МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ

ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

другого (магістерського) рівня вищої освіти

на тему: **«РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ КІБЕРФІЗИЧНИХ ОБ'ЄКТІВ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ»**

Виконав: студент 6 курсу групи ІТ-62
Спеціальності 126 – «Інформаційні системи та технології»
(шифр і назва)

Джуман В. Р.
(Прізвище та ініціали)

Керівник: Чаплига В. М.
(Прізвище та ініціали)

ДУБЛЯНИ-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Освітній ступінь «Магістр» за спеціальністю –
126 – «Інформаційні системи та технології»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри_____
д.т.н., проф. А.М. Тригуба
"____"_____2024_ р.

ЗАВДАННЯ

на кваліфікаційну роботу студенту

Джуман Володимир Романович

1. Тема роботи: **«Розробка інформаційної системи автентифікації кіберфізичних об'єктів агропромислового комплексу».**

Керівник роботи Чаплига Вячеслав Михайлович, д.т.н., професор.

Затверджені наказом по університету від «28» квітня 2023 р. № 133 /к-с.

2. Строк подання студентом роботи: 15.01.2024 року.

3. Початкові дані до роботи: Нормативно-правові документи, міжнародні на національні стандарти, завдання на розробку інформаційної системи автентифікації кіберфізичних об'єктів агропромислового комплексу.

4. Зміст пояснювальної записки:

Вступ.

Розділ 1. Аналіз технологічного процесу автентифікації кіберфізичних об'єктів агропромислового комплексу та його автоматизації.

Розділ 2. Дослідження та вибір методів і програмно-технічних засобів автентифікації кіберфізичних об’єктів агропромислового комплексу.

Розділ 3. Розробка інформаційної системи автентифікації кіберфізичних об’єктів агропромислового комплексу.

Розділ 4. Розрахунок економічної ефективності системи автентифікації кіберфізичних об’єктів агропромислового комплексу.

Розділ 5. Охорона праці та безпека в надзвичайних ситуаціях.

Висновки.

Список використаної літератури.

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3, 5	*Чаплига В.М., професор кафедри інформаційних технологій*		
4	*Городецький І.М., доцент кафедри управління проектами та безпеки виробництва*		

7. Дата видачі завдання 3 травня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Приміт-ка
1	*Написання Вступу, першого розділу та означення головних завдань роботи*	03.05 - 31.05.23	
2	*Виконання другого розділу та формування початкових даних*	01.06 - 30.06.23	
3	*Виконання третього розділу та узагальнення отриманих результатів роботи*	04.09 - 30.09.23	
4.	*Написання розділу: «Охорона праці»*	02.09 - 31.09.23	
5	*Вартісна оцінка ефективності пропозицій роботи*	01.10 - 31.10.23	
6	*Завершення роботи*	01.11 - 30.11.23	
7	*Виправлення зауважень та перевірка на плагіат*	01.12.23 – 10.01.24	

Студент Джуман В.Р.

(підпис)

Керівник роботи _____ Чаплига В.М.

АНОТАЦІЯ

УДК 635.1

Розробка інформаційної системи автентифікації кіберфізичних об’єктів агропромислового комплексу

Джуман В.Р. Кафедра ІТ. – Дубляни, Львівський НУП, 2024.

Кваліфікаційна робота: 76 с. текст. част., 14 рис., 7 табл., 2 слайдів, 28 джерел.

В роботі розглянуто визначення понять «кіберфізична система», автентифікація, а також технологічний процес автентифікації електронних пристроїв кіберфізичних об’єктів АПК.

Метою роботи є вдосконалення методів та розробка інформаційної системи автентифікації кіберфізичних об’єктів АПК.

Наукова значимість роботи полягає в обґрунтуванні методів, розробленні структурних схем та програмно-алгоритмічному забегпеченні інформаційної системи автентифікації електронних пристроїв кіберфізичних об’єктів АПК на основі їх шумових характеристик з використанням нееквідистантної дискретизації.

Практична значимість роботи полягає в тому, що результати дослідження можуть бути використані для вдосконалення існуючих та розробки нових методів і систем автентифікації електронних пристроїв кіберфізичних об’єктів.

Розділ "Охорона праці" містить перелік заходів щодо забезпечення унормованих умов праці та безпеки при роботі з інформаційною системою автентифікації кіберфізичних об’єктів агропромислового комплексу.

Обґрунтовано економічну ефективність пропонованих рішень виконаної кваліфікаційної роботи.

Ключові слова: кіберфізичний об’єкт, автентифікація, шумові характеристики, інформаційна система, сенсор, комп’ютер, мобільний пристрій.

SUMMARY

UDC 635.1

Development of an information system for authentication of cyber-physical objects of the agro-industrial complex

Juman V.R. Department of IT. – Dublyany, Lviv State University, 2024.

Qualification work: 76 p. text. chast., 14 figures, 7 tables, 2 slides, 28 sources.

The work considers the definition of the concepts of "cyber-physical system", authentication, as well as the technological process of authentication of electronic devices of cyber-physical objects of the agricultural industry.

The purpose of the work is to improve the methods and develop an information system for authentication of cyber-physical objects of the agricultural industry.

The scientific significance of the work consists in the substantiation of methods, development of structural schemes and software-algorithmic backup of the information system of authentication of electronic devices of cyber-physical objects of the agricultural industry based on their noise characteristics using non-equidistant discretization.

The practical significance of the work is that the research results can be used to improve existing and develop new methods and systems for authentication of electronic devices of cyber-physical objects.

The section "Labor protection" contains a list of measures to ensure standardized working conditions and safety when working with the information system of authentication of cyber-physical objects of the agro-industrial complex.

The economic efficiency of the proposed solutions of the completed qualification work is substantiated.

Keywords: cyber-physical object, authentication, noise characteristics, information system, sensor, computer, mobile device.

ПЕРЕЛІК СКОРОЧЕНЬ

ЛНУП – Львівський національний університет природокористування;

КФС – кіберфізична система;

АПК – агропромисловий комплекс

ЄС - Європейський Союз

GDPR - загальний регламент з захисту даних в ЄС

КФС - кіберфізична система

АСУ – автоматизована система управління

ТОПВ - технологічні об’єкти процесів виробництва

IoT - Інтернет речей

АЦП –аналогово-цифровий перетворювач

ЦАП – цифро-аналоговий перетворювач

ЦОС - цифрова обробка сигналів

ЦФ – цифрова фільтрація

ПЗ - програмне забезпечення

ENF (Electric Network Frequency) – частота електричної мережі

ШС - шумовий сигнал

АКФ ШС – автокореляційна функція шумового сигналу

ЗМІСТ

3.2. Алгоритмічне забезпечення автоматичної автентифікації сенсорів та інтегральних мікросхем з використанням їх шумових характеристик	
3.3. Алгоритмічне забезпечення автоматичної автентифікації персональних комп'ютерів і ноутбуків на основі шумових характеристик	
РОЗДІЛ 4. РОЗРАХУНОК ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ СИСТЕМИ АВТЕНТИФІКАЦІЇ КІБЕРФІЗИЧНИХ ОБ’ЄКТІВ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ.	
4.1. Фактори, що впливають на ефективність системи автентифікації кіберфізичних об’єктів агропромислового комплексу	
4.2. Розрахунок економічної ефективності системи автентифікації кіберфізичних об’єктів агропромислового комплексу	
РОЗДІЛ 5. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	
5.1. Нормативно-правові положення з охорони праці та безпеки в надзвичайних ситуаціях.	
5.2. Удосконалення охорони праці та безпеки в надзвичайних ситуаціях системи автентифікації кіберфізичних об’єктів агропромислового комплексу	
5.3. Розрахунок заземлення в виробничих приміщеннях	
ВИСНОВКИ	
Список використаної літератури	

ВСТУП

Актуальність теми дослідження. Динамічна цифрова трансформація галузей агропромислового комплексу (АПК) України в сучасних умовах значного рівня невизначеності, ризиків та загроз продовольчій безпеці країни супроводжується широким використанням кіберфізичних систем в автоматизованих виробничих комплексах, що потребує їх захисту від несанкціонованого доступу неавторизованих електронних пристроїв.

Поняття «кіберфізична система (КФС)» не визначене в законодавстві України, але в науковій літературі і практичній діяльності під цим цей терміном розуміють інтегровану систему, яка поєднує фізичні та кібернетичні (комп'ютерні) складові для ефективної взаємодії та керування фізичними процесами в реальному часі. У такій системі фізичні об'єкти АПК взаємодіють з комп'ютерними системами та мережами, щоб досягти певних цілей, оптимізувати роботу та забезпечити високий рівень їх ефективності. КФС об'єднує апаратні та програмні компоненти для спільної роботи та досягнення поставлених завдань, фунціонуючи в реальному часі, що дозволяє швидко реагувати на зміни в фізичних процесах. КФС взаємодіє з фізичним середовищем, контролює та моніторить фізичні процеси. Кіберфізичні системи можуть бути частинами розширених мереж, таких як Інтернет речей (IoT), де вони в автоматичному режимі реального часу обмінюються інформацією та координують свою діяльність через мережу на основі алгоритмів автоматизації та інтелектуальних алгоритмів, щоб оптимізувати та автоматизувати процеси управління. Приклади КФС стосуються сучасних виробничих систем в різних галузях АПК, електроенергетичних мереж та інших інтегрованих систем, які поєднують фізичні та кібернетичні компоненти для досягнення високої ефективності та автоматизації. Більших таких систем відносяться до критичної інфраструктури АПК

Термін «Автентифікація (Authentication)» в законодавстві України визначається наступним чином [1].

Термін «Автентифікація (Authentication)»

Повернутися назад Перелік термінів Текст для друку

Перелік термінів

Кількість: 1 термін

Автентифікація (Authentication)

Автентифікація (Authentication) - процедура підтвердження достовірності реєстраційних даних об'єкта (користувача, пристрою, процесу тощо), встановленої за процедурою ідентифікації

Методика вимірювань параметрів якості послуг передачі даних та доступу до Інтернету
НКРЗІ; Рішення, Методика від 02.03.2021 N° **80**

Автентифікація — шлях встановлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право.

Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи
Постанова Кабінету Міністрів України; Концепція від 20.01.1997 N° **40**

Автентифікація — процедура встановлення належності працівникові володільця або розпорядника бази персональних даних пред'явленого ним ідентифікатора.

Про затвердження Типового порядку обробки персональних даних у базах персональних даних
Наказ Міністерства юстиції України; Порядок від 30.12.2011 N° **3659/5**

Автентифікація - електронна процедура, яка дає можливість підтвердити електронну ідентифікацію фізичної особи та/або походження і цілісність електронних даних

Про функціонування Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування
НА запобігання корупції; Рішення, Порядок, Повідомлення, Форма, Декларація від 10.06.2016 N° **3**

Автентифікація - електронна процедура, яка дає можливість підтвердити електронну ідентифікацію фізичної особи та/або походження і цілісність електронних даних;

Про функціонування Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування
НА запобігання корупції; Рішення, Порядок, Повідомлення, Форма, Декларація від 10.06.2016 N° **3**

Автентифікація - електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної особи

Про затвердження Положення про Систему BankID Національного банку України
Постанова Національного банку України; Положення, Форма типового документа від 30.08.2016 N° **378**

Автентифікація - електронний процес, який дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної, телекомунікаційної, інформаційно-телекомунікаційної системи, а також походження та цілісність електронних даних

Про схвалення Концепції розвитку системи електронних послуг в Україні
Розпорядження Кабінету Міністрів України; Концепція, Перелік від 16.11.2016 N° **918-р**

Автентифікація - електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних

Про електронні довірчі послуги
Закон України від 05.10.2017 N° **2155-VIII**

Автентифікація - електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних

Про електронні довірчі послуги
Закон України від 05.10.2017 N° **2155-VIII**

Автентифікація - електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних

Про електронні довірчі послуги
Закон України від 05.10.2017 N° **2155-VIII**

Таким чином, автентифікація кіберфізичних об'єктів - це процес перевірки та підтвердження автентичності фізичних об'єктів, які взаємодіють у кіберфізичних системах.

Актуальність автентифікації кіберфізичних об'єктів визначається ростом використання інтернету речей (IoT) та кіберфізичних систем у різних сферах життя і галузях агропромислового комплекксу (АПК). Це пов’язано із низкою факторів, серед яких: постійне збільшення кількості підключених пристроїв; динамічні зміни ландшафту загроз кібербезпеки і тому заходи безпеки стають все більшим пріоритетом у зв'язку з розширенням атак на кібербезпеку; застосування кіберфізичних систем у критичних об’єктах та галузях АПК; проблема забезпечення конфавтенційності та цілісності даних; забезпечення відповідності нормативно-правовому регулюванню питань кібербезпеки в Україні та світі. Так, з кожним роком кількість підключених пристроїв, таких як Сенсори, вбудовані системи, інтелектуальні пристрої та обладнання IoT, значно зростає. Автентифікація стає важливою для забезпечення того, що тільки легітимні пристрої мають доступ до мережі та інших ресурсів. Автентифікація є однією з основних заходів для запобігання несанкціонованому доступу та кібератакам.

Кіберфізичні системи використовуються у критичних галузях, таких як медицина, енергетика, АПК, транспорт та інші. Недостатня безпека цих систем може призвести до серйозних наслідків. Автентифікація не тільки забезпечує доступ до систем, але і гарантує, що передані дані залишаються конфавтенційними і недоступними для зловмисників. Використання ефективних засобів автентифікації вимагають законодавство та стандарти України щодо захисту особистих даних і кібербезпеки, а також Загальний регламент з захисту даних (GDPR) в Європейському союзі.

Усі ці фактори підкреслюють важливість розробки та впровадження надійних та ефективних методів автентифікації для кіберфізичних об'єктів з метою забезпечення безпеки, автенційності та цілісності кіберфізичних систем АПК.

Об'єкт дослідження: процеси забезпечення інформаційної безпеки розподілених кіберфізичних систем.

Предмет дослідження: автоматизація процесів автентифікації кіберфізичних об’єктів АПК.

Мета дослідження: вдосконалення методів та розробка інформаційної системи автентифікації кіберфізичних об’єктів АПК.

Для досягнення поставленої мети були визначені та вирішені наступні завдання:

- проаналізувати терміни та їх визначення щодо кібербезпеки та автентифікації кіберфізичних об’єктів;
- проаналізувати нормативно-правові документи щодо кібербезпеки та автентифікації кіберфізичних об’єктів;
- здійснити аналіз типів загроз та ризиків у кіберфізичних системах;
- здійснити аналіз методів та процесів автентифікації у кіберфізичних системах;
- дослідити загрози та ризики кіберфізичних систем;
- дослідити методи та засоби автентифікації у кіберфізичних системах
- розробити систему автентифікації у кіберфізичних системах.

Методологічною основою кваліфікаційної (магістерської) роботи є наукові методи: терміногічного аналізу понять щодо автентифікації у кіберфізичних системах; системного аналізу при вивченні елементів та зв’язків кіберфізичних систем; методи автентифікації у кіберфізичних системах при виборі інформативних параметрів для автентифікації; порівняння при співставленні методів та засобів автентифікації у кіберфізичних системах; синтезу для розробки інформаційної системи автентифікації кіберфізичних об’єктів; табличний і графічний методи для представлення результатів кваліфікаційної роботи.

Інформаційною основою роботи є нормативно-правові акти, міжнародні і національні стандарти; наукова та спеціальна література, а також підручники з кібербезпеки.

Наукова новизна одержаних результатів полягає в обґрунтуванні та розвитку методів, розробленні структурних схем та програмно-алгоритмічного забегпечення інформаційної системи автентифікації електронних пристроїв кіберфізичних об’єктів АПК на основі їх шумових характеристик з використанням нееквідистантної дискретизації.

Практичне значення одержаних у кваліфікаційній роботі результатів полягає можливості використання результатів роботи, зокрема, інформаційної системи для для вдосконалення існуючих та розробки нових методів і систем автентифікації електронних пристроїв кіберфізичних об’єктів у різних галузях АПК.

Апробація результатів роботи. Основні теоретичні та практичні результати кваліфікаційної (магістерської) роботи доповідались та отримали хороші відгуки на наукових семінарах кафедри інформаційних технологій, на студентських міжнародних форумах, зокрема, на Міжнародному студентському науковому форумі «Студентська молодь і науковий прогрес в АПК» (2023, Львів, ЛНУП).

Публікації здобувача за темою кваліфікаційної роботи.

Джуман В. Аналіз сучасного стану методів і засобів автентифікації електронних пристроїв. Студентська молодь і науковий прогрес: тези доп. Міжнар. студ. наук. форуму, 4 – 6 жовт. 2023 р. [Електронний ресурс]. Львів, 2023. С. 452.

Структура та обсяг кваліфікаційної роботи. Кваліфікаційна робота містить вступ, п’ять розділів, висновки, список використаної літератури та додатки.

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ АВТЕНТИФІКАЦІЇ КІБЕРФІЗИЧНИХ ОБ'ЄКТІВ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ ТА ЙОГО АВТОМАТИЗАЦІЇ.

1.1. Аналіз технологічного процесу автентифікації кіберфізичних об'єктів агропромислового комплексу

В сучасному інформаційному середовищі та Інтернеті речей (IoT), автентифікація електронних фізичних об'єктів (як от сенсорів, пристроїв, розумних об'єктів тощо) важлива для забезпечення безпеки та захисту від несанкціонованого доступу кіберфізичних об'єктів та систем агропромислового комплексу.

