Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
*Факультет комп'ютерно-інформаційних систем і програмної інженерії*
(назва факультету )
*Кафедра кібербезпеки*
(повна назва кафедри)

# ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній рівень)

на тему: *«Створення захищеного методу реплікації даних з використанням NFC-технології»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*

Спеціальності:
*125 «Кібербезпека»*
(шифр і назва напряму підготовки, спеціальності)

*Ситник О. І.*
підпис (прізвище та ініціали)

Керівник *Загородна Н.В.*
підпис (прізвище та ініціали)

Нормоконтроль *Кареліна О.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 20*19*

# АНОТАЦІЯ

Створення захищеного методу реплікації даних з використанням NFC-технології // Дипломна робота ОР «Магістр» // Ситник Олександр Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // С. , рис. – , табл. – , кресл. – , додат. – .

Ключові слова: NFC-ТЕХНОЛОГІЯ, РЕПЛІКАЦІЯ, ОС ANDROID, ДВОХФАКТОРНА АУТЕНТИФІКАЦІЯ, ВІДКРИТИЙ КЛЮЧ, СЕАНСОВИЙ КЛЮЧ, ШИФРУВАННЯ, ПРОФІЛЬ MOZILLA.

Дана магістерська кваліфікаційна робота присвячена створенню захищеного методу реплікації даних використовуючи NFC-технологію. Проводиться аналіз існуючих механізмів синхронізації призначених для користувача даних і протоколу NFC та представляються їхні переваги та недоліки.

Досліджуються загрози, які можуть виникати при передачі даних за допомогою технології NFC. Досліджуються методи захисту від атак на канали NFC. Досліджується можливість використання технології NFC в мобільних телефонах на базі ОС Android. Розробляється метод захищеної реплікації профілю користувача використовуючи NFC-технологію.

У першій главі проводиться аналіз існуючих механізмів синхронізації призначених для користувача даних і протоколу NFC.

У другій главі досліджується перелік загроз, що виникають при передачі даних за технологією NFC та визначаються особливості встановлення безпечного каналу для NFC. Досліджується технологія NFC в мобільних телефонах на базі ОС Android.

У третій главі розробляється  метод, що полягає у використанні технології NFC для автоматизованої реплікації профілю користувача та визначається прототип системи реплікації профілю користувача за допомогою технології NFC.

В спеціальній частині приведено опис застосунку «SyncManager».

В п’ятому розділі обчислено основні показники економічної ефективності від розробки і реалізації запропонованого алгоритму.

У підрозділі "Охорона праці" розглянуто вимоги щодо охорони праці в приміщеннях та їх оснащення. У підрозділі "Безпека життєдіяльності" описано безпеку приміщень та розлади здоров'я користувачів, що формуються під впливом роботи за комп'ютером.

В розділі "Екологія" описано формування бази статистичних даних в екології. Також розглянуто джерела шуму і вібрацій та методи їх знешкодження.

# ANNOTATION

Development of a protected method of data replication using NFC technology // Thesis of the Master degree // Sytnyk Oleksandr // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2019 // P. , Tables – , Fig. – , Diagrams – , Annexes. – , References – .

Keywords: NFC TECHNOLOGY, REPLICATION, ANDROID OPERATING SYSTEM, TWO-FACTOR AUTHENTICATION, PUBLIC KEY, SESSION KEY, ENCRYPTION, MOZILLA PROFILE.

This master's qualification paper is devoted to the creation of a secure data replication method using NFC technology. An analysis of the existing mechanisms for synchronizing user data and NFC protocols and their advantages and disadvantages are presented.

The threats that may arise when transmitting data using NFC technology are explored. Methods of protection against attacks on NFC channels are explored. Exploring the possibility of using NFC technology in mobile phones based on the Android operating system. The method of protected replication of a user profile is being developed using NFC technology.

The first chapter analyzes the existing synchronization mechanisms for user data and the NFC protocol.

In the second chapter the threats posed by NFC data transmission were explored and the features of establishing a secure NFC channel were identified. NFC technology is explored in Android-based mobile phones.

In the third chapter a method that uses NFC technology for automated replication of a user profile was developed and a prototype of a user profile replication system using NFC technology was defined.

A special section describes the SyncManager application.

The fifth section includes calculations of the main cost-effectiveness indicators for developing and implementing the proposed algorithm.

The "Occupational Safety and Health" section reviews the requirements for occupational safety of rooms and equipment. The Life Safety section describes the security of rooms and the health computer-generated disorders of users.

The section "Ecology" describes the formation of a database of statistics in ecology. The sources of noise and vibration and methods of their neutralization are also considered.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

| | |
|---|---|
| ОС | Операційна система |
| РЧ | Радіочастотне поле |
| ФС | Файлова система |
| AID | Application Identifier – унікальний ідентифікатор сервісу-обробника NFC-команд |
| APDU | Application Protocol Data Unit - формат команд обміну даними між NFC-пристроями |
| GUI | Graphical User Interface - графічний інтерфейс користувача |
| HCE | Host-Card Emulatio – емуляція смарткарт на мобільних пристроях |
| Message-reply | Протокол повідомлення-відповідь |
| MITM | Man-in-the-middle - атака «людина посередині» |
| NFC | Near Field Communication - технологія передачі даних на невеликих відстанях |
| RFID | Radio Frequency Identification- технологія радіочастотної ідентифікації |

# ВСТУП

Підтримка призначених для користувача даних в актуальному стані і можливість доступу до них з будь-якого пристрою - головний принцип забезпечення зручності взаємодії користувача з інформаційними системами.

Кількість пристроїв для особистого користування вже не обмежується тільки телефоном і комп'ютером. У багатьох людей так само присутні планшети, ігрові приставки, «розумна побутова техніка». Часто виникає необхідність роботи з розрахованими на багато користувачів пристроями - наприклад, комп'ютери в інтернет-кафе або в навчальній аудиторії. Щоб забезпечити максимально зручну взаємодію користувача незалежно від пристрою, з яким в даний момент відбувається робота, необхідно використовувати синхронізацію даних. Дані, що синхронізуються, в подальшому в роботі будемо називати призначеним для користувача профілем.

Профіль користувача може складатися як з неважливих даних, на кшталт налаштувань користувача оточення, так і з даних, загроза розкриття яких може бути критична. Серед них, наприклад, можна виділити:

- списки контактів;
- закладки браузера;
- платіжні дані;
- календарі;
- списки зустрічей;
- призначені для користувача файли.

Існує безліч технологій синхронізації даних між пристроями. Технології різняться в залежності від того:

- де зберігається синхронізований профіль;
- які канали зв'язку використовуються для синхронізації;
- який протокол синхронізації застосовується;
- чи використовуються засоби захисту, і які саме.

Незалежно від описаних вище чинників, необхідно забезпечити безпеку даних, що синхронізуються. У даній роботі було розглянуто перелік існуючих технологій і каналів синхронізації. Були відзначені відмінності між ними. В якості вирішення для забезпечення безпеки синхронізації обрана порівняно молода технологія NFC. В роботі розглянута її безпеку в якості носія даних, а також в якості каналу для первинної установки безпечного з'єднання.

*Метою роботи* є створення захищеного методу реплікації даних використовуючи NFC-технологію.

*Об'єктом дослідження* є процес реплікації даних, які потребують захисту.

*Предметом дослідження* є методи та засоби реплікації.

Для досягнення поставленої мети вирішуються *наступні завдання*:

1. Проводиться аналіз існуючих механізмів синхронізації призначених для користувача даних і протоколу NFC;
2. Досліджуються загрози, які можуть виникати при передачі даних за допомогою технології NFC;
3. Досліджуються методи захисту від атак на канали NFC;
4. Досліджується можливість використання технології NFC в мобільних телефонах на базі ОС Android;
5. Розробляється метод захищеної реплікації профілю користувача.

Наукова новизна та практична цінність роботи:

1. Проведений аналіз рівнів реплікації на основі хосту, мережі та контролеру системи зберігання даних показав, що реплікація на основі контролеру системи є одною з найгнучкіших для проведення реплікації, основною перевагою якої є об'єднання всіх переваг систем реплікації на рівні мережі, проте визначені недоліки кожного з рівнів реплікації доводить необхідність шукати нові шляхи і рівні для проведення більш захищеної реплікації.

2. Аналіз загроз, що виникають при передачі даних за технологією NFC показав, під час реплікації даних цією технологією можуть бути загрози

пов’язані з  пасивним прослуховуванням каналів, пошкодженням переданих даних, модифікацією даних, вставки даних та атак типу Relay, проте на основі проведених досліджень, можна стверджувати що атака типу «людина посередині» для протоколу NFC є практично нездійсненою.

3. На основі аналізу загроз, що виникають при передачі даних за технологією NFC, запропоновано методи і шляхи їх усунення, де основним новим шляхом їх подолання є використання засобів рівня додатків, завдяки яким можна домогтися переваг які не існують на канальному рівні.

4. З урахуванням виявлених слабких і сильних сторін існуючих каналів реплікації, проведеного аналізу загроз та методів їх подолання запропоновано та представлено новий метод реплікації, заснований на застосуванні технології NFC в якості каналу установки сеансового ключа. Проведений аналіз захищеності запропонованого методу реплікації за допомогою технології NFC мобільного телефону на ОС Android показав, що отриманий метод є більш стійким до існуючих загроз при передачі інформації, є більш гнучким і простим у використанні, і може використовуватись для тимчасової реплікації профілю користувача, наприклад, при створенні спеціальних додатків для ОС Android.

*Апробація результатів роботи*. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

# РОЗДІЛ 1. ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕХАНІЗМІВ СИНХРОНІЗАЦІЇ ПРИЗНАЧЕНИХ ДЛЯ КОРИСТУВАЧА ДАНИХ І ПРОТОКОЛУ NFC

## 1.1. Проблема синхронізації при передачі даних призначених для користувача

Синхронізація даних – ліквідація відмінностей між двома копіями даних. Передбачається, що раніше ці копії були однакові, а потім одна з них, або обидві були незалежно змінені.

Спосіб синхронізації даних залежить від додаткових припущень, що робляться. Головною проблемою тут є те, що незалежно зроблені зміни можуть бути несумісні одна з одною (так званий «конфлікт правок»), і навіть теоретично не існує загального способу вирішення подібних ситуацій.

Проте, є низка окремих способів, застосовних в тих або інших випадках:

- Найпростіший спосіб: припускають, що зміни вносилися лише до однієї з копій — «робочу» — і інша копія просто перезаписується її вмістом. Цей спосіб реалізують більшість застосунків синхронізації; через безповоротність змін, що робляться, користувачеві дається вибір, яку копію вважати «головною».
- Якщо дані є набором незалежних записів (тобто будь-яке поєднання записів є коректним — це, наприклад, телефонна книга), то можна просто об'єднати множини записів. Це ліквідовує ризик втрати інформації, але щоб видалити запис з набору, цей спосіб доводиться поєднувати з першим.
- Якщо набори синхронізуються неодноразово, можна автоматично вводити в них додаткову службову інформацію: дата і час останньої зміни запису, позначки про видалені записи (вилучаються після наступної синхронізації або через деякий час) тощо. Цей підхід використовується, наприклад, в Outlook.

- Обробляти конфлікти правок: автоматично (якщо можливо), інакше — вручну. Цей найзагальніший спосіб застосовується тільки якщо вказані вище спрощення недопустимі — наприклад, в системах контролю версій. Так, CVS при виявленні двох незалежних змін оголошує про «конфлікт» і або (у простих випадках) вирішує його автоматично, або надає користувачеві вирішити його вручну. У цих випадках конфліктів прагнуть просто уникати — наприклад, розподілом областей компетенції.

Синхронізації підлягають різні дані:

- списки контактів;
- браузерні закладки;
- календарі;
- файли.

## 1.2. Реплікація, як окремий випадок синхронізації

Реплікація даних - сучасна технологія управління даними в декількох точках, при якій вибудовується загальна система обробки та консолідації даних. У загальних рисах, реплікація це процес, при якому дані записуються і зберігаються вгорі окремих серверів, але, за допомогою управління інформаційним потоком, досягається систематизування результатів в центральному сервері.

Реплікація надає наступні можливості:

- автоматизоване і надійне переміщення змін даних з однієї системи в іншу (дозволяє автоматично вносити зміни при появі їх в джерелі);
- створення ідентичних копій в двох системах (наприклад, підтримка другої копії даних для їх відновлення);
- копіювання підмножини даних з однієї системи в багато (наприклад, з метою синхронізації інформації в різних системах). Такий вид реплікації називається розподілом даних;

- копіювання вибраних даних з багатьох джерел в одне (наприклад, щоб об'єднати інформацію в інформаційне сховище). Такий вид реплікації називається консолідацією даних.

### 1.2.1 Види реплікації

Існують різні критерії за якими можна класифікувати реплікацію.

Так *за напрямом реплікації* поділяються на

- односторонні (однонаправлені);
- багатосторонні (мульти-направлені).

Якщо дані змінюються тільки в одній з БД, а в іншій дані тільки зберігаються і не піддаються змінам, то таку реплікацію будемо називати односпрямованою або односторонньою. Якщо ж дані можуть змінюватися і вводитися на всіх БД, то такий вид реплікації будемо називати мультинаправленою або багатосторонньою.

Існує поділ реплікації за часом:

- синхронна реплікація;
- асинхронна реплікація.

*Синхронна реплікація* (рис.1.1). Синхронна реплікація проходить в реальному часі, інформація мультиплікується на всіх серверах. У разі синхронної реплікації, якщо якась репліка оновлюється, всі інші репліки того ж фрагменту даних також повинні бути оновлені в одній і тій же транзакції. Логічно це означає, що існує лише одна версія даних.

