Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
"Допущено до захисту"

« »_____2025р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
на тему: «Порівняння технологій NFC та RFID»

оцінка « _____ »
Голова ЕК
Мичуда Л.З.

Керівник: к.т.н. Шеханін К.Ю.
Рецензент: к.т.н. Лещинин Ю.З.
Виконавець: студент групи КБ-41
Куніцин О.В.

Харків 2025

РЕФЕРАТ

Пояснювальна записка до бакалаврської дипломної роботи містить 40 сторінок, 3 рисунка, 3 таблиці, 2 додатки, 25 джерел посилань.

Метою цієї роботи є всебічне дослідження та порівняльний аналіз сучасних смарт-карток, які використовують технології радіочастотної ідентифікації (RFID) та комунікації ближнього поля (NFC).

Об’єктом дослідження є смарт-картки, що функціонують на основі зазначених безконтактних технологій. Предмет дослідження охоплює специфіку використання RFID і NFC у таких картках, з особливою увагою до аспектів кіберзахисту та способів протидії потенційним загрозам і атакам.

У рамках роботи здійснено зіставлення ключових характеристик технологій RFID і NFC, зокрема таких параметрів, як відстань дії, швидкість передачі даних, галузі впровадження, економічна ефективність та рівень захищеності інформації. Основний акцент зроблено на виявлення переваг і відмінностей між двома підходами, а також на вивчення ризиків, пов’язаних із їх використанням, можливих вразливостей та засобів їх нейтралізації.

Отримані результати можуть бути використані як база для подальших наукових досліджень, а також для розробки практичних рекомендацій щодо підвищення рівня кібербезпеки при експлуатації смарт-карток на основі RFID та NFC.

Ключові слова: КІБЕРБЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ЗЧИТУВАЧ, МІТКА, МІКРОЧІП, СМАРТ-КАРТКА, ПОРІВНЯЛЬНИЙ АНАЛІЗ, РАДІОХВИЛІ, RFID, NFC, ЗАХИСТ, РЕКОМЕНДАЦІЇ.

ABSTRACT

The explanatory note to the master's project contains 40 pages, 3 images, 3 charts, 2 appendices, and 25 references to sources.

The objective of this study is to conduct a comprehensive examination and comparative analysis of modern smart cards that operate using Radio Frequency Identification (RFID) and Near Field Communication (NFC) technologies.

The object of the research includes smart cards based on these contactless technologies. The subject of the research focuses on the specific features of applying RFID and NFC in smart cards, with particular attention to cybersecurity aspects and methods of countering potential threats and attacks.

Within the scope of the work, a comparison of the key characteristics of RFID and NFC technologies is carried out. This includes analysis of parameters such as communication range, data transfer speed, areas of application, cost-effectiveness, and the level of information security. The emphasis is placed on identifying the advantages and distinctions between these technologies, as well as examining the associated cyber risks, vulnerabilities, and protection mechanisms for smart cards.

The findings of this analysis serve as a foundation for further research and the development of practical recommendations aimed at enhancing cybersecurity when using smart cards based on RFID and NFC.

Keywords: CYBERSECURITY, THREATS, VULNERABILITIES, READER, TAG, MICROCHIP, SMART CARD, COMPARATIVE ANALYSIS, RADIO WAVES, RFID, NFC, PROTECTION, RECOMMENDATIONS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

RFID — Radio Frequency Identification

NFC — Near Field Communication)

HF — High Frequency

EPC — Electronic Product Code

LF — Low Frequency

UHF — Ultra High Frequency.

ISO — International Organization for Standardization

IEC —International Electrotechnical Commission

ВСТУП

У сучасному цифровому світі технології RFID (радіочастотна ідентифікація) та NFC (зв'язок ближнього поля) міцно закріпилися в повсякденному житті. Вони суттєво змінили підхід до доступу до інформації та надання послуг, забезпечуючи зручність і швидкість. Проте, разом з їхнім поширенням виникають нові виклики в галузі інформаційної безпеки.

Смарт-картки, що функціонують на базі цих технологій, дедалі ширше впроваджуються в таких сферах, як транспорт, банківська справа, охорона здоров’я, торгівля, системи контролю доступу тощо. Їхня популярність пояснюється зручністю використання, високою швидкістю обробки даних та можливістю безконтактної взаємодії. Проте зростання використання таких карток призводить і до підвищеного ризику кіберзагроз, зокрема можливості несанкціонованого доступу, перехоплення інформації та зловмисних атак.

За даними дослідницької компанії MarketsandMarkets, обсяг ринку смарт-карток до 2026 року досягне $16,9 млрд при середньорічному темпі зростання 4,0% у період з 2021 по 2026 роки.

Безконтактні смарт-картки обладнані мікрочіпами, внутрішньою пам’яттю та компактною антеною, яка забезпечує зв'язок із зчитувачем за допомогою радіочастотного інтерфейсу. В основі таких карток лежать технології RFID або NFC. Їх застосовують у різноманітних галузях — від комерційного використання до державних проєктів. Зокрема, пандемія COVID-19 стала стимулом для активнішого впровадження безконтактних рішень, які сприяють дотриманню соціального дистанціювання, рекомендованого ВООЗ.

Ефективність смарт-карток також підтверджена в контексті протидії шахрайству та крадіжкам. Наприклад, проєкт Aadhaar в Індії значно посилив попит на подібні рішення. Крім того, зростання занепокоєння з приводу безпеки в громадських місцях сприяє подальшому розширенню ринку безконтактних систем доступу.

Попри численні переваги, смарт-картки залишаються вразливими до кіберзагроз. Атаки на ці системи можуть призвести до витоку персональних даних і порушення конфіденційності. У зв’язку з цим питання кіберзахисту є надзвичайно актуальним і вимагає комплексного підходу.

Метою даної роботи є всебічне дослідження та порівняльний аналіз смарт-карток, що базуються на RFID та NFC, з точки зору їхнього захисту від кіберзагроз. Дослідження має на меті виявлення основних вразливостей цих технологій і розробку ефективних методів їх захисту.

До основних завдань дослідження входять:

1) аналіз сучасного стану RFID- та NFC-технологій;
2) вивчення сфер їхнього практичного застосування;
3) ідентифікація можливих загроз для безпеки;
4) розгляд типових сценаріїв атак;
5) оцінка та рекомендації щодо методів захисту даних, що зберігаються на смарт-картках.

1 ТЕХНОЛОГІЧНА БАЗА RFID ТА NFC

1.1 Загальні поняття про технології ідентифікації

Смарт-картки є одним з найважливіших досягнень у сфері цифрової ідентифікації та зберігання даних. Вони значно змінили способи обробки інформації, підтвердження особи, а також забезпечення безпеки у багатьох сферах — від банківської справи до охорони здоров’я.

Ідея використання картки з вбудованим мікропроцесором виникла ще в середині XX століття. Перші згадки про пристрої, які нагадували сучасні смарт-картки, з’явились у 1960-х роках. Проте лише у 1974 році французький винахідник Ролан Морено запатентував першу смарт-картку з мікросхемою. Його технологія поклала початок новому етапу в розвитку ідентифікаційних систем.

У 1980-х роках смарт-картки почали активно впроваджуватись у банківському секторі, особливо у Франції та Німеччині. Спочатку вони використовувались для зберігання фінансової інформації та виконання безпечних транзакцій. Згодом, із розвитком телекомунікацій, смарт-картки стали основою для SIM-карт у мобільних телефонах.

У 1990-х роках популярність смарт-карток зросла завдяки впровадженню стандартів ISO/IEC 7816, які регламентували фізичні та електричні характеристики карток, а також протоколи обміну даними. Водночас почалося активне впровадження безконтактних технологій, що зробило смарт-картки зручнішими у використанні та придатними для таких сфер, як громадський транспорт, медичне страхування, контроль доступу тощо.

З початку 2000-х років відбувся значний перехід до безконтактних рішень на основі технологій RFID (Radio Frequency Identification) та NFC (Near Field Communication). Ці технології дозволили передавати дані між карткою та зчитувачем на відстані кількох сантиметрів без фізичного контакту, що значно підвищило зручність і швидкість обслуговування.

Смарт-картка, незалежно від типу (контактна чи безконтактна), містить вбудований мікрочіп, який може виконувати різноманітні функції — від простого зберігання даних до обробки складних криптографічних операцій. Основними елементами такої картки є процесор, пам’ять (енергозалежна та енергонезалежна), операційна система і, у випадку безконтактних карток, антена для обміну інформацією через радіочастотний інтерфейс.

Принцип роботи смарт-картки полягає у взаємодії зчитувача з вбудованим мікрочіпом. При зчитуванні даних із контактної картки чип активується через спеціальні металеві контакти. У випадку безконтактних карток зчитувач створює електромагнітне поле, яке активує мікросхему картки та дозволяє обмінюватися інформацією за допомогою радіохвиль.

Смарт-картки можуть мати різні рівні захисту, включаючи PIN-коди, криптографічні ключі, біометричні дані, а також алгоритми автентифікації. Завдяки цьому вони широко застосовуються у сферах, де критично важливо забезпечити конфіденційність та цілісність інформації. На рисунку 1.1 зображений принцип функціонування смарт-картки.

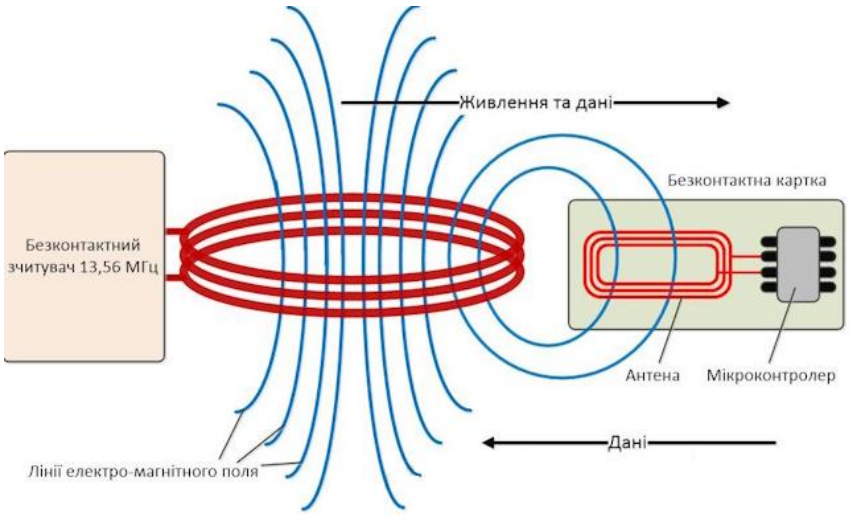

Рисунок 1.1 – Принцип функціонування смарт-картки

1.2 Технологія RFID

RFID (Radio-Frequency Identification) — це сучасна безконтактна технологія автоматичної ідентифікації об’єктів, що базується на використанні радіохвиль для передачі даних між спеціальними пристроями — RFID-мітками (тегами) та зчитувачами (ридерами). В основі роботи RFID-систем лежить принцип бездротової комунікації, що дозволяє отримувати інформацію з міток без необхідності прямого візуального контакту чи фізичного дотику.

До основних компонентів RFID-системи належать:

1) RFID-мітка (тег). Це невеликий електронний пристрій, який містить унікальний ідентифікатор та, залежно від типу, додаткові дані. Мітки поділяються на:

- Пасивні, які не мають власного джерела живлення та отримують енергію для роботи від радіосигналу, що надходить від зчитувача. Вони активуються лише у зоні дії антени зчитувача.
- Активні, які обладнані власним джерелом живлення (батареєю або акумулятором) і здатні самостійно генерувати сигнал, що дозволяє збільшити дальність зчитування.

2) Зчитувач (ридер). Пристрій, який генерує електромагнітне поле для живлення пасивних міток або прийому сигналів від активних. Зчитувач також отримує закодовані дані від міток, розшифровує їх і передає у комп’ютерні системи для подальшої обробки.

3) Антена. Елемент, що забезпечує передачу та прийом радіохвиль між міткою та зчитувачем. Антена може бути інтегрована як у мітку, так і у зчитувач.

4) Система обробки даних. Програмне забезпечення або апаратні засоби, які приймають, зберігають і аналізують інформацію, отриману від зчитувача, інтегруючи її у бізнес-процеси або автоматизовані системи управління.

