними процесами в режимі моніторингу (кіберрозвідки). Це включає виявлення відмов (наслідків кібератаки, прийняття рішення за результатами показань множини периферійних пристроїв, оптимізацію і планування процесу, управління великими мережами, розподіленими СУБД, здатність підказувати оператору (кіберспеціалісту), як діяти у складних умовах, а в критичних ситуаціях – брати управління на себе.

Нині лідером у сфері створення динамічних експертних систем реального часу є продукт *G*2 (*Gensym*, США), який представляє собою

об'єктно-орієнтоване інтегроване середовище для розроблення і супроводу додатків реального часу, що використовують бази знань. Продукт *G*2 розроблений як відкрита система, зв'язок із зовнішніми джерелами даних будується на основі бібліотеки стандартних інтерфейсів і сервера *GSI* (*G*2 *Standart Interface*) (рис. 3) [11].

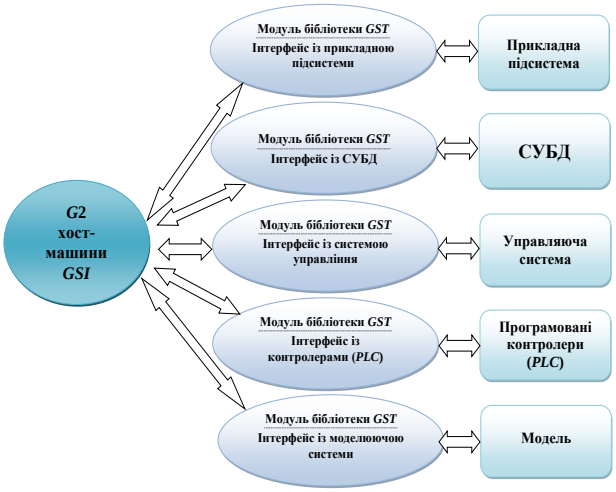


Рис. 3. Інтерфейс експертної системи G2

Підсистема *GSI* працює паралельно з прикладною системою як незалежний обробник подій і забезпечує її двосторонню взаємодію із широким спектром програмованих контролерів (мікросхем), систем збору даних, концентраторів даних і розвинених СУБД.

Продукт *G*2 унікальним чином поєднує в собі технології міркування, включаючи правила, процедури, моделювання об'єктів і процесів, імітаційне моделювання та графічне представлення в єдиному середовищі розроблення і впровадження, інтегрує в собі множину взаємодоповнюючих методів штучного інтелекту, що спрощує і прискорює процес розроблення додатків і дозволяє робити їх універсальними. Дуже важливою особливістю *G*2 є можливість редагування додатків у режимі реального часу.

Основою середнього і нижнього рівнів ієрархії побудови інтелектуальної системи кібербезпеки АСУ ТП повинні стати апаратно-програмні засоби, які належать до КАІС. Причому необхідно чітко розуміти різницю між поняттям "відмовостійкість" і "катастрофостійкість". У понятті "відмовостійкість" акцент робиться на відновлення працездатності після одиничних, випадкових, не пов'язаних між собою відмов компонентів. Технологія відпрацювання таких відмов передбачає, як правило, що в роботу вводять резервні компоненти кожної підсистеми або компоненти, які залишилися при багаторазовому дублюванні, перерозподіляють між собою роботу незалежно від того, що відбувається в цей час в інших підсистемах [12].

У понятті "катастрофостійкість" головне – збереження даних і продовження роботи в умовах масових і, можливо, послідовних відмов систем (кібератак) і пов'язаних між собою підсистем. Як основний показник у цьому випадку використовується показник доступності КАІС, який характеризує ступінь можливості отримання необхідних даних і здійснення взаємодії із заданими додатками у прийнятні терміни і з необхідним рівнем продуктивності. У цьому контексті складовими показника доступності КАІС є показники надійності апаратно-програмних засобів КАІС, а також показник продуктивності вказаної системи, що представляє собою відношення часу відгуку інформаційної системи до її пропускної здатності [13].

Слід підкреслити, що створення КАІС ведеться з припущення, що катастрофа, на відміну від відмови (події можливої, прогнозованої, імовірної) – це подія можлива, але малоймовірна, або ймовірність якої мала і не може бути обґрунтовано оцінена у процесі проєктування. В іншому випадку йшлося б не про катастрофу (кібератаку), а про умови функціонування.

Таким чином, можна зробити висновок, що для побудови КАІС потрібні відповідні інструментальні засоби – операційні системи, що підтримують багатопроцесорну (разпаралелену) роботу і мови програмування, здатні конструювати віртуальні обчислювальні структури спеціального виду й описувати виконання масово-паралельних, локальних алгоритмів розв'язання трудомістких завдань.

Нині переважним способом разпаралелювання завдань є великоблочне разпаралелювання, коли задача розбивається на великі підзадачі і кожен процесор у складі суперкомп'ютера розв'язує виділену йому частину. Однак подібний підхід має ряд недоліків. По-перше, процесори загального призначення менш ефективні, ніж спеціалізовані пристрої. По-друге, для розв'язання певної задачі велика частина процесорної логіки є надмірною. Створення спеціалізованого комп'ютера, який розв'язував би конкретне завдання, вимагає великих фінансових і часових витрат [14].

Інший шлях – використання реконфігурованих логічних пристроїв, які реалізують технологію дрібнозернистої, локально-паралельної архітектури, даючи можливість змінювати "внутрішню логіку" процесорів, оминаючи перераховані

вище проблеми. Під поняттям дрібнозернистий паралелізм будемо розуміти можливість розбити задачу на множину невеликих однотипних підзадач, які будуть виконуватися паралельно на окремих простих процесорах, у цьому процесі дані максимально розподілені по системі, а кожен процесор використовує мінімально можливий набір даних [15].

Таким чином, дрібнозернистість, або масове разпаралелювання, означає, що в кожному обчислювальному процесі в кожен момент часу міститься мінімальна кількість команд (тіло внутрішнього циклу) і даних (елементи масивів, необхідні для обчислення одного витка циклу).

На сьогоднішній день логічними пристроями, які здатні реалізувати технологію дрібнозернистої, локально-паралельної, багатопроцесорної архітектури є ПЛІС (*PLD – Programmable Logic Device*) – електронні компоненти (інтегральні схеми), які використовуються для створення конфігурованих цифрових електронних схем. На відміну від звичайних цифрових мікросхем, логіка роботи ПЛІС не визначається під час виготовлення, а задається за допомогою програмування (проєктування), при цьому використовується програматор і середовище для налаштування (*IDE – Integrated Development Environment*), які дозволяють задати бажану структуру цифрового пристрою у вигляді принципової електричної схеми або програми на спеціальних мовах опису апаратури: *AHDL, VHDL, Verilog* та інші, причому теоретичною базою проєктування є булева алгебра, двійкова арифметика і теорія кінцевих автоматів [16].

Сучасні ПЛІС представляють собою матрицю програмованих логічних елементів із *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) структурами, на базі яких створюється абсолютно новий напрямок розвитку мікроелектроніки – універсальні мікропроцесорні системи на кристалі (*System-on-Chip – SoC, SoPC – System-on-a-Programmable-Chip, MPSoC – Multiprocessor System-on-Chip*). Такі складні інформаційні системи класу *SoC* складаються з трьох основних цифрових системних блоків: процесор, пам'ять і логіка (рис. 4).

Процесорне ядро реалізує потік управління, коли кожна програма встановлює послідовність виконання операції оброблення даних, дозволяє задавати один із можливих алгоритмів роботи всієї інформаційної системи. Пам'ять використовується за її прямим призначенням – зберігання коду програми процесорного ядра і даних. І нарешті, логіка використовується для реалізації спеціалізованих апаратних пристроїв оброблення і проходження даних, склад і призначення яких визначаються кінцевим додатком – потоком даних.

В основі методології проєктування *SoC* лежить принцип повторного використання блоків (*reuse*-блок, *IP*-блок (*Intellectual Property*), складний функціональний блок – СФ-блок), що розробляються в межах одного проєкту, потім використовуються в інших проєктах.

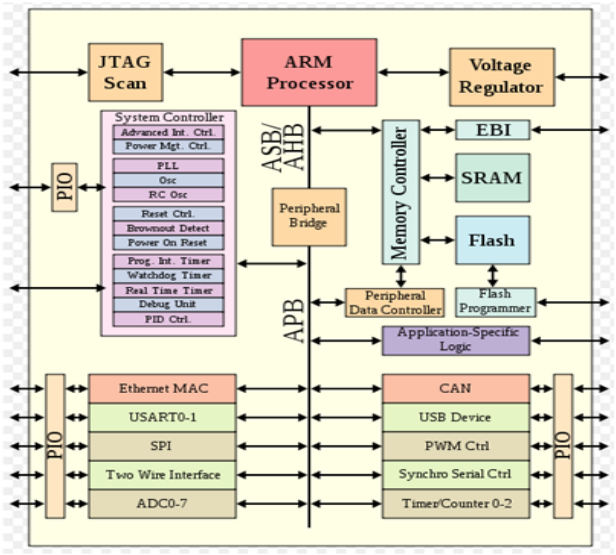


Рис. 4. Структура типової системи на кристалі, побудованої на основі ARM-мікропроцесора

Фактично весь процес розроблення *SoC* містить чотири етапи: розроблення архітектури *SoC* на системному рівні; вибір *IP*-блоків із бази даних; проєктування блоків, які залишилися; інтеграція всіх блоків на кристалі.

Інша принципова особливість *SoC* – це наявність програмованих блоків – процесорів, з урахуванням цього *SoC* є не просто інтегральна схема, а комплекс, до складу якого входять як апаратна частина – чіп, так і програмна частина – вбудоване програмне забезпечення (*Linux, Windows* тощо) [17–18].