У більшості продуктів синхронна реплікація реалізується за допомогою тригерних процедур (можливо, прихованих і керованих системою). Одним з недоліків синхронної реплікації є те, що вона створює додаткове навантаження при виконанні всіх транзакцій, в яких оновлюються будь-які репліки (крім того, можуть виникати проблеми, пов'язані з доступністю даних).Особливість синхронної реплікації в тому, що при втраті зв'язку між серверами ніхто не відображає зміни, цикл зупиняється і процес практично не може бути продовжений. Необхідно, щоб всі дані були на 100% однакові у

всіх серверів і клієнтів. Цей режим не застосовується в реальних торгових системах, тому що є залежність від зв'язку.

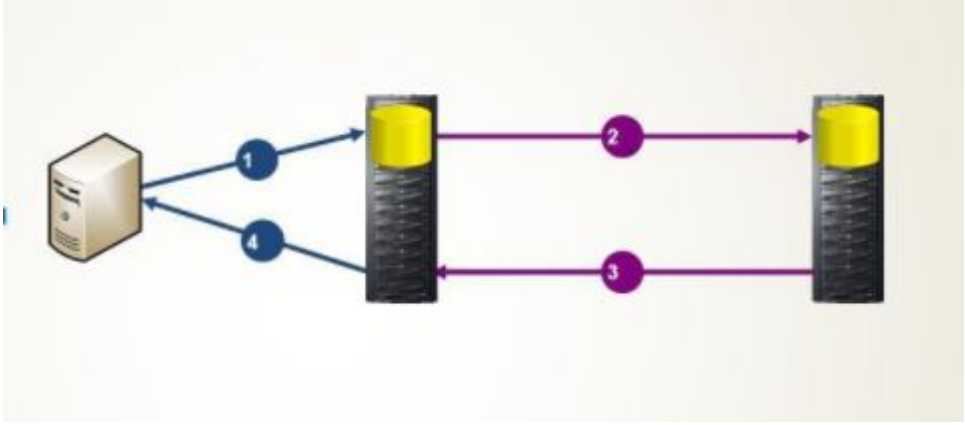


Рисунок 1.1 - Синхронна реплікація

*Асинхронна реплікація.* Асинхронна реплікація - це технологія, при якій дані зберігаються в локальному сервері, який, зі свого боку, піклується про їх передачу до наступного і передає тільки різницю. Це правильна технологія для побудови торгової системи, тому, що немає вимог до безперебійного зв'язку, і дані передаються при першій нагоді, але не обов'язково в реальному часі.


Рисунок 1.2 - Асинхронна реплікація

У разі асинхронної реплікації оновлення однієї репліки поширюється на інші через деякий час, а не в тій самій транзакції. Таким чином, при асинхронній реплікації вводиться затримка, або час очікування, протягом якого окремі репліки можуть бути фактично неідентичними (тобто визначення реплікації виявляється не зовсім відповідним, оскільки ми не маємо справу з точними і своєчасно створеними копіями).

У більшості продуктів асинхронна реплікація реалізується за допомогою читання журналу транзакцій або постійної черги тих оновлень, які підлягають поширенню. Перевага асинхронної реплікації полягає в тому, що додаткові втрати на реплікацію не пов'язані з транзакціями оновлень, які можуть мати важливе значення для функціонування всього підприємства і ставити високі вимоги до продуктивності. До недоліків цієї схеми відноситься те, що дані можуть виявитися несумісними (тобто несумісними з точки зору користувача). Іншими словами, надмірність може проявлятися на логічному рівні.

Розглянемо коротко проблему узгодженості (або, скоріше, неузгодженості). Справа в тому, що репліки можуть ставати несумісними в результаті ситуацій, яких важко (або навіть неможливо) уникнути і наслідки яких важко виправити. Зокрема, конфлікти можуть виникати з приводу того, в якому порядку повинні застосовуватися поновлення. Наприклад, припустимо, що в результаті виконання транзакції A відбувається вставка рядка в репліку X, після чого транзакція B видаляє цей рядок, а також припустимо, що Y - репліка X. Якщо поновлення поширюються на Y, але вводяться в репліку Y в зворотному порядку ( наприклад, через різні затримки при передачі), то транзакція B не знаходить в Y рядок, що підлягає видаленню, і не виконує свою дію, після чого транзакція A вставляє цей рядок. Сумарний ефект полягає в тому, що репліка Y містить зазначений рядок, а репліка X - ні.В цілому завдання усунення конфліктних ситуацій і забезпечення узгодженості реплік є досить складними. Слід зазначити, що, по крайній мірі, в співтоваристві користувачів комерційних баз даних термін реплікація став означати переважно (або навіть виключно) асинхронну реплікацію.

*Поділ реплікації за завданнями:*

- Реплікація Master-Slave.
- Реплікація з рівноправними серверами (Multi Master).

*Реплікація Master-Slave* (рис.1.3). Реплікація Master-Slave залежить від одного центрального Master сервера, який акумулює всі дані і передає різницю

до підлеглих Slave серверів. Таким чином, Master сервер завжди має актуальну копію даних, поки Slave сервери чекають змін і підкоряються інформації, відправленої від Master. Вони актуалізують свої дані із запізненням. Перевага цієї технології в простому виконанні, недолік - записи завжди робляться в Master сервері, що вимагає постійно зв'язку з цим сервером. Якщо пропаде зв'язок з центральним сервером, в системі не зможуть виводитися нові операції, але можна буде робити довідки. Ця технологія реалізована в MySQL сервері і часто використовується в торгових системах. Звичайно, Master-сервер стоїть в центральному офісі фірми.

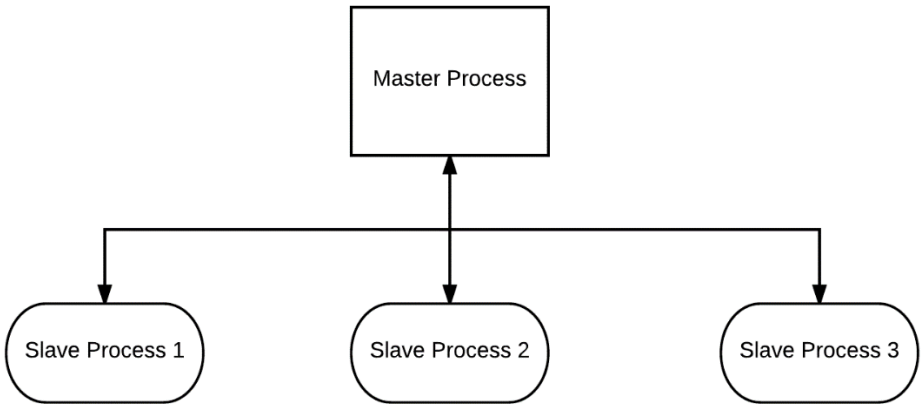


Рисунок 1.3 - Реплікація Master-Slave

*Реплікація з рівноправними серверами.* Реплікація з рівноправними серверами - прогресивна технологія, де кожен сервер є самостійним і, одночасно з цим, частиною загальної мережі. При цій технології так само існує центральний сервер, який управляє зв'язком між іншими серверами. Перевага технології в повній незалежності від зв'язку в роботі. Коли є зв'язок, дані передаються до центрального серверу. Підлеглі сервери передають тільки свою різницю і не завантажують канал обміну даними. Коли не існує зв'язку між серверами, дані акумулюються локально для подальшого об'єднання при відновленні зв'язку. Ця технологія називається Transactional Merge і реалізується в MS SQL Server.

Реплікація є підвидом синхронізації. Реплікацію називають односторонньою (One-Way) синхронізацією. При реплікації очікується зміна файлів тільки в одній локації. Для цього спочатку обмовляється, яка з сторін, що синхронізуються буде джерелом, а яка ціллю. Таким чином, після процесу реплікації ціль і джерело повинні стати ідентичними.

Деякі можливі стани при реплікації наведені на рис.1.4. Наприклад, проводиться реплікація з джерела 1 в джерело 2. Якщо деякий файл на джерелі 1 новіше, ніж файл в джерелі 2, то він буде скопійований з заміною на джерело 2. Якщо ж даний файл новіше на джерелі 2, то він не буде скопійований на джерело 1, а швидше за все буде замінений більш старим файлом з джерела 1.

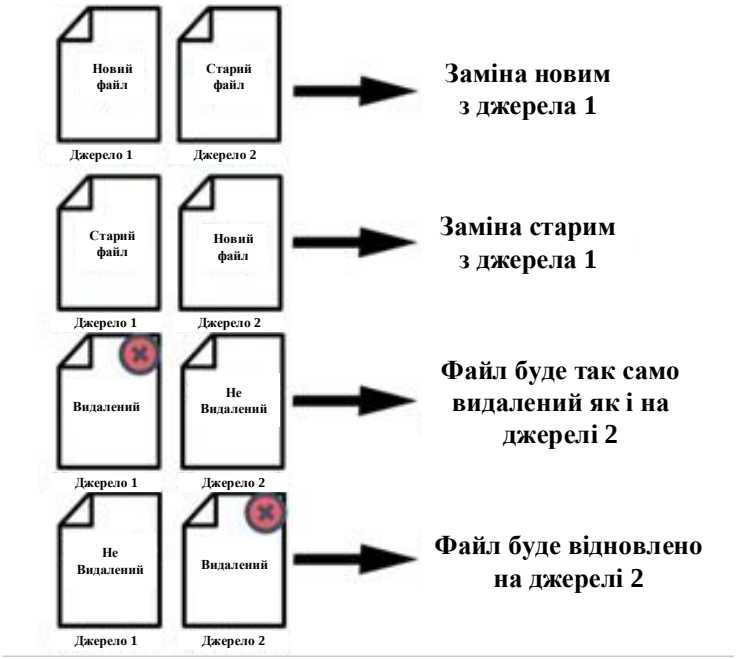


Рисунок 1.4 - Схема реплікації даних

Якщо файл був видалений на джерелі 1, то після реплікації на джерелі 2 цей файл буде так само видалений, але якщо файл видалений на джерелі 2, то в кінцевому рахунку він буде відновлений з копії.

Види реплікації з*а способом передачі інформації під час процесу* поділяються на:

- прямий;

- ймовірнісний.

Якщо з'єднання серверів, що зберігають розподілені БД, відбувається за допомогою програми клієнта, яка з одного боку приєднується до свого облікового запису, а з іншого кінця має прямий зв'язок з БД іншого сервера і може підключитися безпосередньо до даних іншого сервера, для прямої зміни і аналізу даних, що підлягають реплікації з обох кінців, маючи при цьому гарантований стійкий канал зв'язку (ADSL, виділений канал, двопровідна лінія Dial-Up та ін.), то такий вид синхронізації назвемо *прямим*.

Якщо ж канал нестійкий і не гарантує стійкий зв'язок без падінь під час процесу синхронізації і дані доводиться передавати цілісними пачками, при цьому приймаюча сторона під час закачування і аналізу даних не має негайної можливості опитати джерело при виникненні на її погляд сумнівних моментів, а рішення потрібно приймати в будь-якому випадку, то такий вид синхронізації будемо називати недетермінованою або *ймовірнісною*.

*За способом аналізу інформації*, що реплікується можна виділити:

- реплікація моментальних знімків;
- реплікація транзакцій;
- реплікація об’єднанням

*Реплікація моментальних знімків* (snapshot replication) - це періодична реплікація цілісного набору даних, зафіксованого за станом на певний момент часу, з локального сервера на віддалені. Краще використовувати цей тип реплікації в БД, де кількість даних невелика, а джерело даних є статичним. Реплікація моментальних знімків найбільш підходить для роботи з даними, що не змінюються інтенсивно, для невеликих обсягів реплікуємої інформації, які можуть оновлюватися повністю без істотного збільшення навантаження на мережу, а також для даних, які не потрібно постійно підтримувати в актуальному стані (припустимо, архівні дані по обсягах продажів підприємства).

*Реплікація транзакцій* (transactional replication) - це реплікація початкового моментального знімка даних на віддалені сервери, а також

реплікація окремих транзакцій, які працюють на локальному сервері і виконують послідовні зміни даних в початковому моментальному знімку.Ці репліковані транзакції виконуються над даними, що реплікуються на кожному віддаленому сервері для синхронізації даних на віддаленому сервері з даними локального сервера. Ми можемо використовувати цей тип реплікації, якщо необхідно постійне оновлення даних на віддалених серверах.

*Реплікація об'єднанням (*merge replication) - це реплікація початкового моментального знімка даних на віддалені сервери, а також реплікація змін, що відбуваються на якомусь віддаленому сервері, назад на локальний сервер з метою синхронізації, вирішення конфліктів і повторної реплікації на віддалені сервери. Ми можемо використовувати реплікацію зведенням в разі, коли чисельним змінам піддаються одні й ті ж дані, або коли віддалені незалежні комп'ютери працюють автономно, наприклад, як у випадку автономного користувача.

*За часом проведення сеансу реплікації* поділяють на:

- в реальному часі;
- відкладені.

Якщо дані повинні бути синхронізовані негайно після змін, то таку реплікацію будемо називати реплікація в реальному часі. Якщо ж процес реплікації запускається за якою-небудь подією в часі або за вказівкою адміністратора БД, то такий вид реплікації назвемо відкладена реплікація.

### 1.2.1. Аналіз рівнів реплікації IT-інфраструктури

Реплікація може здійснюватися на різних рівнях IT-інфраструктури:

- на рівні хосту (використовується як для серверів, так і для ПК);
- на рівні мережі (зазвичай в мережі зберігання даних);
- на рівні контролеру системи зберігання даних.

Реплікацію на рівні хосту можна здійснювати на різних підрівнях, в тому числі на рівні додатків, а також на рівні файлової системи, на рівні менеджера

томів або її можна впровадити в ОС на рівень, який дозволяє абстрагуватися від файлової системи, забезпечуючи блочну реплікацію.