Принцип функціонування RFID базується на передачі радіохвиль у визначеному частотному діапазоні. Зчитувач випромінює електромагнітний сигнал, який живить пасивні мітки у зоні дії. Пасивна мітка за допомогою вбудованої антени

приймає цей сигнал, перетворює його в електричну енергію, що живить її мікрочип, який у свою чергу формує відповідь — унікальний ідентифікатор чи інші дані. Ця відповідь повертається до зчитувача, який приймає сигнал, розшифровує його та передає далі на обробку. У разі активних міток вони можуть самостійно передавати сигнали без необхідності живлення від зчитувача, що дозволяє збільшити дальність зчитування.

RFID-технологія функціонує у кількох основних частотних діапазонах, кожен з яких має свої особливості та області застосування:

1) Низькочастотний діапазон (LF): 125–134 кГц. Зазвичай використовується для ідентифікації тварин, контролю доступу та інших завдань, де дальність зчитування не перевищує кількох сантиметрів. Цей діапазон характеризується стабільною роботою у складних середовищах (метал, вода).

2) Високочастотний діапазон (HF): 13,56 МГц. Використовується у багатьох системах контролю доступу, бібліотечних системах, електронних квитках та безконтактних платіжних картах. Дальність зчитування — до одного метра. Переважно забезпечує високу швидкість передачі даних.

3) Ультрависокочастотний діапазон (UHF): 860–960 МГц. Забезпечує дальність зчитування до 10 метрів і більше, що робить його оптимальним для логістики, складського обліку та промислового виробництва. Проте UHF-системи чутливіші до перешкод, таких як металеві поверхні чи волога.

4) Мікрохвильовий діапазон: близько 2,45 ГГц. Застосовується рідко, у спеціалізованих системах з високими вимогами до дальності і швидкості передачі даних.

1.3 Технологія NFC

NFC (Near Field Communication) — це технологія бездротового зв’язку ближнього радіусу дії, яка забезпечує обмін даними між пристроями на відстані до 10 сантиметрів. Вона є розвитком технологій радіочастотної ідентифікації (RFID) та базується на стандартах, що визначають радіоінтерфейс, протоколи обміну, а також

рівень безпеки під час передавання інформації. Особливістю NFC є можливість як односпрямованого, так і двонаправленого зв’язку між пристроями, що дозволяє використовувати її не тільки для ідентифікації, а й для взаємодії пристроїв у реальному часі. Технологія NFC працює на частоті 13,56 МГц у високочастотному (HF) діапазоні та дозволяє передавати дані на швидкості 106, 212 або 424 кбіт/с. Комунікація між пристроями відбувається за допомогою електромагнітної індукції, тобто один з пристроїв (активний) створює змінне магнітне поле, в яке потрапляє другий пристрій (пасивний або інший активний), що дозволяє здійснити обмін інформацією.

Усі NFC-пристрої можуть працювати у трьох основних режимах:

- Режим емуляції карти (Card Emulation Mode): пристрій виступає у ролі безконтактної картки, наприклад, банківської або проїзного квитка.
- Режим зчитувача (Reader/Writer Mode): пристрій читає або записує інформацію на NFC-мітки (теги), які не мають власного джерела живлення.
- Режим однорангового обміну (Peer-to-Peer Mode): два пристрої обмінюються даними між собою, наприклад, для передавання контактної інформації, фотографій або посилань.

Основними складовими, які забезпечують функціонування NFC-системи, є:

- NFC-контролер — мікросхема, що керує обміном даними та сигналами.
- Антена — забезпечує прийом і передавання радіосигналів у потрібному частотному діапазоні
- ПЗ (програмне забезпечення) — модулі операційної системи або окремі додатки, які реалізують сценарії використання NFC (платежі, доступ, спарювання пристроїв тощо).

Технологія NFC широко використовується у повсякденному житті:

- Мобільні платежі (NFC-payments): реалізовані в платформах Google Pay, Apple Pay, Samsung Pay та ін., де смартфон виступає в ролі платіжної карти.
- Електронні квитки: оплата проїзду у громадському транспорті шляхом піднесення пристрою до валідатора.

- Безконтактна ідентифікація: заміна пластикових карт для контролю доступу.
- Обмін даними між пристроями: передача контактів, файлів або налаштувань без потреби у підключенні до мережі.
- Інтерактивна реклама та інформаційні стенди: зчитування даних із вбудованих NFC-міток для отримання додаткової інформації.

Незважаючи на близьку відстань передавання, NFC реалізує низку механізмів захисту даних:

- Шифрування передаваних даних;
- Аутентифікація сторін;
- Захищене середовище виконання (Secure Element) — спеціалізований апаратний модуль, який зберігає конфіденційну інформацію (ключі, сертифікати, токени)

NFC може бути інтегрована з іншими бездротовими технологіями, такими як Bluetooth або Wi-Fi. Наприклад, використання NFC для швидкого сполучення пристроїв без необхідності ручного введення пароля або налаштувань.

Іншою важливою перевагою NFC є її енергоефективність. У порівнянні з Bluetooth, NFC споживає значно менше енергії, що робить її придатною для пристроїв з обмеженими ресурсами, наприклад, смарт-міток або смарт-карток. Це дозволяє забезпечити тривале використання пристроїв без необхідності частого підзаряджання або заміни батарейок.

Крім того, завдяки короткому радіусу дії, NFC забезпечує більш контрольовану і безпечну взаємодію, оскільки ризик несанкціонованого перехоплення сигналу значно зменшується. Саме тому вона активно використовується в системах, де важлива безпека транзакцій — банківські операції, контроль доступу до будівель або систем, а також ідентифікація особи.

У сфері Інтернету речей (IoT) NFC відкриває нові можливості для налаштування, конфігурування та спарювання пристроїв. Наприклад, NFC може використовуватися для ініціалізації з'єднання між "розумним" пристроєм (розумною

лампою, термостатом, колонкою тощо) та смартфоном без введення паролів чи сканування QR-кодів.

Нарешті, розвиток NFC-технологій сприяє впровадженню цифрових посвідчень особи, студентських квитків, медичних карток та інших електронних документів. У майбутньому це може стати основою для створення єдиної цифрової ідентичності громадян, інтегрованої в смартфони або носимі пристрої.

1.4 Переваги та обмеження RFID та NFC у порівняльному контексті

До ключових параметрів, що впливають на результативність використання технології RFID, відносяться:

- Швидке зчитування та передача інформації — система здатна в автоматичному режимі розпізнавати значну кількість RFID-міток за секунду, забезпечуючи можливість неодноразового запису й оновлення даних.
- Мінімізація впливу людського чинника: процес зчитування та реєстрації даних здійснюється автоматично, без необхідності ручного втручання оператора.
- Пошук об'єктів без прямої видимості: завдяки радіочастотному принципу роботи, зчитування міток можливе навіть через фізичні перешкоди (упаковку, непрозорі матеріали), з відстані до 10 метрів і більше.
- Забезпечення безпеки та конфіденційності: кожна мітка має унікальний ідентифікатор (ID), а доступ до даних може бути обмежений засобами шифрування або автентифікації.
- Стійкість до впливу агресивних середовищ: мітки здатні функціонувати в умовах підвищеної вологості, забруднення, температурних коливань, під дією механічного тиску або хімічних речовин.
- Гнучкість використання: можливість застосування в різноманітних сферах діяльності, включно з логістикою, виробництвом, медициною, торгівлею та ін.

У той же час, технологія RFID має певні обмеження:

- Чутливість до електромагнітних завад: наявність сильних електромагнітних полів може впливати на якість сигналу та точність зчитування;

- Обмеження щодо зчитуваної відстані: хоча деякі типи RFID-міток забезпечують дальність зчитування понад 10 метрів, існують типи, які ефективно працюють лише на малих відстанях;
- Вразливість до впливу вологи: за умови недостатнього захисту мітки можуть втрачати функціональність у вологому середовищі або при зануренні у рідину.

Щодо технології NFC, її ключовими функціональними перевагами є:

- Підвищений рівень безпеки при короткодіапазонній взаємодії пристроїв, що значно знижує ризики перехоплення даних і забезпечує безпечне виконання транзакцій;
- Миттєва передача даних для виконання безконтактних платежів, при цьому сигнал активується менш ніж за 0,1 секунди;
- Підтримка як зчитування, так і запису даних, що дає змогу реалізовувати широкий спектр сценаріїв взаємодії;
- Мультифункціональність: технологія дозволяє як обмін даними між пристроями (режим peer-to-peer), так і взаємодію з безконтактними картками або інформаційними носіями (наприклад, смарт-плакатами).

Попри це, NFC також має низку технічних обмежень:

- Обмежена відстань роботи: ефективна взаємодія пристроїв можлива лише на відстані до 10 см, що суттєво обмежує зону дії;
- Порівняно невисока швидкість передавання даних: максимальна пропускна здатність становить близько 424 кбіт/с;
- Неоптимальність для передавання великих обсягів інформації: з огляду на швидкість і радіус дії, технологія не є ефективною альтернативою Bluetooth або Wi-Fi у сфері мультимедійного обміну.

1.4.1 Основні стандарти для реалізації RFID та NFC-рішень

Основні стандарти для реалізації RFID та NFC-рішень є ключовими для забезпечення сумісності, безпеки та ефективності цих технологій. Серед них найбільш поширеним для RFID є сімейство стандартів ISO/IEC 18000, яке охоплює

різні частотні діапазони та специфікації. Наприклад, ISO/IEC 18000-3 описує параметри RFID-систем на частоті 13,56 МГц, яка часто використовується у смарт-картках і системах контролю доступу.

Окрему увагу слід приділити стандарту ISO/IEC 15963, що визначає механізми присвоєння унікальних ідентифікаційних номерів (UID) для RFID-міток. Цей стандарт забезпечує унікальність кожного RFID-тегу у глобальному масштабі, що є критично важливим для ідентифікації об’єктів, обліку товарів, а також безпеки систем. Використання ISO/IEC 15963 дозволяє запобігти дублюванню ідентифікаторів, що підвищує надійність і точність роботи RFID-систем.

Для NFC основними стандартами є ISO/IEC 14443, який регламентує фізичні параметри та протоколи зв’язку безконтактних карток ближнього радіуса дії, і ISO/IEC 18092, що описує активні та пасивні режими взаємодії між NFC-пристроями. Ці стандарти визначають сумісність пристроїв, швидкість передачі даних, а також вимоги до енергоспоживання і безпеки. Крім того, NFC Forum розробляє додаткові специфікації та рекомендації, що допомагають уніфікувати протоколи обміну даними та підвищують інтеграцію NFC-технологій у різні платформи.

Впровадження цих стандартів дозволяє створювати надійні, безпечні та сумісні RFID і NFC-системи, які можуть ефективно застосовуватися в різних сферах — від логістики і торгівлі до контролю доступу і мобільних платежів. Стандарти ISO/IEC 15963, ISO/IEC 18000, ISO/IEC 14443 та ISO/IEC 18092 є фундаментальними для розвитку та широкого використання безконтактних технологій у сучасному світі.

Крім технічних аспектів, стандарти також враховують вимоги до захисту інформації, щоб протидіяти різноманітним атакам, таким як підслуховування, підробка або клонування смарт-карток. Ці норми сприяють розробці безпечних протоколів автентифікації і шифрування, що знижують ризики несанкціонованого доступу(особливо важливо в таких критичних сферах, як фінансові послуги, охорона здоров’я та державне управління.) В таблиці 1.1 наведені продукти стандарту ISO/IEC 15963.

Таблиця 1.1 – Продукти стандарту ISO/IEC 15963

Продукт	Опис
Унікальний ідентифікатор (UID)	Це основний елемент стандарту, який забезпечує глобальну унікальність кожного RFID-тега. UID складається з унікального набору символів, який не повторюється у світі, що дозволяє однозначно ідентифікувати кожен об’єкт із RFID-маркуванням.
Система присвоєння номерів	Механізм, що відповідає за централізоване присвоєння унікальних ідентифікаційних номерів для RFID-тегів. Забезпечує керування ресурсом ідентифікаторів, щоб уникнути дублювання ідентифікаторів у різних виробників і застосунках.
Реєстр EPC (Electronic Product Code)	Глобальна база даних, яка зберігає та управляє унікальними кодами RFID-міток, дозволяючи відстежувати об’єкти у ланцюгах постачання та логістиці. Реєстр забезпечує прозорість і стандартизацію в обміні даних між різними організаціями.

2 ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ У МІЖНАРОДНОМУ КОНТЕКСТІ

2.1 Глобальний розвиток рішень на базі RFID та NFC

Технології ідентифікації на основі радіочастотного зв’язку, зокрема RFID (Radio Frequency Identification) та NFC (Near Field Communication), за останні десятиліття набула широкого поширення у світі та стала ключовим елементом цифрової трансформації в різних галузях. Вони активно розвиваються завдяки високому попиту на автоматизацію процесів, покращення безпеки, оптимізацію логістики, спрощення транзакцій і вдосконалення систем управління даними.