Розвиток методів та засобів автентифікації кіберфізичних систем є результатом спільних зусиль багатьох вчених, інженерів та дослідників у галузі кібербезпеки та інформаційних технологій. Зокрема, Рівест, Шамір та Адлеман розробили алгоритм RSA, який може використовуватися для забезпечення процесів автентифікації та обміну ключами; Уїтфілд Діффі та Мартін Хеллман розробили протокол Діффі-Хеллмана, який дозволяє двом сторонам безпечно обмінюватися ключами через ненадійний канал, що використовується для забезпечення безпеки та автентифікації в мережевих системах; Леонард Адлеман (Zero-Knowledge Proofs) розробив протоколи доказу нульового знання, що дозволяє одній стороні довести іншій свою автентичність без розкриття конкретної інформації; Вітс Діффі розробив протокол Kerberos, який використовується для автентифікації користувачів у комп'ютерних мережах. Серед українських вчених слід відзначити таких, як Валерій Дудикевич, Олена Нємкова, Олександр Шологон та інші, які досліджували загрози у кіберфізичних системах, методи та засоби автентифікації кіберфізичних систем в корпоративних та глобальних мережах. Тобто, процес автентифікації забезпечує визначення та перевірку того, що конкретний фізичний об'єкт або пристрій (девайс) є тим, за що він себе видає.

Надійна автентифікація є важливим аспектом для забезпечення безпеки та ефективності кіберфізичних систем в АПК. При цьому, кожен електронний кіберфізичний об'єкт повинен мати унікальний автентифікатор чи ключ, який можна використовувати для його автентифікації в мережі. Автентифікатори мають бути захищені шляхом шифрування, використання бездротових технологій забезпечення, таких як Secure Sockets Layer (SSL) або Transport Layer Security (TLS) тощо. Також кіберфізична система повинна забезпечувати механізми оновлення та управління автентифікаторами для забезпечення безпеки протягом тривалого періоду служби об'єкта. Електронний кіберфізичний об'єкт передає свій автентифікатор чи ключ через мережу. Це може бути здійснено за допомогою різних технологій зв'язку, таких як Wi-Fi, Bluetooth, NFC (Near Field Communication), RFID (Radio-Frequency Identification) та інші. Сервер або центральна система отримавши автентифікатор перевіряє його валідність (прав доступу, часові обмеження та інші параметри безпеки) і, якщо автентифікатор визнаний як валідний, електронний кіберфізичний об'єкт може отримати доступ до інших систем чи ресурсів. Це може включати в себе передачу даних, керування пристроями чи виконання інших дій.

До основних операцій процесу автентифікації кіберфізичних об'єктів вітчизняні та закордонні автори відносять наступні [2 - 7], які зведені нами в табл. 1.1.

Таблиця 1.1.

Послідовність та зміст операцій технологічного процесу автентифікації кіберфізичних об'єктів АПК. *Власна розробка на основі [1 - 8].*

Послідовність операцій	**Зміст операцій (процедур) технологічного процесу автентифікації кіберфізичних об'єктів АПК**
1	Аналіз унікальних інформативних параметрів кіберфізичних об’єктів конкретного типу в АПК
2	Класифікація кіберфізичних об’єктів АПК за інформативними параметрами
3	Визначення та присвоєння унікального автентифікатора кожному фізичному об'єкту АПК або пристрою у системі

Продовження таблиці 1.1.

4	Використання методів та технік для перевірки, чи відповідає автентифікатор, вказаний об'єктом, дійсній автентичності, наприклад, методів з використанням паролів, цифрових підписів, біометричних сканерів, фізичних маркерів або комбінацій цих методів
5	Підтвердження автентичності на основі представленої інформації, такої як пароль, ключ або біометричні дані тощо
6	Забезпечення безпечних механізмів автентифікації для запобігання несанкціонованому доступу та автентифікації фізичних об'єктів
7	Інтеграція в загальну систему керування кіберфізичною системою для ефективного управління та моніторингу
8	Моніторинг, ведення журналу та аналіз всіх спроб автентифікації для виявлення можливих загроз безпеці та виявлених спроб несанкціонованого доступу, неординарних або підозрілих активностей.
9	Ефективне управління автентифікаторами, включаючи їх оновлення, зберігання у захищеному вигляді, створення, видачу та відкликання для забезпечення безпеки протягом тривалого періоду служби кіберфізичного об'єкту

Зауважимо, що залежно від конкретного сценарію використання та характеристик кіберфізичного об'єкта, можуть використовуватися різні методи і технології для забезпечення безпеки та ефективності процесу автентифікації оскільки це є критично важливим завданням тому, що дозволяє запобігати несанкціонованому доступу, зберігати конфавтенційні дані та забезпечувати інтеграцію кіберфізичного об'єкта в більш складні системи АПК. Головним тут є дотримання

Для цього використовують спеціальні методи автентифікації, такі як багатофакторна автентифікація (МФА), що включає в себе щось, що користувач знає (пароль) або має (фізичний об'єкт, наприклад, смарт-карта), чи йому притаманне (біометричні дані). Під час передачі даних від кіберфізичного об’єкта забезпечують шифрування всіх комунікацій між електронними пристроями та системою автентифікації, використовуючи такі протоколи, як

TLS або SSL. Має регулярно оновлюватись програмне забезпечення електронних пристроїв кіберфізичних об’єктів, включаючи системи автентифікації, та забезпечуватись постійний захист фізичного доступу до електронних пристроїв, особливо якщо вони містять конфавтенційні дані або ключі автентифікації.

Взагалі для усунення вразливостей та покращення безпеки процесу автентифікації дуже важливим є дотримання стандартів безпеки, які визначають вимоги та процедури для забезпечення безпеки електронних пристроїв кіберфізичних об’єктів АПК та систем їх автентифікації. Такі заходи слугуватимуть гарантією того, процес автентифікації відбуватиметься безпечно та ефективно, зменшуючи ризик несанкціонованого доступу та інших загроз.

1.2. Аналіз типів загроз та ризиків від неавтефікованих об’єктів у кіберфізичних системах

Кіберфізичні системи об'єднують фізичні об'єкти та кібернетичні складові, що робить їх уразливими перед різними типами загроз та ризиків від неавтентифікованих об’єктів, зокрема до прикладу наступних.

Неавтентифіковані об'єкти у кіберфізичних системах можуть призводити до різних загроз та ризиків, які можуть впливати на безпеку, конфавтенційність та доступність системи. Типи таких загроз та ризиків нами зведені в табл. 1.2.

Таблиця 1.2.

Типи загроз та ризиків від неавтефікованих об’єктів у кіберфізичних системах. *Власна розробка на основі []*.

Тип загрози, ризику	Вплив на кіберфізичну систему
Несанкціонований доступ	Загроза несанкціонованого доступу до системи чи мережі може призвести до витоку конфавтенційної інформації, порушення приватності чи навіть знищення даних
Втрата конфавтенційності	Виток чутливих для кіберфізичного об’єкту даних
Втрата доступності ресурсів	Тимчасова або повна відмова в обслуговуванні (DoS або DDoS атаки).

Продовження таблиці 1.2.

Введення в оману системи	Імітація легітимних пристроїв або введення фальшивих даних в систему
Автентифікаційні атаки	Перехоплення автентифікаторів чи паролів шляхом атак man-in-the-middle або фішингу.
Недостатній контроль доступу	Користувачам, які не мають прав доступу, дозволяється отримати несанкціонований доступ до ресурсів системи
Компрометація цілісності даних	Вплив на цілісність даних, втрати довіри до інформації системи
Використання як ботнету	Компрометовані об'єкти можуть бути використані для створення ботнетів, що може призвести до розповсюдження шкідливого програмного забезпечення чи атак на інші системи
Введення шкідливого ПЗ	Може викликати різноманітні проблеми, включаючи втрату даних та порушення нормального функціонування
Вплив на надходження даних від сенсорів	Фальсифікації або зміна даних з метою прийняття невірних рішень системою підтримки прийняття рішень (СППР)

Ці загрози та ризики вимагають комплексного підходу до кібербезпеки, щоб забезпечити ефективний захист кіберфізичних систем від різноманітних небезпек. Для зменшення ризиків важливо використовувати надійні методи автентифікації, застосовувати принцип найменших привілеїв, регулярно оновлювати системи та слідкувати за новими загрозами та вразливостями.

1.3. Автентифікація електронних пристроїв кіберфізичних об’єктів АПК та підходи до її автоматизації

Електронні пристрої кіберфізичних об’єктів використовуються для передачі, перетворення та зберігання інформації, вони широко використовуються в сучасному житті для створення нових цінностей і розширення зони комфорту. В основному це електронні пристрої, які взаємодіють і обмінюються інформацією в мережі; їх різноманітність і кількість постійно збільшується. Аналітик We Are Social і Hootsuite SMM Platform у

спільному звіті за 2022 рік навели дані світового цифрового ринку [8], згідно з якими кількість підключених IP-адрес у 2022 році перевищила 14 мільярдів. Це значно підвищує ризик уразливості до кібератак і призводить до необхідності надійної взаємної автентифікації між пристроями. Поточна система автентифікації пристрою на основі IP- і MAC-адрес не надто надійна. Наприклад, MAC-адреса, визначена драйвером на програмному рівні, має пріоритет над апаратним рівнем. Це дає можливість замінити MAC-адресу, яка є апаратною характеристикою мережевої карти. Обсяг кіберзлочинності зростає з року в рік як кількісно, так і якісно. Існує також клас завдань, де потрібно автентифікувати електронний пристрій, який не обов'язково підключений до інформаційної мережі. В основному це криміналістичні завдання, або виявлення фальсифікату або контрафактної продукції.

Автоматизація процесів автентифікації електронних пристроїв є важливою частиною сучасних інформаційних систем, особливо в контексті Інтернету речей (IoT) та розумних пристроїв. Застосування автоматизації дозволяє покращити ефективність та безпеку процесу автентифікації. Основні методи та підходи до автоматизації автентифікації електронних пристроїв зведені нами в табл. 1.3.

Таблиця 1.3.

Основні методи та підходи до автоматизації автентифікації електронних пристроїв об'єктів АПК. *Власна розробка на основі []*.

Автоматизовані методи автентифікації та приклади застосування	**Ефект автоматизованої автентифікації**
1	2
Багатофакторна автентифікація	Забезпечення додаткового рівня безпеки
Автентифікація на основі біометричних даних (Touch ID, Face ID, Windows Hello, Google Smart Lock тощо)	Автоматичний процес автентифікації на основі унікальних фізіологічних ознак
Використання сертифікатів та ключів	Автоматична автентифікація електронних пристроїв об'єктів АПК і може використовувати інфраструктуру відкритих ключів (PKI)

Продовження табл. 1.3.

1	2
Багатофакторна автентифікація	Забезпечення додаткового рівня безпеки
Автентифікація на основі біометричних даних (Touch ID, Face ID, Windows Hello, Google Smart Lock тощо)	Автоматичний процес автентифікації на основі унікальних фізіологічних ознак
Використання сертифікатів та ключів	Автоматична автентифікація електронних пристроїв об’єктів АПК і може використовувати інфраструктуру відкритих ключів (PKI)
Використання токенів або JWT (JSON Web Tokens), Smart Cards та RFID	Автоматичний обмін інформацією про автентифікацію без необхідності повторно вводити автентифікатори та паролі
API та цифрові підписи	Автоматична автентифікація електронних пристроїв об’єктів АПК на основі обміну цифровими підписами для підтвердження автентичності
Управління автентифікацією та доступом (IAM)	Автоматизація процесів налаштування прав доступу на основі ролей, політик та інших параметрів, що регулюють автентифікацію
Захист на рівні пристроїв - Secure Elements, Trusted Platform Modules (TPM) тощо	Автоматизація процесів безпеки та автентифікації
Використання інтелектуальних аналітичних систем	Автоматизація виявлення аномалій в поведінці пристроїв та автоматичної реакції на потенційні загрози
Використання штучного інтелекту	Автоматизація процесу автентифікації із забезпеченням високого рівеня безпеки та ефективності в кіберфізичних системах та мережах
Використання профілів Bluetooth	Автоматична автентифікація електронних пристроїв об’єктів АПК, коли вони знаходяться у зоні зв'язку між собою
Використання захищених протоколів зв’язку	Забезпечення конфавтенційності та автентифікації під час обміну інформацією між кіберфізичними об'єктами
Використання технологій блокчейну	Інформація про автентичність об'єкта зберігається децентралізовано та захищено

Застосування конкретного методу залежить від контексту використання та вимог до безпеки кіберфізичних об’єктів АПК. Комбінація різних методів часто

використовується для створення більш надійних систем автентифікації кіберфізичних об'єктів, оскільки це дозволяє подолати можливі недоліки окремих методів та покращувати загальний рівень безпеки.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТА ВИБІР МЕТОДІВ І ІПРОГРАМНО-ТЕХНІЧНИХ ЗАСОБІВ АВТЕНТИФІКАЦІЇ КІБЕРФІЗИЧНИХ ОБ'ЄКТІВ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ

2.1. Дослідження методів автентифікації кіберфізичних об'єктів агропромислового комплексу

Різноманітність електронних пристроїв у складі кіберфізичних об'єктів АПК надає широкий спектр можливостей використання їх індивідуальних відмінностей для цілей автентифікації. Основними вимогами до рішень автентифікації є практичність (автоматичність, оперативність, віддаленість), економічна виправданість і надійність.

Останнім часом зріс інтерес дослідників до систем автентифікації електронних пристроїв на основі їх індивідуальних відмінностей. Виробництво електронних пристроїв забезпечує їх функціонування в межах відмовостійкості і не має на меті фізичної автентичності. Незначні допустимі відхилення в технологічному процесі виготовлення інтегральних схем призводять до нерівномірного розподілу акцепторних або донорних домішок, що визначає специфіку внутрішніх електричних перешкод при роботі з мікросхемами. Також в процесі складання електронних пристроїв використовується обладнання з певними допустимими електричними параметрами, що також впливає на вихідні електричні сигнали або специфіку внутрішніх електричних перешкод. Таким чином, кожен електронний пристрій має фізичні особливості, які можна використовувати для його автентифікації.

Для завдань автентифікації електронних пристроїв прийнято використовувати поняття, термінологію та алгоритми, аналогічні біометрії

людини [2 - 5]. Перш за все, це стосується загального підходу до процесу автентифікації пристрою за шаблоном. Шаблон T (підпис) — це відображення вимірювань фізичних величин, за якими пристрій автентифіковано за набором із N чисел. Шаблон ($\{T_i\}, i = \overline{1,N}$) має бути індивідуальним для кожного пристрою та стабільним для однотипних вимірювань. На практиці ознака, за якою здійснюється автентифікація, може змінюватися несуттєво в залежності від непередбачених зовнішніх і внутрішніх умов, що призводить до зміни поточної картини - для кожної процедури вимірювання l вони отримують свій набір $\{T_{i,l}\}$. Тому, як правило, здійснюється процес усереднення шаблону в серії L вимірювань:

$$T_i = \overline{T_{i,l}} = \frac{1}{L}\sum_{l=1}^{L} T_{i,l} \tag{2.1}$$

Це призводить до того, що отримана при наступних вимірюваннях сигнал від приладу може не збігатися з усередненим шаблоном. Для проходження автентифікації пристрій вводить поріг D - максимально допустиме відхилення між усередненим і поточним шаблонами одного пристрою.

Завдяки відмові від двох закономірностей або, навпаки, подібності, для різних практичних завдань можна використовувати один із чотирьох типів коефіцієнтів [6]: коефіцієнти кореляції, міри відстані, коефіцієнти асоціативності та коефіцієнти ймовірності подібності. З перерахованих коефіцієнтів для завдань автентифікації найчастіше використовують форми спеціального класу метричних функцій відстані, відомих як метрики Мінковського.

$$d_{T1m1,Tm} = \left(\sum_{i=1}^{N}\left|T_{m1,i} - T_{m,i}\right|^{r}\right)^{1/r} \tag{2.2}$$

Для евклідової метрики r = 2, для відстані Хемінга r = 1.

Також використовується відстань Махаланобіса, яка враховує кореляцію між змінними $\{T_{i,l}\}$. Якщо кореляція відсутня, то відстань Махаланобіса еквівалентна відстані Евкліда.

Позначимо{m} = M — різні пристрої, які які потрібно автентифікувати. Для кожного m приладу вимірювання виконуються на початку процедури автентифікації і створюється шаблон *Tm*, який потім зберігається в базі даних і може бути наданий для порівняння на вимогу. Таким чином, база даних містить набір шаблонів $\{Tm\}$. Якщо потрібно провести автентифікацію приладу m 1, потрібно знову виміряти фізичні сигнали і отримати шаблон T 1 $m1$для порівняння. Наступна процедура автентифікації залежить від того, що потрібно зробити: автентифікувати пристрій – автентифікувати один з багатьох (One-to-Many [7]), перевірити його – підтвердити, що це один і той же пристрій (One-to-One [8]), або перевірити наявність шаблону даного пристрою в базі даних - провести відкриту автентифікацію (Open-Set Identification [9]). Типова система автентифікації виконує розпізнавання одного електронного пристрою *m1* з безлічі *M* на основі мінімальної відстані між парами шаблонів, одна з яких є шаблоном *T1m1*, а друга береться з набору $\{Tm\}$:

$$d_{T1m1,Tm} \rightarrow \min,\ m = \overline{1, M} \tag{2.3}$$

У цьому випадку *m1* автентифікується як *m*-тий пристрій, для якого виконується верхня умова.

Поріг перевірки використовується для перевірки пристрою. Якщо відстань між моделями *T1m1* і *Tm* не більше *D*, то прилад *m1* автентифікується як *m*:

$$d_{T1m1,Tm} \leq D \tag{2.4}$$

Якщо потрібно, по-перше, перевірити, чи є шаблон пристрою *m1* у базі даних {Tm}, а по-друге, автентифікувати пристрій у разі успішної перевірки, то маємо *M* порівнянь:

$$d_{T1m1,Tm} \leq D, m = \overline{1, M} \quad (2.5)$$

Якщо є шаблон *Tm*, для якого знайдено останню умову, то пристрій *m1* автентифікується системою як *пристрій m*.