Програмне забезпечення реплікації на рівні хосту здійснює синхронізацію даних на різних сховищах, відправляючи дані на віддалену клієнтську програму або ж на локальний або мережевий диск. Використання копіювання на віддалену клієнтську програму зазвичай дозволяє більш гнучко управляти даними, наприклад, використовувати шифрування, стиснення даних або двосторонню реплікацію з підтримкою цілісності даних.

*Переваги реплікації на рівні хосту:*

- простота використання при малій кількості хостів;
- найдешевший метод для малої кількості хостів;
- велика гнучкість рішень;
- простота реалізації реплікації з підтримкою цілісності даних;
- не потрібно використовувати додаткове обладнання;
- не залежить від використовуваних систем зберігання даних.

*Недоліки:*

- впливає на продуктивність хостів;
- висока складність управління і ціна при великій кількості хостів;
- залежність від програмного забезпечення хоста (ОС, файлової системи, менеджера томів або додатки), яка в принципі не є великим недоліком, в разі якщо обраний продукт прекрасно інтегрується з уже встановленим на хості програмним забезпеченням.

Реплікація на рівні мережі здійснюється за допомогою спеціальних додаткових пристроїв (appliances) або за допомогою комутаторів, які мають функціонал, що забезпечує реплікацію (зазвичай це ті ж додаткові пристрої, виконані у вигляді спеціального модуля комутатора). Для підтримки цілісності даних при такому рішенні використовуються агенти застосувань, як і при інших методах.

Існує два підходи до розташування пристроїв, які здійснюють реплікацію в мережі, - це in-band та out-of-band розташування відповідно на шляху

проходження даних і за його межами. Обидва підходи досить цікаві і мають як переваги, так і недоліки. Але останнім часом in-band технологія отримала розвиток у вигляді пристроїв, що підтримують кластеризацію, таким чином, було нівельовано основний недолік in-band технології - обмежене масштабування, в той час як використання кластеризації для out-of-band пристроїв не дозволяє повністю усунути такий же недолік.

*До переваг реплікації на рівні мережі відносяться:*

- простота використання при великій кількості хостів;
- недорогий метод для великої кількості хостів;
- велика гнучкість рішень і простота управління;
- не залежить від використовуваних систем зберігання даних і хостів;
- не зменшує продуктивність додатків (при кількості хостів більше 100 використовується кластерізіція).

*Недоліки:*

- необхідність використання додаткового обладнання;
- висока ціна при малій кількості хостів.

Реплікація на рівні контролера системи зберігання даних є певним окремим випадком варіанту реплікації на базі мережі. Іноді системи зберігання даних, що використовують реплікацію на базі контролера, використовують практично аналогічні попередньому типу архітектурні рішення, з тією лише відмінністю, що пристрій реплікації вбудовано в систему зберігання даних і не може бути використано окремо від неї. До найбільш цікавих рішень реплікації на рівні контролера можна віднести складні потужні рішення віртуалізації серії Universal Storage Platform Hitachi Data Systems і прості недорогі репліки на базі контролера початкового і середнього рівня від Dothill. USP Hitachi практично реалізує модель віртуалізації (в т.ч. реплікації) в мережі зберігання, дозволяючи підключати до контролера не тільки власні диски системи зберігання, але і інші цілісні системи.

Система самостійно забезпечує управління даними на всіх підключених сховищах. Системи зберігання даних від DotHill, що реалізують реплікацію,

забезпечують цю функцію засобами пакетного віддаленого копіювання моментальних знімків, здійснених засобами контролера системи зберігання даних. Таким чином, копія даних відкладається на рівні контролера системи зберігання даних.

*Переваги:*

- Простота використання для одного сховища в простих системах.
- Об'єднання всіх переваг систем реплікації на рівні мережі для просунутих рішень.
- Відсутність необхідності у використанні додаткового обладнання.
- Простота управління однією системою (в простих рішеннях) або групою підключених сховищ (в просунутих системах).

*Недоліки:*

- Дороге рішення при використанні просунутих потужних систем.
- Прив'язка до одного виробника.
- Відсутність гнучкості при використанні простих рішень.
- З лишком спрощений функціонал недорогих рішень.

### 1.2.2. Класифікація механізмів реплікації

Механізми реплікації даних можна класифікувати, ґрунтуючись на тому, де зберігаються дані, що піддаються реплікації, і які канали передачі даних використовуються. І місце зберігання, і канали передачі можна розділити на локальні і віддалені. У кожному конкретному механізмі вибір місця зберігання і каналу передачі визначається вимогами до функціонування та безпеки.

На рис.1.5. зображено класифікація механізмів реплікації, а також технології, які можуть бути використані для реалізації конкретних рішень.

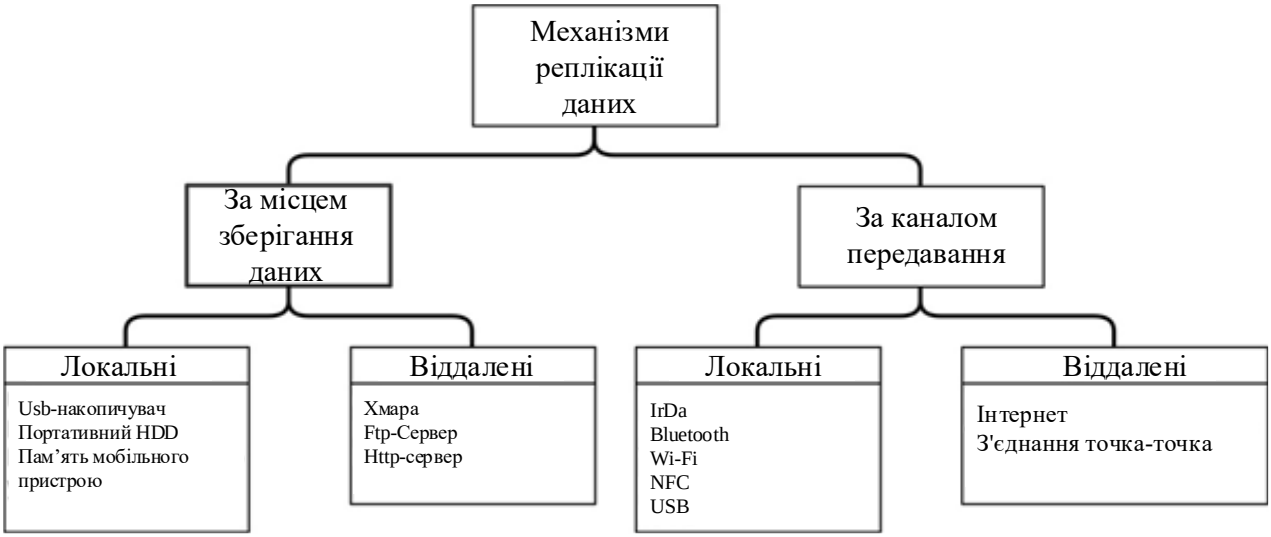


Рисунок 1.5 - Класифікація механізмів реплікації даних

Синхронізація даних виконується з використанням проміжних інформаційних каналів. При локальній синхронізації пристрої, що синхронізуються розташовуються в безпосередній близькості. Даний підхід використовує технології IrDA, Bluetooth, Wi-Fi, NFC. Можливо безпосереднє з'єднання пристроїв мережевим або usb-кабелем.

При віддаленій синхронізації передбачається, що синхронізуються пристрої географічно розподілені. Тут мається на увазі використання стека мережевих технологій. Як приклад віддаленої синхронізації можуть бути використані протоколи FTP, SFTP, HTTP (запит змін за допомогою XML, JSON) та інші. Багато FTP-клієнтів підтримують функції синхронізованого перегляду директорій, а також приведення папок в синхронізований стан шляхом звірки всіх файлів на клієнті і сервері.

Синхронізація через інтернет може проходити в режимі завантаження даних з віддаленого сервера. Так само можливий варіант з встановленням з'єднання точка-точка між пристроями, що синхронізуються.

Призначені для користувача дані можуть завантажуватися і зберігатися в хмарних середовищах, звідки за допомогою інтернету вони викачуються на цільовий пристрій. В цьому випадку відповідальність за безпеку зберігання і доставки даних покладається на постачальника хмарних послуг. Однак, якщо

безпеку призначених для користувача даних не може бути довірено хмарним сервісам, або, якщо використовуються пристрої, що не мають доступу до таких сервісів, то можливе використання локальних сховищ типу:

- usb-накопичувача;
- портативного HDD;
- Інших портативних пристроїв, що мають необхідні інтерфейси і пам'ять для роботи з даними, що проходять реплікацію.

### 1.2.3. Порівняння каналів синхронізації даних

Безпека передачі даних в механізмі реплікації може бути реалізована на рівні додатку, але також вона залежить і від каналу передачі даних. В табл.1.1. наведено порівняння існуючих бездротових каналів локальної передачі даних. В силу того, що розглядаються бездротові канали варто відзначити, що всі вони схильні до пасивної прослуховування. [1]

Таблиця 1.1 - Порівняння характеристик каналів передачі даних

| Характеристика | Wi-Fi | Bluetooth | IrDA | NFC |
|---|---|---|---|---|
| Дальність | 30-100м | 10м | <2м | <10см |
| Енергоспоживання | Високе | Середньо-низьке | Дуже низьке | Дуже низьке |
| Можливість пасивного прослуховування | + | + | + | + |
| Можливість MITM | + | + | + | – |

В ході аналізу було виявлено, що використання каналу NFC для передачі даних дозволяє позбутися від атак типу «людина посередині». Таким чином,

з точки зору безпеки даний канал передачі даних підходить для створення захищеного з'єднання. [2]

## 1.3 Дослідження протоколу NFC

Технологія NFC описана в стандарті ISO 18092. NFC являє собою бездротової канал обміну даними на коротких відстанях до 10 см. NFC може оперувати в двох режимах, які представлені в табл. 1.2. Дані режими розрізняються тим, що в першому випадку пристрій створює своє РЧ поле, а в другому випадку пристрій отримує енергію від РЧ поля, що генерується іншими пристроями. Якщо пристрій генерує поле сам, то він називається активним пристроєм, інакше - пасивним. Активні пристрої завжди мають зовнішнє електроживлення. Пасивні пристрої, такі як безконтактні смарт-карти, додаткової енергії, крім як від РЧ поля активного пристрою, не отримують.

Таблиця 1.2 - Можливі конфігурації взаємодіючих пристроїв

| **Пристрій 1** | **Пристрій 2** | **Опис** |
|---|---|---|
| активний | активний | Коли пристрій пересилає дані, він генерує РЧ поле, а приймаючий пристрій не генерує РЧ поле. Таким чином, в один момент часу РЧ поле генерується тільки одним з пристроїв. |
| активний | пасивний | РЧ поле генерується тільки пристроєм 1 |
| пасивний | активний | РЧ поле генерується тільки пристроєм 2 |

Дані конфігурації взаємодіючих пристроїв важливі, так як тип передачі інформації цілком залежить від того чи є передавальний пристрій активним чи пасивним.

В активному режимі дані передаються з використанням амплітудної модуляції. Базова частота радіосигналу в 13,56 МГц модулюється у відповідність зі схемою кодування. Широко поширені дві схеми кодування. Для швидкості передачі в 106 Кбод застосовується кодування Міллера, для швидкостей вище – Манчестерське кодування. В обох схемах кодування біт відсилається за фіксований часовий слот. Цей слот розділяється на дві половини – полубіти.

У кодуванні Міллера 0 передається, як пауза в першому полубіті і відсутністю паузи в другому полубіті. 1 ж кодується як відсутність паузи в першому полубіті і пауза в другому. У модифікованому кодуванні Міллера додаються деякі особливості для кодування нулів. У разі якщо за одиницею слід нуль, то два послідовних полубіта для кодування Міллера будуть заповнені паузою. Модифікована кодування Міллера уникає цього шляхом кодування 0, який слідує за 1 двома полубітамі без паузи. Манчестерське кодування багато в чому схоже, але замість того, щоб використати паузу в першому або другому полубіті, нуль і одиниця повністю кодуються або паузою в обох полубітах, або модулюванням. Крім схеми кодування, на швидкість передачі так само впливає коефіцієнт модуляції. Для 106 кБод використовується 100% модуляція. Це означає, що в паузах, переданий сигнал дійсно нульовий. Для пропускної здатності вище 106 кБод використовується 10% коефіцієнт модуляції. Відповідно до визначення коефіцієнта модуляції це означає, що в моменти пауз сигнал становить близько 82% від сигналу в активний момент. [3] Ця різниця в силі модуляції дуже важлива з точки зору безпеки. Як показано в таблиці 2, в пасивному режимі дані надсилаються з використанням Манчестерського кодування з коефіцієнтом модуляції 10%. Як буде показано далі, цей режим забезпечує підвищену безпеку для деяких видів[3]. Ця різниця в силі модуляції дуже важлива з точки зору безпеки. Як показано в таблиці 1.3, в пасивному режимі дані надсилаються з використанням Манчестерського кодування з коефіцієнтом модуляції 10%. Як буде показано далі, цей режим забезпечує підвищену безпеку для деяких

випадків [3]. Ця різниця в силі модуляції дуже важлива з точки зору безпеки. Як показано в таблиці 1.3, в пасивному режимі дані надсилаються з використанням Манчестерського кодування з коефіцієнтом модуляції 10%. Як буде показано далі, цей режим забезпечує підвищену безпеку для деяких видів атак.