Загальносвітовий ринок RFID демонструє стабільне зростання, що зумовлено значним попитом на цю технологію у таких галузях, як торгівля, логістика, охорона здоров’я, транспорт, сільське господарство та промислове виробництво. За даними міжнародних аналітичних агентств, ринок RFID у 2023 році перевищив $15 млрд і продовжує зростати зі середньорічним темпом понад 10%.

У США RFID активно використовується у військовій логістиці, супермаркетах (наприклад, у мережі Walmart), системах обліку медичних препаратів, а також у програмах контролю ланцюгів постачання продуктів харчування. Університети та дослідницькі центри, зокрема MIT Auto-ID Labs, відіграють важливу роль у розробці нових стандартів і впровадженні рішень на базі RFID.

У країнах Європейського Союзу впровадження RFID також підтримується на державному рівні. У Німеччині, Франції та Нідерландах технологія активно інтегрується у сферу охорони здоров’я (ідентифікація пацієнтів, облік медикаментів), в бібліотечні системи, управління багажем у авіації, а також у сільське господарство для відстеження тварин і продукції.

У Китаї RFID став невід’ємною частиною «розумних» міст та інфраструктурних проектів. Зокрема, він широко застосовується у платформах громадського транспорту, логістичних системах, електронному маркуванні товарів і в системах контролю виробництва.

Значна частина RFID-міток та обладнання виробляється саме в Китаї, що робить країну лідером із виробництва у цій галузі.

Японія зосереджується на високоточних RFID-рішеннях, особливо у сфері автоматизації торгівлі та роботизованого складування. У багатьох японських магазинах товари оснащуються RFID-мітками, що дозволяє покупцям здійснювати самостійний розрахунок без участі касира.

У свою чергу, технологія NFC, що є різновидом RFID, орієнтована переважно на короткодіапазонну безпечну взаємодію між пристроями. Вона особливо активно розвивається у сфері мобільних безконтактних платежів, електронного квиткування, ідентифікації користувачів та обміну даними.

Південна Корея та Японія були піонерами в масовому впровадженні NFC ще з початку 2010-х років. У Сеулі NFC широко використовується для оплати проїзду в громадському транспорті, в мобільних гаманцях та в системах доступу до будівель. Японська компанія Sony була серед перших розробників технології (через платформу FeliCa), яка згодом стала стандартом для NFC.

У США та країнах Європейського Союзу NFC став стандартом для безконтактних банківських карток і мобільних платіжних рішень. Такі сервіси, як Apple Pay, Google Pay та Samsung Pay, інтегрують NFC як основну технологію для здійснення транзакцій. Крім того, NFC застосовується в системах контролю доступу, електронних паспортах та смарт-ключах для автомобілів.

У країнах Південно-Східної Азії (особливо в Сінгапурі, Малайзії, Індонезії) NFC активно інтегрується у сферу мобільних фінансів та ідентифікації особи. У багатьох державах впроваджуються національні електронні ідентифікатори з вбудованими NFC-чіпами, що дозволяє громадянам отримувати адміністративні послуги в цифровій формі. На рисунку 2.1 зображений світовий обсяг ринку RFID/NFC.

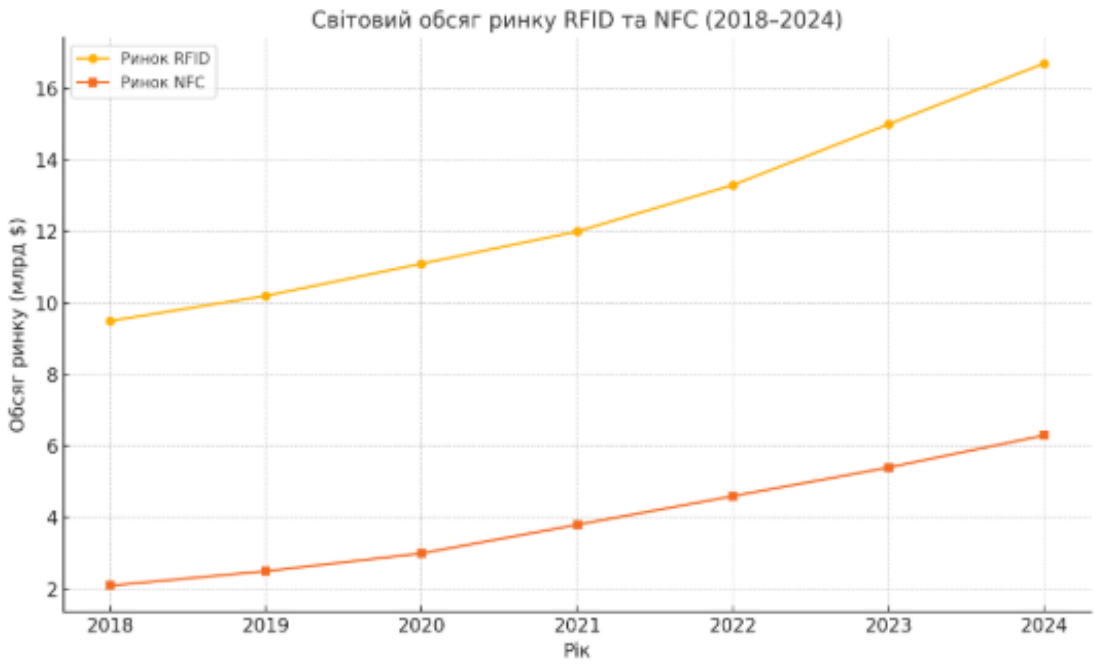

Рисунок 2.1 – Світовий обсяг ринку RFID та NFC

2.1.1 Приклади інтеграції RFID у системах контролю доступу

Одним із найяскравіших прикладів ефективного використання технології RFID у світі є її впровадження компанією Walmart — найбільшою роздрібною мережею у США та однією з найбільших у світі. Walmart почав активно застосовувати RFID ще з початку 2000-х років для оптимізації логістичних процесів, управління запасами та контролю постачання товарів.

У межах цієї ініціативи RFID-мітки були розміщені на транспортних коробках і палетах, які постачалися від постачальників до центрів дистрибуції та далі — до магазинів. За допомогою RFID-зчитувачів у режимі реального часу здійснюється контроль над кожною одиницею вантажу без потреби у візуальному контакті. Такий підхід дозволив значно скоротити витрати, пов’язані з браком товарів на полицях, підвищити точність інвентаризації до 99% та зменшити крадіжки й втрати в ланцюгу постачання.

Окрім Walmart, RFID також активно впроваджується в таких галузях, як охорона здоров’я (наприклад, у лікарнях Великобританії для відстеження руху медичного обладнання), авіація (використання у компаніях Delta Airlines, Qatar

Airways для моніторингу багажу пасажирів), а також у бібліотечних системах (наприклад, у Сінгапурі — повна автоматизація видачі та повернення книг).

2.1.2 Перспективні інтеграції NFC в громадському житті

Одним із найпоказовіших прикладів впровадження технології NFC є використання цієї системи у транспортній інфраструктурі Японії, зокрема — у системі безконтактних смарт-карт Suica та Pasmo, що функціонують у залізничній мережі Токіо та інших регіонах.

Картки Suica/Pasmo, розроблені відповідно компаніями JR East (East Japan Railway Company) і Tokyo Metro, оснащені вбудованими NFC-чипами, які дозволяють пасажирам здійснювати швидку оплату проїзду шляхом прикладання картки або смартфона до турнікету. Час реакції системи становить менше ніж 0,1 секунди, що забезпечує високу пропускну здатність навіть у години пік. Крім транспорту, ці NFC-картки також використовуються для мікроплатежів у магазинах, автоматах із напоями, парковках, а також для доступу до певних об'єктів.

Крім Японії, активне використання NFC також спостерігається у європейських країнах, зокрема у Франції та Німеччині, де NFC застосовується в системах безконтактної оплати проїзду в громадському транспорті. У Південній Кореї NFC є частиною платформи T-money, яка дозволяє розраховуватися за проїзд, покупки та послуги за допомогою смарт-карток або смартфонів з підтримкою NFC.

2.1.3 Застосування смарт-карток із RFID/NFC у ключових галузях за кордоном

Смарт-картки з технологіями RFID та NFC все ширше використовуються у світі завдяки своїй надійності, зручності та здатності підвищувати рівень безпеки у різних сферах. Ці технології активно впроваджуються у фінансовому секторі, транспорті, охороні здоров’я, системах контролю доступу, а також у роздрібній торгівлі та освіті.

У фінансовій сфері безконтактні платіжні картки на базі NFC є одним із найпоширеніших рішень. У Великобританії та країнах ЄС широко використовують платіжні системи Visa Contactless та MasterCard PayPass, які дозволяють оплачувати покупки простим доторком картки до терміналу без необхідності введення PIN-коду для сум до певного ліміту. В Японії технологія NFC впроваджена в мобільних гаманцях, наприклад, у сервісі Suica для оплати проїзду та покупок, що значно підвищує зручність для користувачів.

У транспортній галузі RFID та NFC використовуються для автоматизації оплати проїзду та контролю доступу. Наприклад, у Лондоні карта Oyster базується на RFID-технології та дозволяє швидко проходити через турнікети метро та автобусів. У Сінгапурі популярна система EZ-Link поєднує NFC-картки для оплати транспорту з іншими сервісами, такими як платіж у роздрібних магазинах. Аналогічні системи є у Нью-Йорку (MetroCard), Токіо (Pasmo) та багатьох інших мегаполісах.

У сфері охорони здоров’я RFID/NFC-смарт-картки застосовуються для ідентифікації пацієнтів та збереження медичних даних. У Німеччині та Швейцарії впроваджено електронні медичні картки, що дозволяють лікарям швидко отримувати доступ до історії хвороби пацієнта та медикаментів. Це підвищує точність діагностики та якість лікування, одночасно захищаючи конфіденційність інформації.

У системах безпеки і контролю доступу RFID і NFC-картки використовують для ідентифікації співробітників і відвідувачів у корпоративних, урядових та житлових будівлях. Наприклад, у США багато офісних центрів та урядових установ застосовують смарт-картки для обмеження доступу до приміщень. В Ізраїлі та Південній Кореї подібні рішення використовують для захисту житлових комплексів, де власники мають персоналізовані картки для входу, а система фіксує всі входи та виходи.

У роздрібній торгівлі та сфері послуг смарт-картки використовують для програм лояльності, персоналізації сервісів та прискорення процесу оплати. У

Франції та Італії розповсюджені NFC-картки, що поєднують функції клубних карток із платіжними засобами. Вони дозволяють накопичувати бонуси та швидко оплачувати товари через термінали.

В освітніх закладах у США та Канаді смарт-картки використовуються для ідентифікації студентів, контролю відвідуваності, доступу до бібліотек, їдалень і комп'ютерних класів. Такі системи підвищують безпеку та оптимізують адміністративні процеси.

Таким чином, глобальна практика застосування смарт-карток із RFID та NFC демонструє значні переваги цих технологій, які охоплюють зручність, безпеку та автоматизацію процесів. Постійний розвиток стандартів та технологій сприяє їхній більш широкій інтеграції в різноманітні сфери життя, що підтверджує перспективність використання безконтактних рішень у майбутньому.

2.2 Аналіз реальних кейсів і впровадження RFID/NFC у світі

На національному рівні використання смарт-карток, заснованих на технологіях RFID та NFC, демонструє широке різноманіття ініціатив у багатьох галузях. Сучасний розвиток безконтактних технологій та підвищений інтерес до швидких і зручних засобів комунікації сприяють їхній активній інтеграції в повсякденне життя. Смарт-картки все частіше застосовуються не лише для спрощення користувацького досвіду, але й для оптимізації бізнес-процесів, підвищення рівня безпеки, а також пришвидшення транзакцій та взаємодії з інфраструктурою. Різноманіття варіантів використання таких технологій свідчить як про широкий потенціал їхнього застосування, так і про виклики, які можуть виникати при впровадженні. Кожен проєкт, що використовує подібні рішення, має свої ризики — він може стати як прикладом успішної реалізації, так і зазнати невдачі.