Індивідуальність кожного електронного пристрою сьогодні безпомилково впізнавана і підтверджена експериментально. При автентифікації електронних пристроїв виникають дві проблеми. По-перше, це доступність засобів автентифікації, тобто наявність апаратних засобів для виявлення та вимірювання індивідуальних відмінностей, які реалізуються у вигляді фізичних сигналів. По-друге, це наявність методів, які на основі вимірювань реалізують алгоритми створення шаблонів, їх порівняння та прийняття рішень щодо автентифікації електронного пристрою.

Комбінація методів і засобів повинна давати статистично повторюваний результат, який можна охарактеризувати наступними чотирма варіантами: істинно позитивна автентифікація, істинно негативна автентифікація, помилково позитивна автентифікація (FRR, False Recognition Rate) і помилково негативна автентифікація (FAR, False Acceptance Rate - помилка другого роду). Для характеристики біометричних систем прийнято наводити залежність значень FRR і FAR від порогу розпізнавання.

Точність будь-якої системи автентифікації повинна характеризуватися двома змінними: величиною помилки першого роду при заданому значенні помилки другого роду. Значення FRR і FAR також залежать від розміру вибірки - кількості об'єктів автентифікації. Чим вище зразок, тим більш достовірний результат можна отримати щодо якості розпізнавання. Тому знання тільки порогового значення недостатньо, необхідно вказати кількість об'єктів, що перевіряються.

2.2. Кластеризація електронних пристроїв об’єктів АПК відповідно до завдань автентифікації

Різноманіття завдань, для вирішення яких здійснюється автентифікація електронних пристроїв, пояснюється досить великим переліком методів і засобів їх вирішення. Можна розділити всі методи і засоби відповідно до класів завдань, які необхідно вирішити.

1. Клас завдань цифрової експертизи, який є частиною доведення автентичності медіафайлів. Можливість використання таких файлів як доказів доводиться обґрунтовувати використанням специфічних медіа-рекордерів, які рідше можуть бути представлені цифровими мікрофонами, цифровими та аналоговими відеокамерами, мобільними телефонами, WEB-камерами, автомобільними відеореєстраторами, комп'ютерами. Дуже важливою вимогою є відсутність компіляції медіафайлів, в тому числі відсутність цифрової постобробки для забезпечення запису тих чи інших властивостей або введення додаткової інформації.

До цього пункту класифікації можна віднести завдання доказу авторського права на автентичний медіаконтент.

2. Геолокація електронного пристрою. Необхідність визначення точної геолокації обумовлена вимогами безпеки при автентифікації користувача - власника електронного пристрою в корпоративних мережах для вирішення різних завдань, наприклад, доступу до баз даних електронної бібліотеки університетської бібліотеки, проведення фінансових операцій через банківські сервіси on-line або безпосередньо за допомогою поштових терміналів або банкоматів і так далі.

3. Виявлення підроблених електронних пристроїв кіберфізичних систем АПК таких, як контролери, ПК, ноутбуки, мобільні телефони тощо або їх підробки є класом завдань, пов'язаних з фінансовими та іміджевими інтересами провідних виробників сучасної високоякісної електронної техніки, а також може стосуватися захисту прав споживачів.

4. Віддалена автоматизована автентифікація в реальному часі різних SCADA-систем (Supervisory Control and Data Acquisition), або Сенсорів, розташованих в місцях з високим ризиком для людини; системи автоматичного управління об'єктами критичної інфраструктури - електричними мережами промислового та побутового споживання, електротранспортом тощо. Набуття стрімкого розвитку парадигми розумного середовища життєдіяльності людини - розумні виробничі приміщення, будівлі АПК, будинки і міста, де проживають працівники галузей АПК. Середня кількість найменувань різних Сенсорів тільки в розумному виробничому приміщенні може перевищувати десятки одиниць. На основі сенсорних дисплеїв підтримується управління системами клімат-контролю, системи підтримуються в штатному режимі або надходить сигнал тривоги.

5. Віддалена автоматизована автентифікація в режимі реального часу контролерів, персональних комп'ютерів або ноутбуків в корпоративних мережах. Вирішення завдань цієї категорії дасть можливість:

- підвищити безпеку обміну інформацією в корпоративних мережах з рольовим доступом до ресурсів;

- забезпечити безперервну інвентаризацію контролерів та комп'ютерів в бездротових мережах з обмеженим доступом як засіб аудиту інформаційної безпеки;

- підвищити рівень безпеки систем планування ресурсів підприємств АПК (ERP) та фінансових операцій в них, надійності DLP (Data Leak Prevention System) та інших інформаційних систем..

6. Автентифікація інтегральних мікросхем, які можуть бути невід'ємними частинами блоків управління кіберфізичними об’єктами АПК, побутовою технікою тощо. При цьому застосовують методи автентифікації, засновані на використанні або фізично недомінантних функцій, або характерного випромінювання електромагнітного поля.

Методи і засоби автентифікації електронних пристроїв для виконання різних класів завдань можуть сильно відрізнятися. В основі різноманіття методів

і засобів автентифікації лежать як фізичні причини виникнення індивідуальних відмінностей в електронних пристроях, так і методологія їх розпізнавання. Фізичні причини існування індивідуальних відмінностей пристроїв полягають у відсутності необхідності їх абсолютно точних копій на фізичному рівні - для стандартної роботи послідовних пристроїв; Обов'язкова гарантія роботи в межах відмовостійкості. Методика автентифікації індивідуальних характеристик пов'язана з вимогами до швидкості розпізнавання, можливості дистанційного проведення, повної автоматизації або за участю людини-експерта, і в основному полягає у виявленні статистичних характеристик шуму зареєстрованих сигналів, не пов'язаних з корисними сигналами, тобто таких шумів, що видаються самим електронним пристроєм або навколишнім середовищем. Виявлення ознак здійснюється за допомогою спектрально-кореляційного аналізу, так як перетворення Фур'є або вейвлети найчастіше використовуються в якості ортогональних перетворень для отримання періодограм (для стислості їх називають спектрами). Відомі також інші методи автентифікації деяких нешумних пристроїв.

Розглянемо більш детально класи завдань автентифікації електронних пристроїв кіберфізичних об’єктів з точки зору застосовуваних методів і засобів.

2.3. Дослідження методів та засобів автоматизації процесу автентифікації медіа-обладнання диспетчерських центрів в галузях АПК

Методи та засоби автентифікації медіа-обладнання диспетчерських центрів найбільш повно представлені для ознайомлення порівняно з іншими класами завдань автентифікації в [2, 4-15]. У роботі [16] представлено сучасні системи, призначені для автентифікації цифрового зображення або аудіозапису, які вже впроваджені або впроваджуються в експертних установах України. Підставою для автентифікації є фізичні відмінності медіа-обладнання, що проявляється у вигляді адитивного шуму цифрового зображення або аудіозапису, накладеного на корисний сигнал при записі аудіо- та відеозаписів або фотографій. Технологія перевірки автентичності аудіоапаратури заснована

на припущенні, що шум є випадковим стаціонарним процесом, тому необхідно порівнювати характеристики двох випадкових стаціонарних процесів. Найбільш повний випадковий процес можна охарактеризувати функцією розподілу. Порівняння двох варіантів з двох випадкових процесів для ситуації, коли процес розподілу процесів невідомий, може бути проведено за критерієм узгодженості Колмогорова-Смірнова. Алгоритм автентифікації складається з наступних кроків (див. рис. 2.1) [16]:

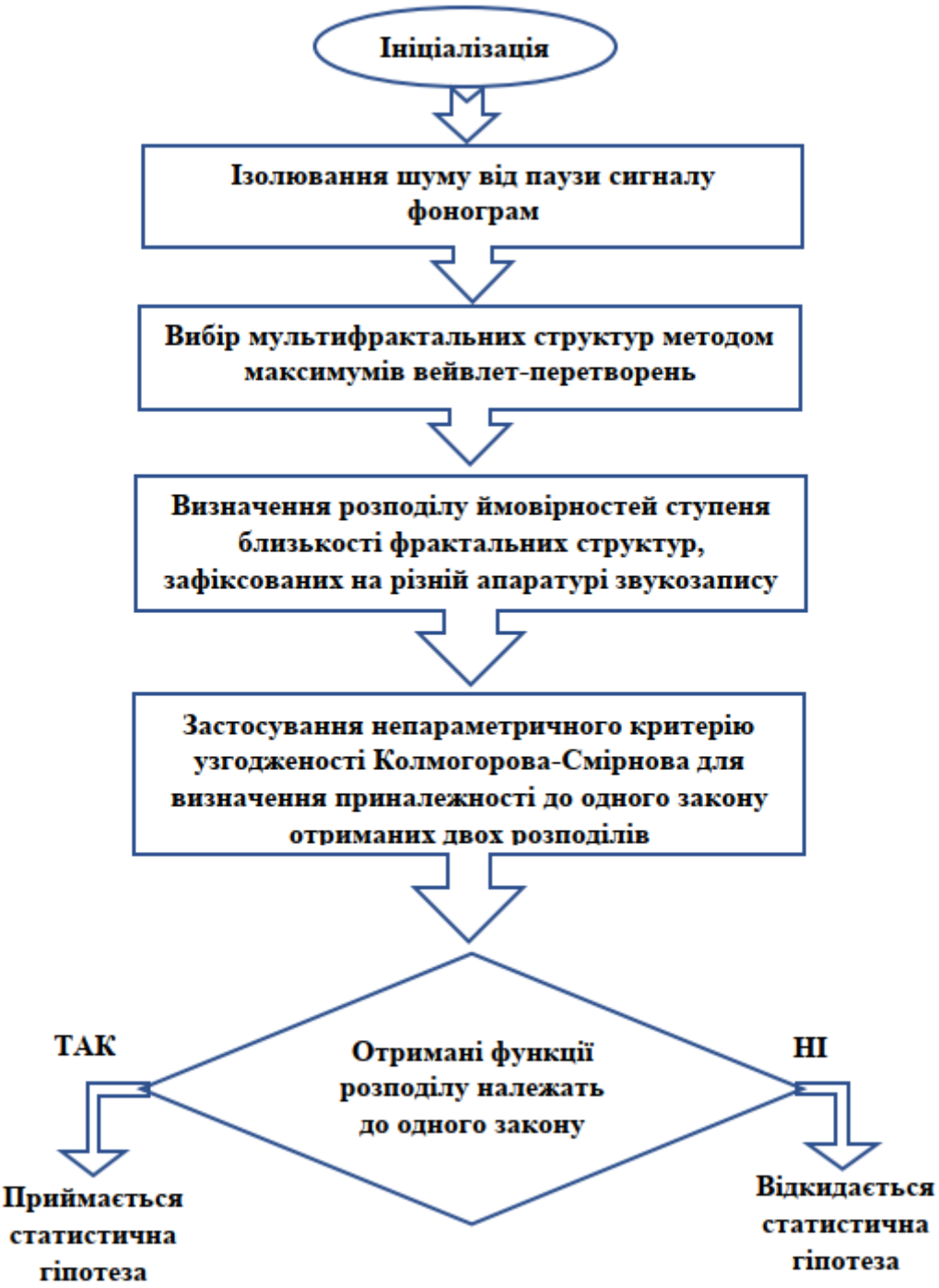

Рис. 2.1. Алгоритм автентифікації аудіоапаратури.

У дослідженні інших авторів автентифікація цифрових мікрофонів проводилася за допомогою кореляції пари усереднених за багатьма аудіозаписами спектрів шуму [17].

Багато аудіозаписів записуються пристроями, які підключені до джерела живлення. Зазвичай номінальна частота блоку живлення становить 50 Гц або 60 Гц. Встановлено, що при підключенні до мережі різної потужності споживачів спостерігаються незначні відхилення частоти потужності від номінального значення до 0,1% [18]. Ці випадкові коливання записуються в аудіофайли і можуть бути вилучені для порівняння з відомою еталонною «траєкторією» зміни джерела живлення [19-24]. Протягом останнього десятиліття дослідники використовували значення випадкових коливань частоти джерела живлення (), як природну сигнатуру в багатьох аудіозаписах [25-27]. Рішення на базі ENF (Electric Network Frequency) можуть бути використані у випадках підтвердження або відхилення компіляції аудіофайлів, або доказу запису конкретного аудіофайлу в більш-менш визначеному географічному регіоні в конкретний час [28], залучаючи як академічних дослідників, так і правоохоронні органи. Для успішного застосування методу необхідно створити надійну базу довідкових даних ENF з прив'язкою до географічного положення [29]. Хоча ідея ENF не має прямого відношення до автентифікації конкретних аудіопристроїв, можна сказати, що вона дозволяє підтвердити час запису для конкретного географічного розташування записуючого пристрою. Відомо кілька алгоритмів, які дозволяють доводити звукові файли, засновані на ідеї ENF. Один з таких алгоритмів складається з двох блоків [30]:

1. Вилучення послідовності випадкових значень флуктуацій ENF з аудіофайлу за допомогою використання вузькосмугових цифрових фільтрів для трьох гармонік 50/100/150 Гц або 60/120/180 Гц.

2. Процедура порівняння послідовності випадкових значень флуктуацій ENF з опорною послідовністю відповідно до міток часу та географічних місць за допомогою кореляційної функції.

Цей алгоритм був застосований на експерименті, в якому напруга від блоку живлення через дільник подавалося на лінійний вхід одного комп'ютера і одночасно записувало аудіофайл на другий комп'ютер. Експеримент отримав 99% збіг між сигналом ENF, витягнутим із тестового аудіозапису, та еталонним сигналом ENF.

Застосування методу ENF ускладнюється тим, що в спектральний діапазон досліджуваного обстежуваного входить власний шум диктофона і спектральні складові звуку. Також існує потреба у веденні довідкових баз даних ENF для різних географічних регіонів.

Як правило, часу на проведення цифрової експертизи аудіофайлів вистачає, тому вимога роботи в режимі реального часу не є критичною.

Автоматизована система автентифікації апаратури аналогового та цифрового звукозапису «Фрактал», розроблена на основі цих алгоритмів, забезпечує високу достовірність результатів обстеження.

Програмне забезпечення «Фрактал» призначене для ідентифікаційних та діагностичних досліджень фонограм та цифрових звукозаписуючих пристроїв. Запис фонограми характеризується впливом шумів записуючого пристрою, тому в разі перезапису або запису на іншу апаратуру власні шуми фонограм мають інші характеристики. Це дає можливість ідентифікувати компіляцію аудіофайлу. Дана система дозволяє проводити автентифікацію звукозаписуючої апаратури, встановлювати оригінальність фонограм і виявляти в них сліди цифрової обробки (див. рис. 2.1).

Рис. 2.1а – Автоматизовані системи автентифікації апаратури аналогового та цифрового звукозапису

Рис. 2.1б – Автоматизовані системи автентифікації апаратури аналогового та цифрового звукозапису.

Системи даного типу використовуються, наприклад, в диспетчерських центрах та центрах технічної пітримки в різних галузях АПК.

РОЗДІЛ 3. РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ АВТЕНТИФІКАЦІЇ КІБЕРФІЗИЧНИХ ОБ'ЄКТІВ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ

3.1. Обґрунтування, структурна схема та програмне забезпечення інформаційної системи автентифікації електронних пристроїв кіберфізичних об'єктів АПК на основі їх шумових характеристик

Практично усі працюючі електронні пристрої разом з інформативними сигналами генерують і природний унікальний шум, який можна використати для розв'язання задач автентифікації цих пристроїв у кіберпросторі. Для цього потрібно вибрати такий параметр шуму, який буде залежати тільки від фізичних характеристик самого електронного пристрою.

Будь-який електронний пристрій складається з набору компонентів, які відрізняються граничними параметрами, що змінюються. Ніхто не може створити абсолютно однакові компоненти на мікроскопічному рівні, тому ці відмінності проявляються у вигляді відхилень у макроскопічних параметрах

пристрою: лінійних характеристиках посилення, резонансній частоті, коефіцієнті шуму тощо.

Процес сертифікації електронних пристроїв визначається параметрами вимірювання. Таким чином, імпульсний шум використовується для автентифікації чіпів шляхом реалізації функцій фізичного неклонування. Точність автентифікації визначається показниками якості, які залежать від технічного оснащення, методу вимірювання та обраного автентифікатора. Тому для вирішення проблеми автентифікації електронних пристроїв необхідний комплексний підхід.

Через коливання внутрішнього електромагнітного поля електронне обладнання може зазнавати неконтрольованих змін сигналу під час роботи. Коливання можуть поширюватися через кабелі чи дроти або через випромінювання у формі електромагнітних хвиль. Тому виникають перешкоди, які шкодять нормальній роботі пристрою. Розлади виникають з багатьох причин. Основними причинами є різкі зміни струму або напруги.

В середині електронного обладнання, підключеного до джерела живлення, виникають складні моделі електромагнітних полів, спричинені взаємодією компонентів обладнання. В результаті у вихідних ланцюгах електронних пристроїв з'являються помилкові сигнали. Параметри паразитних сигналів (наприклад, фаза, амплітуда, частота, динамічний спектр) визначаються цими внутрішніми електромагнітними полями, які, в свою чергу, залежать від компонентної основи та конструктивних особливостей пристрою. Через природну дисперсію параметрів на мікроскопічному рівні неможливо забезпечити повну автентичність пристрою, навіть якщо вибрано однакові компоненти та їхнє внутрішнє розташування. Взаємодія електромагнітних полів в середині приладу залежить від його резонансних частот, які є наслідком процесів в ланцюгах з розподіленими параметрами. На виході пристрою будуть присутні сигнали, які потрапили в область резонансних частот.