Таблиця 1.3 - Схема кодування в залежності від режиму роботи пристрою

| **швидкість** | **активний пристрій** | **пасивний пристрій** |
|---|---|---|
| 424 кбод | манчестерське, 10% АМн | манчестерське, 10% АМн |
| 212 кбод | манчестерське, 10% АМн | манчестерське, 10% АМн |
| 106 кбод | модифікований код Міллера, 100% АМн | манчестерське, 10% АМн |

Окрім активного і пасивного режиму пристрої можуть виступати так само в ролі ініціатора спілкування і цілі. Протокол NFC заснований на моделі message-reply, це означає, що пристрій 1 посилає повідомлення пристрою 2, в свою чергу пристрій 2 обов'язково відповість пристрою 1. Пристрій 2 не може послати повідомлення пристрою 1, не отримавши від нього першого повідомлення. В даному конкретному випадку пристрій 1 є ініціатором, а пристрій два метою. У таблиці 1.4 надані всі можливі комбінації пристроїв з урахуванням ролей і режимів роботи.

Таблиця 1.4 - Можливі конфігурації пристроїв

| | **ініціатор** | **мета** |
|---|---|---|
| **активний** | можливо | можливо |
| **пасивний** | неможливо | можливо |

Так само варто відзначити, що NFC з'єднання не лімітовано двома пристроями. Пристрій-ініціатор може посилати повідомлення кільком

цільовим пристроям. У такому випадку всі пристрої-приймачі активуються одночасно, але, перед тим, як послати повідомлення, пристрій-ініціатор має вибрати єдиний пристрій. Таким чином, всі інші приймачі, крім обраного, проігнорують відправлене повідомлення. Реалізовано це за допомогою механізму антиколізій. Існує два алгоритму для запобігання колізій. Перший заснований на безпосередньому запиті ідентифікатора, з яким хоче спілкуватися пристрій-ініціатор. Другий - послідовний перебір всіх можливих пристроїв в полі дії за бітами, поки не буде вибрано єдиний. Хоча подібна ситуація малоймовірна, але алгоритм антиколізій для 200 карток буде працювати всього секунду. Тому час для роботи цього алгоритму для малої кількості карт незначний.

Таким чином, посилка повідомлень декільком пристроям (широкомовлення) не дозволена. [4]

### 1.3.1. Застосування NFC

Технологія NFC використовується в багатьох галузях. Широке застосування обґрунтовано відносною дешевизною і функціональністю даної технології. NFC може бути використаний для створення «розумних» візиток, як ключ, що відмикає замок тощо. Останнім часом, поширюється використання NFC в цілях безконтактної оплати покупок або в якості транспортних квитків.

Практично всі сучасні смартфони оснащені NFC-модулями за замовчуванням, а виробники мобільних пристроїв просувають свої платіжні системи.

Технологія NFC може бути дуже ефективною в різних областях. На рис. 1.6 наведено приклади NFC-застосувань.


Рисунок 1.6 – Області NFC-застосувань

Основними застосунками, які можуть отримати користь від його впровадження, є:

- Оплата через мобільні пристрої, такі як смартфон та планшети.
- Електронна ідентичність.
- Електронний квиток на перевезення.
- Інтеграція кредитних карток у мобільних пристроях.
- Передача даних між будь-якими типами пристроїв, таких як цифрові камери, мобільні телефони, медіаплеєри.
- P2P (одноранговий) зв’язок між бездротовими пристроями для передачі даних.
- Лояльність та купонування / цільовий маркетинг / послуги на основі локації
- З'єднання пристроїв
- Охорона здоров'я / моніторинг пацієнтів
- Ігри

- Контроль доступу / патрулювання безпеки / контроль запасів (теги та зчитувачі).

Можливість інтеграції всіх перерахованих вище функцій в унікальне мобільне рішення робить NFC дуже привабливим для телекомунікаційної галузі. Більшість проектів зосереджена на використанні одного пристрою, який інтегрує кілька функцій, покращуючи досвід роботи користувача в різних умовах. З точки зору користувача, NFC являє справжню революцію: мобільний телефон може використовуватися для надсилання мікроплатежів або як пристрій управління доступом для динамічної ідентифікації. Пристрої NFC також можуть обмінюватися даними з існуючими пристроями зчитування карт та сумісними стандартами ISO 14443, такими як інші мобільні телефони NFC. Цей високий рівень інтеграції технології NFC є надзвичайно великою перевагою, що робить можливою взаємодію з існуючими інфраструктурами RFID.

Короткі відстані між терміналами зв'язку роблять її більш безпечною, ускладнюючи sniffing-атаки.

Коли згадується технологія NFC, існує негайне посилання на мобільний зв’язок та можливість розширення використання мобільних пристроїв як платіжних терміналів. Великі фірми, такі як Nokia та Google розробляють безліч проектів за допомогою NFC; слід врахувати, що технологія може бути застосована в різних сферах, таких як охорона здоров'я.

Пристрої NFC можуть працювати в основному в трьох режимах:

- Як емулятори карт, що забезпечують альтернативне зберігання інформації, що знаходиться в пам'яті на пластиковій картці.
- У режимі однорангового доступу, що дозволяє здійснювати з'єднання за допомогою іншого протоколу зв’язку, такого як Bluetooth або WiFi.
- У режимі читання та запису картки / тегів, де пристрій NFC може читати або змінювати інформацію, що зберігається в тезі RFID або безконтактній картці.

### 1.3.2. Безконтактна мітка

Даний вид додатків використовує пасивні мітки, щоб зчитувати з них дані. В якості пасивної мітки може виступати смарт-карта, RFID - мітка або брелок. Так само мітка може бути фізичною частиною іншого електронного пристрою (Наприклад, мітки вбудовують в сучасну побутову техніку).

Окремо варто відзначити, що єдиним інтерфейсом мітки є бездротовий інтерфейс. Це означає, що неможливо отримати доступ до центрального процесора пристрою, так як мітка не може отримати доступ за контактним інтерфейсом. Так само потрібно розуміти, що мітка має обмежену обчислювальну потужність і не може виконувати протоколи, які потребують складних обчислень. Основний метод використання міток - зберігання даних, які можуть бути зчитані активним пристроєм NFC. Прикладом таких даних можуть служити:

- URL-посилання;
- візитки;
- мітки для систем розумний будинок.

Користувач зчитує подібну мітку і відразу ж перенаправляється на цікавий для нього сайт. Іншим прикладом використання пасивних NFC-міток може бути зберігання даних необхідних для доступу до закритої точки доступу Wi-Fi. Нові користувачі можуть налаштувати свої пристрої для роботи в мережі простим зчитуванням мітки.

### 1.3.3. Квитки , мікроплатежі

Даний приклад являє собою додатки, які використовують NFC-інтерфейс для передачі конфіденційної інформації, в якості якої, як правило, виступає інформація про банківські платежі, або квитки.

Як пристрій може виступати безконтактна смарт-карта або мобільний телефон. Коли користувач хоче здійснити платіж або скористатися збереженим квитком він підносить свій пристрій до зчитувача, який перевіряє отриману з пристрою інформацію, проводить платіж або перевіряє квиток. У

даних видах додатків для користувача пристрій повинен використовувати певний протокол зі зчитувачем. Простої операції зчитування буде недостатньо для забезпечення безпеки в багатьох випадках.

Також необхідно організувати альтернативний інтерфейс для програми, за допомогою якого користувач зможе поповнювати рахунок, або купувати квитки. Такий інтерфейс, наприклад, може бути пов'язаний з центральним процесором мобільного пристрою, а дані можуть бути завантажені в апарат через стільникову мережу.

### 1.3.4.Сполучення (синхронізація) пристроїв

Даний спосіб застосування використовується для установки каналу зв'язку між різними пристроями. Як приклад можна привести ноутбук і фотокамеру. Користувач хоче встановити Bluetooth-канал між пристроями для передачі фотографій і відеороликів. Досягти цього можна шляхом піднесення пристроїв близько один до одного, що дозволить запуститися обміну інформацією по каналу NFC для первинної ініціації Bluetooth-з'єднання. Це набагато зручніше, так як для кінцевого користувача набагато очевидніше, що між пристроями можна зробити синхронізацію шляхом близького їх розташування, замість того, щоб використовувати установку з'єднання через громіздке меню.

Варто відзначити, що в даному прикладі NFC використовується тільки для встановлення Bluetooth-каналу. Пропускна здатність NFC не оптимальна для передачі фото і відео-даних і використання його в якості каналу даних недоцільно.

# РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ І МЕТОДИ ЗАХИСТУ ВІД НИХ ПРИ ПЕРЕДАЧІ ДАНИХ ПО ТХЕХНОЛОГІІ NFC

## 2.1. Перелік загроз, що виникають при передачі даних за технологією NFC

В рамках дослідження безпеки технології NFC була розглянута можливість проведення різних атак на канал передачі даних. Перелік атак представлений в таблиці 2.1.

Даний перелік відображає можливість проведення атаки на незахищений канал, який встановлюється за замовчуванням. Уникнути багатьох атак можливо на рівні додатку, використовуючи криптографію і інші засоби захисту.

Таблиця 2.1 - Безпека технології NFC

| Атаки на бездротові канали | Актуальність для NFC | Метод захисту |
|---|---|---|
| Пасивне прослуховування | + | Криптографія |
| Пошкодження даних | + | Криптографія + атаки виявляються пристроями |
| Модифікація даних | багато обмежень | Криптографія |
| Вставка даних | багато обмежень | Криптографія |
| Relay-атаки | + | Екранування, підтвердження користувача при передачі |
| MITM-атаки | - | - |

### 2.1.1. Пасивне прослуховування каналу

Через те, що NFC - бездротова технологія, то гостро стоїть проблема з прослуховуванням каналу. Коли два пристрої з'єднуються один з одним, вони використовують радіохвилі. Атакуючий може використовувати спрямовану антену, щоб прослухати сигнали, що передаються. Експериментальним шляхом або шляхом зчитування специфікації протоколів комунікації пристроїв атакуючий може дізнатися яким чином з знятого сигналу може бути отримана інформація. Варто враховувати, що пристрої для перехоплення і декодування радіочастотного сигналу широко доступні.

У NFC обмін інформацією відбувається при безпосередньо близькому контакті пристроїв. Це означає, що пристрої знаходяться на відстані не більше ніж на 10 см. Основним питанням є наскільки близько повинен знаходитися зловмисник, щоб зуміти перехопити радіочастотний сигнал, що буде придатним для подальшої роботи з ним. На жаль, однозначної відповіді на це питання не існує. Основною причиною є безліч факторів, що визначають цю відповідь:

- радіочастотні характеристики трансмітера (наприклад, геометрія антени, ефект екранування корпусу, оточення);
- радіочастотні характеристики антени атакуючого (наприклад, форма антени, можливість зміни положення у всіх трьох вимірах);
- якість приймача атакуючого;
- якість декодера атакуючого;
- локація в якій ведеться зняття сигналу (рівень радіошуму, бар'єри у вигляді стін);
- потужність з якою працює NFC пристрій.

Таким чином, як ми бачимо, використовуються безліч параметрів для оцінки, і не можна дати якесь усереднене значення, яке буде вірне для більшості випадків. На рис.2.1 зображено схема пасивного прослуховування.

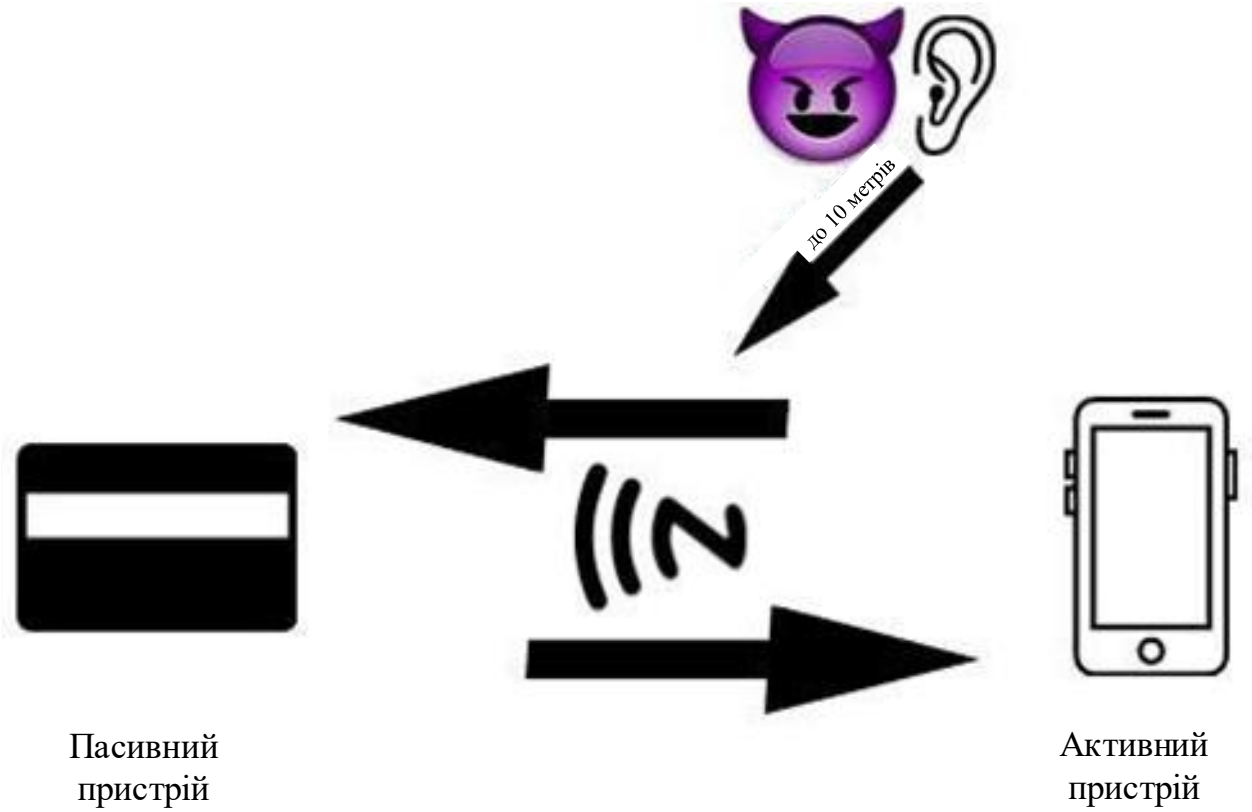


Рисунок 2.1 - Схема пасивного прослуховування

Також важливу роль відіграє те, в якому режимі знаходиться відправник даних. Залежно від режиму (активний чи пасивний) змінюється методологія знімання даних. У пасивному режимі знімати дані складніше. Загалом же можна сказати, що прослуховування в активному режимі може здійснюватися з 10 метрів, в пасивному режимі ця відстань зменшується до 1 метра. [5]

### 2.1.2 Пошкодження переданих даних

Крім прослухоування даних, зловмисник може спробувати модифікувати дані, що передаються за допомогою NFC каналу. У найпростішому випадку атакуючий може спробувати перервати спілкування між пристроями, забивши канал випадковими даними, таким чином, цільовий пристрій не зможе зрозуміти дані, що надіслані іншим легітимним пристроєм. На рис.2.2 зображена схема подібної атаки.