Одним із прикладів ефективного застосування смарт-карток є ініціатива в галузі охорони здоров'я в Сингапурі — програма HealthHub. Це цифрова медична платформа, що дозволяє громадянам зберігати особисті медичні дані на

спеціальних смарт-картках, надаючи постійний доступ до них. HealthHub забезпечує низку функцій: перегляд електронних медичних записів, запис на прийом до лікаря, дистанційний моніторинг стану здоров'я, онлайн-консультації, доступ до медичної інформації, а також підтримку ведення здорового способу життя завдяки інтегрованим фітнес-програмам та рекомендаціям з харчування. Важливою особливістю цієї програми є тісна співпраця з клініками та медичними працівниками, що дозволяє пацієнтам отримувати послуги в зручний час та в будь-якому місці. Крім того, система надає користувачам можливість аналізувати свої фізіологічні показники, що сприяє кращому розумінню стану здоров'я та ухваленню виважених рішень.

Ще один приклад успішного впровадження — система TWIC у США. Програма Transportation Worker Identification Credential застосовується для безконтактної ідентифікації працівників, які мають доступ до стратегічних транспортних об'єктів — портів, терміналів, вантажних зон тощо. Смарт-картки TWIC містять персональні дані, фото, а також біометричну інформацію (наприклад, відбитки пальців), яка зчитується за допомогою RFID або NFC-технології. Це дозволяє оперативно перевіряти особу та її дозвіл на вхід до об'єкта. TWIC значно покращує контроль за доступом до критичної інфраструктури, знижує ризик проникнення сторонніх осіб та сприяє підвищенню загального рівня безпеки в транспортній галузі.

Водночас, є й приклади невдалого застосування смарт-карток, що вказують на можливі технічні, організаційні та безпекові ризики. Одним із таких кейсів є програма Aadhaar в Індії — національна система ідентифікації населення, яка базується на біометричних та персональних даних і присвоює кожному громадянину унікальний 12-значний номер. Попри масштабність і амбітність проєкту, він зіткнувся з низкою проблем:

- Недостатній рівень захисту інформації: система неодноразово ставала об'єктом критики через уразливості, які могли призвести до витоку особистих даних.

- Технічні труднощі: пристрої для зчитування біометричних даних часто працювали нестабільно, що спричиняло затримки або помилки при автентифікації користувачів.
- Інфраструктурні бар’єри: через нерозвинену інфраструктуру в деяких регіонах доступ до системи був обмежений, а її використання — ускладнене.

2.3 Тенденції майбутнього розвитку та потенціал ринку

На державному рівні застосування смарт-карток із технологіями RFID та NFC охоплює різноманітні ініціативи у багатьох сферах. Сучасний розвиток безконтактних технологій та підвищений інтерес до швидких і зручних засобів комунікації сприяють їхній активній інтеграції в повсякденне життя. Смарт-картки все частіше застосовуються не лише для спрощення користувацького досвіду, але й для оптимізації бізнес-процесів, підвищення рівня безпеки, а також пришвидшення транзакцій та взаємодії з інфраструктурою. Різноманіття варіантів використання таких технологій свідчить як про широкий потенціал їхнього застосування, так і про виклики, які можуть виникати при впровадженні. Кожен проєкт, що використовує подібні рішення, має свої ризики — він може стати як прикладом успішної реалізації, так і зазнати невдачі.

Одним із прикладів ефективного застосування смарт-карток є ініціатива в галузі охорони здоров’я в Сингапурі — програма HealthHub. Це цифрова медична платформа, що дозволяє громадянам зберігати особисті медичні дані на спеціальних смарт-картках, надаючи постійний доступ до них. HealthHub забезпечує низку функцій: перегляд електронних медичних записів, запис на прийом до лікаря, дистанційний моніторинг стану здоров’я, онлайн-консультації, доступ до медичної інформації, а також підтримку ведення здорового способу життя завдяки інтегрованим фітнес-програмам та рекомендаціям з харчування. Важливою особливістю цієї програми є тісна співпраця з клініками та медичними працівниками, що дозволяє пацієнтам отримувати послуги в зручний час та в будь-якому місці. Крім того, система надає користувачам можливість аналізувати свої

фізіологічні показники, що сприяє кращому розумінню стану здоров’я та ухваленню виважених рішень.

Ще один приклад успішного впровадження — система TWIC у США. Програма Transportation Worker Identification Credential застосовується для безконтактної ідентифікації працівників, які мають доступ до стратегічних транспортних об’єктів — портів, терміналів, вантажних зон тощо. Смарт-картки TWIC містять персональні дані, фото, а також біометричну інформацію (наприклад, відбитки пальців), яка зчитується за допомогою RFID або NFC-технології. Це дозволяє оперативно перевіряти особу та її дозвіл на вхід до об’єкта. TWIC значно покращує контроль за доступом до критичної інфраструктури, знижує ризик проникнення сторонніх осіб та сприяє підвищенню загального рівня безпеки в транспортній галузі.

Водночас, є й приклади невдалого застосування смарт-карток, що вказують на можливі технічні, організаційні та безпекові ризики. Одним із таких кейсів є програма Aadhaar в Індії — національна система ідентифікації населення, яка базується на біометричних та персональних даних і присвоює кожному громадянину унікальний 12-значний номер. Попри масштабність і амбітність проєкту, він зіткнувся з низкою проблем:

- Недостатній рівень захисту інформації: система неодноразово ставала об’єктом критики через уразливості, які могли призвести до витоку особистих даних.
- Технічні труднощі: пристрої для зчитування біометричних даних часто працювали нестабільно, що спричиняло затримки або помилки при автентифікації користувачів.
- Інфраструктурні бар’єри: через нерозвинену інфраструктуру в деяких регіонах доступ до системи був обмежений, а її використання — ускладнене.

Відсутність альтернативи у разі втрати: у випадку пошкодження чи втрати картки, користувачі могли повністю втратити доступ до державних послуг, що створювало соціальні проблеми.

Додатково, серед організаційних аспектів варто відзначити необхідність стандартизації технологій та інтероперабельності між системами різних постачальників. Впровадження таких рішень вимагає комплексного підходу — від підготовки персоналу до розробки нормативної бази, що забезпечує захист персональних даних та відповідальність за їх обробку.

Також важливо враховувати етичні аспекти використання біометричних і персональних даних, зокрема прозорість збору інформації, обізнаність громадян про обсяги та мету її використання, а також надання можливості контролю над власними даними.

Успішне впровадження смарт-карток на базі RFID/NFC передбачає баланс між інноваціями та безпекою**,** зручністю та конфіденційністю, а також державною підтримкою та технічною надійністю. Тільки в цьому випадку технологія зможе ефективно слугувати громадянам і державі, приносячи довготривалі позитивні результати.

Водночас, для ефективного впровадження RFID та NFC технологій необхідно враховувати низку організаційних аспектів. Зокрема, важливо забезпечити міжвідомчу взаємодію та уніфікацію стандартів, що дозволить уникнути проблем несумісності різних рішень. Також суттєвим є питання навчання персоналу, належної технічної підтримки та роз’яснення переваг таких систем кінцевим користувачам, аби підвищити рівень довіри та уникнути саботажу з боку населення чи працівників установ.

Не менш важливим залишається і правовий аспект — забезпечення дотримання норм захисту персональних даних згідно з чинним законодавством, а також прозорість у процесі зберігання та обробки інформації. Успішність проєктів зі смарт-картками значною мірою залежить від здатності забезпечити баланс між зручністю, функціональністю та безпекою.

3 АНАЛІЗ БЕЗПЕКИ ТА МЕТОДИ ЗАХИСТУ

3.1 Актуальні загрози для безконтактних систем

Смарт-картки — це компактні пристрої з вбудованим мікропроцесором, які широко використовуються у сфері інформаційної безпеки для зберігання та обробки конфіденційної інформації, аутентифікації користувачів, цифрового підпису, захисту банківських транзакцій тощо. Незважаючи на високий рівень захисту, смарт-картки можуть бути вразливими до різних типів атак, які можна класифікувати за характером впливу на логіку, апаратну частину чи поведінку пристрою.

Одним із основних типів атак є логічні атаки (software attacks). Вони спрямовані на програмне забезпечення смарт-картки та здійснюються через комунікаційні інтерфейси. Сюди входить використання шкідливого програмного забезпечення, яке може змінити логіку роботи картки, зламати або підмінити захищені функції. Також до логічних атак належать атаки на криптографічні алгоритми, зокрема підбір ключів методом brute-force, аналіз шифротексту, атаки на протоколи автентифікації та захищеного обміну даними. Зловмисники можуть перехопити обмін повідомленнями між карткою та пристроєм, підмінити їх або повторно використати команди — так звані replay-атаки.

Інший клас — фізичні атаки (hardware attacks), які потребують фізичного доступу до смарт-картки. Такі атаки включають мікроскопічний аналіз мікросхеми за допомогою спеціального обладнання, зондування шин пам’яті для зчитування даних або сигналів, а також декупсуляцію, тобто видалення захисного шару чипа для дослідження його внутрішньої структури. Метою фізичних атак зазвичай є отримання секретної інформації, наприклад криптографічних ключів або PIN-кодів, що зберігаються у пам’яті картки.

Ще один важливий вид загроз — це сторонні атаки (side-channel attacks). Вони не впливають безпосередньо на логіку чи структуру пристрою, а використовують побічні характеристики його роботи: споживання електроенергії, електромагнітне випромінювання, час виконання операцій тощо. Наприклад, атаки по споживанню

електроенергії (Simple Power Analysis — SPA, Differential Power Analysis — DPA) дозволяють аналізувати, які операції виконує картка, і на основі цього відновити частини ключів. Аналогічно, за допомогою електромагнітного аналізу (Electromagnetic Analysis — EMA) зчитується випромінювання мікросхеми під час її роботи. Атаки за часом виконання (timing attacks) базуються на вимірюванні затримок при обробці різних команд і дозволяють зробити висновки про структуру даних.

Окрему групу становлять активаційні атаки (fault injection attacks), метою яких є створення навмисних збоїв у роботі смарт-картки. Ці атаки можуть реалізовуватись через зміну умов навколишнього середовища: коливання напруги, температури, світлове або лазерне опромінення мікросхеми, порушення тактового сигналу (clock glitching). У результаті таких впливів пристрій може обробити дані некоректно, допустити помилки у верифікації або розкрити частину секретної інформації. Такі збої складно виявити, особливо якщо картка не має спеціального захисту від подібних впливів.

Крім технічних методів, існують також соціотехнічні атаки, коли зловмисники отримують доступ до інформації не через уразливості пристрою, а шляхом обману користувача. Наприклад, користувача можуть переконати надати PIN-код, передати картку або вставити її в фальшивий термінал. Фішинг, підміна пристроїв введення, встановлення шкідливого ПЗ на банкомати чи термінали — все це методи соціотехнічного впливу, що часто виявляються ефективнішими за складні технічні атаки.

Для протидії вказаним загрозам застосовують комплекс заходів. На апаратному рівні це: екранування мікросхем, вбудовані сенсори виявлення сторонніх впливів, автоматичне стирання пам’яті при спробі злому. На програмному рівні використовуються шифрування даних, складні протоколи автентифікації, захист від повторного використання команд, контроль кількості спроб введення PIN-коду тощо. Важлива також політика фізичної безпеки пристроїв, навчання користувачів і аудит системи безпеки. Базові типи фізичних атак наведені у таблиці 3.1.

Таблиця 3.1. – Основні види фізичних атак

Вид атаки	Опис
Відкритий доступ (Тампінг)	Фізичне розкриття корпусу пристрою або смарт-картки з метою отримання прямого доступу до внутрішніх компонентів, мікросхем або контактів. Це дозволяє зловмиснику читати або змінювати дані, впроваджувати шкідливий код або обходити захисні механізми. Такі атаки часто проводяться з використанням спеціального обладнання та інструментів.
Випромінювання (Емінація)	Збір інформації шляхом аналізу електромагнітних хвиль, які пристрій випромінює під час роботи. Навіть без фізичного контакту з пристроєм, нападник може за допомогою чутливих антен перехоплювати сигнали, що містять конфіденційну інформацію, наприклад, криптографічні ключі або персональні дані. Цей метод відомий як побічний канал атаки.
	Методи включають зміну тактових імпульсів, зміну живлення, вплив лазером або електронними променями. На відміну від пасивних атак, ефективні методи захисту від DFA ще не стандартизовані, хоча виробники смарт-карт ведуть активні розробки в цьому напрямку.
Аналіз відпаду (Форензика)	Метод полягає у вивченні залишкових даних, що залишаються у пам’яті пристрою або на носіях після виконання операцій. Навіть після видалення інформації з пристрою, експерти можуть за допомогою спеціалізованого обладнання та програмного забезпечення відновити ці дані, що створює ризик витоку конфіденційної інформації.