Вихідний сигнал буде різним для різних пристроїв одного типу, іншими словами, паразитний вихідний сигнал схожий на індивідуальні біометричні

характеристики різних людей. Тому можна використовувати їх для автентифікації електронних пристроїв. Завдяки його мінімізації помилкових сигналів дуже мало, зазвичай мова йде про шуми на виході пристрою.

Коли справа доходить до автентифікації, необхідно визначити функцію автентифікації та знайти процес, який може чітко охарактеризувати пристрій. Виникнення паразитних сигналів на виході пов'язане з внутрішньою структурою пристрою. Після відповідного вибору паразитних параметрів сигналу можна визначити автентифікаційні характеристики (автентифікатори). Наприклад, на характеристики запису платівки впливає шум записуючого обладнання, тому у випадку перезапису чи запису на іншому обладнанні шум самого запису має інші характеристики. Це дозволяє розпізнавати збірку аудіофайлів.

В роботі [10] запропоновано метод автентифікації комп’ютерів у мережі за допомогою фазової діаграми Фур’є шумових компонент інтегрованої звукової карти (див. рис. 3.1).

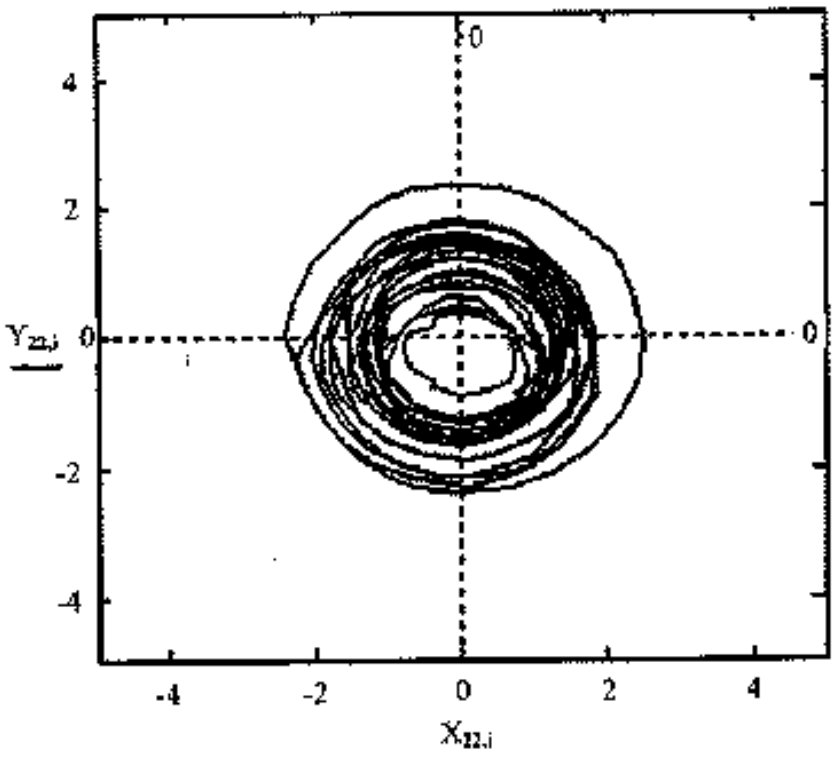

Рис. 3.1 – Приклад фазових портретів (n = 22) для складової низької частоти шумового сигналу досліджуваного комп’ютера [10].

Автентифікація акустичних пристроїв кіберфізичних об’єктів АПК здійснюється шляхом побудови фазової діаграми кожної фур'є-компоненти і розрахунку її параметрів, тобто зміщення центру дивного аттрактора фур'є-компоненти відносно початку координат. Перевірка виконується шляхом порівняння положення центру атрактора відносно початку координат. Атрактор – це траєкторія руху системи, яка не відхиляється від стійкої точки у фазовому просторі і відповідає за розсіювання коливального процесу в системі. Точка стабільності визначає набір власних частот системи, які є різними для конкретного електронного пристрою. Для цих вимірювань атрактор приймає форму набору граничних циклів. У цій роботі використовується зміщення центру атрактора як знак автентифікації (див. рис. 2).

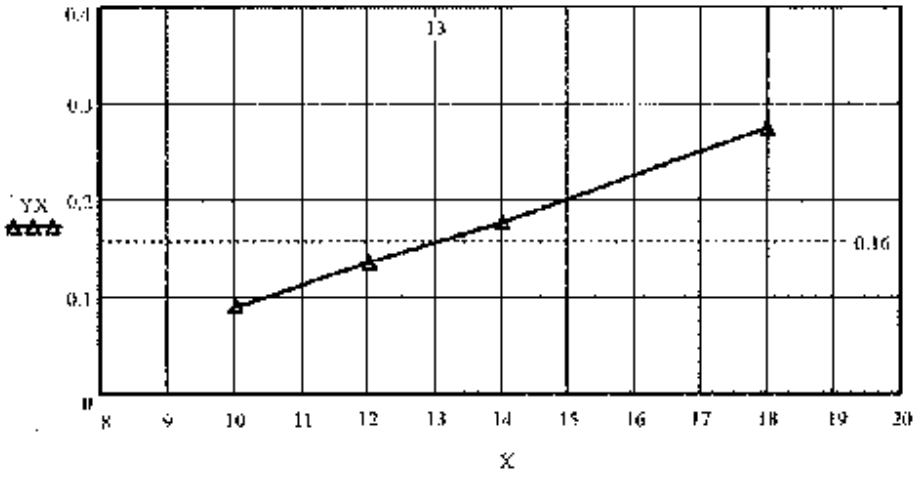

Рис. 3.2 – Відносне зміщення (по вертикалі) центру граничного циклу фазового портрету сигналу на низькій частоті досліджуваного комп’ютера [10].

Проблема автентифікації складних систем, а не лише компонентів кіберфізичних систем, повинні вирішуватися на системному рівні. Щоб отримати доступ до конфіденційної інформації або систем управління кіберфізичним об’єктом IoT, складні системи в АПК повинні бути ідентифіковані. Основні вимоги до такої ідентифікації полягають у наступному. По-перше, серед багатьох таких систем потрібно вибрати систему з правами доступу. По-друге, розпізнавання має бути в режимі реального часу, тобто виконуватись протягом короткого періоду часу. По-третє, процес ідентифікації

не повинен бути обчислювально інтенсивним і забезпечувати повну автоматизацію.

Інваріантні характеристики складної системи на основі даних часового ряду $x_j(t_i)$ не зазнають зовнішнього впливу складної системи, і немає необхідності розраховувати спектральні характеристики. В якості такої інваріантної характеристики застосуємо автокореляційну функцію шумового сигналу (АКФ ШС), яка забезпечує автентифікацію електронного пристрою кіберфізичного об'єкту АПК.

Зауважимо, що усі гіпотези щодо поведінки кіберфізичної системи повинні бути експериментально перевірені для кожного типу складної системи, яку необхідно ідентифікувати. Графік автокореляційної функції часового ряду являє собою набір дискретних точок. Якщо з'єднати ці точки прямою лінією, то вийде ламана, яка для кожної складної системи розраховується і будується своя полілінія.

Розроблена методика обробки вихідного сигналу електронного пристрою, яка дозволяє розрізняти відмінності між еталонним та іншими пристроями об'єктів АПК. Для цього оцифровуються автокореляційні функції на основі осцилограм їх вихідних сигналів. АКФ ШС являють собою дискретну послідовність значень n (де n - еталонне число автокореляційної функції) для N еквідистантних через час Δt вибірок з частотою дискретизації $f_d = 1/\Delta_t$.

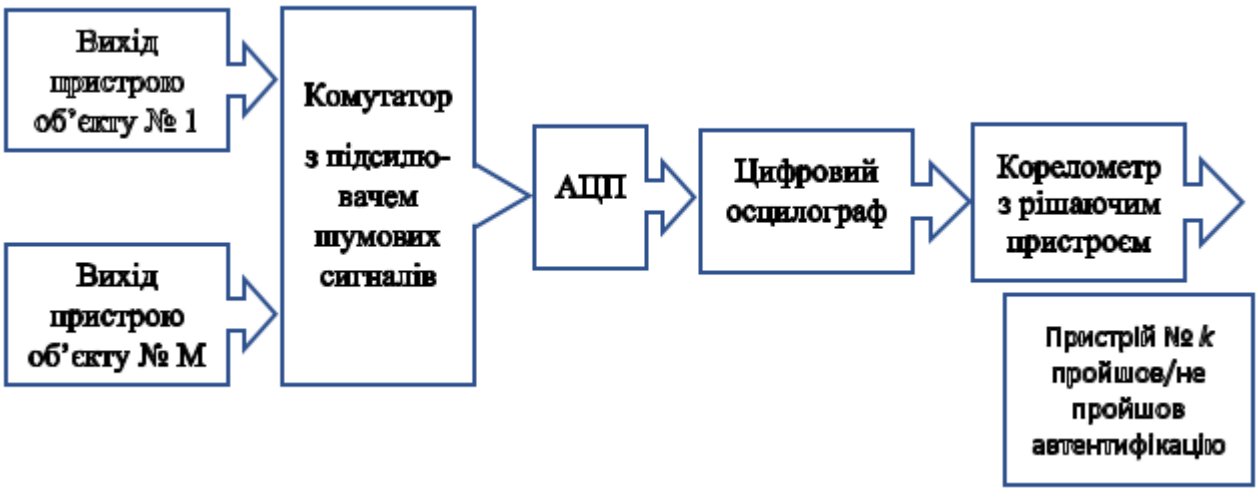

Рис. 3.2. Структурна схема інформаційної системи автентифікації електронних пристроїв об'єктів АПК за їх шумовими характеристиками.

Результати цифрових вимірів шумових сигналів записуються у файл з розширенням wav. Тривалість кожного файлу становить до 10 секунд. Регульований АЦП та осцилограф дозволяють змінювати $f_d \epsilon$ [2 кГц - 400 кГц] та надає можливість візуалізувати на екрані монітора зміни в часі спектру шумового сигналу. Для дискретизації низькочастотного шумового сигналу вибрано $f_d = 44{,}1$ кГц. Корелометр обчислює автокореляційну функцію з центруванням її за середнім значенням і нормалізацією оціночної дисперсії.

Як показуть експериментальні дані (див. рис. 3.3) форма m автокореляційних функцій для конкретного електронного пристрою не змінюється і, навпаки, відрізняється по формі від автокореляційних функцій інших пристроїв (див. рис. 3.4).

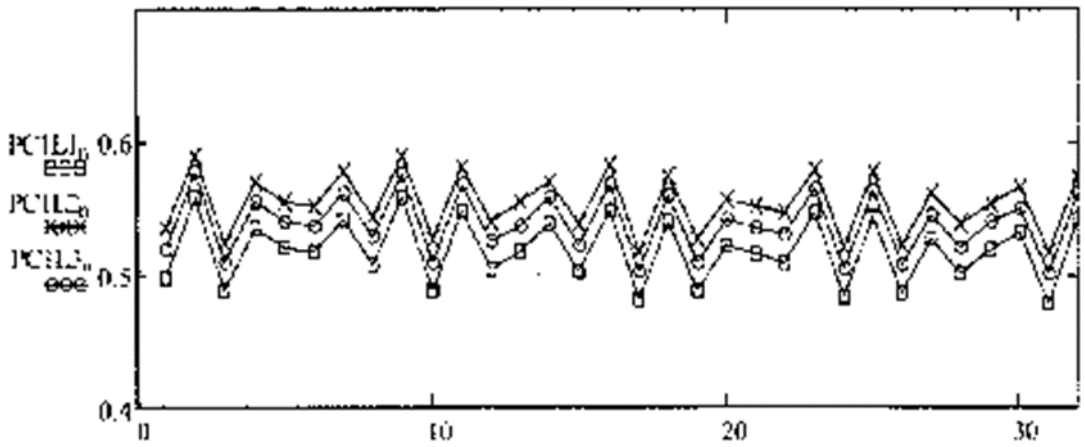

Рис. 3.3 – Порівняння форми автокореляційних функцій шумових сигналів конкретного електронного пристрою (РС) кіберфізичного об’єкту АПК.

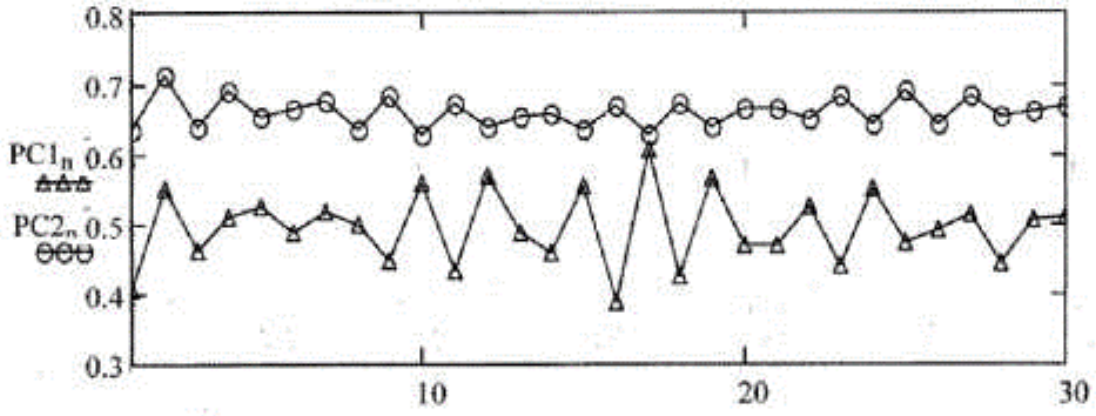

Рис. 3.4 – Порівняння форми автокореляційних функцій шумових сигналів різних електронних пристроїв (РС) кіберфізичних об’єктів АПК.

Властивість зберігати форму функції автокореляції досліджуваних шумових сигналів дає можливість решаючому блоку при перевищенні заданого порогу неподібності автокореляційних функцій еталонного шаблону та конкретного пристрою і приймати в автоматичному режимі рішення про його неавтентифікацію.

Зауважимо, що автентифікація електронних пристроїв з використанням індивідуальних відмінностей їх фізичних сигналів в реальному часі вимагає отримання і вивчення їх інтегральних характеристик. Для цього пропонується використати запропоновані в [10-12] алгоритми детермінованої нееквідистантної цифрової фільтрації в реальному часі сигналів в часовій області на основі «Кодів з мінімальною періодичністю», що дозволяють поєднувати позитивні властивості як періодичних, так і стохастичних процесів. Мінімальна середня частота дискретизації, можливість розпаралелення обчислень при кореляційно-спектральному аналізі, щільна прив'язка вибірок до часової осі є вагомими перевагами такого детермінованого процесу. Останнє необхідно в тих випадках, коли потрібно реконструювати форму сигналу з безлічі зразків. Ці алгоритми дозволяють легко розпаралелювати структуру обчислювального пристрою, їм притаманні простота адресних обчислювальних пристроїв і, як наслідок, простота пристрою управління.

Для обчислення автокореляційної функції використаємо бібліотеку *NumPy* у мові програмування *Python*, яку наведено нижче.

```
python
import numpy as np
import matplotlib.pyplot as plt
def autocorrelation_function(data):
"""
Обчислює автокореляційну функцію для заданого масиву даних.
Параметри:
- data: numpy.ndarray або список, масив даних для обчислення автокореляції.
Повертає:
- Масив автокореляційних коефіцієнтів.
"""
# Перевірка, чи переданий масив як список, і перетворення його у numpy.ndarray
if not isinstance(data, np.ndarray):
```

```
data = np.array(data)
# Обчислення автокореляції
n = len(data)
mean = np.mean(data)
autocorrelation = np.correlate(data - mean, data - mean, mode='full') /
(std(data) * n)
return autocorrelation[n-1:]
#Приклад використання
data = np.array([1, 2, 3, 4, 5, 4, 3, 2, 1])
autocorr_result = autocorrelation_function(data)
# Графік автокореляційної функції
plt.stem(autocorr_result)
plt.title("Автокореляційна функція")
plt.xlabel("Зсув")
plt.ylabel("Автокореляція")
plt.show()
```

У цьому коді функція *autocorrelation_function* обчислює автокореляційну функцію для введеного масиву даних. Потім графік автокореляційної функції можна візуалізувати за допомогою бібліотеки *Matplotlib*.

Програмне забезпечення обчислення (на мові програмування Python) інформаційною системою автентифікації кореляційної функції відповідності шумового сигналу *x(t)* визначеному шаблону *y(t)* представлена нижче:

```
import numpy as np
def correlation_function(x, y):
"""
Обчислює кореляційну функцію між двома масивами x та y.
Параметри:
- x, y: numpy.ndarray або списки, масиви даних для обчислення кореляції.
Повертає:
- Коефіцієнт кореляції між x та y.
"""
# Перевірка, чи передані масиви як списки, і перетворення їх у numpy.ndarray
if not isinstance(x, np.ndarray):
x = np.array(x)
if not isinstance(y, np.ndarray):
y = np.array(y)
# Визначення середніх значень
mean_x = np.mean(x)
mean_y = np.mean(y)
# Розрахунок коваріації
```

```
covariance = np.sum((x - mean_x) * (y - mean_y))
# Розрахунок стандартних відхилень
std_dev_x = np.sqrt(np.sum((x - mean_x)**2))
std_dev_y = np.sqrt(np.sum((y - mean_y)**2))
# Обчислення коефіцієнта кореляції
correlation_coefficient = covariance / (std_dev_x * std_dev_y)
return correlation_coefficient

# Приклад використання
data_x = [відліки сигналу]
data_y = [значення шаблону]
result = correlation_function(data_x, data_y)
print(f"Коефіцієнт кореляції: {result}")
```

Цей код обчислює функцію correlation_function, яка приймає два масиви (або списки) *X* та *Y* і визначає коефіцієнт кореляції між ними. У прикладі використання програми вхідні дані data_x та data_y подаються у вигляді списків.