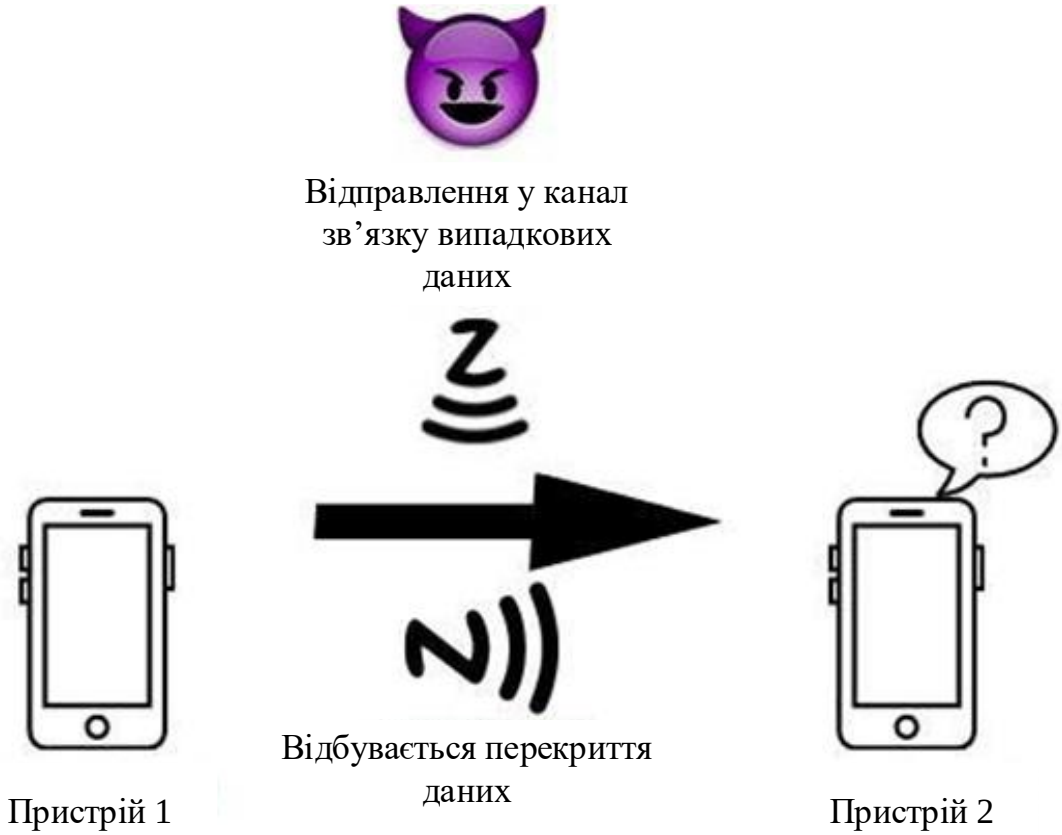


Рисунок 2.2 - Схема атаки пошкодження даних

Пошкодження даних може бути досягнуто шляхом відсилання вірних частот в певний проміжок часу. Проміжок часу визначається з урахуванням використовуваної модуляції і схеми кодування. Дана атака не надто складна в реалізації, але не дозволяє атакуючому якось маніпулювати переданими даними, таким чином дана атака є підвидом атаки відмови в обслуговуванні.

### 2.1.3. Модифікація даних

Дана атака має на увазі, що зловмисник хоче, щоб приймаючий пристрій отримав коректні, але змінені дані. Даний вид атак значно відрізняється від атаки з п.2.1.2.

Доцільність даної атаки сильно залежить від коефіцієнта модуляції.

Коефіцієнт модуляції є відношенням різниці мінімальної і максимальної амплітуди до їх же сумі: $M = \frac{A_{max} - A_{min}}{A_{max} + A_{min}}$.

Декодування сигналу відрізняється для 100% і 10% коефіцієнта модуляції. Для 100% коефіцієнта модуляції декодер перевіряє два полубіта на присутність радіочастотного сигналу (відсутність паузи) або відсутність сигналу (пауза). Для того, щоб декодер прийняв одиницю за нуль або навпаки атакуючий повинен зробити дві речі. По-перше, пауза при модуляції повинна бути заповнена частотою - це можливо. По-друге, атакуючий повинен згенерувати паузу радіочастотного сигналу. Це означає, що атакуючий повинен створити таке поле, яке ідеально перекриє вихідне на антені приймача, і одержувач отримає нульовий сигнал. На практиці таке неможливо. Однак, при використанні модифікованої схеми Міллера, при передачі двох послідовних одиниць, атакуючий може змінити другу одиницю на нуль, заповнивши паузу, яка кодує другу одиницю. Декодер побачить відсутність паузи у другому біті і декодує її як правильний 0, оскільки йому передує одиниця. Таким чином, при 100% модуляції зловмисник не може змінити значення 0 на 1, але може змінити бітове значення 1 на 0, в разі, якщо цьому біту передує 1, тобто з ймовірністю 0.5.

Для 10% модуляції декодер заміряє обидва рівня сигналу (82% і повний) і порівнює їх. У разі, якщо сигнали у вірних межах, сигнал вважається коректним і декодується. Атакуючий може спробувати додати рівень сигналу 82% таким чином, щоб повний сигнал став 82%, а 82% – повним. Таким чином, декодування інвертується. Можливість проведення даної атаки залежить від динамічного діапазону вхідного сигналу приймача. Досить імовірно, що рівень модифікованого сигналу перевищить максимально можливий діапазон вхідного.

Отже, для 100% модифікованого кодування Міллера атака здійснюється тільки для певних бітів, а для Манчестерського кодування атака може здійснюватись для всіх біт.

### 2.1.4. Вставка даних

Даний тип атаки має на увазі вставку свого повідомлення в NFC-канал передавання двох пристроїв. Як було зазначено раніше, NFC організовує передачу даних за принципом повідомлення-відповідь. У тому випадку, якщо пристрою, що відповідає, необхідний довгий проміжок часу щоб згенерувати відповідь, зловмисник має можливість вставити в канал своє повідомлення, і воно буде сприйнято пристроєм, який ініціює спілкування як легітимна відповідь. Схема даної атаки зображена на рис.2.3.

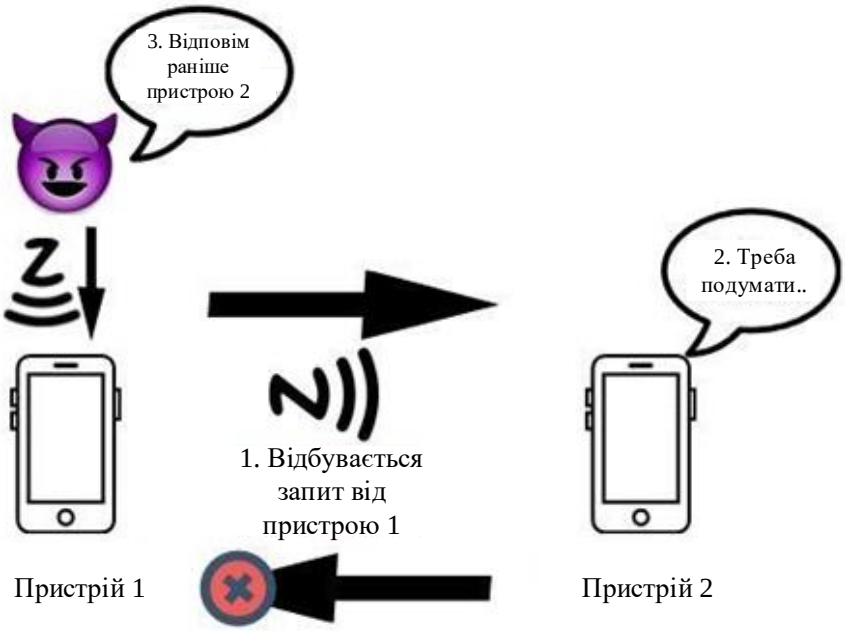


Рисунок 2.3 -Схема атаки за допомогою вставки даних

Якщо для другого пристрою, що приймає участь в обміні інформації, необхідні тривалі розрахунки, то у атакуючого з'являється можливість послати відповідь швидше, ніж це зробить легітимний пристрій. Вставка даних буде успішною тільки в тому разі якщо передача даних зловмисника почнеться строго раніше, ніж відповідь легітимного пристрою. Якщо обидва пристрої почнуть віщати одночасно, то їх радіочастоти перекриються і дані буде пошкоджено, що побічно але може рахуватися атакою пошкодження даних.

### 2.1.5. Атака «людина посередині»

У класичному поданні атаки «людина посередині» або MITM два суб'єкта здійснюють спілкування. Назвемо ці суб'єкти Аліса і Боб.Третій суб'єкт є зловмисником, назвемо цей суб'єкт Єва. Єва шляхом певних маніпуляцій може встати в канал між Алісою і Бобом і читати їх повідомлення, причому ні Аліса, ні Боб не будуть підозрювати, що хтось прослуховує їх канал спілкування, але насправді між ними стоїть Єва. В її можливості входить прослуховування і модифікація переданих даних. Схема атаки зображена на рис.2.4.

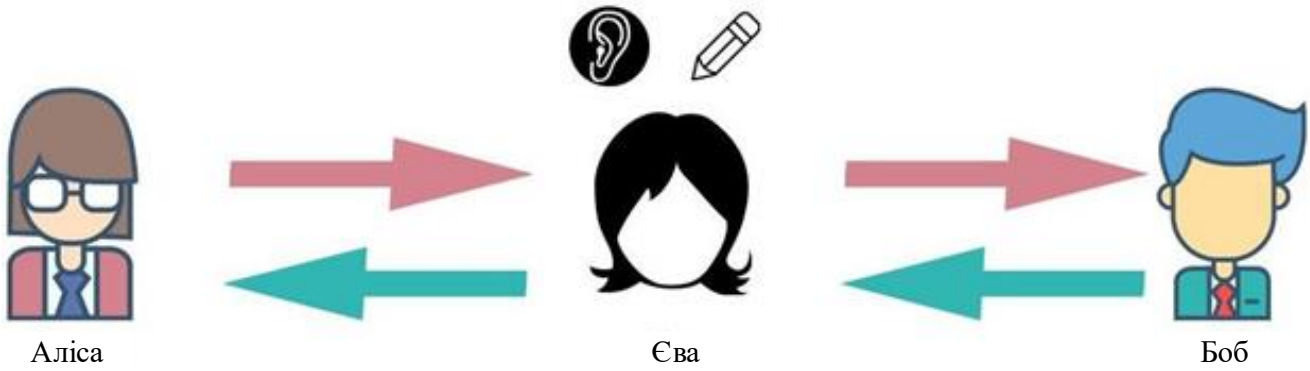


Рисунок 2.4 - Загальна схема атаки MITM

Даний сценарій є типовим для нешифрованих каналів або каналів з не аутентифікованим обміном ключами (наприклад, алгоритм Діффі-Хеллмана). Припустимо, Аліса і Боб хочуть встановити безпечний канал, обмінявшись секретним ключем. Однак, Єва може встановити один ключ з Алісою і інший ключ з Бобом. Згодом, коли Аліса буде пересилати дані Бобу, Єва буде отримувати їх і розшифровувати наявним ключем, потім зашифровувати на ключі Боба і пересилати його Бобу. Таким чином і Аліса, і Боб думатимуть, що спілкуються по захищеному каналу один з одним, але насправді все спілкування буде відбуватися через посередника.

Розглянемо подібну схему перехоплення повідомлень стосовно NFC-каналу.

Розглянемо випадок, коли Аліса оперує в активному режимі, а Боб в пасивному. Аліса генерує РЧ поле і посилає деякі дані Бобу. У разі, якщо Єва

знаходиться на досить близькій відстані, вона може прослухати дані послані Алісою, крім того, Єва може перервати передачу даних Аліси і бути впевненою в тому, що Боб не отримає повідомлення. Але, так як для переривання буде використано те саме РЧ поле, Аліса може помітити це і зупинити протокол обміну ключами.

Припустимо, що на стороні Аліси перевірка на переривання повідомлення не виконується, і протокол обміну ключами продовжиться. На наступному кроці Єва повинна буде послати Бобу дані. Але, так як поле, створене Алісою, все ще діє, а для відсилання даних Єва повинна також згенерувати нове поле, виникає проблема інтерференції полів. На практиці Єві неможливо створити таке РЧ поле, щоб Боб зрозумів, що йому хоче сказати Єва.

Таким чином, через те, що дана атака може бути помічена на стороні Аліси, і, через накладання двох РЧ полів, атака типу «людина посередині» неможлива в подібній конфігурації.