Атаки на логічному рівні зазвичай ґрунтуються на традиційних методах криптоаналізу, експлуатації вразливостей операційної системи смарт-картки або інтеграції шкідливого коду (т.зв. "троянських програм") у програмне забезпечення картки. Згідно зі статистичними даними, саме ці типи атак нерідко демонструють найвищу ефективність.

3.2 Особливості атак на нестандартні протоколи карток

Безконтактні смарт-картки — це тип смарт-карток, що обмінюються даними з зовнішнім зчитувачем за допомогою радіочастотної ідентифікації (RFID) або технології NFC (Near Field Communication), без фізичного контакту з пристроєм. Ці картки працюють на відстані кількох сантиметрів і живляться

електромагнітним полем, що генерується зчитувачем.

На відміну від контактних карток, які використовують стандартні протоколи (наприклад ISO/IEC 7816), безконтактні картки часто використовують унікальні формати обміну даними, визначені виробником або специфікою застосування. Такі формати визначають структуру команд, відповідей, довжину полів, порядок автентифікації, алгоритми шифрування та методи захисту доступу до пам’яті картки.

Одним із найвідоміших прикладів є картки MIFARE Classic, які використовуються у транспортних системах, системах доступу, контролю присутності тощо. Ці картки мають власний пропрієтарний протокол обміну (не повністю відкритий стандарт), який базується на ISO/IEC 14443-A, але використовує спеціальні команди для автентифікації та зчитування/запису блоків пам’яті.

Формат обміну в MIFARE Classic включає:

- автентифікацію через ключі A і B;
- команду READ/WRITE, яка працює з 16-байтовими блоками;
- розділення пам’яті на сектори з контрольними блоками доступу;
- криптографічний алгоритм Crypto-1 (зараз вважається слабким і вже зламаний).

Через унікальність протоколу і недостатній рівень захисту, картки MIFARE Classic стали об’єктом численних атак, включаючи клонування, відновлення ключів через сторонні канали, і аналітичні атаки на протокол автентифікації.

Для покращення безпеки сучасні картки, як-от MIFARE DESFire, вже підтримують більш захищені формати обміну, включаючи AES-шифрування, гнучкі політики доступу та відкриті стандарти сумісності. На рисунку 3.1 зображено сторінку реєстрації картки MIFARE DESFire Classic.

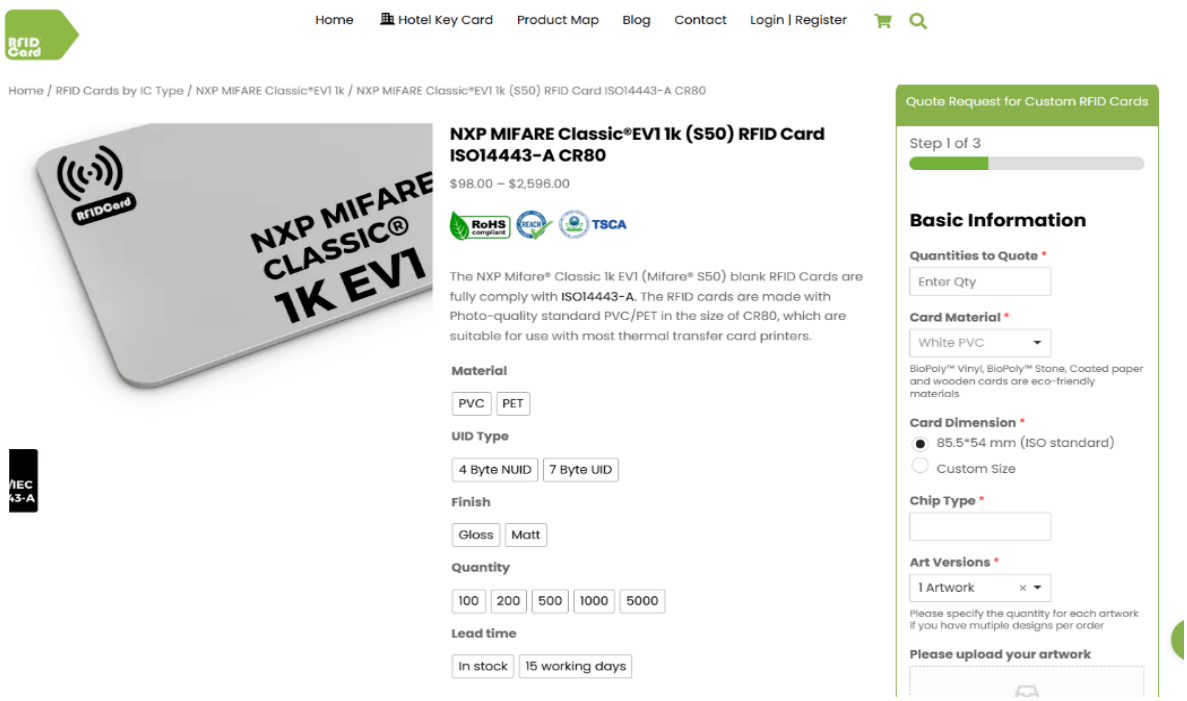

Рисунок 3.2 – Сторінка реєстрації картки MIFARE DESFire Classic

3.2.1 Проблеми безпеки при використанні безконтактних технологій

Однією з головних загроз при використанні смарт-карток із технологіями RFID та NFC є потенційна можливість витоку конфіденційної або чутливої інформації. Це може статися як у результаті технічних недоліків самих карток або зчитувачів, так і через недосконалу реалізацію захисту в програмному забезпеченні. Наприклад, у разі недостатнього шифрування переданих даних зловмисник може перехопити трафік, зчитати і проаналізувати його, використовуючи спеціальні пристрої (так звані RFID/NFC сніфери).

Крім того, ризики збільшуються при використанні карток у публічних місцях, де картка може бути зчитана без відома власника за допомогою прихованих або портативних зчитувачів на близькій відстані. Такий тип загрози називається "безконтактним скімінгом" (англ. skimming) і полягає у несанкціонованому доступі до інформації з карти — наприклад, платіжних реквізитів або ідентифікаційних даних.

Окрему небезпеку становить небажаний ретрансляційний (relay) напад, при якому зловмисники імітують присутність справжньої картки поблизу зчитувача, фактично здійснюючи транзакцію або авторизацію без участі власника. У поєднанні з соціально-інженерними методами такі атаки можуть мати серйозні наслідки для безпеки користувача.

Також варто зазначити, що деякі моделі карток зберігають персональні дані (наприклад, ПІБ, номер документа, дату народження), що становить загрозу у разі несанкціонованого доступу. Зібрана інформація може бути використана не лише для шахрайства, а й для соціальної інженерії або створення фальшивих документів.

Для запобігання витокам важливо застосовувати сучасні засоби захисту: шифрування каналів зв'язку, автентифікацію пристроїв, регулярне оновлення прошивок зчитувачів, а також фізичні захисні засоби, як-от RFID-блокувальні гаманці, що запобігають несанкціонованому зчитуванню.

Для ефективного зниження ризиків витоку даних також варто впроваджувати багатофакторну аутентифікацію, коли для доступу до функціоналу картки необхідно не лише фізичне наближення, але й введення PIN-коду або біометричної інформації. У промисловості та державному секторі особливо актуальним стає впровадження спеціалізованих протоколів шифрування (наприклад, DESFire EV2 або MIFARE Plus), які забезпечують додатковий рівень захисту.

Освітні кампанії для користувачів щодо безпечного використання карток, небезпеки відкритого носіння картки в громадських місцях і важливості зберігання її у захищеному чохлі або гаманці також відіграють важливу роль у запобіганні інцидентам.

Таким чином, проблема витоку чутливої інформації при експлуатації безконтактних карток залишається актуальною та потребує комплексного підходу до захисту — як на апаратному, так і на програмному рівнях.Детальніше про основні типи соціальної інженерії йдеться у таблиці 3.2.

Таблиця 3.2 – Форми соціального інжинірингу із прикладами атак стосовно смарт-карток

Форма	Опис
Фішинг	Надсилання підроблених електронних листів або SMS із посиланням на фальшиві сайти, де користувач вводить дані смарт-картки чи PIN-код.
Пре-текстинг	Шахрай створює переконливу легенду (наприклад, працівника банку), щоб телефоном або особисто виманити конфіденційну інформацію про смарт-картку.
Вішинг	Аудіофішинг: жертві дзвонять, представляються співробітником служби безпеки банку та просять вказати реквізити картки або підтвердити операцію.
Скіллінг	Встановлення підроблених вебсайтів або мобільних застосунків, які імітують справжні платформи, де користувач вводить дані своєї смарт-картки.
Підглядання	Зловмисник спостерігає за користувачем під час введення PIN-коду або застосування смарт-картки в банкоматі чи платіжному терміналі.

3.3 Засоби і стратегії захисту RFID/NFC-карток

Із розширенням сфери застосування безконтактних технологій, зокрема RFID (радіочастотна ідентифікація) та NFC (зв’язок ближнього поля), питання безпеки таких рішень набуває особливої актуальності. Смарт-картки на основі цих технологій широко використовуються у фінансовій сфері, охоронних системах, громадському транспорті, охороні здоров’я, в освітніх установах, що зумовлює підвищені вимоги до їх захищеності від різноманітних загроз.

Одним з основних засобів захисту є використання криптографічних методів. У сучасних картках впроваджуються алгоритми шифрування, такі як AES, 3DES або ECC, які забезпечують надійне кодування переданих даних. Це унеможливлює

їх перехоплення або підміну при зчитуванні. Додатково реалізуються протоколи автентифікації — як односторонньої, так і взаємної — між карткою та зчитувачем, що дозволяє уникнути атак з використанням фальшивих пристроїв зчитування.

Захист також може реалізовуватися на фізичному рівні. Використання спеціальних екранованих гаманців або обкладинок, що блокують радіосигнал, дозволяє уникнути несанкціонованого дистанційного зчитування даних у громадських місцях. Такі засоби особливо ефективні проти атак у натовпі або у транспорті.

Серед більш комплексних стратегій варто виокремити багатофакторну аутентифікацію, коли для доступу недостатньо лише наявності картки. Додатковими факторами можуть бути PIN-код, біометричні дані (наприклад, відбиток пальця), або підтвердження через мобільний додаток. Такий підхід значно ускладнює використання картки зловмисником у разі її втрати або крадіжки.

Ще одним напрямом є впровадження часових та просторових обмежень. Наприклад, карта може працювати лише в межах певної будівлі або лише у визначений час (робочі години). Це зменшує можливості її використання поза контрольованою зоною.

Окрім цього, важливим елементом захисту є системи моніторингу та аудиту. Ведення журналів дій користувачів дозволяє швидко виявляти підозрілі операції, аналізувати інциденти безпеки та оперативно реагувати на загрози. Також необхідно своєчасно оновлювати прошивки карток і програмне забезпечення зчитувачів, аби усувати вразливості, виявлені в процесі експлуатації.

Удосконалення захисту RFID/NFC-карток передбачає також інтеграцію адаптивних механізмів, здатних реагувати на зміну ризиків у реальному часі. Наприклад, сучасні системи можуть автоматично блокувати доступ до функціоналу картки у разі підозрілої активності або при перевищенні встановленого ліміту транзакцій. Інтелектуальні алгоритми аналізу поведінки користувача дозволяють виявляти нетипові дії, що можуть свідчити про несанкціоноване використання картки.

Також важливим напрямом є впровадження технологій динамічного кодування, коли ідентифікатор, що передається з картки, змінюється з кожною новою транзакцією. Така технологія, аналогічна до одноразових паролів, значно ускладнює реалізацію атак типу повторного відтворення сигналу (replay attack). Крім того, підтримка ізольованих середовищ виконання (sandboxing) у деяких моделях смарт-карток дозволяє запускати додатки без загрози для ядра операційної системи картки.

Окрему увагу слід приділяти навчанню користувачів правилам безпечного користування картками. Людський фактор залишається одним із найслабших ланцюгів у системі безпеки, тому інформування про ризики соціальної інженерії, небезпеку публічного зчитування або пошкодження картки має стати частиною загальної стратегії кібергігієни.

Нарешті, розвиток правових і нормативних механізмів, зокрема гармонізація стандартів у межах міжнародних організацій (наприклад, ISO/IEC), створює єдині вимоги до виробників карток та систем зчитування. Це сприяє зменшенню ризику використання небезпечних або несумісних рішень і підвищує загальний рівень довіри до безконтактних технологій. У сукупності ці підходи забезпечують надійне функціонування RFID/NFC-систем у сучасному цифровому середовищі.