3.2. Алгоритмічне забезпечення автоматичної автентифікації сенсорів та інтегральних мікросхем з використанням їх шумових характеристик

Сенсори - це первинні вимірювальні перетворювачі, які в результаті взаємодії з об'єктом вимірювання виробляють сигнали і через інтерфейс передають їх в систему реєстрації або автоматичного управління [26]. Найбільш поширеними є Сенсори з електричним вихідним сигналом, який генерується компонентами - електронними компонентами. Шум робочих сенсорів електронних компонентів може бути використаний для їх автентифікації.

Електричний сигнал з виходу сенсора є сумою корисного сигналу і запису шуму. З метою автентифікації шуму видаляється корисний сигнал, пропускаючи вихідний сигнал через фільтр. Шаблон для кожного сенсора створюється в результаті чергової обробки шумового сигналу (див. рис. 3.5).

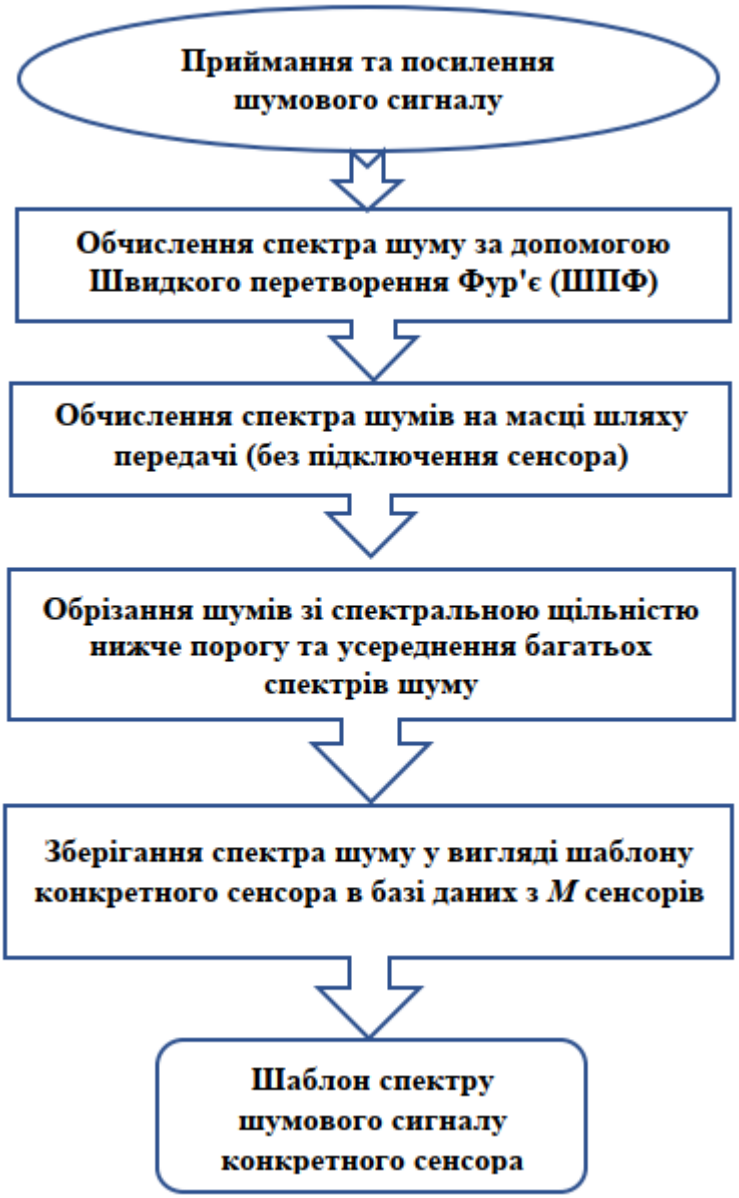

Рис. 3.5 – Алгоритм створення шаблону шумового сигналу для конкретного сенсора.

Алгоритм працює наступним чином. Посилення шумового сигналу (ШС) в часовій області в кілька сотень разів для потрапляння в динамічний діапазон АЦП. Дискретні характеристики шумового сигналу отримуються при частототі дискретизації 1 МГц. При отриманні спектра шуму за допомогою Швидкого перетворення Фур'є (ШПФ) відстань між частотними складовими становила 30 Гц для випробувального стенду і 60 Гц для зразка стенду, виготовленого для використання з метою автентифікації. Шумова складова сигналу, спектральна щільність якого менше заданого порогу відсікається. Введення порогового

значення спектральної щільності логічно пов'язане з тим, що АЦП має власні шуми, які додаються до досліджуваного шуму. Оцінка шуму АЦП повинна бути виконана перед експериментами, але вони можуть бути оцінені як значення мінімального рівня сигналу, який може бути виміряний конкретним АЦП. Множення спектра шумів на масці шляху передачі - це вимірювання, яке виходить без підключеного сенсора, а усереднення багатьох спектрів шуму необхідне для усунення випадкових шумів. Спектр шуму зберігається у вигляді шаблону конкретного сенсора в базі даних з *M* сенсорів. У цьому дослідженні сенсорна діаграма має базовий спектральний пік (його частоту та висоту) та гармоніки, а також їх ширину. Дослідники пов'язують такий спектр з імпульсним живленням сенсора.

Для перевірки автентифікації кожного з сенсорів була використана схема автентифікації (один до багатьох) і отриманий стійкий позитивний результат однозначного розпізнавання Сенсорів. Відстань між шаблоном з бази даних Сенсора, що перевіряється, і повторно виміряним шаблоном принаймні вдвічі менша, ніж відстані до шаблонів інших подібних сенсорів. Паралельно було виявлено, що шаблони сенсорів індивідуально реагують на температуру навколишнього середовища, що також може служити додатковою функцією автентифікації. Для цього потрібно порівняти зміну графіку сенсора зі змінами температури в приміщенні.

Істотним плюсом досліджуваної схеми автентифікації сенсорів є її віддаленість. Застосування однієї і тієї ж маски вимірювальної траєкторії проблематично. На перший погляд, використання маски дає можливість мати на виході алгоритму періодограми шумів тільки досліджуваний сенсор. Але через непередбачуваний вплив зовнішніх електромагнітних полів маска, отримана в попередніх вимірюваннях, може не збігатися з отриманою маскою при подальших вимірюваннях. Тоді це може призвести до неприємних результатів автентифікації. Крім того, при зміні конфігурації тракту передачі потрібно повторно виміряти, щоб створити малюнок маски. Крім того, орієнтація на автентифікацію тільки сенсора з усього вимірювально-передавального тракту

може призвести до неможливості відстеження інших несанкціонованих дій, спрямованих на фальсифікацію даних моніторингу радіоактивної обстановки.

Потрібно звертати увагу на перевірену базу сенсорів, що пояснюється специфікою їх використання. Цілком імовірно, що неможливості розпізнавання однотипних сенсорів може бути виявлено через досить низьку спектральну роздільну здатність стенду автентифікації для більшої доказової бази. Залежність картини сенсора температури від температури також може призвести до неадекватних результатів усереднення, оскільки середні оцінки для шаблонів можуть бути зміщені.

Основною метою автентифікації сенсорів є необхідність отримання від них достовірної інформації. Сенсори можуть встановлюватися у важкодоступних місцях для регулярної перевірки, наприклад, місцях з високим радіоактивним фоном. Візуальний моніторинг сенсорів може бути утруднений. Також слід враховувати, що контроль повинен здійснюватися на всьому протязі шляху вимірювання - передачі даних. Повинна бути гарантія, що не було несанкціонованого підключення до кабелів, наприклад, генераторів передачі помилкових сигналів. Тому потрібно говорити про автентифікацію шляху вимірювання - передачі сигналів.

Метод пасивного аналізу шуму може бути використаний для індикації несанкціонованих перешкод. Основна ідея виявлення фальсифікацій заснована на припущенні, що кожен елемент вимірювального тракту - сигнал, що передається, формує свій характерний шум в загальний сигнал, який доходить до блоку автентифікації. Для цього встановіть метрику для виявлення відмінностей у енергетичному спектрі та використовуйте її для виявлення несанкціонованих перешкод. Для більшої точності фіксації втручань проводять спостереження і контроль в різних спектральних діапазонах.

Алгоритм автентифікації полягає у вимірюванні напруги на виході з тракту передачі сигналу, застосуванні ШПФ для отримання спектра та порівнянні його з базовим спектром. У загальній формі спектра можна виділити кілька різних компонентів, кожен з яких відповідає за різні явища. По-перше, це спектр

сигналу реєстрації радіоактивного випромінювання, а по-друге, це менші по висоті спектральні печі, що характеризують Сенсор і підсилювач сигналу. По-третє, це компонент з мінімальною спектральною щільністю, яка вноситься АЦП, кабелями, пристроями комутації та підключення.

Інтервенційні експерименти були проведені для різних сценаріїв атаки: заміна сенсорів, заміна кабелю, факти відключення - кабельних з'єднань, а також підключення кабелів осцилографа та роботизованого генератора сигналів [25]. Залежно від типу атаки спостерігалися різні варіації зміни спектрального складу шуму - підвищення загального рівня мінімального шуму, а також зсув спектральних піків. Результати експериментів свідчать про те, що за допомогою радіочастотного спектра шумів і імпульсів можна виявити і розпізнати більшість сценаріїв атаки, включаючи найкритичніший - підключення пристрою з низьким опором до фальсифікації сигналу, від'єднання кабелю, зняття Сенсора, заміна його початкового підсилювача.

Експериментально встановлено, що різниця в автентифікації, пов'язана з несанкціонованим втручанням, залежить від відстані між точкою втручання і блоком автентифікації. Зі збільшенням відстані відбувається нівелювання ознак несанкціонованих перешкод, для яких спектральна прозорість шуму значно менша за спектральну щільність корисного сигналу. Якщо змоделювати тракт передачі у вигляді набору блоків, кожен з яких характеризується значеннями загасання електричного сигналу і власного шуму, то видно, що зі збільшенням числа таких блоків тракт передачі «забуває» шум, який був при його виникненні. Зауважимо, що цей факт обумовлює обмеження на використання даного методу виявлення несанкціонованих перешкод і виявлення несанкціонованого доступу за допомогою дистанційної сигналізації може зіткнутися з низкою проблем.

У процесі виготовлення інтегральних мікросхем виникають випадкові відхилення від заданих параметрів: концентрація донорних або акцепторних домішок, геометрія транзисторів, товщина оксидного шару або інші технологічні неточності. Це призводить до невідповідності кожного мікроскопічного транзистора інтегральних мікросхем ТТЛ (транзисторно-транзисторна логіка)

[56], що в свою чергу впливає на значення порогових напруг транзисторів, швидкість наростання і зменшення фронтів імпульсів, різні затримки поширення сигналів в залежності від тракту і так далі. Ці неконтрольовані явища використовуються для автентифікації цифрових пристроїв. Наприклад, виробники FPGA Xilinx і Altera (Intel) використовують ППУ як вбудований неклонований автентифікатор FPGA (програмована логічна інтегральна схема) [5, 7, 28].

Фізично неклоновані функції, засновані на затримці сигналу (кільцеві генератори), використовують різницю в часі проходження декількох копій одного сигналу через задану конфігурацію симетричних шляхів. У заданому запиті в двійковій формі, в даному випадку має місце конфігурація шляхів; Відповідь є результатом порівняння затримок часу поширеннягналів CI [25].

Фізично неклоновані функції статичної пам'яті (SRAM) використовують унікальність значень бітів, що зберігаються в кожному елементі пам'яті. В результаті відмови елементів пам'яті (польових транзисторів) відбувається зміна значень (0 або 1), для кожної мікросхеми це унікальна конфігурація [6, 0].

Однією з основних проблем прикладу ППУ, наведеного на основі статичної пам'яті, є нестабільність деяких значень стану, що вимагає використання кодів корекції помилок. Друга проблема - старіння польових транзисторів з плаваючим затвором, що призводить до зміни ID мікросхеми.

Нова технологія автентифікації чіпа, розроблена компанією Toshiba. В основі лежить випадковий RTG (Random Telegraph Noise) в транзисторах, який виникає через дефекти ізоляційного матеріалу [61]. Цей вид ППУ на основі РТН більш стабільний, ніж попередні електричні навантаження, фактичні дані вимірювань можуть бути використані більше одного мільйона разів. Toshiba розробляє технологію інтер-автентифікації для пристроїв IoT, видаляючи відбиття ППУ в напівпровідникових чіпах для якнайшвидшого розгортання для створення більш безпечних систем IoT.

Toshiba не розкриває подробиць використання RTN для автентифікації, але виходячи із загальних характеристик цього типу шумів [23] - концентрації

спектральної щільності в області низьких частот (≈1 Гц) - можна уточнити, що процедура автентифікації застосовуватись для обмеженої швидкості роботи електронних пристроїв.

3.3. Алгоритмічне забезпечення автоматичної автентифікації персональних комп'ютерів і ноутбуків на основі шумових характеристик

Автентифікація персональних комп'ютерів і ноутбуків за фізичними властивостями важлива з багатьох причин. Це може бути захист від підміни логічних адрес для автентифікації в корпоративній мережі та мережі Інтернет, автентифікація товарно-матеріальних цінностей. За допомогою цієї автентифікації можна дізнатися, чи не відбулася несанкціонована заміна компонентів. Також можна стежити за якістю виробництва комп'ютерів і багато іншого. Тому інтерес до завдань автентифікації ПК і ноутбуків досить великий. На сьогоднішній день завдання автентифікації ПК і ноутбуків є доцільними з точки зору вивчення спектрального складу їх електромагнітного випромінювання. Аналогічні завдання існують і для автентифікації гаджетів і широкого спектру електронного обладнання, яке використовується щодня.

Традиційно електромагнітне випромінювання електронних пристроїв розглядається як випадковий системний шум, інтенсивність якого повинна бути нижче певного порогу для відповідності державним стандартам. Кожен електронний прилад характеризується унікальним електромагнітним випромінюванням, яке можна використовувати як пристрій радіочастотної автентифікації. Зі спектра для певного частотного діапазону, як правило, вказується тип пристрою: ПК, побутова техніка, гаджети, електроінструменти, автомобілі; цей експеримент був доведений експериментально [4, 6]. Класифікація типу пристрою виконана на основі методу опорного вектора (СВМ), який містить складні обчислення і вимагає процедури навчання. Власне, електромагнітне випромінювання пристрою можна використовувати як інструмент автентифікації, замість використання технології RFID-міток. Це

дозволяє значно знизити витрати на логістичні операції з управління активами та відстеження запасів.

У даній роботі використано ідею застосування електромагнітного випромінювання для автентифікації ноутбуків, смартфонів та інших електронних пристроїв [4, 7]. Розглянута технологія пропонується нами для автентифікації ноутбуків та інших пристроїв за допомогою зовнішнього реєстратора. При цьому процедура автентифікації вимагає прямого доступу до досліджуваних приладів, які повинні знаходитися в робочому стані.

В даному випадку в якості реєстратора сигналу використовується зчитувач RTL-SDR (монопольна антена) на базі мікросхеми Realtek RTL2832. Мікросхема містить два 8-розрядних АЦП з частотою дискретизації до 3 МГц і оцінює сигнал від I/Q модуляції. Алгоритм наступний (див. рис. 3.6).

Прийом і оцінка сигналу від включеного пристрою з частотою дискретизації 1 МГц. Попереднє дослідження показало, що сигнали розташовуються в низькочастотній області. Це пояснює вибір частоти дискретизації. Час читання займає частки секунди. Використання ШПФ зі зворотним відліком 2^{17}, що дає роздільну здатність 7,6 Гц.

Видалення шумів з низькими значеннями спектральної щільності на підставі встановленого Порогу, який на 1% перевищує різницю між піковою і середньою спектральною глибиною шумового сигналу:

Поріг = (*пік-середнє*) *1%* + *середнє значення*).

Точки, що з'явилися вище порогу, записуються у вигляді пар значень (частота-величина). Набір пар значень утворює шаблон пристрою. Шаблон за замовчуванням містить від 1000 до 2000 пунктів. Шаблон зберігається в базі даних.