В іншій конфігурації і Аліса, і Боб оперують в активному режимі. Єва знову може перервати повідомлення Аліси, і Аліса знову може це помітити. Припустимо, що дана перевірка не виконується і перейдемо до наступного кроку. Тепер Єва повинна послати повідомлення Бобу, при цьому Аліса вимикає своє РЧ поле, тому що передача завершена. Однак, вимкнувши своє РЧ поле, Аліса переходить в режим прослуховування і так само отримає повідомлення, яке Єва послала Бобу. В даному випадку Єва не може послати повідомлення ні окремо Бобу, ні окремо Алісі, повідомлення будуть отримані обома пристроями.

Таким чином, можна стверджувати, що атака типу «людина посередині» для протоколу NFC нездійсненна.

### 2.1.6. Атака типу Relay

Даний вид атак застосуємо для нелегітимного використання чужих карток NFC. Підхід заснований на «розширенні» області дії NFC. Насправді, запит від легітимного зчитувача передається по швидкісному каналу на віддалений зчитувач зловмисника, який безпосередньо взаємодіє з карткою. Потім відповідь картки перенаправляється через швидкий канал назад на легітимний зчитувач. Для здійснення даної атаки, зловмисник повинен отримати безпосередній фізичний доступ до смарт-картки. [6] Схема relay-атаки зображена на рис.2.5.

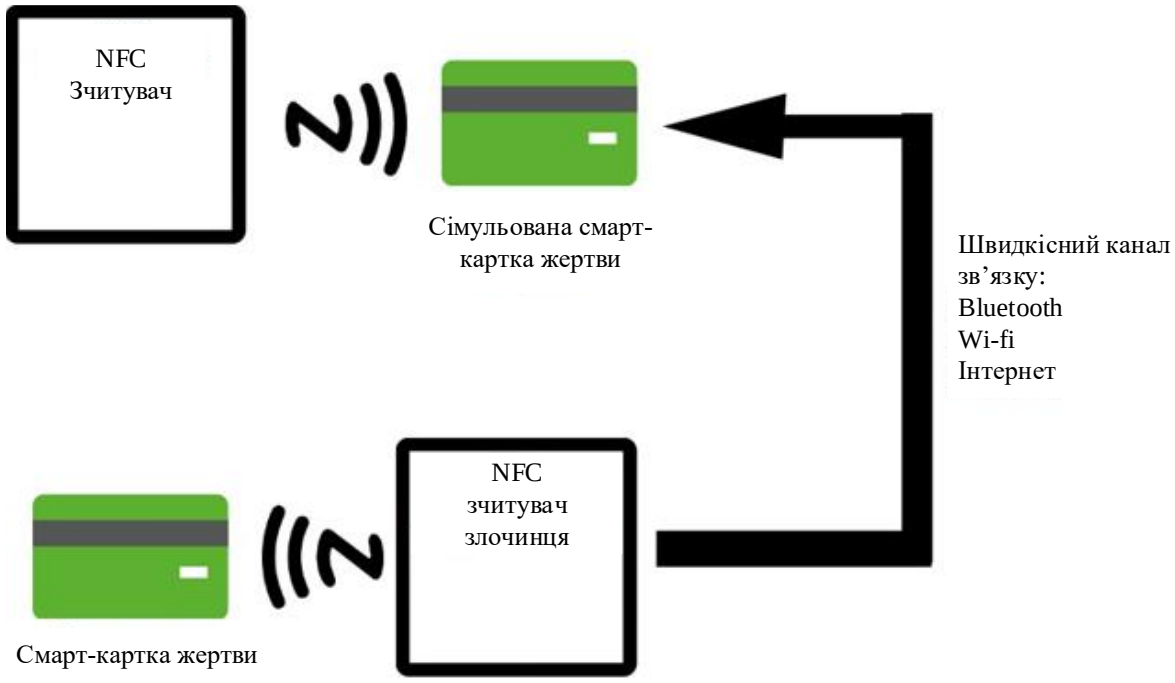


Рисунок 2.5 - Схема relay-атаки

Атака ускладнюється, тим, що можливі тимчасові затримки через використання стороннього каналу. Згідно ISO 14443-4 тимчасові затримки ранжуються від 302 s to 4949 ms. [7]

## 2.2. Захист від атак на канал NFC

Захист від розглянутих раніше атак може бути реалізований на рівні додатку. Як правило, для цих цілей використовується криптографія.

### 2.2.1. Захист від пасивного прослуховування

Дані, що передаються з пасивного пристрою набагато складніше піддаються прослуховуванню, проте, використання пасивного режиму для додатків, що передають конфіденційну інформацію не є достатньою мірою захисту. Єдиним дієвим рішенням може бути використання каналу, захищеного криптографією.

### 2.2.2. Захист від пошкодження даних

NFC-пристрої можуть протистояти даному типу атак шляхом перевірки РЧ поля під час передавання даних. Потужність, що витрачається для пошкодження даних, набагато більше потужності, використовуваної при штатній передачі даних. Таким чином, ці атаки легко виявляються.

### 2.2.3. Захист від модифікації даних

Захист від модифікації даних може бути досягнуто декількома шляхами.

По-перше, використання швидкості в 106 кбод в активному режимі дозволяє запобігти зміні біт в деяких випадках. Таким чином, при використанні активних передавачів в обох напрямках можна частково захиститися від модифікації даних. Однак, активний режим погано захищений від прослуховування.

Так само передавальний пристрій NFC може перевіряти РЧ поле в момент посилки і при детектуванні подібної атаки припиняти передачу.

Третій і найдієвіший спосіб - використовувати канал, захищений криптографією.

### 2.2.4. Захист від вставки даних

Для даної атаки можливі три методи протидії. По-перше, пристрій, що дає відповідь повинен посилати відповідь без затримки. Таким чином, атакуючий не зможе послати своє повідомлення, так як основною умовою проведення даної атаки є довга генерація відповіді. Проте, даний метод не є вичерпним і не може бути застосований, якщо обчислення необхідні для роботи самої програми.

По-друге, пристрій, що відповідає може прослуховувати канал під час підготовки своєї відповіді. І, при наявності сторонніх повідомлень, припиняти спілкування.

По-третє, рекомендується використовувати канал, захищений криптографією.

### 2.2.5. Захист від атаки «людина посередині»

Як було зазначено раніше, реалізація атаки «людина посередині» практично неможлива при обміну інформацією за допомогою NFC. Проте за можливістю, рекомендується використовувати пристрої в конфігурації активний-пасивний, щоб в каналі завжди було згенеровано РЧ поле.

Так само передавальний пристрій може постійно прослуховувати канал, щоб мати можливість помітити підозрілі дії з боку потенційного атакуючого.

### 2.2.6. Захист від Relay-атак

Стосовно смарт-карток можуть бути використані наступні методи для захисту від даного різновиду атак:

- клітки Фарадея.Екранування карток під час її невикористання;
- використання цифрового підпису для переданих даних;
- застосування distance-bounding protocols. [8]

## 2.3. Встановлення безпечного каналу для NFC

Встановлення безпечного каналу між двома пристроями, що обмінюються даними з NFC є кращим способом захисту від атак підслуховування і модифікації даних в каналі. Через те, що NFC не схильний до атак типу «людина посередині», то для встановлення сеансового ключа підійде стандартний протокол узгодження ключа, наприклад, алгоритм Діффі-Хелмана, заснований на RSA [9] або еліптичних кривих. Після встановлення загального секретного ключа можна передати ключ 3DES або AES, який потім буде використаний для надання конфіденційності, цілісності і аутентифікації переданих даних.

NFC дозволяє створити специфічний протокол обміну ключами. Його застосування не використовує криптографію з відкритим ключем, таким чином, значно знижується обчислювальна складність. Теоретично, цей метод надає хорошу захищеність. Схема працює для 100% амплітудної модуляції і не є частиною стандартів з NFC.

Ідея полягає в тому, що взаємодіючі пристрої посилають випадкові дані в один момент часу. Під час установки з'єднання обидва пристрої синхронізуються за швидкістю передачі, амплітуді і фазі РЧ сигналу. Це можливо, завдяки тому, що пристрої починають передавати інформацію одночасно. Після синхронізації, пристрій 1 і пристрій 2 починають синхронну передачу і слухають те, що передає інший пристрій. Коли обидва пристрої посилають 0, сумарний сигнал так само є нулем, і атакуючий може його перехопити. Схожим чином можна перехопити одночасну відправку одиниці обома пристроями - сумарний сигнал буде дорівнює подвоєному сигналу одиниці. Але, якщо пристрої посилають різні сигнали, то атакуючий вже не зможе зрозуміти, що було послано кожним з пристроїв, а пристрої зможуть зрозуміти, так як вони мають у своєму розпорядженні дані про те, що послали вони самі. Всі представлені випадки зображені на рис.2.6.

На верхньому графіку зображено сигнал пристрою 1 червоним кольором, сигнал пристрою 2 синім кольором. Нижній графік показує результуючий сигнал, який може зчитувати атакуючий.

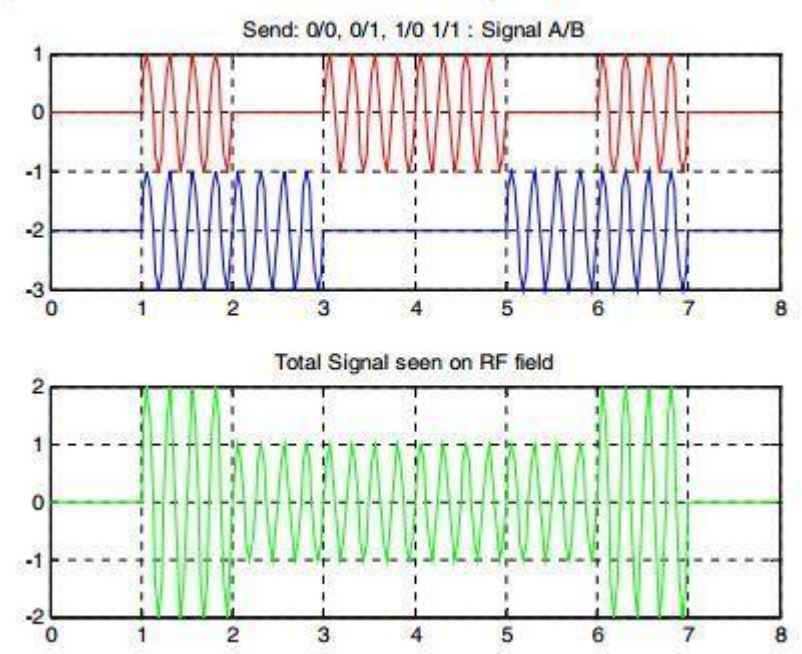


Рисунок 2.6 - Загальний сигнал, одержуваний на виході

Обидва пристрої відкидають біти, якщо були послані однакові значення і приймають, якщо були послані різні. Залежно від домовленості приймаються біти пристрою 1, або пристрою 2 - це може бути обумовлено в процесі синхронізації, але особливої ролі не грає. Таким чином, пристрої можуть згенерувати секретний ключ. Нові біти генеруються з ймовірність 50%, таким чином, в середньому, для генерації ключа 128 біт нам знадобиться згенерувати 256 бітів. При швидкості генерації в 106 кбод це займе близько 2,4 мілісекунд, що є прийнятним за часом.

Безпека даного протоколу на практиці залежить від якості синхронізації, яка досягається між двома пристроями. Очевидно, що, якщо зловмисник зможе розпізнати дані відправлені пристроєм 1 від пристрою 2, то безпека буде порушена. Дані повинні строго відповідати як за амплітудою, так і за фазою. Після того, як відмінності між пристроями, що обмінюються даними

стають нижче рівня шуму, протокол є безпечним. Також на безпеку має вплив якість с игналу в приймачі.

## 2.4. Технологія NFC в мобільних телефонах на базі ОС Android

Більшість Android-телефонів, що підтримують технологію NFC, так само підтримують технологію HCE - емуляцію NFC карт. Ця технологія, отримала розвиток в ОС Android, починаючи з API версії 19, KitKat 4.4.

Емуляція карт була можлива і до Android KitKat, але це було реалізовано за допомогою Secure Element. Реалізація за допомогою Secure Element представлено на рис.2.7. Додаток встановлював образ карти на Secure Element, пристрій подносився до зчитувача і до моменту закінчення передачі користувач не мав доступу до ходу транзакції. [10]

HCE ж перенаправляє NFC дані відразу в процесор, де запущені інші програми. Там ці дані обробляються за допомогою компонент, відомих як HCE-сервіси. Обробка за допомогою HCE-сервісів представлено на рис.2.8.

Окремо варто відзначити, що технологію HCE підтримують не тільки телефону на базі ОС Android, а також смартфони на базі ОС Windows і Blackberry.