До додаткових сучасних методів захисту RFID/NFC-карток належить впровадження криптографії на апаратному рівні, зокрема використання апаратних модулів безпеки (HSM) для зберігання ключів і проведення операцій шифрування безпосередньо на чіпі. Це виключає можливість викрадення ключів навіть у разі успішної логічної атаки на систему, оскільки ключі не покидають межі захищеного середовища. Зокрема, використання алгоритмів з еліптичними кривими (ECC) дозволяє досягти високого рівня криптостійкості за відносно низьких витрат обчислювальних ресурсів, що критично для вбудованих рішень, таких як смарт-картки.

Не менш важливими є методи обфускації коду та захисту від реверс-інжинірингу. Програмне забезпечення картки може бути модифіковано таким

чином, щоб ускладнити його аналіз зловмисниками — шляхом шифрування внутрішніх структур, перемішування логіки обробки запитів, введення контрольних пасток, які активують самознищення даних при спробі несанкціонованого доступу.

У фізичному аспекті активно застосовуються екрануючі технології, такі як RFID-блокатори або захисні гаманці з шаром фольги, які запобігають несанкціонованому зчитуванню інформації з картки. Крім того, розробляються рішення з вимикачем передачі сигналу – користувач може активувати або деактивувати антену вручну або автоматично через програму. Такі підходи особливо ефективні в умовах підвищеної загрози безконтактного сканування у громадських місцях.

Інтеграція біометричної автентифікації, наприклад, зчитування відбитка пальця або сканування обличчя, дозволяє встановити додатковий бар'єр перед здійсненням транзакцій. У новітніх моделях смарт-карток уже впроваджуються сенсори біометричних даних, які забезпечують подвійний фактор підтвердження дій користувача.

Не можна оминути увагою важливість побудови безпечної інфраструктури навколо самої картки. Впровадження надійних протоколів обміну даними між карткою і терміналом, наприклад, із підтримкою шифрування TLS або захищених каналів (Secure Channel Protocol), значно ускладнює можливість перехоплення або підміни даних під час комунікації.

Таким чином, ефективний захист RFID/NFC-карток вимагає комплексного підходу, що включає технічні засоби, організаційні заходи, шифрування, багатофакторну перевірку, фізичний захист та постійний контроль. Впровадження цих заходів дає змогу суттєво знизити ризик витоку даних і несанкціонованого доступу до інформаційних систем.

ВИСНОВКИ

У сучасному цифровому середовищі технології радіочастотної ідентифікації (RFID) та зв’язку ближнього поля (NFC) стали важливими інструментами взаємодії між пристроями, що значно спростили доступ до різноманітних сервісів і даних. Безконтактний спосіб обміну інформацією значно покращив зручність користування, однак це також актуалізувало питання захисту даних та особистої інформації. Хоча ці інновації забезпечують низку переваг, вони водночас супроводжуються ризиками, які не можна ігнорувати.

У порівнянні з традиційними магнітними картками, RFID-технології вирізняються вищою ефективністю. Їх використання не потребує фізичного контакту зі зчитувачем, що пришвидшує процес і підвищує зручність. Крім того, RFID-картки зазвичай мають довший термін експлуатації та більшу ємність для зберігання даних. Водночас такі характеристики підвищують імовірність загроз, пов’язаних із несанкціонованим зчитуванням, дублюванням або перехопленням інформації.

Однією з основних загроз є можливість зчитування даних сторонніми пристроями без відома користувача, що отримало назву "сканування" або "знімання". Використовуючи портативний зчитувач, зловмисник може отримати доступ до ідентифікаційних номерів або інших даних з RFID-картки, не торкаючись її фізично. Ця вразливість відкриває шлях до потенційного використання інформації без згоди власника картки.

Ще однією серйозною проблемою є клонування RFID-карт. У разі, якщо інформація на картці не шифрується, зловмисник може швидко скопіювати її вміст і створити ідентичну копію, яка дозволить проходити контроль доступу або здійснювати транзакції від імені іншої особи. Це підриває довіру до систем, що використовують RFID як основний інструмент ідентифікації.

Додатково, існує загроза перехоплення інформації в процесі передачі даних між RFID-карткою та зчитувачем. За допомогою спеціалізованого обладнання хакери можуть аналізувати та декодувати сигнали, що передаються, отримуючи таким чином доступ до конфіденційної інформації.

Щоб знизити ризики, пов’язані з використанням RFID, важливо впроваджувати комплексні заходи захисту. До таких заходів належать використання шифрування даних, автентифікаційні механізми, що підтверджують особу користувача, а також фізичний захист картки за допомогою спеціальних чохлів або гаманців, що блокують сигнали.

Технологія NFC, що є різновидом RFID, також широко використовується у повсякденному житті — зокрема для безконтактних платежів, проходу через електронні турнікети або передачі даних між пристроями. Вона забезпечує високий рівень зручності, однак при цьому супроводжується подібними ризиками. Зокрема, уразливості у реалізації NFC можуть дозволити зловмисникам здійснювати несанкціоновані транзакції, перехоплювати дані або стежити за переміщенням користувачів.

З метою мінімізації загроз необхідно приділяти особливу увагу захисту персональних даних, шифруванню каналів передачі інформації та своєчасному оновленню програмного забезпечення пристроїв, що використовують технології NFC.

У підсумку, RFID та NFC є технологіями з великим потенціалом, проте їх ефективне та безпечне використання можливе лише за умов впровадження надійних систем захисту. Виважений підхід до питань конфіденційності й кібербезпеки дозволить повною мірою скористатися перевагами цих інновацій без шкоди для приватної інформації користувач.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) NXP Semiconductors. Introduction to NFC Technology and Applications. [Електронний ресурс]. – Режим доступу: https://surl.lu/fmucdb
2) NFC Forum. NFC Technology Overview. [Електронний ресурс]. – Режим доступу: https://nfc-forum.org/our-work/nfc-technology/
3) RFID Journal. What is RFID? [Електронний ресурс]. – Режим доступу: https://www.rfidjournal.com/articles/view?133
4) Juels A. RFID Security and Privacy: A Research Survey. [Електронний ресурс]. – Режим доступу: https://www.cs.virginia.edu/~evans/cs551/spring11/papers/rfid-privacy.pdf
5) Coskun V., Ok K., Ozdenizci B. Near Field Communication (NFC): From Theory to Practice. – Wiley, 2012. [Електронний ресурс]. – Режим доступу: https://onlinelibrary.wiley.com/doi/10.1002/9781119379072.ch3
6) ISO/IEC 14443-1:2018. Identification cards – Contactless integrated circuit cards – Proximity cards. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/73598.html
7) ISO/IEC 15693-3:2019. Vicinity cards – Anticollision and transmission protocol. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/73589.html
8) ISO/IEC 15963:2020. Unique identification for RF tags. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/73195.html
9) ESET. QR Codes and NFC Chips. [Електронний ресурс]. – Режим доступу: https://www.welivesecurity.com/2012/04/23/qr-codes-and-nfc-chips-preview-and-authorize-should-be-default/

10) HID Global. What is NFC and how does it work? [Електронний ресурс]. – Режим доступу: https://surl.li/lrvopb

11) STMicroelectronics. NFC technology for secure applications. [Електронний ресурс]. – Режим доступу: https://www.st.com/en/nfc.html

12) Texas Instruments. Introduction to RFID. [Електронний ресурс]. – Режим доступу: https://surl.li/mfiqwu

13) Infineon Technologies. Securing NFC with embedded solutions. [Електронний ресурс]. – Режим доступу: https://www.infineon.com/cms/en/product/security-smart-card-solutions/nfc-solutions/

14) NXP Semiconductors. NFC Everywhere: Applications and Use Cases. [Електронний ресурс]. – Режим доступу: https://www.nxp.com/nfc

15) SML Group. RFID in Retail: Use Cases and Benefits. [Електронний ресурс]. – Режим доступу: https://surl.lu/rmdyiw

16) IBM. Using RFID for Smart Inventory Management. [Електронний ресурс]. – Режим доступу: https://surl.li/jfwpfa

17) Gartner. Emerging Technology: NFC and the IoT. [Електронний ресурс]. – Режим доступу: https://surl.li/mxuwld

18) Number of debit cards and credits issued in the United Kingdom (UK) with contactless/NFC functionality from January 2016 to February 2025 [Електронний ресурс]. – Режим доступу: https://surl.li/irunyq

19) ResearchGate. Security Issues in NFC Applications. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/325735467

20) MDPI. Recent Advances in RFID and NFC Technologies. [Електронний ресурс]. – Режим доступу: https://www.mdpi.com/2071-1050/14/3/1179

21) Finkenzeller, K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. Wiley, 2010. [Електронний ресурс]. – Режим доступу: https://surl.li/xkepeh

22) Want, R. An Introduction to RFID Technology. IEEE Pervasive Computing, 2006. [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/document/1619438

23) Madakam, S., Ramaswamy, R., & Tripathi, S. Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 2015. [Електронний ресурс]. – Режим доступу: https://www.scirp.org/journal/paperinformation.aspx?paperid=57242

24) Coskun, V., Ozdenizci, B., & Ok, K. Near Field Communication: Principles, Practices, and Applications. Wiley, 2013. [Електронний ресурс]. – Режим доступу: https://www.wiley.com/en-us/Near+Field+Communication%3A+Principles%2C+Practices%2C+and+Applications-p-9781119975287

25) TechTarget. RFID vs. NFC: What's the difference? [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/searcherp/tip/RFID-vs-NFC-Learn-the-pros-and-cons-of-each

ДОДАТОК А

4.2 Near Field Communication

This section presents an overview of the NFC technology, in section 4.2.1 the NFC protocol will be presented, hereafter in section 4.2.2 the utilization of NFC in current smartphones will be presented and in section 4.2.3 the security of NFC is explained. The main sources used to form this chapter are [33, 34, 41, 45, 46].

Near Field Communication (NFC) is a short range wireless communication technology which is promoted by the NFC Forum which was formed in 1983. The purpose of the NFC forum was to "enable the use of touch-based interactions in consumer electronics, mobile devices, PCs, smart objects and for payment purposes"

[17]. The physical layer of NFC NFCIP-1 has since been standardized in 2004 in ISO 18092 which is compatible the previous standard ISO 14443. Later the NFCIP-2 has been standardized in ISO 21481 which defines the selection mechanism between different technologies at 13.56 MHz. On top of the NFCIP-1 the NFC Forum has published technical specifications on the higher level communication between NFC devices to benefit interoperability. With the introduction of NFC enabled smartphones, developers have been given a platform with many capabilities to run their applications on.

NFC offers its users an intuitive approach to exchange of information. When the user wants information from some NFC enabled source she only needs to bring her NFC enabled device in contact with that source and the content is transferred to her device. The same procedure is applied when the user wants to push information to another NFC device. This seamless and intuitive data exchange is only possible because NFC does not require any configuration such as other wireless communication technologies such as Wi-Fi or Bluetooth.

RFID which is considered as NFC predecessor considers participants in the communication as either a RFID reader or as transponder, which is a storage entity also referred to as a tag. This technology is used in many industrial applications especially to identify products from one another. Because the NFC technology is compatible with the RFID standard ISO 14443 many existing systems can be utilized by NFC enabled devices. Entities in NFC communication are referred to as peers this is because they can behave as both passive storage entities and as active reader/writers depending on which mode they are communicating in. NFC incorporates 3 modes of communication Reader/Writer mode, Card Emulation mode and Peer-to-Peer mode, a description follows below.

Reader/Writer mode: In this mode the NFC device takes the role as a RFID reader. The device transmits a continuous signal which enables transponders in close proximity to communicate with the device by load modulation. This mode enables NFC devices to communicate with passive RFID tags which power their chip by inducing a current from the received signal.

Card Emulation mode: This mode enables the NFC devices to emulate a RFID transponder and thereby allowing the device to communicate with a RFID Reader. This can be utilized to authenticate the device in many existing systems which incorporate the ISO 14443 standard. Communication between two NFC enabled devices is also provided by this mode in cooperation with the Reader/Writer mode. When communicating with another NFC device one part may take the role as a RFID Reader while the other takes the role as transponder. This allows two NFC devices to communicate while at the same time offering a skewed energy consumption policy between the two participants. The energy consumption of the transponder role is far less than that of the RFID Reader role because the transponder only needs to generate a load modulation on top of the existing signals from the RFID Reader.