Нині проєктування *SoC* є розвитком технологій і засобів розроблення спеціалізованих інтегральних мікросхем (*ASIC – Application-Specific Integrated Circuit*) і ПЛІС. Узагальнену схему традиційного маршруту показано на рис. 5.

Процес проєктування *SoC* є послідовним, із виділенням технологічних етапів – рівнів, та ітеративним, тобто на кожному етапі можна зробити відкат назад для коригування проєкту. Проєктування програмного забезпечення виконується відокремлено від розроблення апаратних засобів, після отримання віртуальних або фізичних прототипів апаратури. На всіх рівнях використовують компонентний підхід. Компоненти –

функціональні, топологічні і програмні блоки – організовуються в бібліотеки, для повторного використання [19, 20].

Фактично описаний маршрут проєктування не має жодних принципових відмінностей порівняно з традиційною технологією створення мікропроцесорних систем. З особливостей слід виділити те, що центральну позицію зайняла програмована апаратура – ПЛІС, з'явилися засоби структурної конфігурації процесорних ядер, САПР ПЛІС, причому пакети розроблення програмного забезпечення об'єднуються в потужні інструментальні комплекси.

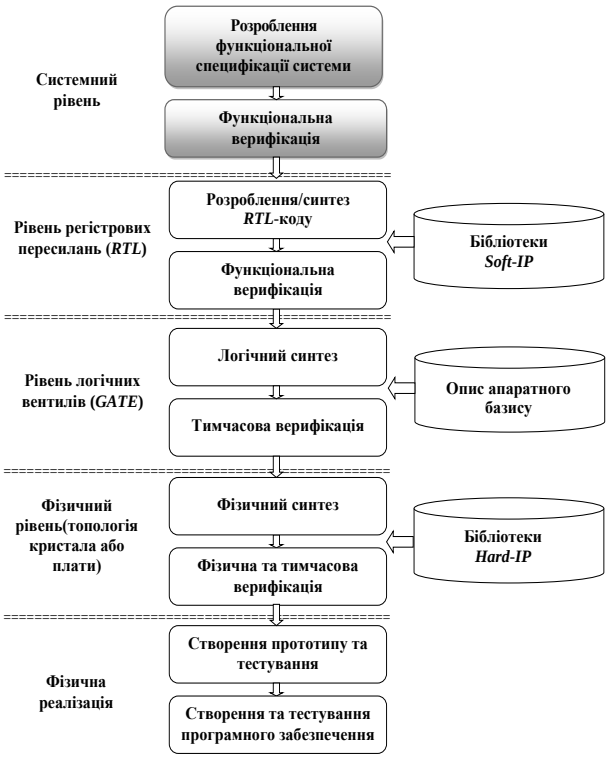


Рис. 5. Узагальнена схема традиційного маршруту

Прикладом такого комплексу може бути САПР фірми *Altera* для проєктування *SoPC* на базі ПЛІС і процесорного ядра *NIOS II*, який включає базові пакети *Quartus II* (ПЛІС), *SoPC Builder* (конфігурується процесорне ядро), *NIOS II IDE* (програмне забезпечення) і багато інших розширень (*DSP Builder*, *C-to-Hardware Compiler* тощо).

5. ВИСНОВКИ

Таким чином, доходимо висновку, що використовуючи реконфігуровані логічні пристрої (ПЛІС) для створення багатопроцесорних (розпаралелених) "живучих" структур у процесі побудови інтелектуальної системи кібербезпеки АСУ ТП, ми отримуємо переваги: висока катастрофостійкість (кіберстійкість), а також продуктивність системи при розв'язанні завдань, пов'язаних із забезпеченням її кібербезпеки.

Зазначимо, що запропоновані КАІС мають величезний ресурс резервування і дистанційного перепрограмування, подальше використання яких пов'язано з оснащенням їх необхідними сенсорами/датчиками в супроводі програм первинного оброблення отриманих даних і передачі цих даних на наступні ієрархічні рівні оброблення, з метою зберігання і вироблення управлінських рішень.

6. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подальший розвиток технології *System-on-Chip* (*SoC*) надасть можливість реалізувати технологію "мережа на кристалі" *Network-on-Chip* (*NoC*) – мережна система з комутацією пакетів на основі маршрутизатора між модулями *SoC*. Пропонується на базі технології *NoC* у подальшому створення платформи – розподіленої інфраструктури помилкових цілей, *DDP* (*Distributed Deception Platform*), яка дозволяє розгорнути мережу підроблених пристроїв-приманок (*honeypot* – "горщик меду"), які практично не відрізняються від реальних і можуть служити об'єктами зондування, атак і зломів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] А.А. Карцхия, "Кибербезопасность и интеллектуальная собственность (часть 1)", *Вопросы кибербезопасности*., vol. 1(2), pp. 61–66, 2014.

[2] Закон №2163 VIII от 05.10.2017 Про основні засади забезпечення кібербезпеки України.

[3] Ю.В. Бородакий, "Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2)", *Вопросы кибербезопасности*., vol. 1(2), pp. 5–12, 2014.

[4] В.Б. Тарасов, М.Н. Святкина, "Интеллектуальные SCADA-системы: истоки и перспективы", *Машиностроение и компьютерные технологии*., vol. 13, p. 35, 2011.

[5] Е.М. Самойлова, А.А. Игнатьев, "Интеграция искусственного интеллекта в автоматизированные системы управления и проектирования технологических процессов", *Вестник Саратовского государственного технического университета*, vol. 1, pp. 127–132, 2010.

[6] А. Чертков, "Кибербезопасность промышленной автоматизации", *Control engineering*, vol. 2(68), pp. 22–25, 2017.

[7] Е.П. Попова, "Автоматизированные системы управления технологическими процессами", *Краснодар: ГБПОУ КК КТК*, 2015. – 44 с.

[8] М. Небайкин, "Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты", https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review.

[9] П. Волобуев, "Безопасность SCADA: Stuxnet – что это такое и как с этим бороться? "

[10] https://lib.itsec.ru/articles2/Oborandteh/bezopasnost-scada-stuxnet-chto-eto-takoe-i-kak-s-etim-borotsya.

[11] Ю.В. Бородакий, "Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1)", *Вопросы кибербезопасности*., vol. 1(2), pp. 2–9, 2013.

[12] Е.М. Самойлова, А.А. Игнатьев, "Интеграция искусственного интеллекта в автоматизированные системы управления и проектирования технологических процессов", *Вестник Саратовского государственного технического университета*, vol. 1, pp. 127–132, 2010.

[13] А.Н. Павлов, Б.В. Соколов, "Структурный анализ катастрофоустойчивой информационной системы", *Труды СПИИРАН*, vol. 8, pp. 128–151, 2009. ISSN 2078-9181.

[14] П.А. Елугачев, Н.В. Лаходынова, Б.М. Шумилов, Э.А. Эшаров,"Проблемы математического моделирования кибер-физических систем на транспорте", *Информационные системы. автоматизация и системы управления известия*, *СПБГТИ(ТУ)*, vol. 53(79), pp. 107–115, 2020.

[15] В.А. Воробьёв, "Об эффективности параллельных вычислений", *Автометрия*, vol. 1, pp. 55–58, 2000.

[16] О.А. Юфрякова, "Оптимизация количества процессоров для эффективного исполнения параллельных алгоритмов" *Научный сервис в сети Интернет: поиск новых решений*: тр. междунар. Суперкомпьютерной конфер. М., 2012.

[17] И.Е. Тарасов, "Проектирование конфигурируемых процессоров на базе ПЛИС", *Компоненты и технологи*., vol. 2, pp. 78–83, 2006.

[18] И.Е Тарасов, "ПЛИС Xilinx. Языки описания аппаратуры VHDL и Verilog, САПР, приемы проектирования", *Горячая линия*, – Телеком, p. 358, 2021.

[19] Vaibbhav Taraate. PLD Based Designwith VHDL RTL Design, Synthesisand Implementation, Springer Nature Singapore Pte Ltd, p. 423, 2017.

[20] А.В. Строгонов, "Реализация Verilog-проектов в базисе академических ПЛИС с применением САПР VTR7.0", *Компоненты и технологи,* vol. 5, pp. 12–17, 2017.

[21] Bogdan Belean. Application-Specific Hardware Architecture Designwith VHDL. – Springer International Publishing, 2018. – 191 p.

Стаття надійшла до редколегії 15.07.2021

Ensuring cyber security of ACS TP by using FPGA technology

In modern conditions, cybersecurity issues are moving from the level of information protection at a separate object of computer technology to the level of creating a single cybersecurity system of the state, as part of the information and national security system responsible for protecting not only information in the narrow sense, but also all cyberspace. In the process of forming global cyberspace, military and civilian computer technologies are converging, new means and methods of influencing the information infrastructure of a potential adversary are being developed, and specialized cyber centers are being created and implemented on high-tech platforms. At present, the cybersecurity procedure does not fully reflect the issues related to the cybersecurity of the ACS TP. This is due to the fact that the ACS PA was originally developed based on the ideology of physical isolation from external networks and strict delimitation of access by service personnel, using specific software, information exchange via industrial communication protocols Modbus, Profibus, etc., which often work on top of the TCP / IP protocol. Accordingly, there are many vulnerabilities in the ACS TP, the probability of which in various cyber incidents is directly proportional to the importance and significance of the object. Given the fact that the ACS TP have become an integral part of our existence, respectively, the problem of cybersecurity of the systems under consideration is today an urgent and timely task. The article discusses an approach to ensuring the cybersecurity of automated process control systems (APCS) by creating intelligent cybersecurity systems (ISCs). It is assumed that the construction of the proposed systems should be based on the concept of "evolution (development)", that is, the ability of the system to adapt through changes in parameters under the influence of external and internal cyber threats (cyber attacks), through the applied technologies, to counter cyber attacks throughout the entire life cycle. Technically, it is proposed to implement the ISCs by means of using an expert system and disaster-tolerant information systems (DIS), a characteristic feature of which, in contrast to fault-tolerant systems, is the continuation of work in conditions of massive and, possibly, consecutive failures of the system or its subsystems as a result of cyberattacks. These properties (catastrophic properties – system survivability) are possessed by programmed logic integrated circuits (FPGA) – a class of microprocessor systems, a characteristic feature of which is the ability to implement a multiprocessor (parallelized) structure that can withstand external influences (cyber attacks). By themselves, FPGA are an integrated circuit, the internal configuration of which is set by programming using special languages for describing hardware.