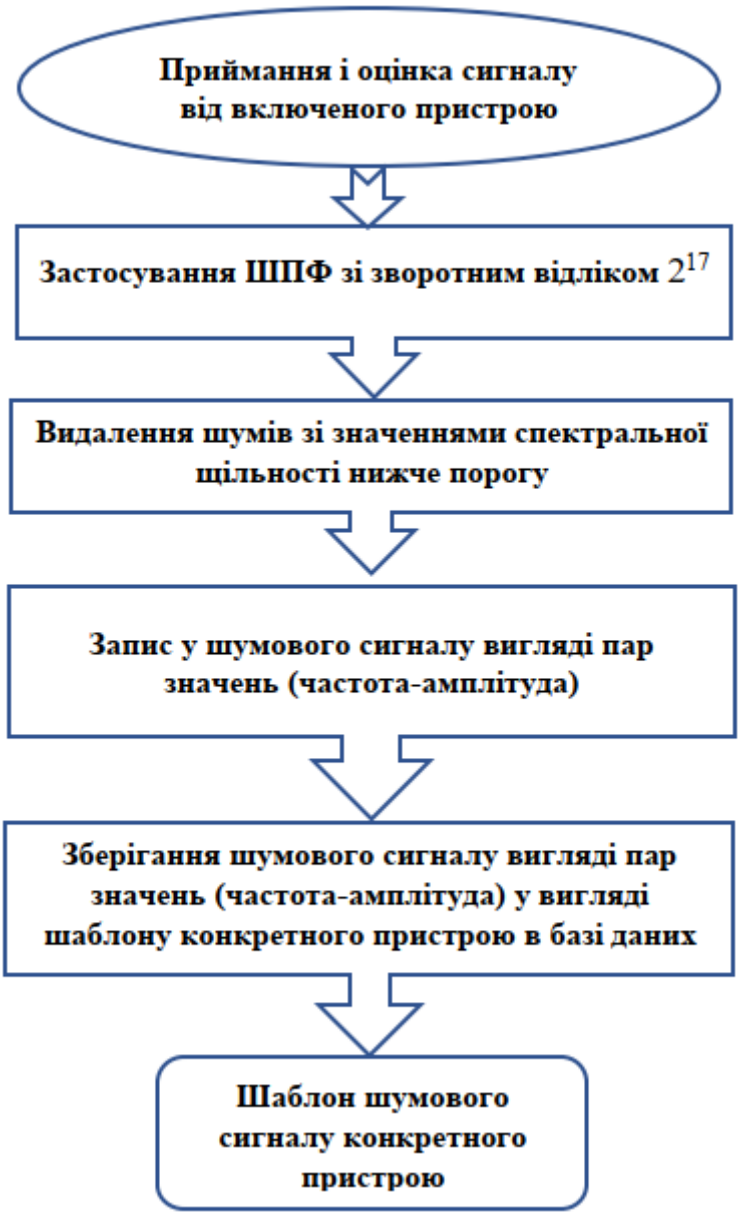

Рис. 3.6 – Алгоритм створення шаблону шумового сигналу для конкретного електронного пристрою кіберфізичного об’єкту АПК.

Для однозначної автентифікації пристрою використовується 2-етапна процедура ранжування, в результаті якої пристрій спочатку класифікується за типом (ноутбук, мобільний телефон і т.д.), а потім відбувається індивідуальна автентифікація всередині типу.

Оцінка типу пристрою здійснюється шляхом порівняння наборів частот, а індивідуальна автентифікація всередині типу відбувається шляхом порівняння величин, що відповідають частотам.

Для ранжування використовується подібність косинусів, C.S. [18, 19]. Однією з переваг подібності косинусів є можливість її швидкої реалізації, особливо для розріджених векторів, для яких слід враховувати тільки ненульові значення. Нехай і — $\{X_i\}$ дві множини, які утворюють два шаблони, де X і$\{Y_i\}$, Y $_i$ — величини спектральних складових електромагнітного випромінювання від приладу *X* і приладу *Y*. Тоді косинусна подібність множин визначається виразом:

$$C.S. = \frac{\sum_{i=1}^{N} X_i Y_i}{(\sum_{i=1}^{N} X_i^2 \sum_{i=1}^{N} Y_i^2)^{1/2}} \quad (3.1)$$

Різні пристрої в межах одного типу мають більшу косинусну схожість, ніж пристрої різних типів. Перевага використання косинусної подібності для ранжування полягає в тому, що її результат інваріантний до різних коефіцієнтів посилення модуля реєстрації електромагнітного випромінювання. Таким чином, шаблон пристрою можна отримати за допомогою одного зчитувача, а перевірити за допомогою іншого; Крім того, кут між площиною антени і поверхнею пристрою не повинен строго підтримуватися.

Автентифікація в межах одного типу пристроїв за допомогою косинусної подібності ґрунтується на принципі максимальної подібності. В результаті перевірки «один до багатьох» з'являється шаблон, косинусна схожість якого з невідомим пристроєм буде максимальною.

Подібні пристрої можуть зовні дуже схожі на шаблони. Так як для кожної автентифікації шаблон нових вимірювань з одного приладу зазвичай відрізняється від того, що написано в базі даних, може виникнути ситуація, що прилад буде помилково автентифікований. З'ясувалося, що для різних типів пристроїв методом електромагнітного випромінювання ймовірність правильної автентифікації різна. Так, найбільшою ймовірністю правильної автентифікації характеризуються монітори комп'ютерів, рідше мають ноутбуки, а найменші мають мобільні телефони.

Для дослідження похибок автентифікації використано гістограми розподілу евклідових відстаней, обчислених між закономірностями, отриманими

в результаті багатьох вимірювань електромагнітного випромінювання від одного приладу та двох шаблонів з бази даних, один з яких є шаблоном *T* досліджуваного приладу, а другий шаблон *F* беруться з аналогічного приладу, аналізуються. Гістограми моделюються як розподіли Гаусса з математичними очікуваннями та середніми квадратичними відхиленнями $\mu_T, \mu_F \quad \sigma_T, \ . \ \sigma_F$Чим більша площа гістограм, що перекриваються (розподіли Гауса), тим більша ймовірність помилкової автентифікації. Для оцінки ймовірності правильної автентифікації приладу *T* як приладу *T* необхідно обчислити площу:

$$P_T = \frac{1}{\sqrt{2\pi}} \int_{\mu_T - 3\sigma_T}^{x_0} \left(\frac{1}{\sigma_T} \exp\left(-\frac{(x-\mu_T)^2}{2\sigma_T^2}\right) - \frac{1}{\sigma_F} \exp\left(-\frac{(x-\mu_F)^2}{2\sigma_F^2}\right)\right) dx \qquad (3.2)$$

Так як 99,73% Гаусса знаходиться в області відносно $\pm 3\sigma \quad \mu$, то в інтегралі нижня межа замінюється на -∞ . Це несуттєво впливає на точність обчислення. Точка x $\mu_T - 3\sigma_{T0}$ є x-координатою точки перетину двох гауссів. Аналогічно можна оцінити ймовірність правильної неавтентифікації приладу T як пристрою F:

$$P_F = \frac{1}{\sqrt{2\pi}} \int_{x_0}^{\mu_F + 3\sigma_F} \left(\frac{1}{\sigma_F} \exp\left(-\frac{(x-\mu_F)^2}{2\sigma_F^2}\right) - \frac{1}{\sigma_T} \exp\left(-\frac{(x-\mu_T)^2}{2\sigma_T^2}\right)\right) dx \qquad (3.3)$$

Спільна область обох гауссових оцінок суми ймовірностей FRR і FAR.

Таким чином, моделювання гістограми у вигляді розподілу Гаусса може бути використане для прогнозування здатності системи автентифікації правильно автентифікувати пристрої за їх електромагнітним випромінюванням. Якщо відстань між центрами Гаусса більше $3(\sigma_T + \sigma_F)$, то ці два пристрої можна практично однозначно автентифікувати.

Метод електромагнітного випромінювання дав однозначну автентифікацію типів пристроїв (досліджувалися ноутбуки, рідкокристалічні екрани, мобільні телефони, люмінесцентні лампи і світлові мечі). Експерименти з автентифікації окремих пристроїв в межах одного типу показали наступний

результат: п'ять ноутбуків MacBook Pro мали середню точність автентифікації 94,6%, двадцять РК-екранів відповідно 94,7%, iPhone 6 були автентифіковані менш надійно - з точністю 71,2%, люмінесцентні лампи автентифіковані з точністю 86%, світлові мечі - 100%.

Факт точної автентифікації всередині одного типу пристроїв, в порівнянні з іншими, вказує на те, що вплив зовнішніх полів в цьому експерименті було незначним. Але вимога про відсутність зовнішніх електромагнітних полів при автентифікації може бути практично нереалістичним. Неточна автентифікація інших типів пристроїв, в першу чергу ноутбуків і рідкокристалічних екранів, може пояснюватися декількома причинами. Основною причиною, швидше за все, є помилка зчитувача RTL-SDR, яка може породити пробій частот до 20 Гц. Другою причиною може бути нестійкість електромагнітного випромінювання, про яке автори дослідження нічого не пишуть. Слід зазначити, що метод призначений для роботи пристроїв, тоді як RFID-мітка автентифікує пристрій незалежно від його стану включення / виключення. Цей метод вимагає наявності зовнішнього лічильника і оператора, тому він не підходить для автентифікації комп'ютерів в мережі [25].

3.4. Алгоритмічне забезпечення автоматичної автентифікації мобільних телефонів (пристроїв) за параметром геолокації без використання ідентифікаторів IMSI та IMEI

У класі завдань для визначення геолокації для мобільних телефонів можна розглядати два завдання:

1) визначення геолокації мобільного телефону як фактора для вирішення різноманітних задач віддаленої автентифікації особи,

2) отримання інформації про місцезнаходження користувача при його спробах входу в кіберсистему на основі відносної близькості місця розташування мобільного телефону відносно конкретного комп'ютера системи як фактора автентифікації.

Стандарт 802.11 [24] визначає спосіб кодування інформації для її передачі за допомогою мобільного зв'язку (див. рис. 3.7).

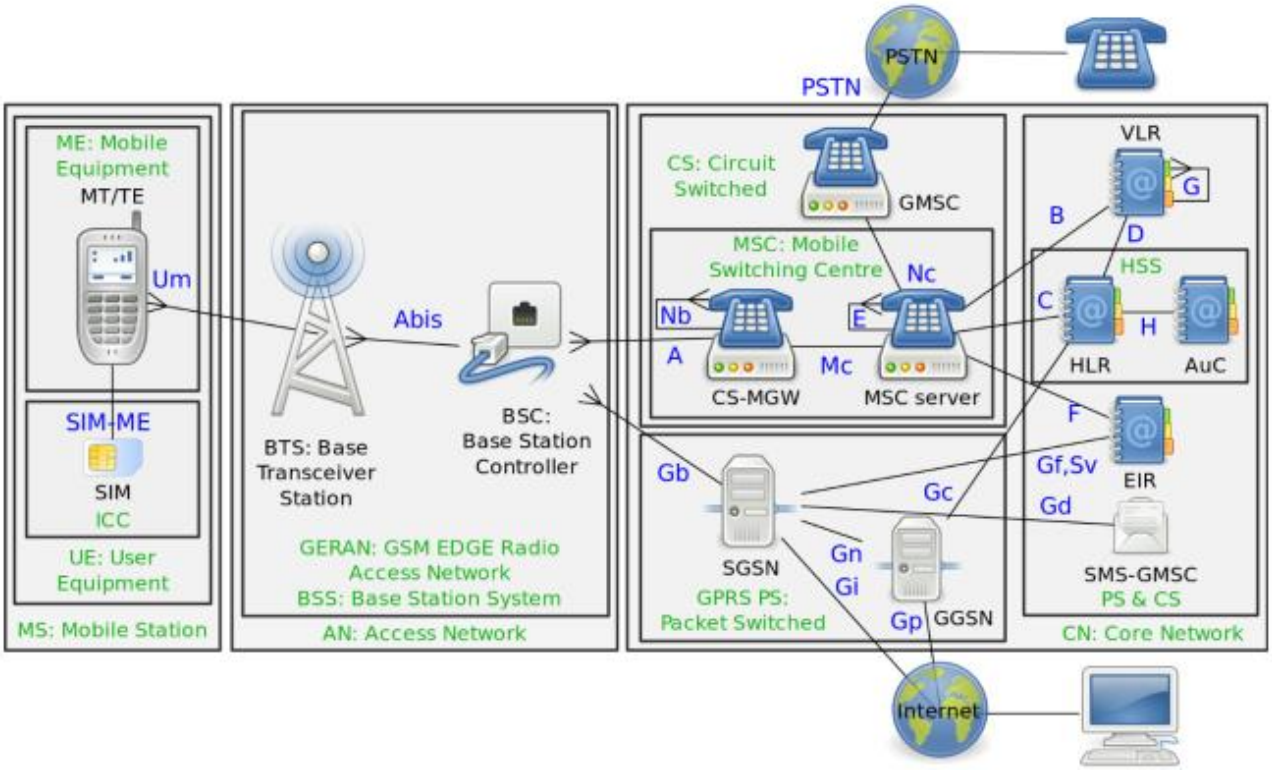

Рис. 3.7 – Структурна схема мережі стільникового зв’язку [24].

Вихідний сигнал в мобільному телефоні спочатку формується в цифровому вигляді і проходить через цифро-аналоговий перетворювач. Далі, використовуючи технологію GMSK (Gaussian Minimum Shift Keying), сигнал проходить через смуговий фільтр, мікшер і підсилювач. Символ у вигляді послідовності бітів вихідної інформації перетворюється в модульований радіочастотний сигнал, який зручно описувати за допомогою діаграми множини сигналів. Радіочастотний передавач повинен виконувати декодування і розпізнавання бітових послідовностей символів. Як правило, комплексний вектор вхідного сигналу має невелике спотворення, яке виражається в його відхиленні - похибці від початкового потрібного положення на діаграмі сузір'я сигналу для даної комбінації бітів. Виправлено поправку до найближчої позиції на діаграмі множини сигналів на основі евклідової метричної відстані.

Дослідники з Дрезденського технічного університету запропонували новий метод автентифікації мобільних телефонів з GSM/LTE на основі фізичних

характеристик радіоапаратури без використання автентифікатора SIM-карти IMSI та автентифікатора конкретного мобільного телефону IMEI [35]. При цьому пропонується використовувати характерні шаблони помилок, які є індивідуальними для кожного мобільного пристрою. Індивідуальність мобільного пристрою обумовлена наявністю допусків в характеристиках радіочастотного тракту в класі відмовостійкості через неточності в процесі виробництва і поломки параметрів комплектуючих. У результаті дослідження доведено практичну реалізацію процедури автентифікації на основі відмінностей на фізичному рівні мобільних пристроїв, які можуть бути відстежені за допомогою технології GSM/LTE.

У процесі формування вихідного модульованого сигналу виникають непередбачувані похибки, які можна виміряти і використовувати для створення унікального шаблону для мобільного пристрою.

Алгоритм створення шаблону пропонується наступний (див. рис. 3.6).

При прийомі радіосигналу в демодуляторі оцінка прийнятого символу проводиться методом максимальної правдоподібності. Вибирається найкраще наближення до переданого символу, тобто найближча точка діаграми множини сигналу в термінах евклідової метрики. Якщо похибка сигналу досить велика, то можна вибрати точку, відмінну від переданої. Тоді демодулятор видає неправильний результат.

Далі, на основі вектора похибки для кожного переданого символу обчислюється метрика фазової похибки. Дослідження показали, що фазова похибка є найбільш інформативною для створення шаблону мобільного пристрою.

Траєкторія метрики сигналу фазової похибки для пакета даних обчислюється у відсотках відхиленням від середнього значення фазової похибки в залежності від переданого символу пакета. Ця траєкторія є шаблоном для мобільного пристрою.

Далі за допомогою технології нейронних мереж, а саме машин лінійних опорних векторів, здійснюється навчання, що дозволяє автентифікувати мобільний пристрій за шаблоном.

Рис. 3.8. Алгоритм створення шаблону для автентифікації мобільного телефону (електронного пристрою) без використання автентифікаторів IMSI та IMEI конкретного мобільного телефону.

Оцінка ефективності методу була заснована на TAR (True Acceptance Rate) - ймовірності правильної автентифікації мобільного пристрою і склала 96,67%. Показано, що для створення тестового шаблону достатньо тридцяти пакетів.

До позитивних моментів дослідження можна віднести те, що для автентифікації мобільного пристрою не потрібно зламувати зашифрований GSM/LTE-трафік, до того ж модель мобільного пристрою підробити практично неможливо. Основне зауваження полягає в тому, що шаблон насправді створюється не самим мобільним пристроєм, а сполученням, яке є приймачем мобільного пристрою. Ресивер допускає свої помилки в декодуванні сигналу, тому говорити не про шаблон мобільного пристрою, а про пару закономірностей. Автентифікація мобільного пристрою повинна здійснюватися за допомогою приймача, який створив унікальний шаблон.

При вирішенні другого завдання автентифікації виникає необхідність двофакторної автентифікації користувача при онлайн-сервісі, до якого він звертається через персональний комп'ютер/сервер об’єкту АПК . Це вирішується за допомогою другого фактора автентифікації - мобільного телефону. Сервер системи може перевірити, чи розташовані комп'ютер і мобільний телефон поруч один з одним, порівнюючи їх GPS-координати. GPS-Сенсори є на всіх сучасних телефонах, але рідко зустрічаються на комерційних комп'ютерах. Дослідники з Інституту інформаційної безпеки в Цюріху запропонували способи проведення двофакторної автентифікації на основі звуків навколишнього середовища [36]. Другим фактором автентифікації методу є близькість мобільного телефону користувача до пристрою (персонального комп'ютера, ноутбука), який використовується для входу в систему. Близькість розташування двох пристроїв (мобільного телефону і комп'ютера) перевіряється шляхом порівняння шуму навколишнього середовища, який фіксується мікрофонами пристроїв. Істотною перевагою запропонованого методу є зручність користувача - автентифікація відбувається без будь-яких дій з його боку.

Оскільки в основі методу лежить порівняння шуму навколишнього середовища обох пристроїв, яке залежить від розташування точки входу

(аудиторія університету, кафе, вокзал і т.д.), то картина шуму в звичному розумінні не створюється. Замість цього порівнюється схожість звуків, одночасно записаних комп'ютером і мобільним телефоном. Для цього використовується перехресно-кореляційна функція амплітуди шуму першого *x*(i) і другого *y*(*i*) пристроїв.

$$c_{x,y}(l) = \sum_{i=0}^{n-1} x(i) \cdot y(i-l), \qquad l \in [0, n-1] \tag{3.4}$$

Щоб уникнути впливу різниці в трактах запису обох пристроїв, перехресна кореляційна функція нормалізована до середнього квадратичного відхилення шуму

$$c'_{x,y}(l) = \frac{c_{x,y}(l)}{\sqrt{c_{x,x}(0) \cdot c_{y,y}(0)}} \tag{3.5}$$

Для обчислення подібності записів шуму кожен прилад використовує наступний алгоритм шумового забруднення навколишнього середовища (див. рис. 3.9.