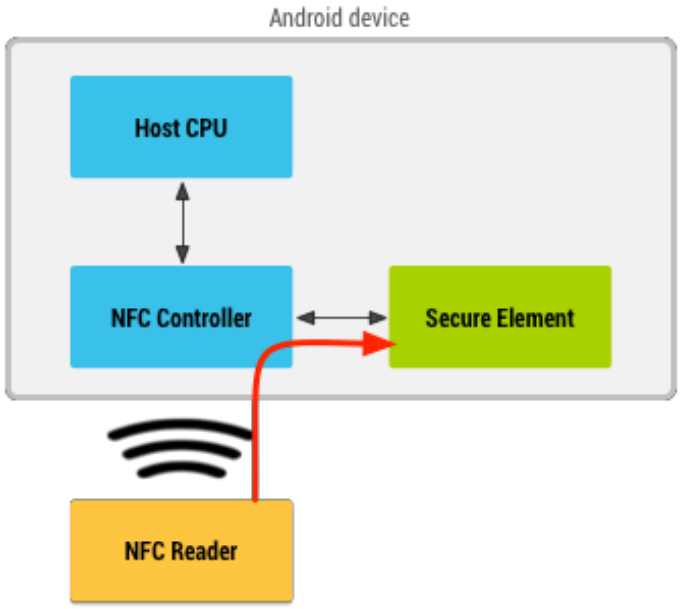


Рисунок 2.7 - Емуляція картки з використанням Secure Element

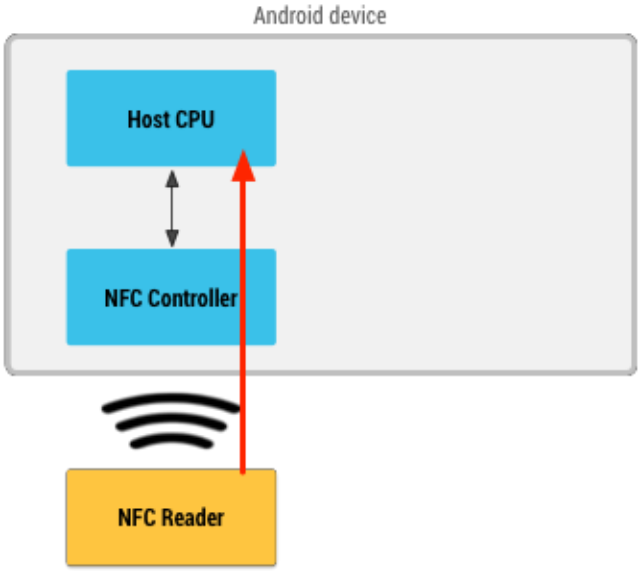


Рисунок 2.8 - Емуляція картки за допомогою HCE

Android 4.4 підтримує більшість протоколів, поширених в даний час. Стек протоколів, підтримуваних реалізацією HCE в ОС Android представлений на рис.2.9.

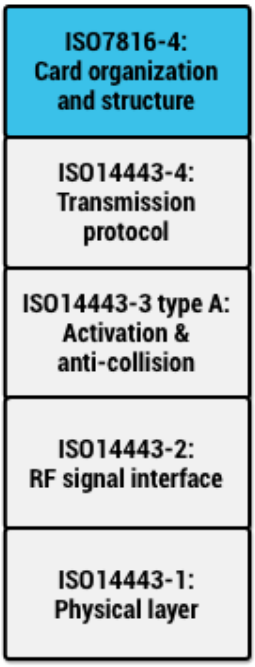


Рисунок 2.9 - Протоколи, які підтримуються реалізацією HCE в ОС Android HCE-сервіси є розширенням звичних сервісів ОСAndroid

Основна перевага даного підходу в тому, що користувачеві не треба включати додаток для виклику емулюємої NFC-карти, сам сервіс може навіть не мати графічного інтерфейсу.

Даний підхід зручний для використання емуляції карт програм лояльності клієнтів - користувачеві не потрібно шукати потрібну програму і включати її. У момент, коли мобільний пристрій підноситься до зчитувача, ОС Android повинна визначити, з яким з HCE-обробників NFC-зчитувач хоче встановити зв'язок. Реалізовано це за допомогою призначення кожному сервісу унікального ідентифікатора AID. Буквально, AID показує який саме обробник необхідно викликати. Процес вибору сервісу обробника показаний на рис.2.10.

Розмір AID може бути до 16 байтів, так само окремо виділяють групи AID зарезервованих для зареєстрованих інфраструктур - Google Wallet, Visa, Master Card і ідентифікатори для вільного користування [9].


Рисунок 2.10 - Процес вибору сервісу-обробника HCE

Щоб уникнути збігу AID`ов у кількох додатків з репозиторію необхідно реєструвати свої AID`и. Тут в силу вступає специфікація ISO / IEC 7816-5. Список AID`ов, задіяних в додатку, міститься в маніфесті.

Іноді виникають ситуації, коли HCE-сервісу необхідно зареєструвати кілька ідентифікаторів в додатку і бути впевненим, що всі запити надійдуть саме в цей додаток. У такому випадку використовуються групи AID`ов. Для всіх AID`ов в групі на рівні ОС буде гарантовано наступні умови:

• всі запити з AID`амі з даної групи будуть переправлені до даного HCE-сервісу;

• жоден із запитів з AID`ом з цієї групи не буде переправлений до даного HCE-сервісу (наприклад, якщо користувач вирішив використовувати інший додаток для обробки будь-якого зарезервованого AID`а з цієї групи або кількох.

Іншими словами, не існує проміжного стану, коли якісь запити з ідентифікаторами з групи AID`ов будуть спрямовані в HCE-сервіс, а інші ні.

### 2.4.1. Безпека HCE

Область дії NFC становить близько 10 сантиметрів. Це ускладнює знімання інформації без безпосереднього знаходження поруч з об'єктом.

Безпека HCE заснована на тому, що сервіс, який відповідає за комунікацію, використовує системне вирішення BIND_NFC_SERVICE. Це означає, що тільки ОС може взаємодіяти з сервісом і дозволяє переконатися в тому, що дані, отримані від NFC контролера ті ж самі, що були послані. Те ж діє і у зворотний бік.

У поточній реалізації ОС, контролер NFC працює тільки при включеному екрані. Це дозволяє уникнути ситуацій непередбаченому використанню HCE-сервісів. Крім того, в маніфесті можна вказати, чи буде сервіс доступний без розблокування екрану. Налаштування за замовчуванням не оптимальні в плані безпеки, сервіс не вимагає введення стандартного пін-коду ОС для своєї роботи. Якщо встановити атрибут android: requireDeviceUnlock в значення true, то пристрій спершу запросить пароль, а після цього попросить користувача знову прикласти телефон до зчитувача, тому що користувач міг прибрати телефон для введення пароля.

### 2.4.2 Реалізація HCE-обробників

Для обробки запитів, що надходять від NFC-зчитувача, використовується HCE-сервіс. Даний клас розширює існуючий клас HostApduService і реалізує дві функції, які необхідно перевизначити.

Перша функція public byte processCommandApdu (byte apdu, Bundle extras). Дані у вигляді байтового архіву потрапляють в цю функцію якщо NFC - зчитувач встановив контакт з даним сервісом за допомогою APDU-команди: SELECT AID, де AID - унікальний ідентифікаційний номер сервісу, який займається обробкою наших запитів. Після даної команди - всі запити від NFC зчитувача будуть гарантовано спрямовані в наш сервіс доти, поки:

• Не прийде інша команда SELECT AID, з іншим номером AID;

• канал передачі даних не буде порушений шляхом вийняття мобільного пристрої з поля дії NFC-зчитувача.

В обох випадках буде викликана функція onDeactivated (), мова про яку піде пізніше.

Повернене функцією processCommandApdu ()значення відсилається в якості відповіді. У відповідь на команду SELECT AID необхідно надіслати 0x9000. Це код успішної операції, він означає, що зв'язок між зчитувачем і сервісом встановлений і дані можуть бути передані.

Далі в даній функції необхідно реалізувати варіанти відповіді на різні команди, в залежності від реалізованого протоколу, якщо ми створюємо свій протокол передавання. Або можна реалізувати вже наявні протоколи згідно їх специфікації. При реалізації запитів і відповідей для реалізованого протоколу необхідно враховувати, що мінімальний розмір APDU - 4байта, максимальний - 259 байт. Цього об'єму достатньо для обміну ключами, текстовою інформацією, інакше можна вдатися до поділу повідомлення на кілька пакетів, але варто пам'ятати, що пропускна здатність каналу NFC не підходить для передачі більших обсягів даних. Як правило, практична швидкість передачі даних складає 424 Кбіт / с. Передача великих обсягів даних може викликати великі затримки.

Якщо обчислення відповіді вимагає великої кількості часу, відповідь можна відправити за допомогою виклику функції sendResponseApdu (byte [] responseApdu), таким чином, можна уникнути зависання GUI, якщо додаток використовує складні обчислення для генерації відповідного повідомлення.

Друга функція, яку необхідно перевизначити void onDeactivated (int reason). У ній необхідно задати дії, що виконуються при деактивації каналу передачі даних.

### 2.4.3 Вирішення конфліктів між обробниками

Так як на одному пристрої може бути встановлено безлічі HCE- компонент, один і той же AID може бути зареєстрований для декількох сервісів. ОС Android вирішує конфлікт вибору сервісу, грунтуючись на його категорії. Наприклад, якщо використовується платіжний сервіс з категорії CATEGORY_PAYMENT, у користувача є можливість вручну вказати який сервіс використовувати за замовчуванням. Для того, щоб упевнитися, що додаток є обробником за замовчуванням для даного AID, можна викликати функцію isDefaultServiceForCategory (ComponentName, String) і в разі негативної відповіді запросити у користувача права на зміну.

# РОЗДІЛ 3. РОЗРОБКА МЕТОДУ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NFC ДЛЯ АВТОМАТИЗОВАНОЇ РЕПЛІКАЦІЇ ПРОФІЛЮ КОРИСТУВАЧА

## 3.1 Задачі і мета методу, що розробляється

Технологія NFC, дозволяє передавати дані на відстані до 10 см за допомогою радіосигналу. Сучасні мобільні телефони на базі ОС Android підтримують технологію HCE, яка дозволяє запрограмувати свій сервіс-обробник для вхідних NFC-команд, при цьому на рівні ОС гарантується, що дані, отримані від контролера, надійдуть виключно в заданий додаток. Практична швидкість роботи NFC (близько 400 кбіт / с) не дозволяє передавати великі обсяги даних, а тому цей канал зв'язку можна використовувати для первинного обміну ключами з метою встановлення альтернативного шифрованого каналу для безпосередньої передачі даних. В якості альтернативного каналу, наприклад, можуть бути використані Bluetooth- з'єднання, wi-fi та інші.

Крім того, використання технології NFC дозволяє використовувати мобільний телефон як ключ і відслідковувати, чи знаходиться він в поле дії NFC-зчитувача. Як тільки телефон забирається, можна проводити очищення синхронізованого профілю з комп'ютера. Таким чином вирішується проблема тимчасового розгортання призначеного для користувача профілю, включаючи логіни, паролі, налаштування браузера та інші дані на робочій станції.

Визначимо перелік вимог щодо розроблюваного методу. Запропонований метод повинен:

- в якості каналу для установки сеансового ключа використовувати NFC- з'єднання;
- в якості каналу для передачі даних використовувати альтернативний канал, а передані дані повинні бути зашифровані на сеансовому ключі;
- для забезпечення безпеки даних забезпечити шифрування переданих даних на джерелі і одержувачі;

- здійснювати очищення даних, що реплікуються, на одержувачі після закінчення роботи

Схема запропонованого методу зображена на рис.3.1.


Рисунок 3.1 - Схема реплікації із застосуванням NFC для установки захищеного каналу

З рис.3.1 очевидно, що розробка повинна враховувати чотири моменти:

- встановлення захищеного NFC каналу при наближенні пристроїв;
- встановлення альтернативного захищеного каналу з великою пропускною швидкістю;
- передавання даних за альтернативних захищеним каналом;
- видалення даних з пристрою А при завершенні NFC-з'єднання.

## 3.2 Прототип системи реплікації профілю користувача за допомогою технології NFC

Для реалізації запропонованої схеми пропонується використовувати Java-додаток, що здійснює обмін даними з Android-пристроєм, на якому

зберігається призначений для користувача зашифрований профіль. В якості профілю пропонується використовувати призначені для користувача дані від браузера Firefox.

Первинне встановлення сеансового ключа необхідно проводити за допомогою технології NFC. На стороні Java-додатка необхідно генерувати пару ключів для реалізації асиметричного шифрування. Потім, на стороні телефону генерувати сеансовий ключ симетричного шифрування і передавати його на відкритому ключі на сторону Java-додатка. Для передачі використовується NFC- зчитувач ACR122U.

Після обміну ключами необхідно зробити установку Bluetooth-каналу і передати у ньому зашифрований профіль.

На стороні Java-додатка профіль розшифрувати і забезпечити його працездатність в браузері Mozilla Firefox.

Функціональна схема прототипу представлена на рис.3.2.