Keywords: *cybersecurity; automated control system; catastrophic system; programmable logic integrated circuit; expert system.*

Сергій Толюпа,
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Serhii Toliupa,
Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Information Protection of the Faculty information technology Taras Shevchenko National University of Kyiv.

Юрій Самохвалов,
доктор технічних наук, професор, професор кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Yuri Samokhvalov,
Doctor of technical sciences, professor, professor of the department of intellectuals Faculty of Technology information technology Taras Shevchenko National University of Kyiv.

Сергій Штаненко,
кандидат технічних наук, доцент, доцент кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Serhii Shtanenko,
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Construction of Telecommunication Systems of the Military Institute of Telecommunications and Informatization named after Heroes of Kruty.

УДК 004.93
DOI https://doi.org/10.17721/ISTS.2021.1.53-60

О. М. Кулінич, orcid.org/0000-0002-0643-6898,
olmaxol@i.ua
А. С. Роскот, orcid.org/0000-0002-8063-4104,
nroskot144@gmail.com
Інститут спеціального зв'язку та захисту інформації
НТУУ КПІ імені Ігоря Сікорського, Київ, Україна

СИСТЕМА БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ

Біометричний підхід вважають одним із найактуальніших у системах ідентифікації та автентифікації. В основі біометричного методу лежить аналіз унікальних характеристик людини. Розпізнавання обличчя – важливе завдання, адже є першим етапом ідентифікації, щоб виявити, кому належить обличчя і чи є воно в базі даних, спочатку потрібно його локалізувати. Для розв'язання цієї задачі застосовують різні підходи, серед них: емпіричні методи, метод на основі навчання, метод на основі порівняння із шаблоном, метод на основі контурних моделей. У розпізнаванні обличчя системі, яка розв'язує таку задачу, необхідно врахувати сукупність факторів: відмінності облич різних людей, зміна ракурсу обличчя, можливість наявності певних особливостей, зміна виразу обличчя, наявність перешкод на зображенні, що можуть частково перекривати об'єкт, умови зйомки. Штучний інтелект є і полем для розвитку, і викликом. Зважаючи на те, що розробки машинного навчання та штучного інтелекту часто орієнтовані на оброблення великих масивів даних, а алгоритми машинного навчання прямо залежать саме від якості інформації, яку він обробляє, то втручання та дезінформація можуть вивести з ладу подальшу роботу алгоритму, що може призвести до неправильних висновків, у коректності яких буде важко переконатися, оскільки великі масиви даних. Вибір методу для розв'язання задачі виявлення обличчя залежить від конкретної задачі й умов, в яких повинен функціонувати алгоритм. У статті розглянуто та проаналізовано можливості нейронних мереж для застосування в системі багатофакторної автентифікації. Розглянуто варіанти можливих реалізацій із використанням штучної мережі, перспективи розвитку цих мереж і їхню важливість у наш час. Проаналізовано сучасні дослідження у вказаній сфері серед провідних країн світу. Одним із методів для застосування є алгоритм розпізнавання облич EIGENFACE. Розглянуто перспективи використання нейронних мереж, штучного інтелекту, виконано огляд особливостей навчання штучної нейронної мережі й алгоритму EIGENFACE для застосування в системі багатофакторної автентифікації та запропоновано етапи для вдосконалення цього алгоритму на основі теорії нечітких множин. У роботі з'ясовано, що таке нейронна мережа, штучний нейрон, роботу алгоритму розпізнавання Eigenface, оскільки знання принципу роботи алгоритму значно полегшує застосування на практиці, розглянуто процес навчання з метою подальшої можливої реалізації. Запропоновано додаткові етапи вдосконалення алгоритму за допомогою теорії нечітких множин, яка стає потужним інструментом для побудови інтелектуальних апаратно-програмних систем розпізнавання образів. Упровадження в алгоритм нечіткого фільтра обчислює нечіткий приріст, так що зображення стають менш чутливими до локальних змін структур, меж об'єктів. Фільтр забезпечуватиме високий ступінь розрізнення між шумом і структурними об'єктами зображення. Сегментація дозволяє розбивати зображення на менші частини, що значно покращує розпізнавання системою.

Ключові слова: *захист інформації; автентифікація; ідентифікація; штучний нейрон; штучна нейронна мережа; нечіткі множини.*

1. ВСТУП

У сучасному глобалізованому суспільстві розвиток технологій і постійний обмін інформацією є основою прогресу. Важко уявити життя без засобів передачі інформації. Проблема захисту інформації є пріоритетною, а питання захисту інформації від витоку, несанкціонованого доступу – невід'ємна складова національної безпеки.

Системи зберігання стратегічно важливих даних є недосконалими, що наражає державу на

небзайнезпеку та на певному етапі поступається місцем у боротьбі розвідувальних служб іншим державам. За винятком цього, варто зазначити, що не тільки державні установи несуть відповідальність за витікання конфіденційної інформації про громадян.

Розвиток та інтеграція штучного інтелекту, машинного навчання нині є вагомим напрямком. У двох провідних держав світу – США та Китаю, розвиток штучного інтелекту є однією з першочергових задач. Найімовірніше, що протягом найближчого часу військові, розвідувальні й інші спеціальні структури триматимуть курс саме на розвиток упровадження використання систем на базі штучного інтелекту та машинного навчання. Потенціал для використання цих технологій у контексті безпеки досить об'ємний і мало досліджений.

На початку XXI століття до розв'язання завдань розпізнавання за біометричними даними під'єдналося безліч наукових лабораторій, найбільших результатів домоглися групи на чолі з професором Джоном Густавом Догманом у Кембриджському університеті (Велика Британія) та професором Кевіном Боуєром в Університеті Нотр-Дам (США), а також професором Уго Проенка – Університет Внутрішньої Бейри (Португалія), професором Адамом Чайка – Варшавська політехніка (Польща). Огляди [1–4] представляють понад 200 робіт із цієї тематики, і це лише незначна частина досліджень. У світі проблемами оброблення та розпізнавання зображень обличчя людини займаються: колектив лабораторії математичних методів обробки зображень факультету обчислювальної математики й кібернетики Московського державного університету імені М. В. Ломоносова під керівництвом професора А. С. Крилова, дослідницька група в Інституті фізики імені Б. І. Степанова Національної академії наук Білорусії під керівництвом доктора фізико-математичних наук Г. І. Желтова, Інститут систем оброблення зображень.

Проблеми розпізнавання за формою обличчя уважно вивчають дослідницькі групи у США (П. Дж. Флінн, А. Росс, Мічиганський державний університет), Англії, Португалії, Польщі, Білорусі. Системи розпізнавання за райдужною оболонкою ока розроблено фірмами IriTech, LG, OKI, Panasonic, Sagem, Neurotechnology, Morpho.

У зв'язку зі збільшенням кількості біженців із зон ведення бойових дій (Сирія, Ірак, Лівія) й активним упровадженням біометричних технологій по Russian Society of Appraisers для їхньої реєстрації виникають проблеми через постійне збільшення об'єму бази даних еталонів і, як наслідок, збільшення часу ідентифікації та автентифікації, а також важливою проблемою є робота системи в режимі один до багатьох [1–4].

Актуальність теми дослідження. Автентифікація людини, тобто підтвердження того, що особа є тим, за кого себе видає, поза всяких сумнівів є актуальним завданням, практичним розв'язанням якого зайняті тисячі й мільйони людей по всьому світу.

Варіанти можливих реалізацій:

- інструменти для аналізу даних у величезному обсязі та з нескінченними можливостями до самовдосконалення через залучення машинного навчання;
- система авторизації на основі нейронних мереж;
- оптимізація роботи систем за допомогою вираховування оптимальних і найшвидших варіантів дій;
- поліпшення захисту існуючих систем методом пошуку в них прогалин за допомогою штучного інтелекту;
- моделювання потенційних ситуацій за допомогою штучного інтелекту та машинного навчання під час підготовки кадрів [5].

Основним завданням алгоритму розпізнавання облич є його впровадження в систему автентифікації для вдосконалення методів захисту інформації, а також зменшення ризиків входження в систему неавторизованих користувачів. Історично в інформаційній сфері сформувалися два напрями захисту від несанкціонованого доступу, які в системах фізичного захисту називають системами управління доступом (СУД), а в комп'ютерній сфері – системами ідентифікації та автентифікації.

Автоматизація цих процесів, зокрема і за допомогою новітніх технологій – важлива складова розвитку сучасного суспільства. Те ж саме можна сказати і про завдання ідентифікації, тобто встановленні особи людини шляхом пошуку його запису в базі даних. Розвиток систем комп'ютерного зору, цифрового оброблення зображень, збільшення потужності обчислювальних засобів останнім часом дало можливість ставити і розв'язувати задачі автоматичної реєстрації, виокремлення, розпізнавання складних, часто змінюваних, важко модельованих і формалізованих об'єктів як біометричних ознак живих організмів. Таким чином, завдання автентифікації та ідентифікації людини тепер вирішуються за допомогою автоматичних біометричних систем, складаючи одну з нових областей прикладної математики, біометричну ідентифікацію.