Peer-to-Peer: In the Peer-to-Peer communication mode the two NFC devices can either take the role as NFC initiator or as NFC target. Both parties take turn sending information to the opposite part by turning on their NFC signal to transmit and turning it off to receive. As oppose to the behavior of the NFC target in the other communications mode the NFC target in Peer-to-Peer mode does not transfer information to the initiator by load modulation. The target activates its own transmitter while the initiator switches into receiver mode. The roles as NFC initiator and NFC target are assigned at the beginning of the protocol; the NFC device which activates its transmitter is the NFC initiator while the device receiving the signal is assigned the role of NFC target. These roles govern the sequence of the messages exchanged by the two devices. The NFC initiator must begin the communication while the NFC target may only communicate to the NFC initiator by replying to received messages. Information transmitted between devices in this mode is contained in NFC Data Exchange Format (NDEF). Peer-to-Peer mode is also referred to as Active mode because both parties use their self-generated magnetic field to transmit as oppose to Passive mode where one party utilizes a load modulation.

6.3.2.2.1 Student Certificate Generator

The certificate is generated in the SA server by using the cryptographic library in the student certificate generator which is BouncyCastle v.1.47. The libraries include an X509v3 certificate builder interface capable of constructing a certificate according to the X509 standards and sign it using a CAs private key. The certificate signature is generated using SHA1 for hashing and RSA for encryption, as specified in PKCS#1. The choice of algorithm is a matter of configuration. Therefore there have not been serious deliberations on the chosen algorithm. However, there has been discovered some weaknesses in the SHA1 hash function as presented in this paper [58]. This leads us to recommend that SHA2 be used instead of SHA1 if this protocol is to be deployed. Below is shown an example of a student certificate:

```
Certificate:
    Data:
        Version: 3
        Serial Number: 013b093baccc
        Signature Algorithm: SHA1WithRSAEncryption
        Issuer: CN=SA Server, O=Aarhus School of Engineering
        Validity
            Not Before: Aug  9 16:04:02 2012 GMT
            Not After : Jan  9 16:04:02 2013 GMT
        Subject: CN=20108775
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00
                    03 81 8d 00 30 81 89 02 81 81 00 a0 29 ae 76 a6 41 04
                    7a 88 11 57 4d cf e0 85 6c de 4e 68 45 12 7d c4 0d 4e
                    3e a4 71 28 b0 5b be 40 c2 0f 45 ce 1c d0 f5 64 ad 61
                    ea 17 f4 02 49 3d 68 15 0a 0e aa 10 bf cb 47 bd 2b bf
                    7d fa 2f e5 99 a5 64 38 53 26 25 a7 aa 97 e0 ed 72 97
                    80 85 12 32 f2 df 79 cc 88 da 9d ad a5 e0 d6 c7 aa 44
                    d6 1f af f2 19 73 fc 70 35 1b b9 e9 cd dc ad 6c 7c ad
                    4e 03 3b 49 cb df b5 56 f7 42 aa 40 bb 02 03 01 00 01
                Exponent: 65537 (0x10001)
    Signature Algorithm: SHA1WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
        92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
        ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
        d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
        0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
        5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
        8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
        68:9f
```

Figure 6.18 X509v3 Certificate Sample

ДОДАТОК Б

Mathematical Model of the Reliability of a Computer System Operating in the Residual Class System, Based on Dynamic Redundancy

Victor Krasnobaev
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
v.a.krasnobaev@gmail.com
https://orcid.org/0000-0001-5192-9918

Oleksandr Bagmut
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
Oleksandr.bagmut@karazin.ua
https://orcid.org/0000-0003-3241-5756

Alexandr Kuznetsov
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
kuznetsov@karazin.ua
https://orcid.org/0000-0003-2331-6326

Yevheniia Matvieieva
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
olga.bulgakova.dp@gmail.com
https://orcid.org/0000-0001-8801-2185

***Abstract*—The article discusses a variant of the mathematical model of the reliability of a computer system (CS) operating in the residual class system (RNS), based on the use of dynamic redundancy. The calculation and comparative analysis of the reliability of the tripled computational structure in the positional number system with an ideal majority element and CS in the RNS with an ideal commutator is carried out. The analysis results showed the following. At the initial stage of the operation of computing systems, the reliability of the CS in the RNS with one control base is higher than the triple positional computing system. At the initial stage of the operation of computing systems, the reliability of the CS in the RNS with one control base is higher than the triple positional computing system. This presupposes the effective use of the COP in the RNS in systems and devices for short-term use. For example, in on-board computers of ballistic missiles and aircraft.**

Keywords*—residual class system, dynamic redundancy, mathematical model of the reliability, computer system

I. Introduction

Note that at present, interest in the use of the residual class system (RNS) is growing again [1]–[3]. It is caused primarily by the following circumstances [4]–[6]:

- the emergence of numerous technological and theoretical publications dedicated to the theory and practice of creating computer systems (CS) and components in the RNS;
- the universal use of mobile processors, which want high data processing performance with little energy consumption;
- no inter-digit transfers in the process of performing arithmetic operations of addition and multiplication of numbers in the RNS allows reducing energy consumption;
- banking configuration demonstrate great interest in RNS, where it is necessary to reliably and reliably process large data arrays in real time, i.e. high-performance tools are required for highly reliable computations with self-correction of errors, which is typical of codes in RNS;
- increasing the density of elements on one chip does not in all cases allow high-quality and complete testing; in this case, the importance of ensuring the fault-tolerant functioning of specialized CS increases;
- the need to use specialized CS to perform a various of operations on vectors that require a high speed of performing integer addition and multiplication operations (matrix multiplication problems, vector scalar product problems, transformation Fourier, etc.);
- the widespread introduction of microelectronics into all spheres of average life has significantly increased the relevance and importance of previously rare, and now such massive scientific and practical tasks as digital processing of signals and images, pattern recognition, cryptography, processing and storage of multi-bit information, etc.; this circumstance requires huge computing resources that exceed existing capabilities;
- the current level of development of microelectronics is approaching the limit of its capabilities in terms of ensuring performance and reliability of existing and future CS and components for real-time processing of large data arrays; nanoelectronics, molecular electronics, micromechanics, bioelectronics, optical, optoelectronic and photonic computers, biological, etc., which are coming to replace it, are still very far from real wide industrial production and application.

The article discusses a variant of the mathematical model of the reliability of a computer system, functioning in the residual class system, based on the use of dynamic redundancy.

The article is structured as follows. Section 2 briefly analyzes recent publications in the subject area. Section 3 provides basic theoretical information about number systems in residual classes. Section 4 is devoted to the presentation of the main results. In particular, a mathematical model of the reliability of a computer system operating in a residual class system is described. It also provides several examples that

clearly demonstrate the proposed solutions, as well as figures and calculations that give an idea of the reliability of a computer system operating in a residual class system. In the "Conclusion" section, the results obtained are summarized, some conclusions and recommendations are stated.

II. Related Works

The problems of constructing computer systems operating in the residual class system have been studied by many authors. In works [4], [6], [7] and many others, the general theoretical provisions of the residual class systems, as well as the techniques for their use in computer systems, were investigated. In works [2], [8] - [11], etc., the possibilities of the residual class system for error correction were investigated. This is a very important property, which was also studied in works [12] - [16]. Articles [17] - [19] are devoted to the study of new techniques for constructing specialized computing devices operating in the system of residual classes. The papers [1], [20] - [23] investigate new directions in computer science devoted to systems of residual classes. For example, in [2] artificial intelligence methods are investigated, in [20] methods of fast Fourier transform are studied, in [21] digital filters are considered, in [22], [23] some cryptography problems using computations in the system of residual classes.

Many works are also devoted to research of methods of increasing the reliability and fault tolerance of computer systems. For example, these are fundamental works [24] - [27], etc. In articles [2], [3], [28] aspects of increasing the reliability of computer systems are investigated, and in [2], [10], [12], [13] issues of fault tolerance of computing devices operating in the system of residual classes. However, the issues of quantifying the probability of failure-free operation of computer systems in residual class systems have not been studied enough.

This article proposes a mathematical model of the reliability of a computer system operating in the residual class system. This model makes it possible to quantify the main indicators of the reliability of the computer system functioning in the residual class system. We also provide several examples with a visual calculation of the probability of no-failure operation of computer systems in residual class systems.

III. Basic Properties of Non-Positional Arithmetic in RNS

First, preliminary, before taking into consideration a version of the mathematical model of the reliability of a CS operating in the residual class system (RNS), we will deal with the consequence of the leading properties of a non-positional number system on the structure and principles of operation of the CS [7]–[9].

A. Independence of the residues.

This property makes it possible to produce a CS in the RNS in the form of a set of independent, parallel operating in time, break computing paths (BT) for data processing, functioning severally of each other agreement with their particular modulus m_i. Thus, the CS operating in the RNS has a modular design, which allows maintenance and elimination of failures and malfunctions of the computing paths by replacing an inoperative VT with an efficient one without interrupting the solution of the problem. The time for the implementation of arithmetic operations in the CS is determined by the time for the implementation of the operation in the BT according to the greatest radix m_i RNS.

In addition, errors arising from failures (failures) of the binary bit circuits in an arbitrary TC of the CS do not "multiply" into neighboring paths (remain within one remainder), which makes it possible to increase the reliability of calculations in the RNS. It does not matter whether there was a single or multiple errors or a burst of errors no longer than $[\log_2(m_i-1)] + 1$ binary digits. A mistake that has arisen in the CS in the base m_i is either stored in this path until the end of the calculations, or is self-eliminated in the process of further calculations (for example, by multiplying the remainder of the number by zero). This property of the RNS made it possible to create a unique system for monitoring and correcting errors in the dynamics of the computational process (without stopping the computation process) of the CS with the introduction of a minimum information code redundancy, which is essential for data processing systems operating in real time.

B. Equality of residues.

Note that there is a close relationship between arithmetic codes in RNS and arithmetic AN-codes in a positional number system (PSS). Arithmetic codes in RNS are an advanced development of the known positional arithmetic noise-immune many-residual AN-codes [3], [10], [11].

Based on the procedure for generating numbers in the RNS, it is obvious that any remainder ai of the number $A = (a_1, a_2, \dots, a_n)$ carries information about the entire original number A, which makes it possible by software methods to replace the failed computational path modulo m_i with an operable path modulo m_j (provided that $m_i < m_j$) without interrupting the solution of the problem. Thus, the CS functioning in the RNS having, for example, two control bases, retain their operability in the event of failure of any two computing paths. In the event of failures in the third or fourth paths, the CS continues to execute the computation program with a slight decrease in the computational accuracy, i.e. CS in RNS has the property of gradual degradation. This property determines the characteristic feature of the functioning of the CS in the RNS: a CS, depending on the requirements imposed on it, can have different reliability, accuracy of calculations and speed in the dynamics of the computational process. Thus, in the process of solving the problem, it is possible to vary the reliability of the CS, the reliability, accuracy and speed of calculations. Indeed, let the data be determined by a numerical code represented by a set of bases $\{m_i\}$ $(i = \overline{1, n+k})$ RNS.

It is known that the execution time of arithmetic operations and the accuracy of the solution depends on the number n of information bases, and the reliability of the functioning of the CS and the reliability of calculations depends on the number k of the control bases of the RNS. Let in the process of calculations the need arose to improve the reliability of the functioning of the CS and (or) the reliability of the calculations. In this case, in real time, without interrupting the calculations, the bases $\{m_i\}$ of the RNS are redistributed as follows

$$i = \overline{1, n'+k'}$$

and

$$n' < n,\ k' > k\ .$$

Moreover,

$$n + k = n'' + k'' = const .$$

In this case, the accuracy of calculations decreases and the speed of performing arithmetic operations increases, which are determined by the number of information bases n′. If there is a need to increase the accuracy of the solution in a separate section of the computed program, then the program is redistributed as follows:

$$i = \overline{1, n'' + k''} \quad (n + k = n'' + k'' = const).$$

In this case, with an increase in the accuracy of calculations ($n'' > n$), the reliability of the CS (reliability of calculations) decreases and the time for solving this problem increases.

Furthermore, the redistribution of information n and k control bases takes place with the execution of non-modular functions in the RNS (operation of control, correction, comparison, etc.). The time required to perform non-modular operations in the RNS is proportional to the number n of information bases, i.e. the number of bases that determine the accuracy of the calculations.

The transition to computations with lower accuracy makes it possible to increase the speed of the CS. If an ordered ($m_i < m_{i+1}$) RNS is expanded by adding l bases, each of which is larger than the previous base of the original RNS, then the minimum code distance d_{min} is automatically increased by l.