Шум навколишнього середовища записується кожним пристроєм. За допомогою системи з *m* цифрових фільтрів генерується *m* пар звукових записів для кожного частотного діапазону. Кількість частотних діапазонів – 32.

Для *m* пар записів *x(i)* та *y*(*i*) обчислюються m нормалізованих функцій перехресної кореляції. Для кожного з них існує максимальне значення max $(c_{x,y}^{m}(l))$.

Оцінка подібності розраховується на основі усереднення значень максимальних перехресних кореляційних функцій з пар складових сигналу

$$S_{x,y} = \frac{1}{m} \sum_{i=1}^{i=m} \max\left(c_{x,y}^{m}(l)\right) \tag{3.6}$$

Рис. 3.9 - Алгоритм використання шумового забруднення навколишнього середовища для автентифікації мобільних пристроїв користувачів кіберфізичних систем АПК.

Інтерес представляє протокол автентифікації, також запропонований в [28]. При реєстрації користувача на сервісі сервер надає йому відкритий ключ, який записується на мобільний телефон. Коли користувач вводить логін і пароль через браузер, сервер перевіряє валідність пароля і відправляє команду на

початок запису шуму навколишнього середовища як на мобільному телефоні, так і на комп'ютері, яка в подальшому пересилається відкритим ключем. Після запису комп'ютер шифрує аудіофайл відкритим ключем телефону і відправляє граф шифру на сервер, який в свою чергу відправляє його на мобільний телефон. Мобільний телефон розшифровує аудіофайл, після чого відбувається процедура розрахунку схожості шумових сигналів. Нарешті, телефон повідомляє серверу, чи можна розглядати два пристрої поруч один з одним. Сервер або дозволяє увійти в систему, або відкидає її.

Проведені експерименти дозволили визначити параметри даного методу перевірки близькості розташування обох пристроїв, основним з яких є довжина аудіофайлу, відстань між пристроями і діапазоном. Істотним плюсом методу є його повна автоматична робота в режимі реального часу. Проте автори наголошують, що цей метод не захищає від посилених атак. Також слід звернути увагу на досить високий рівень апаратного та програмного забезпечення. В експериментах використовувалися мобільні телефони iPhone 5 і Nexus 4, ноутбуки MacBook Pro і Dell. РВЧ становив 0,002. Час автентифікації становив близько 5 секунд. Також потрібно переслати зашифрований аудіофайл тривалістю 3 секунди.

Цей спосіб добре підходить для конкретного контингенту користувачів, які використовують аналогічні мобільні пристрої та комп'ютери і не мають жодних обмежень у використанні пристроїв цього класу. Цей клас завдань вимагає рішень в режимі реального часу в умовах повної автоматизації.

Також серйозною проблемою для використання в кіберфізичних системах є виявлення контрафакту та контрафактних пристрої і об’єктів потребує економічно ефективних рішень. Уніфікованим, економічно ефективним рішенням для автентифікації пристроїв на сьогодні є RFID-мітки. Їх використання в широких масштабах коштують дорого. Їх широке використання можливо за умови, що ціна однієї етикетки не перевищує 5 центів, в той час як реальна ціна в десятки разів вище. Тому автентифікація електронних пристроїв

за їх індивідуальними фізичними характеристиками є перспективним ефективним вирішенням проблеми контрафакту.

У 2012 році був опублікований стандарт ISO 12931:2012 (підтверджений у 2017 році), покликаний допомогти організаціям, які мають перевіряти справжність матеріальних благ [27]. У 2015 році був опублікований звіт [38], в якому представлені категорії елементів автентифікації для зниження ризиків контрафактної продукції.

Підроблені електронні пристрої здебільшого відрізняються від оригінальних комплектуючих меншою групою опору напрузі, струму, частоті, температурі, тиску, радіоактивному фону тощо. Щоб це виявити, вдаються до різноманітних тестів:

- Параметричні випробування – це різноманітні електричні випробування (тест контактів, тест споживаної потужності, тести часу наростання вихідного струму тощо). Потрібен висококваліфікований персонал і спеціалізовані лабораторії;

- Функціональні тести є найбільш ефективним засобом перевірки функціональності компонентів, що мають високий ступінь складності. Є одним з найдорожчих методів тестування для виявлення підроблених пристроїв;

- Прохідні випробування призначені для визначення несправності або ненормальної роботи компонента в напружених умовах роботи, наприклад, при підвищених температурах. Проблема з цим тестуванням полягає в тому, що пристрій пошкоджений або пошкоджений. Необхідний висококваліфікований персонал;

- При проведенні структурних випробувань виявляються можливі дефекти і аномалії, пов'язані з внутрішніми конструкціями. У цих тестах використовується декапсуляція - видалення зовнішньої частини електронного компонента для огляду внутрішньої частини. При цьому можуть бути використані хімічно активні речовини, або порушується тіло організму. У будь-якому випадку пристрій знищується.

Всі ці тести проводяться в спеціалізованих лабораторіях, куди потрібно привезти досліджуваний прилад. Персонал повинен володіти високою кваліфікацією. В результаті проходження і конструктивних випробувань пристрій буде зруйновано.

У цьому ж звіті обговорюються можливі випробування, які базуються на інших підходах. Основна ідея полягає в тому, що підроблені електронні пристрої складаються з дешевих компонентів, або вони використовують більш прості та дешеві методи виготовлення. Це відбивається на характеристиках ненавмисного радіочастотного випромінювання працюючого пристрою, які істотно відрізняються від аналогічного випромінювання непорушеного пристрою [39, 40]. Також є відмінності в радіочастотних випромінюванні при передачі сигналів. Наприклад, сигнал мобільного телефону GSM під час розмови має унікальні особливості, які пов'язані з радіокомпонентами (фільтри, підсилювачі, зовнішні інтерфейси). Різницю між сигналами від двох телефонів можна використовувати для автентифікації телефонів, а також можна відрізнити підроблений телефон від справжнього. Точність методу може бути дуже високою, від 94 до 100%, в залежності від моделі телефону [35]. Інший тест заснований на використанні фізично неіснуючих функцій (PUF), які забезпечують надійний і простий для оцінки результат автентифікації пристрою [4, 1].

Нові підходи забезпечують стабільно високоточні результати. Для того, щоб підробити результати випробувань, довелося б використовувати якісне обладнання для мобільних телефонів і комп'ютерів, що звело б нанівець економічну вигоду від виробництва контрафактної продукції.

Виявлення контрафактної та контрафактної продукції методом розпізнавання унікального пристрою радіочастотного випромінювання вимагає лише комутації електронного приладу та вимірювання цього випромінювання, що легко здійснити в будь-якому місті. Це не вимагає високої кваліфікації оператора, який проводить перевірку. Пристрій не руйнується. Перевірка займає небагато часу і економічно виправдана.

РОЗДІЛ 4. РОЗРАХУНОК ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ СИСТЕМИ АВТЕНТИФІКАЦІЇ КІБЕРФІЗИЧНИХ ОБ'ЄКТІВ АГРОПРОМИСЛОВОГО КОМПЛЕКСУ.

4.1. Фактори, що впливають на ефективність системи автентифікації кіберфізичних об'єктів агропромислового комплексу

Автентифікація кіберфізичних об'єктів в агропромисловому комплексі включає в себе узгодження електронних та фізичних систем для забезпечення безпеки та ефективності виробничих процесів. Низка факторів може впливати на ефективність системи автентифікації в агропромисловому секторі:

Різні типи кіберфізичних об'єктів (сільгосптехніка, датчики, робочі інструменти) і систем можуть вимагати різних методів автентифікації через їхню різноманітність та специфічні умови експлуатації. Зовнішні умови, такі як погода, температура, вологість та велика кількість пилу чи грязі, можуть впливати на довговічність та надійність засобів автентифікації. Системи повинні бути адаптовані до важких умов. Також, кіберфізичні об'єкти можуть бути розташовані на великих площах аграрних угідь і складають розподілену кіберфізичну систему. Забезпечення надійності та зв'язку між об'єктами системи може бути складним завданням. Для ефективної автентифікації потрібна стійка та безпечна комунікаційна інфраструктура. Віддалені місця можуть вимагати розгалуженої та надійної мережі для забезпечення зв'язку між об'єктами та системою автентифікації. Багато кіберфізичних об'єктів в АПК мають обмежені джерела енергії, такі як акумулятори або сонячні панелі. Системи автентифікації повинні бути енергоефективними та пристосованими до умов обмеженого живлення. Системи автентифікації повинні інтегруватися з іншими системами управління та моніторингу, які використовуються в галузях АПК, і для забезпечення цілісності та безпеки, захисту від кіберзагроз та недозволених доступів важливо для забезпечення конфіденційності та надійності систем автентифікації. Системи автентифікації повинні бути вартісно-ефективними та

легкими у впровадженні та управлінні, особливо в агропромислових умовах, де ресурси можуть бути обмеженими. Тому потрібно враховувати специфічності віддалених об'єктів та сенсорів АПК, які можуть працювати в умовах відсутності постійного зв'язку або енергії і можуть витримати фізичні навантаження та забезпечити технічну стійкість.

Урахування цих факторів при розробці та впровадженні систем автентифікації кіберфізичних об'єктів в агропромисловому комплексі може покращити їх ефективність та надійність.

Впровадження системи автентифікації кіберфізичних об'єктів в агропромисловому комплексі може мати економічні вигоди, які треба оцінювати в контексті витрат та користі. Так, системи автентифікації можуть підвищити ефективність управління об'єктами та ресурсами в агропромисловому комплексі, сприяючи оптимізації процесів виробництва та зменшенню витрат часу на ручне управління, допомагають у відстеженні розташування та стану об'єктів, що може зменшити втрати через крадіжки, пошкодження чи неправильне використання обладнання. За допомогою систем автентифікації можна досягти кращого використання ресурсів, таких як паливо, вода, добрива та інші агропромислові матеріали. Врахування та керування кіберфізичними об'єктами може позитивно вплинути на якість виробленої продукції, забезпечуючи правильні умови росту та управління процесами вирощування. Автоматизація процесів автентифікації дає змогу зменшити необхідність у ручних операціях та спростити управління, що призводить до економії робочого часу та зменшення витрат на працю. За допомогою систем моніторингу та аналітики, в які включені автентифікаційні дані, можна здійснювати більш ефективний аналіз стану об'єктів та виробничих процесів. Системи автентифікації можуть запобігати крадіжкам та шахрайствам, що може веде до збереження витрат та збільшення прибутковості. Важливо враховувати вартість інтеграції нових систем автентифікації з існуючою агропромисловою інфраструктурою та обладнанням. Важливим аспектом в оцінці ефективності систем автентифікації є вартість підтримки та обслуговування системи, а також наявність кваліфікованих фахівців. Витрати на

впровадження та інтеграцію системи автентифікації повинні бути адекватними до отримуваних вигод і можливостей. Перед впровадженням системи автентифікації в агропромисловому комплексі важливо провести детальний економічний аналіз, який враховує всі аспекти витрат та доходів.

4.2. Розрахунок економічної ефективності системи автентифікації кіберфізичних об’єктів агропромислового комплексу

Розрахунок економічної ефективності системи автентифікації кіберфізичних об'єктів в агропромисловому комплексі включає оцінку витрат та прибутковості (див. табл. 3.1).

Таблиця 3.1.

Порядок розрахунку економічної ефективності системи автентифікації кіберфізичних об’єктів АПК

Назва операції	**Сутність операції розрахунку економічної ефективності**
Оцінка витрат	Визначення загальних витрат на впровадження системи автентифікації, включаючи вартість обладнання, програмного забезпечення, інтеграції, навчання персоналу та підтримки системи
Оцінка вигод	Визначення потенційних вигод від системи автентифікації, такі як підвищення продуктивності, зменшення втрат, оптимізація використання ресурсів, покращення якості продукції та інші
Визначення часу життєвого циклу	Визначення періоду, на який розраховуються витрати та вигоди (це може бути рік, кілька років або інший стратегічний період життєвого циклу системи)
Прогнозна оцінка ефективності	Розрахунок прогнозованої ефективності системи автентифікації з плином часу, враховуючи потенційне вдосконалення, зростання операцій автентифікації,

	модернізація та масштабування системи, зміну обсягів витрат
Розгляд можливих альтернатив	Оцінка можливих альтернатив системи автентифікації та порівняння їхніх витрат та вигод
Оцінка показників окупності	Розрахунок показників окупності, такі як чистий присутній дохід (NPV), внутрішня норма доходу (IRR) та термін окупності, що дозволить оцінити фінансову ефективність проєкту
Оцінка ризиків	Визначення суттєвих ризиків, пов'язаних з впровадженням системи автентифікації, і врахування їх у розрахунках з використанням різних сценаріїв реалізації подій ризику та чутливості до них системи.
Оцінка зміни вартості грошей в часі	Врахування зміни вартості грошей в часі при розрахунках NPV та інших фінансових показників
Порівняння з розробленим бізнес-планом	Визначення відповідності економічних показників системи автентифікації прийнятим бізнес-цілям при порівнянні отриманих результатів з попередніми прогнозами та планами
Підготовка звіту	Детальний звіт з відображенням всіх розрахунків, прогнозами та висновками

Детальний аналітичний підхід допомагає оцінити економічну ефективність системи автентифікації кіберфізичних об'єктів в агропромисловому комплексі та прийняти виважене рішення щодо впровадження такої системи.

Розглянемо характеристики ринку систем автентифікації (див. табл. 3.2)

Враховуючи фактор того, що динаміка ринку постійно зростає, необхідно створювати нові більш швидкодіючі системи автентифікації об’єктів кіберфізичних систем на основі нових алгоритмів та обчислювальних структур.

Таблиця 3.2.

Попередня характеристики ринку систем автентифікації

№ п/п	Показники стану ринку	Характеристика
1	Кількість головних гравців, од	3
2	Загальний обсяг продаж, грн/ум.од	1500000 грн/ум.од. в місяць
3	Динаміка ринку	Зростає
4	Наявність обмежень для входу	Наявність кваліфікованого персоналу в сфері машинного навчання
5	Специфічні вимоги до стандартизації та сертифікації	Відсутні
6	Середня норма рентабельності в галузі (або по ринку), %	30%

Потрібно також розглянути характеристики потенційних покупців Системи автентифікації кіберфізичних об'єктів в АПК (див. табл. 3.3).

Таблиця 3.3.

Характеристика ринку систем автентифікації об’єктів АПК

№ п/п	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці	Вимоги споживачів до
1	Потреба промисловості або швидко ідентифікувати персонал на об’єктах	Власники великих/середніх/малих підприємств, які потребують систему допуску до об’єкту та рівні доступу	Різняться за видом господарської діяльності:	1.Швидкодія системи 2.Безпечність системи

Продовження табл. 3.3.

№ п/п	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
2	Потреба промисловості або інших об’єктів у захисті інформації	Клієнти банків, які хочуть захистити власні активи	перші – це підприємство, другі – сфера обслуговування	3.Здатність запуску проєкту за короткий термін

Як бачимо, головні конкуренти будуть постійно удосконалювати продукт та робити його кращим за інші. Проте це не означає, що заходити у ринок не варто. На нашу думку, найкращим рішенням буде створення та випуск продукту за прийнятними цінами для нових споживачів та виправдано низьких оптових цін для підприємств. Це буде не зовсім вигідно для існуючих клієнтів системи, але така поведінка на ринку допоможе конкурувати з аналогами.

РОЗДІЛ 5. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1. Нормативно-правові положення з охорони праці та безпеки в надзвичайних ситуаціях.

Національна система нормативно-правових актів України з охорони праці та безпеки в надзвичайних ситуаціях включає в себе закони, постанови, накази та інші акти, які регулюють права та обов'язки працівників і роботодавців щодо забезпечення безпечних умов праці і захисту від надзвичайних ситуацій. Ось декілька основних нормативно-правових актів у цій галузі:

Закон України "Про охорону праці" (від 14 грудня 1992 року № 2694-XII) - цей закон встановлює загальні принципи та вимоги щодо охорони праці в Україні.

Закон України "Про надзвичайні ситуації та станом надзвичайної ситуації" (від 21 грудня 1992 року № 2693-XII) - цей закон регулює організацію та управління діяльністю в галузі захисту населення та територій від надзвичайних ситуацій.

Закон України "Про цивільний захист" (від 5 лютого 1993 року № 3206-XII) - цей закон визначає порядок організації цивільного захисту та заходи щодо захисту населення від надзвичайних ситуацій.

Закон України "Про працю" (від 10 грудня 1971 року № 322-VIII) - цей закон встановлює основні права та обов'язки працівників і роботодавців, включаючи вимоги до охорони праці та безпеки на робочому місці.

Постанова Кабінету Міністрів України "Про затвердження Порядку розслідування нещасних випадків на виробництві та професійних захворювань" (від 23 жовтня 1996 року № 1248) - ця постанова визначає процедуру розслідування нещасних випадків на виробництві та професійних захворювань.

Постанова Кабінету Міністрів України "Про затвердження Положення про організацію та проведення заходів з охорони праці" (від 10 грудня 2003 року № 1913) - ця постанова встановлює загальні вимоги до організації та проведення заходів з охорони праці в підприємствах та організаціях.