Ідентифікацію і автентифікацію можна вважати основою програмно-технічних засобів безпеки

тому, що решту сервісів розраховують на обслуговування іменованих суб'єктів. Ідентифікація і автентифікація – це перша лінія захисту інформаційного простору комп'ютерної системи. Саме від коректності розв'язання цих двох завдань залежить, чи можна дозволити доступ до ресурсів системи конкретному користувачеві. Система захисту виконує ідентифікацію та автентифікацію на основі певної унікальної інформації, яка характеризує конкретного користувача системи [6].

2. ПОСТАНОВКА ЗАДАЧІ

Одним із головних напрямів розвитку захисту інформації є вдосконалення існуючих і створення нових систем і засобів, які б задовольняли основні властивості інформації: конфіденційність, цілісність, доступність.

Біометричний підхід вважають одним із найактуальніших у системах ідентифікації та автентифікації. В основі цього методу лежить аналіз унікальних характеристик людини. Його умовно поділяють на фізіологічний і поведінковий методи. Прикладами для фізіологічних можуть слугувати: відбитки пальців, малюнок райдужної оболонки ока, розпізнавання обличчя, долонь рук, сітківки ока тощо, а для поведінкових: підпис, рукописний, клавіатурний почерк, натискання на клавіатуру [7].

Розпізнавання обличчя є важливим завданням, адже є першим етапом ідентифікації. Щоб виявити, кому належить обличчя і чи є воно в базі даних, спочатку потрібно його локалізувати. Для розв'язання такої задачі застосовують різні підходи, серед них: емпіричні методи, метод на основі навчання, метод на основі порівняння із шаблоном, метод на основі контурних моделей. Під час розпізнавання обличчя системі, яка розв'язує задачу, необхідно врахувати сукупність факторів: відмінності облич різних людей, зміна ракурсу обличчя, можливість наявності певних особливостей, зміна виразу обличчя, наявність перешкод на зображенні, що можуть частково перекривати об'єкт, умови зйомки.

Штучний інтелект є як полем для розвитку, так і викликом. Зважаючи на той факт, що розробки машинного навчання та штучного інтелекту часто орієнтовані на оброблення великих масивів даних, а алгоритми машинного навчання прямо залежать саме від якості інформації, яку він обробляє, то втручання та дезінформація можуть вивести з ладу подальшу роботу алгоритму, що може призвести до неправильних висновків, у коректності яких буде важко переконатися, оскільки великі масиви даних. Вибір методу для розв'язання задачі виявлення обличчя залежить від конкретної задачі й умов, в яких повинен функціонувати алгоритм [8].

Метою цієї роботи є аналіз існуючого алгоритму розпізнавання облич на основі нейронних мереж Eigenface та його вдосконалення на базі теорії нечітких множин для підвищення рівня захищеності систем багатофакторної автентифікації у ході використання за рахунок більш надійних методів автентифікації користувачів.

3. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Сучасні дослідження показують, що на основі нейронної мережі можна побудувати систему розпізнавання обличчя людини по зображенню. У нових методах виокремлення ключових ознак для опису об'єкта здійснюється шляхом автоматичного аналізу навчальної вибірки. Проте більша частина інформації щодо ознак вводиться вручну. Для автоматичного застосування таких аналізаторів вибірка має бути досить великою та охоплювати всі можливі ситуації. Головний принцип системи розпізнавання – представити вхідні зображення у вигляді однієї спільної матриці, яка буде складатися із суми базисних компонент зображень.

Штучні нейронні мережі різної топології застосовують для розв'язання різних задач, саме наявність багатьох типів мереж забезпечує їхнє широке використання у різних сферах для розв'язання задач розпізнавання, прогнозування, класифікації, ідентифікації та багатьох інших. З використанням нейронних мереж вирішується проблема проєктування й оптимізації мереж зв'язку, тобто знаходження оптимального шляху трафіка між вузлами, а також для отримання ефективних рішень у галузі їхнього проєктування.

Із часів фундаментальної роботи Віоли та Джонса прискорений каскад із простими ознаками залишається найбільш популярним та ефективним підходом у розробленні програм для практичної детекції облич. Проста природа ознак дозволяє швидко оцінювати і рано відкидати неправильні результати пошуку. Тим часом, прискорений каскад створює групу простих ознак для досягнення точної класифікації облич [9]. Оригінальний детектор Віоли – Джонса використовує ознаки Хаара, які швидко вираховуються, та їх достатньо для опису фронтальних зображень облич. Тим не менш, через простоту ознак Хаара алгоритм відносно слабкий у неконтрольованому середовищі.

В останні роки спостерігається сплеск уваги до нейронних мереж. Посилений інтерес виник, коли Алекс Крижевський за допомогою конвуляційних нейронних мереж переміг у конкурсі ImageNet, понизивши рекорд помилок у класифікації з 26 % до 15 %, що тоді стало проривом.

Сьогодні "глибоке навчання" є основою багатьох систем великих компаній: Facebook використовує нейронні мережі для алгоритмів автоматичного виставлення тегів, Google – для пошуку серед фотографій користувача, Amazon – для генерації рекомендацій товарів, Pinterest – для персоналізації домашньої сторінки користувача, а Instagram – для пошукової інфраструктури.

Задача автоматичного розпізнання облич нині є досить актуальною і через велику кількість наукових досліджень цього питання, і через великий потенціал використання вказаної технології у комерційних проєктах [10].

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для ефективного використання алгоритму розпізнавання необхідно додатково забезпечити як мінімум один етап, а саме вдосконалити якість зображення шляхом фільтрації шумових складових і сегментації або кластеризації.

У статті пропонується аналіз проблеми ефективного розпізнавання облич та її розв'язання за рахунок використання систем штучного інтелекту на базі нечітких множин в алгоритмі Eigenface, оскільки якість результату розпізнавання залежить від ракурсу, положення, умов освітленості приміщень і поворотів відносно осей.

Штучний нейрон – вузол штучної нейронної мережі, що є спрощеною моделлю природного нейрона. Математично, штучний нейрон зазвичай представляють як деяку нелінійну функцію від єдиного аргументу – лінійної комбінації всіх вхідних сигналів.

Штучна нейронна мережа – це набір шарів із так званими штучними нейронами. Штучний нейрон (рис. 1) імітує властивості біологічного нейрона. На вхід штучного нейрона надходить деяка множина сигналів (координат): x_1, x_2, …, x_n, кожний з яких є виходом іншого нейрона. Кожен вхід множиться на відповідну синаптичну вагу w_1, w_2, …, w_n [11, 12].

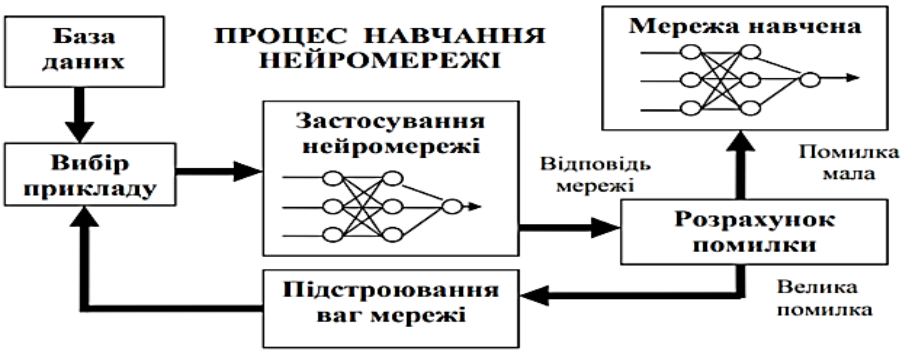


Рис. 1. Процес навчання нейронної мережі

Усі добутки підсумовують, визначаючи рівень активації нейрона NET. Далі сигнал NET перетворюється активаційною функцією F і дає вихідний нейронний сигнал OUT. Активаційна функція може бути лінійною функцією, логічною функцією [13] або функцією гіперболічного тангенса.

Залежно від способу передавання результатів активаційній функції по нейронних шарах нейронні мережі ділять на різні класи.

Оскільки всі штучні нейронні мережі базуються на концепції нейронів, з'єднань і переданих функцій, існує подібність між різними структурами або архітектурами нейронних мереж. Більшість змін походить із різних правил навчання. Нейромережі складені з простих елементів, що діють паралельно. Можна навчити нейромережу, регулюючи значення ваг між елементами. Зазвичай мережа регулюється або навчається так, щоб приватний вхід вів до цільового виходу [15]. На рис. 2 представлено процес навчання нейронної мережі [16].

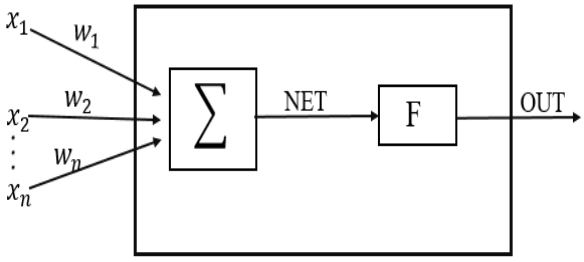


Рис. 2. Структура штучного нейрона

Система, яка виконує нечітке оброблення, має дві основні особливості: по-перше, нечіткий фільтр обчислює нечіткий приріст таким чином, щоб він був менш чутливим до локальних змін структур зображення, таким як кордони об'єктів. По-друге, функція приналежності формується так, щоб адаптуватися до шумових складових для виконання нечіткого згладжування (передбачається, що шум рівномірно розподілений по всьому зображенню). Основна ідея нечіткого фільтра така: значення пікселя визначають залежно від значень навколишніх сусідніх пікселів. Фільтр повинен забезпечувати високий ступінь розрізнення між шумом і структурними об'єктами зображення. Щоб вирішити це завдання для кожного пікселя обчислюється оціночний ступінь, який характеризує те, наскільки великий або малий приріст у певному напрямку. Конструювання нечіткого фільтра базується на такому спостереженні: малий нечіткий приріст відповідає шуму, великий нечіткий приріст – межам об'єктів.