The same can be achieved by decreasing the number n of information bases, i.e. moving on to calculations with less precision. Consequently, there is an inverse relationship between the correcting capabilities of the RNS codes and the computational accuracy. The combined use of the first and second properties of the RNS determines the presence of three types of redundancy in the CS simultaneously: structural, informational and functional.

Based on the idea of structural redundancy, the joint use of the first and second properties makes it possible to synthesize mathematical models of the CS reliability in the RNS, corresponding to the models of constant and dynamic redundancy in the PSS. In this case, the information paths $m_{n+1} \div m_{n+k}$ of the CS plays the role of working elements, and the control $m_{n+1} \div m_{n+k}$ play the role of reserve elements, where k is the number of control (reserve) bases of the RNS.

C. Low bit representation of residues.

This property allows to significantly increase the reliability and performance of the CS. This is achieved both due to the low bit depth of the construction of the CS, and due to the possibility of using (in contrast to the PSS) tabular arithmetic, where the arithmetic operations of addition, subtraction and multiplication are performed practically in one machine cycle. In particular, the small digit capacity of the residuals in the representation of numbers in the RNS makes it possible to choose a wide range of options for system engineering solutions in the implementation of modular arithmetic operations based on the following principles:

- adder principle (based on the use of low-bit binary adders modulo);
- tabular principle (based on the use of read-only memory devices (ROM) of small sizes);
- the principle of ring shift based on the use of ring shift registers.

IV. Mathematical Model of the Reliability of a Computer System Operating in the Residual Class System

Based on the analysis of the possible use of the above three main properties (independence, equality and low bit depth of residuals that determine the non-positional code structure), non-positional arithmetic in the RNS, in comparison with the PSS, has the following significant advantages [13], [17], [29]:

- the ability to parallelize computations at the level of decomposition of the operands, which significantly increases the speed of the CS;
- the possibility of spatial diversity of data elements with the possibility of their subsequent asynchronous independent processing;
- the possibility of tabular (matrix) execution of arithmetic operations of the base set and polynomial functions with a single-cycle selection from the ROM of the result of a modular operation;
- the ability to create a system for monitoring and correcting the CS with effective detection and correction of failures and failures;
- the ability to control and correct errors in the dynamics of the computational process of the CS;
- the possibility of effective use of passive and active fault tolerance based on the operational reconfiguration of the CS structure;
- lower computational and time complexity for individual classes (types) of integer problems;
- manifestation of a special property of the structure of the CS in the RNS, ensuring the absence of the effect of multiplication of errors in the implementation of arithmetic integer operations of addition, subtraction and multiplication;
- the suitability of the structure of the CS in the RNS for carrying out operational diagnostics of blocks and nodes of the calculator;
- the possibility of increasing the reliability of the CS in the RNS due to the efficiency of the simultaneous use of passive and active fault tolerance.

Based on the listed basic properties of the RNS, the probability of no-failure operation of the CS can be represented as the probability of no-failure operation of the CS in the PSS for the case of sliding redundancy with a loaded reserve, taking into account the influence of the listed properties of the RNS. In this case, the formula for determining the probability of no-failure operation of the CS in the RNS will take the form of expression (1).

$$P_{RNS}^{(k)}(t) = \sum_{i=0}^{k} C_{k+n}^{i} P_1^{k+n-i}(t) \sum_{j=0}^{i} (-1)^j C_i^j P_1^j(t) . \qquad (1)$$

Here, on the right-hand side of formula (1), the expression $P_1(t)=exp(-\lambda_1 t)$ is the probability of failure-free operation of the CS data processing path on the largest (least reliable) basis m_{n+k} RNS, and the value λ_1 is the failure rate of the equipment on the largest base m_{n+k}.

Relation (1) can be used to calculate the probability of no-failure operation of the CS in the RNS under the following assumptions:

- This property makes possible to significantly increase the reliability and performance of the CS. This is achieved both because of the low bit depth of the construction of the CS, and due to the possibility of using (in contrast to the PSS) tabular arithmetic, where the arithmetic operations of addition, subtraction and multiplication are performed practically in one machine cycle. In particular, the small digit capacity of the residuals in the representation of numbers in the RNS makes it possible to choose a wide range of options for system engineering solutions in the implementation of modular arithmetic operations based on the following principles: information and control computing paths of the CS are equally reliable (the probability of failure-free operation of all paths is taken to be equal to the probability of failure-free operation $P_1(t)$ of the path on the largest basis m_{n+k} RNS, which has the lowest probability of failure-free operation);
- the possibility of restoring failed CS paths is not taken into account.

Note that the real reliability of the CS in the RNS will be higher than that determined by relation (1), since this formula does not take into account the possibility of replacing one control path on the basis of m_j with one or several inoperable information paths at the same time

$$m_j \geq \prod_{i=1}^{r} m_{k_i},$$

provided where r is the maximum number simultaneously replaced working paths with one control operable path on the base m_j.

Let us carry out a comparative analysis of the reliability of a triple positional CS with an ideal majority element and a CS in an RNS with an ideal fail-safe switch, using the considered reliability model (1). Let us denote by λ_3 the failure rate of the equipment referred to one binary digit (to the unit of the CS bit grid). In this case, the probability of failure-free operation of the equipment, referred to one binary bit of the COP is equal to

$$P_3(t)=e^{-\lambda_3 t}.$$

For a positional l-byte CS, the probability of no-failure operation is equal to

$$P_0(t)=e^{-\lambda_0 t},$$

where

$$\lambda_0=8l\lambda_3, \text{ or } P_0(t)=e^{-\lambda_3 8lt}.$$

It is known that the probability of no-failure operation for a triple majority structure in an PSS containing three computers and an ideal majority element is [24], [30]–[32]:

$$P_M(t)=3P_0^2(t)-2P_0^3(t)=e^{-16\lambda_3 t}(3-2e^{-8\lambda_3 t}). \quad (2)$$

For CS in RNS, the probability of failure-free operation of the path on an arbitrary basis $m_i(i=\overline{1,n+k})$ is equal

$$P_1(t)=e^{-\lambda_1 t}$$

or

$$P_1(t)=e^{-\lambda_3 a_{n+k} t},$$

where

$$a_{n+k}=[\log_2(m_{n+k}-1)]+1.$$

The probability of failure-free operation of the CS in the RNS is determined in accordance with expression (1).

Let us give examples of using formula (1) for various RNS.

Let $l=1$ (single-byte CS) and $k=1$.

Then the RNS can be represented as a set of the following bases

$$m_1=3,\ m_2=4,\ m_3=5,\ m_4=7,\ m_5=11.$$

Moreover,

$$\prod_{i=1}^{4} m_i = 420 > 2^8 = 256$$

and

$$\text{GCD}(m_i,m_j)=1 \text{ for } i\neq j.$$

In this case, relation (1) can be written in the form

$$P_{RNS}^{(1)}(t)=5P_1^4(t)-4P_1^5(t)= \\ =e^{-16\lambda_3 t}(5-4e^{-4\lambda_3 t}). \quad (3)$$

We denote $\lambda^*=8\lambda_3$. In this case, expressions (2) and (3) can be written, respectively, in the form

$$P_M(t)=e^{-2\lambda^* t}(3-2e^{-\lambda^* t}), \quad (4)$$

$$P_{RNS}^{(1)}(t)=e^{-2\lambda^* t}(5-4e^{-4\lambda^* t}). \quad (5)$$

In accordance with expression (4) and (5), the values of the probability of no-failure operation are calculated for the triple positional CS in the PSS and for the CS in the RNS.

In Fig. 1 shows the graphs of the $P(\lambda^* t)$ for single-byte CS: non-redundant (I) in the PSS, three-channel redundant (II) CS in the PSS and CS in the RNS (III) with parameters

$l=1, n=4, k=1.$

From Fig.1, it can be seen that a CS in an RNS with one (k = 1) control base (III) is more reliable than a triple positional computing system (II).

In this case, the critical value of the probability of no-failure operation of the CS in the RNS is equal to 0.425, and the critical value of the tripled computing system is equal to 0.5, i.e. the use of the RNS expands the range of values $\lambda^* t$, at which the reliability of the CS in the RNS is higher than the reliability of the CS in the PSS.

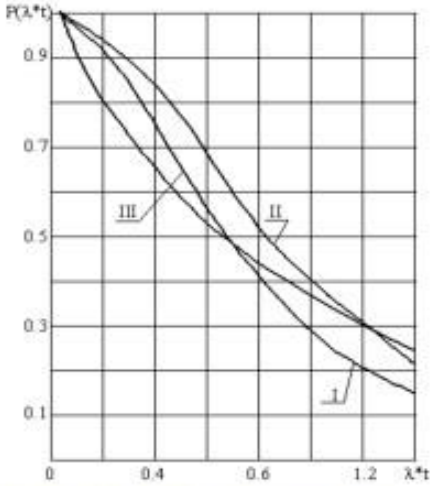

Fig. 1. Graphs of dependencies $P(\lambda^* t)$ of CS reliability, $k=1$

Let $k = 2$.

In this case, the RNS is defined as a set of the following bases:

$$m_1=3, m_2=4, m_3=5,$$

$$m_4=7, m_5=11, m_6=13.$$

For a given RNS, expression (1) is written as follows

$$P_{RNS}^{(2)}(t) = P_1^4(t)\left\{P_1^2(t)+6P_1(t)\left[1-P_1(t)\right]+15\left[1-P_1(t)\right]^2\right\}$$

or

$$P_{RNS}^{(2)}(t) = \\ = e^{-2\lambda^* t}\left[e^{-\lambda^* t}+6e^{-0,5\lambda^* t}\left(1-e^{-0,5\lambda^* t}\right)+15\left(1-e^{-0,5\lambda^* t}\right)^2\right]. \quad (6)$$

The graph of function (6) for k = 2 is shown in Fig. 2.

It can be seen from this graph that the CS in the RNS with two control bases (IV) is more reliable than the triple positional computing system (II) and more reliable than the CS in the RNS with one (k = 1) control base (III).

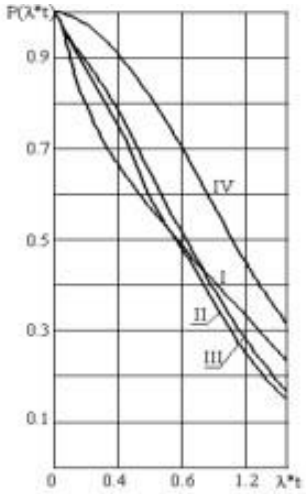

Fig. 2. Graphs of dependencies $P(\lambda^* t)$ of CS reliability, $k=2$

Shown in Fig. 1, 2 dependencies were obtained by calculation using the formulas of the proposed mathematical model. With an increase in the multiplicity of redundancy, the reliability of the CS increases, which corresponds to the provisions of the general theory of reliability [33].

V. Conclusion

The article discusses a variant of the mathematical model of the reliability of a computer system, functioning in the residual class system, based on the use of dynamic redundancy.

The computing and comparative analysis of reliability in terms of the probability of failure-free operation of a triple computing structure in a positional number system with an ideal majority element and a CS in an RNS with an ideal commutator is carried out. The analysis results showed the following. At the initial stage of the operation of computing systems, the reliability of the CS in the RNS with one control base is higher than the triple positional computing system. This presupposes the effective use of the CS in the RNS in systems and devices for short-term use. For instance, in on-board computers of ballistic missiles and aircraft.

References

[1] D. I. Kaplun *et al.*, "Hardware Implementation of Video Processing Device using Residue Number System," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, Jul. 2019, pp. 701–704. doi: 10.1109/TSP.2019.8768827.

[2] T.-C. Huang, "Self-Checking Residue Number System for Low-Power Reliable Neural Network," in *2019 IEEE 28th Asian Test Symposium (ATS)*, Dec. 2019, pp. 37–375. doi: 10.1109/ATS47505.2019.000-3.

[3] Y. Zhang, "An FPGA implementation of redundant residue number system for low-cost fast speed fault-tolerant computations," Thesis, 2018. doi: 10.32657/10220/47113.

[4] P. V. A. Mohan, *Residue Number Systems*. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-41385-3.

[5] I. Koren, "THE RESIDUE NUMBER SYSTEM," *Computer Arithmetic Algorithms*, Oct. 08, 2018. https://www.taylorfrancis.com/ (accessed Aug. 16, 2020).

[6] J. O. Tuazon, "Residue number system in computer arithmetic," Doctor of Philosophy, Iowa State University, Digital Repository, Ames, 1969. doi: 10.31274/rtd-180816-2270.