Накази Державної служби України з надзвичайних ситуацій (ДСНС) та інших відповідних органів, які регулюють конкретні аспекти безпеки та охорони праці в різних сферах діяльності.

Це лише загальні приклади нормативно-правових актів, які стосуються охорони праці та безпеки в надзвичайних ситуаціях в Україні. При вирішенні конкретних питань, пов'язаних з цими питаннями, важливо враховувати чинне законодавство та консультуватися з фахівцями з охорони праці та безпеки.

5.2. Розрахунок заземлення в виробничих приміщеннях

Блискавкозахист — це комплекс захисних пристроїв, призначених для забезпечення безпеки людей, збереження будинків і споруджень, устаткування і матеріалів від можливих вибухів, руйнувань і пожеж, що виникають від удару блискавки, а в будинках сільськогосподарських підприємств — також для забезпечення безпеки тварин і птахів.

Відповідно до курсу України на гармонізацію національної нормативної бази з міжнародною, прийнято чотири стандарти, а саме:

- ДСТУ EN 62305-1:2012 «Захист від блискавки. Частина 1. Загальні принципи» (EN 62305-1:2011, IDT);
- ДСТУ IEC 62305-2:2012 «Захист від блискавки. Частина 2. Управління ризиками» (IEC 62305-2:2010, IDT;)
- ДСТУ EN 62305-3:2021 «Захист від блискавки. Частина 3. Фізичні руйнування споруд та небезпека для життя людей» (EN 62305-3:2021, IDT, далі — ДСТУ EN 62305-3:2021);
- ДСТУ EN 62305-4:2012 «Захист від блискавки. Частина 4. Електричні та електронні системи, розташовані в будинках і спорудах» (EN 62305-4:2011, IDT).

Основним елементом блискавкозахисту є правильно спроєктоване заземлення. При виносній системі заземлення заземлювачі розташовуються на деякій відстані від заземленого обладнання. Тому заземлене обладнання знаходиться поза полем розтікання струму і людина, торкаючись його, опиниться під повною напругою відносно землі. Виносне заземлення захищає тільки за рахунок малого опору ґрунту.

При використанні заземлюючого пристрою одночасно для електроустановок напруга вище 1000 В мережі з ізольованою нейтраллю і для електроустановок до 1000 В з глухозаземленою нейтраллю, опір заземлюючого пристрою має бути не більше 4 Ом при лінійній напрузі 380 В.

Контур штучного заземлення овочесховища має форму прямокутника. Заземлювач передбачається виконати з сталевих електродів завдовжки 3,5 метри. Верхні кінці вертикальних електродів з'єднуються за допомогою горизонтального електроду - сталевої смуги розміром 50х4 мм, укладеної в землю на глибину 0, 7 м.

Початкові дані для розрахунку штучних заземлювачів зведені в табл. 5.1.

Таблиця 5.1 - Початкові дані для розрахунку захисного заземлення

Вид заземлення	**Виносне**
Довжина вертикального електроду *l*, м	3
Діаметр вертикального електроду, м	0,016
Глибина заставляння заземлювачів у грунт *h*, м	0,5
Питомий опір грунту *р*, Ом*м	50
Кліматична зона	II
Розміри горизонтального електроду *b* х *c*, мм	40 х 4
Опір заземлюючого пристрою *R3.n.*, Ом	4

Розрахунок заземлюючого пристрою робитимемо згідно ДСТУ.

Визначаємо значення електричного опору розтіканню струму в землю від поодинокого заземлювача:

$$R_з = \frac{\rho \cdot K_c}{2 \cdot \pi \cdot l}\left(\ln\frac{2 \cdot l}{d} + 0{,}5 \cdot \ln\frac{4t + l}{4t - l} \right),$$

де ρ – питомий опір грунту, Ом · м;

K_c – коефіцієнт сезонності, що враховує промерзання і просихання грунту, в нашому випадку рівний 2;

l – довжина вертикального електроду, м;

d – діаметр вертикального електроду, м;

t – відстань від поверхні грунту до середини вертикального електроду, м.

$$t = h + 0{,}5 \cdot l,$$

де h – глибина заставляння заземлювача в грунт, м

$$t = 0{,}5 + 0{,}5 \cdot 3 = 2\text{м};$$

$$R_з = \frac{50 \cdot 2}{2 \cdot 3{,}14 \cdot 3}\left(\ln\frac{2 \cdot 3}{0{,}016} + 0{,}5 \cdot \ln\frac{4 \cdot 2 + 3}{4 \cdot 2 - 3}\right) = 33{,}6 \text{ Ом}.$$

Розраховуємо число заземлювачів без урахування взаємних перешкод, що робляться заземлювачі один одному, так званим явищем взаємного екранування:

$$n' = \frac{R_{з.}}{R_{З.П}};$$

$$n' = \frac{33{,}6}{4} = 8{,}4 \approx 8 \text{ шт}.$$

Розраховуємо число вертикальних електродів з врахуванням екранування.

$$n = \frac{n'}{\eta_з}$$

де $\eta_з$ – коефіцієнт екранування.

Коефіцієнт екранування приймаємо, за умови, що відстань між вертикальними електродами а = l = 3 м (рис. 5.1).

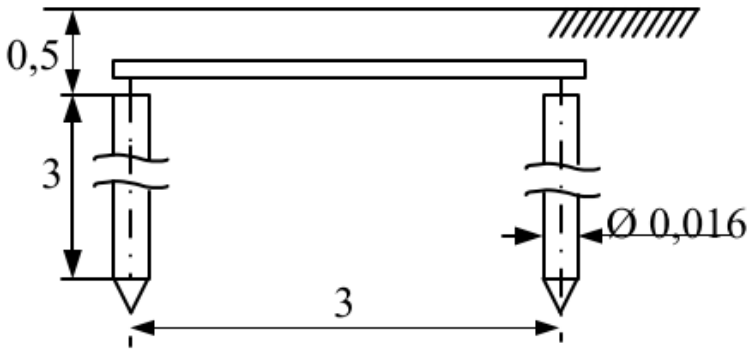

Рис. 5.1 - Схема розташування електродів.

$$n = \frac{n'}{0{,}49} = \frac{8}{0{,}58} = 13{,}8 \approx 14 \text{ шт}.$$

Визначаємо довжину сполучної смуги :

$$l_П = 1{,}05 \cdot n \cdot a;$$

$$l_П = 1{,}05 \cdot 14 \cdot 3 = 44{,}1 \text{ м}.$$

Розраховуємо повне значення опору заземлюючого пристрою :

$$R_{зп} = \frac{R_з \cdot R_п}{R_з \cdot \eta_п + R_п \cdot \eta_з \cdot n},$$

де $\eta_з$ – коефіцієнт екранування смуги, [24];

$$R_{зп} = \frac{33,6 \cdot 4,4}{33,6 \cdot 0,46 + 4,4 \cdot 0,58 \cdot 14} = 2,9 \text{ Ом}.$$

Опір R_{3n} = 2,9 Ом менше ніж допустимий опір 4 Ом. Таким чином, розрахована система заземлення забезпечить захист при винесенні заземлювачів.

ВИСНОВКИ

Прийом, обробка, передача і зберігання технологічної та економічної інформації здійснюється за допомогою різних електронних пристроїв, які працюють в складі інформаційно-комунікаційних систем, або поставляються на ринок для цих цілей. Водночас зростає потреба в автентифікації електронних пристроїв кіберфізичних об’єктів АПК, зокрема, для протидії кібератакам, розповсюдженню контрафактної продукції та медіаконтенту для підвищення безпеки фінансових операцій та доступу до корпоративних або державних онлайн-сервісів. Широкий спектр електронних пристроїв, їх функціональні можливості та застосування в АПК обумовлює актуальність класифікації завдань автентифікації та формування загального підходу до автентифікації електронних пристроїв.

Завдання, які вирішуються на основі автентифікації, пропонується розділити на шість класів, а в якості загального підходу використовувати автентифікацію електронних пристроїв на основі їх індивідуальних відмінностей. Останнє пов'язано з тим, що виробництво електронних пристроїв забезпечує їх роботу в межах відмовостійкості і допускає деяку фізичну неавтентичність.

Ідея використання шумових сигналів для автентифікації електронних пристроїв є цікавою та потенційно ефективною. Однак, наразі, цей підхід не є

дуже поширеним або стандартизованим. Кожен електронний пристрій має свої характеристики шуму, які можуть бути унікальними для кожного пристрою. Ці характеристики можна виміряти та використовувати як "відбитки" для автентифікації.

Програмно-апаратне забезпечення пристрою та самі кіберфізичні об’єкти АПК можуть використовувати вбудовані сенсори (наприклад, мікрофони або акселерометри) для вимірювання шумових характеристик. Представлені в даній кваліфікаційній роботі алгоритми аналізу шумів можуть обробляти ці дані та визначати унікальні шаблони для конкретних пристроїв та об’єктів. Техніки машинного навчання можуть використовуватися для навчання системи розпізнавати та валідувати шумові сигнали, які надає конкретний пристрій. Це дозволяє створити модель, яка може автоматично ідентифікувати пристрій за його шумовими характеристиками.

Автентифікація також може відбуватися в реальному часі, коли пристрій вимірює свої шумові характеристики під час взаємодії з іншими пристроями або системою. Оскільки цей метод використовує фізичні характеристики пристрою, важливо враховувати питання безпеки та конфіденційності. Дані шуму повинні бути ефективно захищені від несанкціонованого доступу. Алгоритми автентифікації повинні бути стійкими до змін шумових умов, таких як різноманітність оточення та взаємодії пристроїв.

Цей підхід є досить новим і вимагає досліджень та вдосконалення. Є питання стосовно стабільності та ефективності в різних умовах. Деякі дослідження вже проводяться в цьому напрямку, але цей метод ще не є загальноприйнятим стандартом у світі автентифікації.

В роботі використано метод аутентифікації компонентів кіберфізичних систем, який базується на інваріантах внутрішніх електричних шумових сигналів. Відстань Хеммінга між двома розрядними послідовностями формується при порівнянні автокореляційнихn функцій двох сигналів від аналогічних електронних пристроїв. Експериментальне дослідження підтвердило запропонований метод аутентифікації. Цей метод може бути

використаний для аутентифікації мережевих пристроїв, для яких існує можливість вимірювання характеристик шуму в режимі реального часу. Надійність аутентифікації (шаблон характеризує тільки цей конкретний пристрій), швидкість обчислень, можливість повної автоматизації є важливими перевагами запропонованого методу. Сферою такої аутентифікації є Інтернет речей, автентифікація пристроїв і людей за допомогою їх шумоподібних сигналів.

Обмеження запропонованого методу полягають у наступному: зовнішні умови не повинні виводити-кіберфізичні системи з квазістаціонарного стану. Додаткові параметри автентифікації можуть зменшити кількість помилкових спрацьовувань і помилкових негативних результатів.

Список використаної літератури

1. Термінологія законодавства (станом на 29.12.2023). Законодавство України. URL: https://zakon.rada.gov.ua/laws/main/termin
2. Міжнародна організація зі стандартизації: ISO/IEC 19794-2:2005 Інформаційні технології - Формати обміну біометричними даними - Частина 2: Finger minutiae data. 2015. URL: https://www.iso.org/standard/38746.html
3. Khana, S.H., Akbar, M.A, Shahzad, F., Farooq, M., Khan, Z.: Secure biometric template generation for multi-factor authentication. Pattern Recognition, No 48 (2), 2015. P. 458-472.
4. Панканті, С., Болле, Р.М., Джейн, А.К. Біометрія: майбутнє ідентифікації. IEEE Computer. 2000. №33(2), С. 46-49.
5. В: Стен, З.Л., Аніл, К.Дж. Ідентифікація «один-до-багатьох». Енциклопедія біометрії. Спрінгер, Бостон, Массачусетс. 2009. С. 138-145.
6. We Are Social Homepage. URLhttps://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/
7. Ідентифікація з відкритим набором. Стен, З.Л., Аніл, К.Дж. (ред.) Енциклопедія біометрії. 2009. Спрінгер, Бостон, Массачусетс.

8. Chaplyga, V., Nyemkova, E., Ministr, J., Chaplyga, V.: Fast Algorithms for Deterministic Non-Equidistant Digital Filtering of Signals in the Time Domain. In: 2018 International Scientific-Practical Conference on Problems of Infocommunications. Science and Technology on Proceedings, IEEE, Kharkiv, Ukraine, 2018. P.135-139.

9. Chaplyha, V., Nyemkova, E.: Using non-uniform sampling in real-time correlation processing of authentication signals. 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology on Proceedings, IEEE, Kharkiv, Ukraine, 2017. P. 474-476.

10. Nyemkova, E., Shandra, Z.: Modelling of the phase portraits of noise for identification of electronic devices. 2016 3rd International Scientific-Practical Conference Problems of Infocommunications. Science and Technology on Proceedings, 2016. P. 125-127. IEEE, Kharkiv, Ukraine.

11. Рибальський, О.В., Соловйов, В.І., Шабля, А.М., Журавель, В.В., Соловйов, В.І.: Система автоматизованого голосового пошуку. Інформатика та математичні методи в моделюванні. 2015. № 5 (4), С. 302–307.

12. Рибальський, О.В., Журавель, В.В.: Метод верифікації особи за фізичними параметрами безмовних сигналів повідомлень, що містяться в голосовій базі даних, за допомогою системи автоматичного пошуку «АВАТАР». Державний науково-дослідний експериментально-криміналістичний центр МВС України, м. Київ. 2018.

13. Джуман В. Аналіз сучасного стану методів і засобів автентифікації електронних пристроїв. Студентська молодь і науковий прогрес: тези доп. Міжнар. студ. наук. форуму, 4 – 6 жовт. 2023 р. [Електронний ресурс]. Львів, 2023. С. 452.

14. Рибальський О.В., Соловйов В.І., Журавель В.В. Системи інструментарію експертизи аудіо- та відеозаписів існують в Україні. Вісник Полоцького державного університету, серія С, Фундаментальні науки. 2018. № 4, С. 1-15.

15. Хуа Г., Бі Г., Річ В.Л.Л.: До практичних питань частотної аудіокриміналістики електричних мереж. IEEE Access. 2017. № 5, С. 2064 – 2065.

16. Лю, Ю., Юань, З., Маркхем, П. Н., Коннерс, Р.В., Лю Ю.: Ширококутна частота як критерій автентифікації цифрових аудіозаписів. Загальні збори Енергетичного товариства IEEE, IEEE, Сан-Дієго, Каліфорнія, США, 2011 С. 1-7.

17. Чай, Дж., Лю, Ф., Юань, З., Коннерс, Р.В., Лю, Ю.: Джерело ENF у цифрових записах, що живляться від батарейок. Аудіо Engineering Society Convention. 2013. С.1-6.

18. Лю, Ю., Юань, З., Маркхем, П. Н., Коннерс, Р.В., Лю Ю.: Застосування частоти системи живлення для цифрової аутентифікації звуку. IEEE Transactions on Power Delivery. 2012. № 27(4), С. 1820-1828.

19. Лв, З., Ху, Ю., Лі, Ч.-Т., Лю, Б.-Б.: Аудіокриміналістична аутентифікація на основі MOCC між ENF та еталонними сигналами. In: 2013 IEEE China Summit and International Conference on Signal and Information Processing, IEEE, Пекін, Китай. 2013. P. 427-431.

20. Чуанг, В.-Х., Гарг, Р., Ву, М.: Антикриміналістика та контрзаходи частотного аналізу електричних мереж. IEEE Transactions on Information Forensics and Security. 2013. No 8(12), P. 2073-2086.

21. Хуа, Г., Чжан, Ю., Гох, Дж., Тінг, В.Л.Л.: Аудіоаутентифікація шляхом вивчення карти абсолютних помилок сигналів ENF. IEEE Transactions on Information Forensics and Security. 2016. No 11(5), P. 1003-1016.

22. Кобб, В.Е., Ласпе, Е.Д., Болдуін, Р.О., Темпл, М.А., Кім, Ю.К.: Внутрішня аутентифікація на фізичному рівні інтегральних схем. IEEE Transactions on Information Forensics and Security. 2012. No 7(1), P 14-24.

23. Свобода Й., Шанфейн М. Апарат, система та метод аутентифікації датчиків. JUSTIA Patents, 2013. No 10066962.

24. Бейкер, Б., Сандерс, Дж., Шанфейн, М., Свобода, Дж., Вест Дж.: Дослідження аналізу пасивного шуму щодо індикації несанкціонованого

доступу. ПРЕПРИНТ INL/CON-15-34213, Національна лабораторія Айдахо , Айдахо. 2015.

25. Лапут, Г., Янг, К., Сяо, Р., Семпл, А., Харрісон, К.: Em-sense: Розпізнавання дотику неінструментальних, електричних та електромеханічних об'єктів. Матеріали 28-го щорічного симпозіуму ACM з технології програмного забезпечення інтерфейсу користувача, ACM, Нью-Йорк. 2015. С. 157–166.

26. Ян С., Зразок, А.П.: EM-ID: Безтегова ідентифікація електричних пристроїв за допомогою електромагнітного випромінювання. IEEE International Conference on RFID, IEEE, Орландо, Флорида, США. 2016. P. 1-8.

27. Подібність, К., Баярдо, Р.Дж., Ма, Ю., Срікант, Р.: Масштабування пошуку подібності всіх пар. In: Матеріали 16-ї Міжнародної конференції з Всесвітньої павутини. ACM, Банф, Альберта, Канада, 2007. С. 131–140/

28. Тата С., Пател Дж.М. Оцінка селективності предикатів косинусної подібності на основі tf-idf. Інформаційний бюлетень ACM SIGMOD Record. 2007, No 36(2), P. 7–12.