Просте збільшення центрального пікселя (x, y) у напрямку *D(D€ {NW,N,NE,E,SE,S,SW,W})* визначається як різниця між пікселем із координатами (x, y) і одним із сусідніх пікселів у напрямку D. Значення збільшення позначається $\nabla_{D(x,y)}$, наприклад:

$$\nabla_N (x, y) = I(x,y-1) - I(x, y), \quad (1)$$

$$\nabla_{SW} (x, y) = I(x-1,y+1) - I(x, y). \quad (2)$$

Якщо два значення збільшень із трьох малі, то можна припустити, що в цьому напрямку відсутні межі об'єктів. Таким чином, щоб визначити нечіткий приріст, потрібно розглянути його якісне поняття мале. Цьому поняттю в рамках теорії нечітких множин відповідає нечітка множина мале. Функція приналежності m_k (u) поняття мале може визначатися як

$$m_k(u)=\begin{cases} 1-\frac{|u|}{k}, & 0 \le |u| \le k, \\ 0, & |u| > k \end{cases} \quad (3)$$

де *k* – адаптивний параметр. Графік виразу побудовано на рис. 3а.

Рис. 3. Функції приналежності якісних понять: а) мале; б) позитивне; в) негативне

Значення нечіткого збільшення для пікселя в напрямку NW обчислюється за такими правилами:

if (∇_{NW}(x,y) мале) and (∇_{NW}(x–1,y+1)) мале)

or (∇_{NW}(x,y) мале) and (∇_{NW}(x+1,y–1) мале)

or (∇_{NW}(x–1,y+1) мале) and (∇_{NW}(x+1,y–1) мале)

then ∇^F NW (x,y) мале. (4)

Вісім таких нечітких правил застосовуються для кожного з напрямків. Як уже згадано раніше, щоб виконати нечітку фільтрацію зображення необхідно усунути шумові складові пікселів шляхом модифікації значень пікселів, тому позначимо модифікаційний параметр difX. Для обчислення значення difX використовуємо пару нечітких правил для кожного напрямку. Сутність цих правил полягає в наступному: якщо передбачається відсутність меж об'єкта в певному напрямку, то чітке значення приросту в цьому напрямку може бути використано для обчислення модифікаційного значення difX.

Відповідно перша частина функціонування алгоритму фільтрації зображень – виявлення меж структурних об'єктів, може бути реалізована у вигляді нечіткого збільшення, друга частина алгоритму повинна бути реалізована у вигляді схеми, яка здатна розрізняти позитивне і негативне значення для нечіткого збільшення:

λ^+_{NW}: if (∇^F NW (x,y) мале) and (∇_{NW} (x,y) позитивне)

then c – позитивне

λ^-_{NW}: if (∇^F NW (x,y) мале) and (∇_{NW} (x,y) негативне)

then c – негативне. (5)

Останній крок – дефазифікація результату: необхідно визначити модифікаційне значення difX, яке буде додано до поточного значення пікселя:

$$\Delta = \frac{L}{8} \sum_{Dedir} (\lambda^+_D - \lambda^-_D), \quad (6)$$

де *D* – означення напрямку, *L* – кількість градацій сірого.

Таким чином, розглянуто перший етап, який має виконувати система розпізнавання образів. Варто зауважити, що цей етап є дуже важливим, тому що багато в чому саме від якості попередньо обробленого зображення залежить стабільна роботи системи в цілому. Наступний етап пов'язаний із сегментацією і виокремленням контурів об'єктів. Мета етапу – знаходження об'єкта на зображенні [17].

В основу алгоритму Eigenface покладено використання фундаментальних статичних характеристик: середніх (математичне очікування) та коваріаційної матриці, застосування методу головних компонент. Як і будь-який інший алгоритм сфери комп'ютерного навчання (machine learning), його необхідно спершу навчити первинній виборці (training set), яка складається з певної кількості зображень облич, які хочемо розпізнавати. Як тільки модель стане навченою, слід подати на вхід деяке зображення і в результаті отримаємо відповідь на питання: якому зображенню із загальної вибірки з найбільшою вірогідністю відповідає дане та чи належить дане зображення виборці взагалі.

Головний принцип алгоритму – представити вхідні зображення у вигляді однієї спільної матриці, яка буде складатися із суми базисних компонент зображень:

$$\Phi_i = \sum_{j=1}^{K} w_j u_j, \quad (7)$$

де Φ_i – відцентроване зображення обличчя, w_j – ваги, u_j – власні вектори.

Маючи w як ваговий коефіцієнт вибраної значущої частини обличчя та u як вибрану ділянку обличчя, вибір необхідної ділянки обличчя можливо описати процесом сегментації. Процес сегментації – це процес, у ході якого відбувається розбиття зображення на складові об'єкти. Причому зазвичай використовується таке формальне визначення. Нехай F – це позначення сітки всіх пікселів зображення, тобто набір усіх пар:

$$F_{MxN} = \{(i,j)\} : i = 1,2,\dots,N; j = 1,2,\dots,M.$$

При цьому $\bigcup_{i=1}^{N} \mathrm{Fi} = \mathrm{F}, \mathrm{Fi} \cap \mathrm{Fj} = 0, i \neq j$ [18].

Система сегментації складається з багатошарового персептрона, який виконує адаптивну багаторівневу сегментацію, використовуючи мітки, отримані за допомогою методу нечіткої кластеризації. Ваги нейронної мережі не можуть бути ініційовані випадковим числом, усі вони встановлюються в 1. Щоб забезпечити більше двох стабільних станів на виході нейрона, розроблена спеціальна функція активації. Ця функція складається з набору сигмоподібної функції з множинними рівнями. Мультисигмоїда утворюється шляхом суперпозиції зсунутих сигмоїдальних функцій і виражається в такий спосіб:

$$f(x) = \sum_{k} \left(\frac{y_k - y_{k-1}}{1 + e^{-\frac{(x-\theta_k)}{\theta_0}}} + y_{k-1} \right) \times$$
$$\times [u(x - y_{k-1} \cdot d^a) - u(x - y_k \cdot d^a)], \quad (8)$$

де u – крокова функція, θ_k – пороги, y_k – цільовий рівень кожної сигмоїди, θ_0 – параметр крутизни, d – ступінь сусідства, a – параметр активності сусідства. Пороги і цільові величини виводяться з функції помилки. Оскільки діапазон значень стану нейронів вхідного шару залежить від кількості нейронів наступного шару, то значення порогів адаптовані таким чином, щоб відображати цю залежність [19].

Нейронна мережа працює з інтенсивностями пікселів. Іншими словами, мережа не змінює значення нечіткої приналежності пікселів для того, щоб зменшити помилку, а замість цього вона відображає початкові значення пікселів на такі значення, які зменшують середню кількість нечіткості відповідно до початкового розподілу. Таким чином, вихід нейронної мережі спочатку розглядається в термінах сірого кольору, який далі перетворюється на нечіткість для визначення помилки. Інформація про значення приналежності пікселів може бути корисна в подальшому залежно від призначення системи.

5. ВИСНОВОК

Узагальнюючи викладене, можна зробити такі висновки: розвиток технологій штучного інтелекту та машинного навчання розпочав нову добу розвинення суспільства, орієнтованість провідних країн світу зумовлює значне пришвидшення цього процесу і тягне за собою як наслідок трансформацію всього світового порядку. Роль цифрового виміру та безпеки цифрової інформації стає все більш значущою і її важливість зростатиме разом із цифровізацією світу, тому одним із вагомих питань безпеки є інформація та її захист, пошук нових шляхів та вдосконалення тих, що вже існують. У цій роботі з'ясовано, що таке нейронна мережа, штучний нейрон, описано роботу алгоритму розпізнавання Eigenface, оскільки розуміння принципу роботи алгоритму значно полегшує застосування на практиці, також розглянуто перспективи розвитку цих мереж і важливість у наш час, навчання з метою подальшої можливої реалізації. Запропоновано додаткові етапи вдосконалення алгоритму за допомогою теорії нечітких множин, яка стає потужним ін-

струментом для побудови інтелектуальних апаратно-програмних систем розпізнавання образів. Упровадження в алгоритм нечіткого фільтра обчислює нечіткий приріст, так що зображення стають менш чутливими до локальних змін структур, меж об'єктів. Фільтр забезпечуватиме високий ступінь розрізнення між шумом і структурними об'єктами зображення. Сегментація дозволяє розбивати зображення на менші частини, що значно покращує розпізнавання системою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Журавель И. Краткий курс теории обработки изображений [Електронний ресурс]. – Режим доступу: http://matlab.exponenta.ru/ imageprocess/index.php.

[2] Вежневец А. Методы сегментации изображений: автоматическая сегментация / А. Вежневец, О. Баринова // Сетевой журнал Компьютерная графика и мультимедия. 2006. [Електронний ресурс]. – Режим доступу: http://cgm.computergraphics.ru/ content/view/147.

[3] Bowyer K.W., Hollingsworth K., Flynn P.J. A Survey of Iris Biometrics Research: 2008-2010, in Handbook of Iris Recognition, Mark Burge and Kevin W. Bowyer, editors, Springer, 2012.

[4] Boyd M., Carmaciu D., Giannaros F., et al. MSc Computing Science Group Project Iris Recognition. Imperial College, London. 2010.

[5] Макс Тегмарк "Життя 3.0. Доба штучного інтелекту" / пер. з англ. Зорина Кораблiна. Видавництво "Наш формат", 2019. Розділ 3, підрозділ "Зброя" та "Кібервійна". С. 137–147.

[6] Основы компьютерной безопасности: курс лекций. Учебное пособие (издание третье). Галатенко В.А. Под редакцией академика РАН В.Б Бетелина. – М.: ИНТУИТРУ "Интернет университет Информацион-ных технологий", 2006. – 208 с.

[7] Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; Перевод с английского под редакцией А.Н. Берлина. – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. – 784 с.: ил., табл. – (Основы информационных технологий). (465–467).

[8] https://bintel.org.ua/nukma/shtuchnij-intelekt-i-rozvidka/ – "How to Win the Battle Over Data. The United States Dithers While Authoritarians Seize the Day" by Eric Rosenbach and Katherine Foreign Affairs. September 17, 2019. Режим доступу: https://www.foreiqnaffairs.com/articles/2019-09-17/how-win-battle-over-data.

[9] P. A. Viola and M. J. Jones. Rapid object detection using a boosted cascade of simple features. In Proc. IEEE Conference on Computer Vision and Pattern Recognition, 2001.

[10] Krizhevsky A., Sutskever I., Hinton G. E. Imagenet classification with deep convolutional neural networks //Advances in neural information processing systems. –2012. – С. 1097–1105.

[11] The Artificial Neural Networks Handbook: Part 4: вебсайт. URL: https://dzone.com/articles/the-artificial-neural-networks-handbook-part-4.

[12] What is an artificial neuron and why does it need an activation function? [Електронний ресурс]. – Режим доступу: https://towardsdatascience.com/what-is-an-artificial-neuron-and-why-does-it-need-an-activation-function-5b4c1e971d80.

[13] Активаційні функції [Електронний ресурс]. – Режим доступу: http://um.co.ua/1/1-1/1-12496.html.

[14] Моделі нейронних мереж [Електронний ресурс]. – Режим доступу: [https://dl.khadi.kharkov.ua/mod/page/view.php?id=106611&forceview=1].

[15] Навчання нейронної мережі [Електронний ресурс]. – Режим доступу: http://um.co.ua/10/10-7/10-78023.html

[16] Простими словами про складні: Що таке нейронні мережі? [Електронний ресурс]. – Режим доступу: https://phoneinfo8.info/prostimi-slovami-pro-skladni-sho-take-neironni-mereji/.

[17] Farbiz F. Fuzzy Techniques in Image Processing / F. Farbiz, B. Menhaj // New York: Springer-Verlag, vol. 52, Studies in Fuzziness and Soft Computing, ch. A fuzzy logic control based approach for image filtering. – 2000. – pp.194 – 221.

[18] Сарапулов Віктор Сергійович Дослідження EIGENFACE алгоритму розпізнавання обличь та його реалізація у MATLAB середовищі. Міжнародний науковий журнал // № 5, 2016.

[19] V. Boskovitz, H. Guterman. An Adaptive Neuro-Fuzzy System for Automatic Image Segmentation and Edge Detection // IEEE TRANSACTION ON FUZZY SYSTEM, VOL.10, NO.2, APRIL 2002.

Стаття надійшла до редколегії **07.06.2021**

Multifactor authentication system based on neural networks

The biometric approach is considered one of the most relevant in identification and authentication systems. The biometric method is based on the analysis of unique human characteristics. Face recognition is an important task, because it is the first stage of identification, to find out who owns the face and whether it is in the database, you must first locate it. To solve this problem, different approaches are used among them: empirical methods, method based on learning, method based on comparison with a template, method based on contour models. When recognizing a face, the system that solves this problem must take into account a number of factors: differences in the faces of different people, changing the angle of the face, the possibility of certain features, changing facial expressions, the presence of obstacles in the image that may partially obscure the subject. Artificial intelligence is both a field for development and a challenge. Due to the fact that the development of machine learning and artificial intelligence is often focused on processing large data sets, and machine learning algorithms directly depend on the quality of the information it processes, interference and misinformation can disable further operation of the algorithm, which can lead to incorrect conclusions, the correctness of which will be difficult to verify because of the large data sets. The choice of method for solving the problem of face detection depends on the specific problem and the conditions in which the algorithm should operate.In this article the possibilities of neural networks for application in the system of multifactor authentication are considered and analyzed. Options for possible implementations using an artificial network, prospects for the development of these networks and the importance in our time are considered. Modern research in this field among the leading countries of the world is analyzed. One of the methods for application is the EIGENFACE face recognition algorithm. Prospects for the use of neural networks, artificial intelligence, review of the features of learning artificial neural network and algorithm EIGENFACE for use in multifactor authentication and proposed steps to improve this algorithm based on fuzzy set theory. The paper clarified what a neural network, an artificial neuron, the operation of the Eigenface recognition algorithm is, because knowledge of the principle of the algorithm greatly facilitates its application in practice, the learning process is considered for further possible implementation. Additional stages of algorithm improvement with the help of fuzzy set theory are offered, which becomes a powerful tool for building intelligent hardware and software pattern recognition systems. The introduction of a fuzzy filter into the algorithm calculates the fuzzy increment so that the images become less sensitive to local changes in structures, boundaries of objects. The filter will provide a high degree of distinction between noise and structural objects of the image. Segmentation allows you to split images into smaller parts, which greatly improves system recognition.

Keywords: *information protection, authentication, identification, artificial neuron, artificial neural network, fuzzy sets.*

Олег Кулінич,
кандидат технічних наук, доцент, Інститут спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

Oleg Kulinich,
Candidate of Technical Sciences, Associate Professor, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine.

Анастасія Роскот,
курсант Інституту спеціального зв'язку та захисту інформації Національний технічний університет України "Київський політехнічний інститут", Київ, Україна.

Anastasia Roskot,
cadet at the Institute of Special Communications and Information Protection, National Technical University of Ukraine, Kyiv Polytechnic Institute, Kyiv, Ukraine.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

UDC 004.931004.94
DOI https://doi.org/10.17721/ISTS.2021.1.61-67

D. N. Andriievskyi, orcid.org/0000-0002-7644-9328,
hoku.dev01@gmail.com
V. L. Shevchenko, orcid.org/0000-0002-7435-3533,
gii2014@ukr.net
V. Petrivskyi, orcid.org/0000-0001-9298-8244,
vovapetrivskyi@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

MOBILE APPLICATION DEVELOPMENT FOR BLIND PEDESTRIANS TO PREVENT ROAD DANGERS

According to the last statistic researches approximately more than one billion people worldwide live with some form of visual impairment. In turn, visual impairments limit people's ability to perform daily functions and affect their quality of life and ability to interact with the world around them. In the article mobile application development for blind pedestrians to prevent road dangers is presented. Short overviews of similar applications like Alexa, Via Opta Nav, and Object Detector are described. Each of described programs has disadvantages like limited use area, real-time object detection absence, use third-party or physical devices need. As a result, the main task of the study is to investigate modern hazard classification algorithms, improve the accuracy of the algorithm and develop software that will be able to identify hazards in real-time, does not require physical devices, and is operated using the simplest possible interface. For solving presented above problem solution based on MobiNetV2 and InceptionV3 open-source models for defining objects in a photo modification is presented. The presented solution consists of several steps like image input with further preprocessing, optimization and result processing. For the image input hosts receive data from the file system or local memory, perform any preprocessing, and then transmit the preprocessed data to the TPU cores. Preprocessing calls the parser, which in turn calls the parser function, where images are preprocessed. For the optimization stochastic gradient descent optimization and momentum optimizer are used. As a result, method of image classification for real-time hazard identification has been further developed. A model layer was developed that interprets the unbalanced results of the model and provides the necessary results to prevent accidents, which increased accuracy by 20%. A mobile application for road hazard recognition for blind pedestrians has been developed using the above. Presented results confirm the efficiency of the described approach. Also, described model and approach can be improved in further investigations.

Keywords: *image processing; road conditions; pedestrian safety; danger determining; visual impairments.*

1. INTRODUCTION

Visual impairments can limit people's ability to perform daily functions and affect their quality of life and ability to interact with the world around them. Blindness, the most severe form of visual impairment, limits people's ability to perform daily functions and move without assistance. Rehabilitation of proper quality allows people with visual impairments to varying degrees to enjoy life, achieve goals, be active and productive in today's society.

It is estimated that approximately 1.3 billion people worldwide live with some form of visual impairment. In terms of long-distance vision, mild visual impairments are observed in 188.5 million people, from moderate to severe - in 217 million, while 36 million people are affected by blindness. As for nearby vision, 826 million people live with such visual impairments.

On Tuesday, on the eve of World Vision Day (2019), which is celebrated on October 10, experts

published for the first time a detailed report on vision problems. Its authors conclude that the number of visually impaired and blind people is increasing, in particular due to limited access to relevant health services in low- and middle-income countries.

2. ANALYSIS OF EXISTING STUDIES AND TASK STATEMENT

2.1. EXTENSION SHOW AND TELL FOR ALEXA

Short Description: Amazon has expanded the capabilities of the audio assistant, and now a visually impaired user can bring the item to the gadget and ask Alex what it is. Currently, this feature is only available to users in the US who use Echo Show devices [1].

The disadvantages are access only for the United States and the fact that you need to have a physical device to use.

2.2. VIA OPTA NAV

Short description: An application with step-by-step navigation. Despite the fact that the application has a slightly different direction, we could not skip such an important product. This program was developed in partnership with visually impaired users [2].

You can add waypoints to the map to increase the accuracy of the route. At any time, the user can specify the location, the remaining distance and get a description of the streets crossing the route. Even with the screen reader turned off, the program voices the necessary information using the built-in function of text-to-speech. The application was developed by the medical corporation Novartis [2].

The disadvantage is that it is still a slightly different but related direction and therefore the application does not contain the functionality of real-time object detection.

2.3. OBJECT DETECTOR

Short description: The application allows the blind user to navigate in space, determine which objects are nearby, which road signs are nearby and inform about doors and ladders. This is the most related application, which was relied on almost all the time of development [3].

The application uses intelligent algorithms to identify objects. How it works: you need to launch the application, select the mode "Signs", "Objects" or "Doors and stairs", bring the camera of the smartphone in front of you, the result is displayed in visual (high contrast letters), sound (voice assistant) and tactile (special vibrations for selected objects) forms. The application can be used by both blind and deafblind people. The application supports voice assistant and Braille displays [3].

The disadvantages are a rather complex interface, many options and the inability to identify multiple groups of objects in real time.

The most important drawback that is present in all competitors is the complexity of the interface. A blind person cannot see the buttons on the screen and is unlikely to navigate the program. The goal is to avoid confusing the interface or interrupting object recognition just because the user has moved to another part of the application. It is better if there are few buttons and the best option – when there are no buttons at all. The user launches the application and immediately begins to perform the main function – a warning of danger.

An equally important disadvantage is the need to use third-party and/or physical devices. Firstly, not all blind people have the money to buy devices, as it is difficult for people with visual impairments to find work. Secondly, although a physical device has (or may have) relatively high accuracy, it can fail and give more error than the device's camera. And if the camera of the device fails, the application will not work, and it will not create an error of malfunction.

The main task of the study is to investigate modern hazard classification algorithms, improve the accuracy of the algorithm and develop software that will be able to identify hazards in real time, does not require physical devices and is operated using the simplest possible interface. The software must be implemented using widely available mobile devices and adapted for use on special embedded processors.

3. DESCRIPTION OF THEORETICAL METHODS USED

There are currently many models for defining objects in a photo, some of which are open-source ML models that can be integrated into the iOS app. These models have similar functionality, but different data sets, so they may produce different results. But the study identified two main ones –MobiNetV2 and InceptionV3. The first is advertised by Apple in its object recognition instructions [4], and the second has a well-known developer – Google. The second model was used during the work as it has a higher level of confidence, and the error in the results is unacceptable.

InceptionV3 is an image classification model, which has many different classifiers in implementation (or "under the hood"). This provides a fairly high accuracy of object recognition, but due to their large variety on the streets, can give an error. There-

fore, to ensure an accurate result, two methods were investigated – input image processing and processing of model results.

Input image processing. This method did not work very well as it did not bring any statistical improvement. His main idea is to change the image according to some criteria:

- RGB tone change (increase of red, blue and/or green dots),
- cleaning background and secondary colors, highlighting image borders.

However, due to the great complexity of the images, such processing gives unexpected results and more often gives an error due to the fact that the error of the basic model is added to the error of preprocessing. Due to this, the processing of the input image was rejected.

Processing of model results. This method does not increase the error because it does not affect the results of object definition at all, but only processes them. The method searches for and ranks keywords for each hazard by:

- hazard priority,
- detection position.

Also, a very important part of the task is the definition of different groups of hazards at the same time, because the existing implementations of hazard identification in the movement of a blind pedestrian are aimed at only one group (e.g., road signs, ladders, etc.).

Inception v3 is a widely used image recognition model that has been shown to achieve an accuracy of over 78.1% in the ImageNet dataset. (The lowest error rate was obtained, giving the model first place in the image classification in ILSVRC (ImageNet Large Scale) 2015. ImageNet is a data set of more than 15 million high-resolution images from approximately 22,000 categories. ILSVRC uses a subset of ImageNet of about 1000 images in each of 1000 categories [5].

The model is the culmination of many ideas developed by many researchers over the years. It is based on the original work: "Rethinking the original architecture for computer vision" Szeged and others [5].

The model itself consists of symmetrical and asymmetrical building blocks, including convolutions, middle joints, maximum joints, concates, screenings, and fully bonded layers. Losses are calculated using Softmax [6].

The TPU version of Inception v3 is written using the TPUEstimator, an API designed to facilitate development, so you can focus on the models themselves rather than the basic hardware details. The API performs most of the low-level grunge work required to run TPU models behind the scenes, while automating common features such as saving and restoring checkpoints [6]. Proposed approach can be seen as a part of an Internet of Things [7] technologies. Besides that, Big Data can be transported in the network and pressing issue is such network stability [8, 9].

3.1. INPUT PROCESSOR

Each TPU cloud device has 8 cores and is connected to a host (CPU). Larger slices have multiple hosts. Other larger configurations interact with multiple hosts. For example, v2-256 communicates with 16 hosts [6].

Hosts receive data from the file system or local memory, perform any preprocessing, and then transmit the preprocessed data to the TPU cores. We consider these three steps of data processing performed by the host separately, and call them phases: 1) storage, 2) preprocessing, 3) transmission [6].

To ensure good performance, the system must be balanced. No matter how long the CPU takes to receive the images, decode them, and perform the appropriate preprocessing, it should ideally be slightly smaller or about the same as that spent by the TPU on the computation. If the CPU takes longer than the TPU to perform the three phases of data processing, then the execution will be associated with the host. (Note: Because TPUs are so fast, this may be unavoidable for some very simple models.) [6].

Storage begins with the creation of a data set and includes reading TFRecords from the repository. Nested data sets are created and their elements are displayed alternately [6].

Preprocessing calls the parser, which in turn calls the parser function, where images are preprocessed [6].

The transfer includes images that return a string, labels. TPUEstimator accepts the returned values and automatically transmits them to the device [6].

3.2 PREPROCESSING

Image preprocessing [10] is an important part of the system and can greatly affect the maximum accuracy that the model achieves during training. At a minimum, the image must be decoded and resized according to the model. In the case of the beginning of the image must be 299x299x3 pixels [6].

However, simple decoding and resizing will not be enough to get good accuracy. The ImageNet training data set contains 1,281,167 images. One passage through a set of educational images is called an epoch. During training, the model will need several passes through the training data set to improve its image recognition capabilities. In the case of Inception v3, the number of required epochs will be somewhere in the range of 140 to 200 depending on the total batch size [6].

It is extremely advantageous to constantly change the images before submitting them to the model, and do it in such a way that a particular image is slightly different in each era. On the one hand, a well-designed preprocessing step can significantly improve model recognition capabilities. On the other hand, too simple a pretreatment step can create an artificial ceiling with the maximum accuracy that the same model can achieve during training [6].

3.3. OPTIMIZER

The current model demonstrates the following optimizer options: SGD and momentum [6, 11].

Stochastic gradient descent (SGD) is the simplest type of optimization: the importance is pushed in the negative direction of the gradient. Despite its simplicity, some models can still get good results. The dynamics of updates can be written as follows [6, 11]:

$$w_{k+1} = w_k - \alpha \nabla f(w_k), \quad (1)$$

where w_{k+1}, w_k – importances, α – coefficient that is equal 0.9.

Momentum is a popular optimizer that often leads to faster convergence than SGD can achieve. This optimizer updates the importance, like SGD, but also adds a component in the direction of the previous update. The dynamics of the update is given by [6]:

$$z_{k+1} = \beta z_k + \nabla f(w_k), \quad (2)$$

where z_{k+1}, z_k – components in the direction of the previous update, β – coefficient that is equal 0.9, w_{k+1}, w_k – importances, α – coefficient that is equal 0.9.

In conclusion, we can say that this model is very functional and powerful, it is used in various spheres of life, but it cannot fully satisfy the condition of the problem. We need high accuracy for complex and object-laden images. Therefore, it was decided to develop and apply a service to process the results of the model.

3.4. MODEL RESULTS PROCESSION

As mentioned earlier, the program has a service processing results. Its main task is to process the results according to some criteria: priority of the result, level of danger, keywords and position in determining.

The essence of the proposed algorithm:

We have the set $Y = \{x_1, x_2, \dots, x_n\}$ containing model results.

First, we set two variables – precision and keywords. The model produces results in the form of an array of terms. We need to choose only the first few elements and do not waste time on the last elements. Therefore, we take only a certain number (precision) elements and receive the set $Y' = \{x_1, x_2, \dots, x_{Precision}\}$.

Keywords – a dictionary with keywords – objects of danger and values – arrays of keywords.

Then the essence is very simple – we go through all the values of the arrays of keywords in keywords (variable) in descending order of priority of the danger-key and look for the entry of texts with the original raw array.

Keywords' check:

$$\forall x \in Y'. \quad (3)$$

4. ANALYSIS OF RESULTS

During the work, the ability of the program to perform its main function, namely – determining the danger on the road for blind pedestrians was tested and the following results were highlighted in Table 1:

***Table* 1**

Results

Name	Service is turned off	Service is turned on	Total number
Correctly identified traffic lights	5	7	10
Mistakenly identified traffic lights	1	0	-
Not identified traffic lights	5	3	10
Traffic lights identification accuracy	50 %	70 %	100 %
Correctly identified autos	8	10	10
Mistakenly identified autos	2	0	-
Not identified autos	2	0	10
Auto's identification accuracy	80 %	100 %	100 %
Total accuracy	69.5 %	89.5 %	100 %

The table clearly shows the improvement of the results after turning on the service: the accuracy of traffic lights has increased by 20%, the accuracy of car detection – also by 20%. In addition, the number of misdiagnosed hazards has been reduced to 0. However, for different data sets, the increase in ac-

curacy may differ slightly for different objects. In this case, it is not entirely clear which is more important, the accuracy of traffic lights, or the accuracy of the car. For the general case, we enter weights that reflect the importance of each of the objects:

K1 = 0.35 – coefficient of traffic lights identification danger;

K2 = 0.65 – coefficient of autos identification danger.

These coefficients were chosen as such because the chance of stumbling on the roadway (car) of a blind pedestrian is higher than he has to stumble on a traffic light. The coefficients were determined by experts.

Next, we make a convolution of the multicriteria assessment of accuracy to scalar with the help of additive convolution [9]:

$$A = \sum_{i=1}^{2} d_i K_i, \qquad (4)$$

where d_i – hazard percentage.

Calculating the overall accuracy by formula 1:

$$A_{f_1} = 0.35 * 50 + 0.65 * 80 = 69.5,$$
$$A_{f_2} = 0.35 * 70 + 0.65 * 100 = 89.5,$$
$$\Delta A_f = A_{f_1} - A_{f_2} = 20.$$

So, we have a difference in overall accuracy of 20%.

As shown on the Figure 1, by turning on service accuracy increases in all aspects of hazard detection (both in traffic lights and autos). Graph shows accuracy with turned off service percentage of accuracy with turned on.

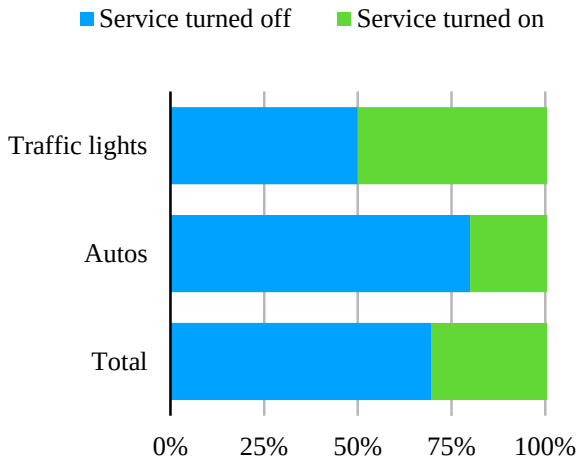


Fig. 1. Graph of improving the accuracy of hazard identification when turning on the service

During the work, a mobile iOS application was developed for the application of the above service in practice. The application uses the service and camera of the device to analyze the environment and danger messages.

The application contains 3 main components:

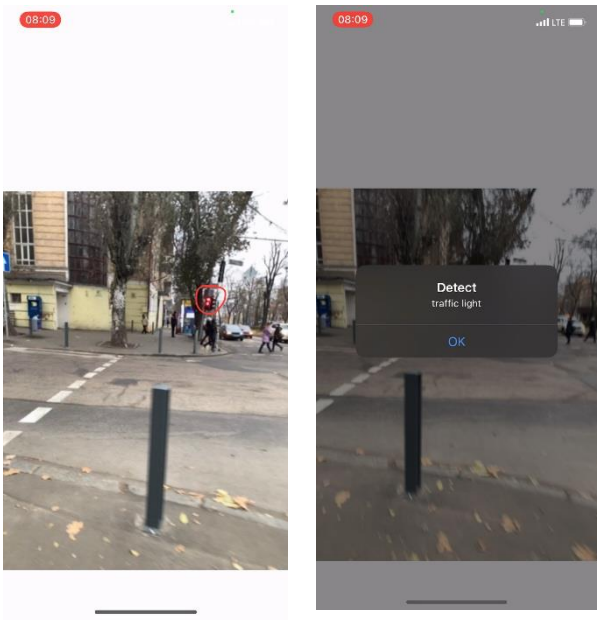
- UI-interface or user interaction part;
- Model results processing service;
- Inception V3 model.

The interface was designed to be as simple as possible so that visually impaired people would not find it difficult to use it.

Main goals of iOS application are:

- accuracy;
- scalability;
- simplicity.

As said before, iOS App has very simple interface. Also, service and its architecture were designed such as adding new road hazard type will not take much time. And great amount of accuracy was introduced by developing model result handler service.



a) b)

Fig. 2. Traffic light detection: a) a pedestrian approaches a traffic light; b) the program recognizes it and displays a warning

As shown on the Figure 2, mobile app can detect traffic light (hazard) in real time by using camera.

5. CONCLUSION

1. The method of image classification for real-time hazard identification has been further developed.

2. A model layer was developed that interprets the unbalanced results of the model and provides the necessary results to prevent accidents, which increased accuracy by 20%.

3. A mobile application for road hazard recognition for blind pedestrians has been developed using the above model and layer of work with it.

4. The application was tested under normal conditions for pedestrians, namely on city streets.

5. The application has a great extensibility, so in the future it is possible to easily add new types of hazards.

6. The software is implemented using widely available mobile devices and adapted for use on special embedded processors.

REFERENCES

[1] App Store, *Amazon Alexa App*, [Online]. Available at: https://apps.apple.com/us/app/amazon-alexa/id944011620

[2] App Store, *Nav by ViaOpta App*, [Online]. Available at: https://apps.apple.com/ua/app/nav-by-viaopta/id908435532?l=ru

[3] App Store, *Object detector App*, [Online]. Available at: https://apps.apple.com/ua/app/определитель-предметов/id1485796154?l=ru

[4] Apple, *Object detection tutorial*, [Online]. Available at: https://developer.apple.com/documentation/vision/classifying_images_with_vision_and_core_ml

[5] Sik-Ho Tsang, *Inception V3 description*, 2015, [Online]. Available at: https://sh-tsang.medium.com/review-inception-v3-1st-runner-up-image-classification-in-ilsvrc-2015-17915421f77c.

[6] Google, *Inception V3 description*, [Online]. Available at: https://cloud.google.com/tpu/docs/inception-v3-advanced.

[7] D. Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything, Cisco Internet Business Solutions Group, 2011, [Online]. Available at: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[8] V. Petrivskyi, G. Dimitrov, V. Shevchenko, O. Bychkov, M. Garvanova, G. Panayotova, P. Petrov, "Information Technology for Big Data Sensor Networks Stability Estimation," Information & Security: An International Journal, Vol. 47, Issue 1, pp. 141–154, 2020.

[9] M. Brazhenenko, V. Petrivskyi, O. Bychkov, I. Sinitcyn and V. Shevchenko, "Enabling Big Data Query with Modern CAD Systems Redundant Data Stores," in CADSM 2021, 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Lviv, Ukraine, February 22–26, 2021.

[10] H. Jeong, K. Park and Y. Ha, "Image reprocessing for Efficient Training of YOLO Deep Learning Networks," in 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), Shanghai, China, January 15–18, 2018, pp. 635–637.

[11] G. Panayotova, G.P. Dimitrov, P. Petrov and O. Bychkov, "Modeling and dataprocessing of information systems," in Artificial Intelligence and Pattern Recognition (AIPR), Xiamen, China, September 19-21, 2016, pp. 154–158.

Стаття надійшла до редколегії 10.06.2021

Розробка мобільних додатків для незрячих пішоходів для запобігання небезпекам на дорозі

Згідно з останніми статистичними дослідженнями більше мільярда людей у всьому світі мають певні вади зору. У свою чергу, порушення зору обмежують здатність людей виконувати щоденні функції і впливають на якість їхнього життя та здатність взаємодіяти з навколишнім світом. У статті представлено розробку мобільного додатка для незрячих пішоходів для запобігання небезпекам на дорозі. Описано короткий огляд подібних програм, таких як: Alexa, Via Opta Nav та Object Detector. Кожна з описаних програм має недоліки, наприклад, обмежена область використання, відсутність виявлення об'єктів у реальному часі, застосування сторонніх або фізичних пристроїв. Як результат, основним завданням цієї роботи є дослідження сучасних алгоритмів класифікації небезпек, підвищення точності алгоритму та розроблення програмного забезпечення, яке зможе ідентифікувати небезпеки в режимі реального часу, що не потребує фізичних пристроїв і експлуатується за допомогою максимально простого інтерфейсу. Для розв'язання описаної вище проблеми використано моделі з відкритим кодом MobiNetV2 та InceptionV3 для визначення об'єктів. Подане рішення складається з декількох етапів, таких як: введення зображення з подальшим попереднім обробленням, оптимізація та оброблення результатів. Для введення зображень хости отримують дані з файлової системи або локальної пам'яті, виконують будь-яке попереднє оброблення, а потім передають попередньо оброблені дані в ядра TPU. Попереднє оброблення викликає парсер, який у свою чергу, викликає функцію синтаксичного аналізатора, де зображення попередньо обробляються. Для оптимізації використовують стохастичну оптимізацію градієнтного спуску й оптимізатор імпульсу. У результаті дослідження отримав подальший розвиток метод класифікації зображень для ідентифікації небезпеки в режимі реального часу. Розроблено модельний шар, який інтерпретує незбалансовані результати моделі та забезпечує необхідні результати для запобігання аваріям, що підвищило точність на 20 %. Розроблено мобільний додаток із використанням наведеної вище моделі для розпізнавання небезпеки дорожнього руху для незрячих пішоходів. Представлені результати підтверджують ефективність описаного підходу. Крім того, описану модель і підхід можна вдосконалити в подальших дослідженнях.

Ключові слова: *оброблення зображень; умови роду; пішохідний сейф; визначення небезпеки; порушення зору.*

Denys Andriievskyi,
Bachelor student of Department of Program System and Technologies of Taras Shevchenko National University of Kyiv.

Денис Андрієвський,
бакалавр кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.

Viktor Shevchenko,
Dr. Sc., Professor,
Professor of Department of Program System and Technologies of Taras Shevchenko National University of Kyiv.

Віктор Шевченко,
доктор технічних наук, професор, професор кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.

Volodymyr Petrivskyi,
PhD student of Department of Program System and Technologies of Taras Shevchenko National University of Kyiv.

Володимир Петрівський,
аспірант кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.