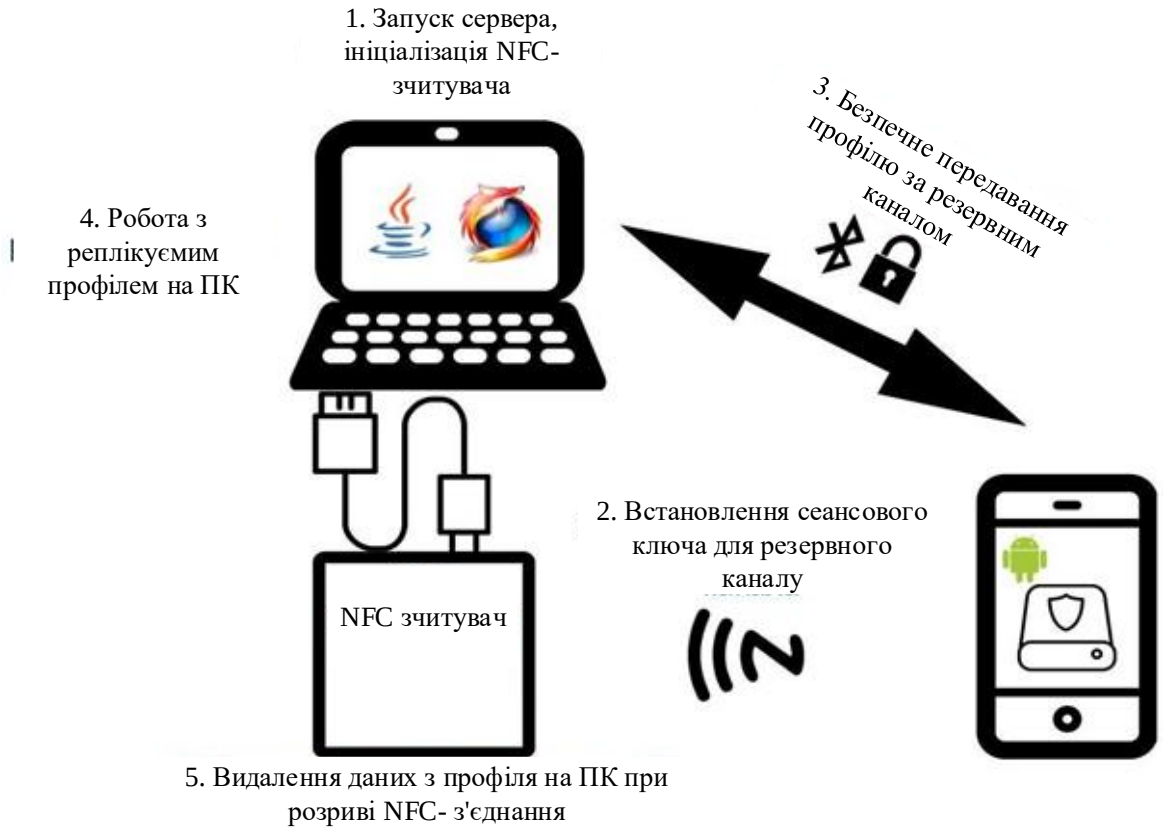


Рисунок 3.2 - Функціональна схема прототипу

### 3.2.1.Профіль Mozilla

Браузер Mozilla Firefox зберігає інформацію користувача: закладки, розширення і призначені для користувача переваги в унікальному профілі користувача. При першому запуску браузера створюється профіль за замовчуванням, додаткові профілі можна створити через меню менеджера профілів. Всі налаштування зберігаються в спеціальній папці, що складається з безлічі файлів.

В ОС Windows Vista і більш пізніх призначені для користувача профілі знаходяться за наступним шляхи:

```
C: \ Users \ <User name> \ AppData \ Roaming \ Mozilla \ Firefox \ Profiles \ <profilefolder>
```

або

```
% APPDATA% \ Mozilla \ Firefox \ Profiles \ <profile folder>,
```

де <User Name> збігається з ім'ям користувача профілю Windows, а <profile folder> – ім'я папки профілю у вигляді "xxxxxxxx.default".

Поточні параметри, пов'язані з існуючим профілем можна подивитися в папці "% APPDATA% \ Mozilla \ Firefox \ profiles.ini". Цей файл використовують при пошуку профілю при запуску браузера. Файл містить інформацію у вигляді зручному для редагування людиною через будь-який текстовий редактор.

Для того, щоб браузер завантажив наш профіль, відредагуємо даний файл програмно, попередньо зберігши його стару версію. Для цього необхідно змінити значення Path таким чином, щоб воно вказувало на папку, в яку буде реплікуватися призначений для користувача профіль, наприклад: "Profiles / tempProfileFolder". Тепер браузер при наступному запуску буде завантажувати профіль з вказаної директорії.

Крім того, засобами самого браузера можна задати майстер-пароль, який буде запитуватися при кожній спробі авторизуватися на сайті з використанням облікових даних, що зберігаються в базах даних браузера.

Ця додаткова міра захисту покликана допомогти при крадіжці файлів key3.db і signons.json, але вона не є вичерпною. Так як крадіжка даних файлів дозволяє проводити локальні атаки перебору і врешті-решт відновлення даних є можливим, але на складність впливає складність майстер-пароля.

Таблиця 3.1 - Вміст профілю Firefox [11]

| | |
|---|---|
| ***Folders*** | |
| Bookmarksbackups | Щоденні бекапи закладок стислі в форматі. jsonlz4 |
| Extensions | Встановлені розширення |
| Minidumps | Службова інформація про «падінні» браузера |
| Searchplugins | Додаткові пошукові движки і іконки для них |
| ***Files*** | |
| Addons.json | Інформація про аддона х браузера |
| Blocklist.xml | Чорний список аддонів, які не пройшли модерацію через несумісність з новою версією браузера, або містять загрози безпеки. Скачується автоматично при старті браузера. |
| Cert_override.txt | Зберігає виключення сертифікатів безпеки, задані користувачем |
| Cert8.db | Сховище сертифікатів безпеки |
| Compatibility.ini | Автоматично генерований файл. Зберігає в собі інформацію, про те, в якій системі в останній раз був завантажений профіль. |

Продовження таблиці 3.1

| | |
|---|---|
| content-prefs.sqlite | База з індивідуальними настройками для сторінок |
| cookies.sqlite | База, що зберігає cookie-файли |
| Extensions.ini | Список папок, в яких знаходяться встановлені розширення і теми. Файл генерується автоматично і є службовим. |
| Formhistory.sqlite | База даних, що містить інформацію, введену в форми. |
| Key3.db | База, що містить ключ для розшифровки збережених паролів. |
| localstore.rdf | Файл з настройками розташування панелей інструментів і їх розмірами / вмістом |
| logins.json | Файл з збереженими обліковими даними для авторизації на сайтах. Дані зашифровані. |
| mimeTypes.rdf | Дії, що вживаються при закачуванні визначених типів даних |
| parent.lock | Маркер того, що профіль в даний момент використовується браузером |
| permissions.sqlite | Файл з дозволами для сайтів: Спливаючі вікна, збережені cookies та ін. |
| places.sqlite | База з закладками, історією завантажень і історією відвідування сторінок. |

Продовження таблиці 3.1

| | |
|---|---|
| pluginreg.dat | Файл для реєстрації специфічних MIME-типів для плагінів. |
| Prefs.js | Всі призначені для користувача настройки |
| secmod.db | База даних з модулями безпеки |
| user.js | Призначені для користувача перевизначення файлу prefs.js |
| webappsstore.sqlite | Сховище DOM |
| xulstore.json | Файл з настройками розташування панелей інструментів і їх розмірами / вмістом |

### 3.2.2 Зберігання профілю в пам'яті телефону

Для передачі по захищеному каналу призначений для користувача профіль архівується в zip-архів для того, щоб знизити обсяг переданих даних і скористатися вбудованими в zip перевірками цілісності.

Після передачі на мобільний пристрій файл відразу ж зберігається у внутрішній пам'яті пристрою. Інші програми не зможуть отримати доступ до внутрішньої пам'яті нашого застосування, тому, що ОС Android використовує ізольовані середовища для кожної програми, що працює в системі.

Для забезпечення додаткової безпеки дані так само шифруються на ключі, який не може бути безпосередньо запитано з самого додатка. Для зберігання ключа використовується механізм KeyStore. За допомогою нього ключ може бути отриманий, тільки якщо користувач введе правильний код доступу. Даний підхід дозволяє уникнути ризиків, пов'язаних з втратою телефону і аналізом нешифрованої ФС. [12]

### 3.2.3 Встановлення захищеного каналу за допомогою NFC

Для безпечної передачі «чутливих» даних пропонується використовувати шифрований канал NFC. Первинна установка шифрованого каналу проводиться з використанням алгоритму RSA (Rivest, Shamir, Adleman). RSA - алгоритм асиметричного шифрування. На стороні комп'ютера генерується пара ключів - закритий і відкритий. Відкритий ключ, як показано на рис.3.2, за допомогою NFC доставляється на мобільний телефон.

Раніше було показано, що канал NFC безпечний для прослуховувань і атак типу «Людина посередині», таким чином ми можемо вільно передати відкритий ключ на мобільний пристрій і надалі на відкритому ключі встановити закритий ключ для алгоритму AES, як показано на рис.3.3, а також передати дані для підключення по альтернативному каналу передачі даних.

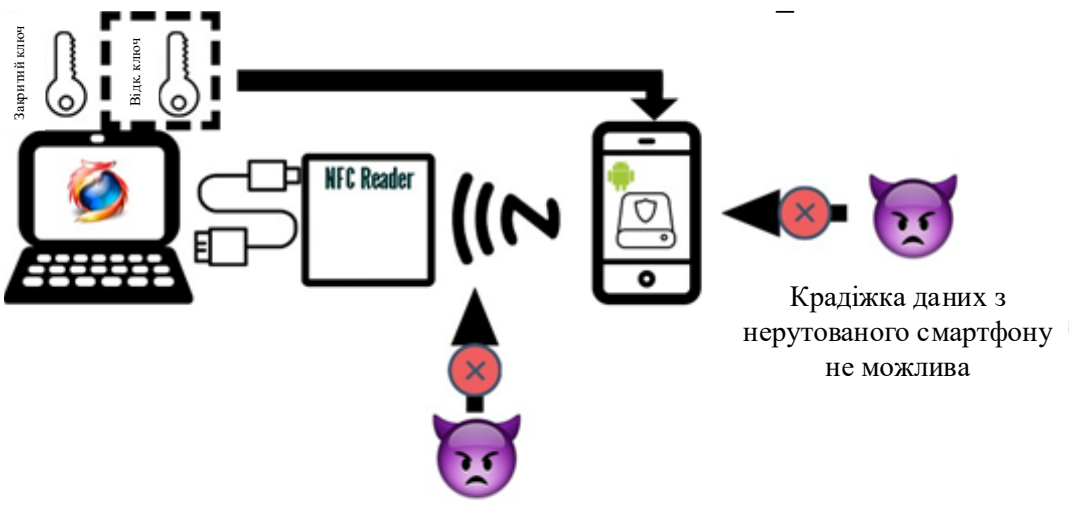


Рисунок 3.2 - Встановлення відкритого ключа

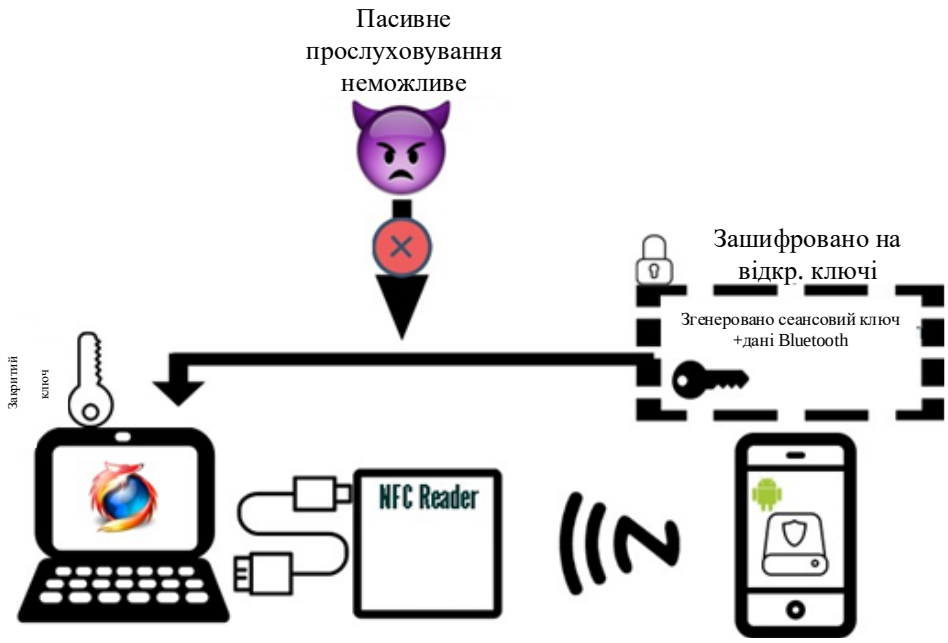


Рисунок 3.3 - Встановлення сеансового ключа протоколу NFC-комунікації

Завдяки технології Android Host Card Emulation, існує можливість створювати свій протокол спілкування пристроїв по NFC. У обробнику вхідних APDU-команд телефону можна запрограмувати як відповідь на вхідну команду, так і дії, що виконуються телефоном при отриманні команди. Наприклад, в таблиці 3.2 описана команда початку передавання профілю. При її отриманні, HCE-сервіс запускає Bluetooth-контролер на телефоні і намагається з'єднатися з пристроєм за допомогою даних, переданих в команді.

Щоб уникнути випадкових передач за допомогою relay-атак, при ініціації NFC-з'єднання, в обробник команди SELECT APDU можна додати підтвердження початку транзакції користувачем у вигляді діалогового вікна.

Крім того, в самому додатку можна використовувати автомат станів, зображений на рис.3.4. Тобто, якщо в додаток прийшов запит, а до нього не було щось ініціалізовано (Даний стан може виникнути, наприклад, в результаті атак зловмисника), то даний запит не виконується, дії заносяться в лог, а в зчитувач відсилається код помилки 0x6300.

Дана ситуація може виникнути, наприклад, якщо до пристрою після команди SELECT AID прийде команда на передачу даних по Bluetooth.

Помилка буде видана, тому, що дії по встановленню шифрованого каналу передачі даних ще не були зроблені.

Таблиця 3.2 - Протокол обміну APDU-командами

| Назва команди | Код запиту | Код відповіді | Опис |
|---|---|---|---|
| SELECT AID | 0x00A40400 0x07 <AID 7bytes> 00 | 0x9000 | Стандартна команда для з'єднання з android-додатком |
| sendOpenRSAKey | 0x00525341 0x <RSA_OPEN_KEY> | 0x9000 | Команда для обміну відкритим ключем, що генерується на стороні додатку |
| queryBTandSessionKey | 0x00525342 | 0x<cipheredBTsetting and generated session key> | Функція для запиту налаштувань Bluetooth- з'єднання і сеансового ключа, що генерується на стороні телефону. |
| startPCtoPhoneTransmit | 0x00525343 | 0x9000 | Почати передачу даних з комп'ютера на телефон |
| startPhoneToPCTransmit | 0x00525344 | 0x9000 | Почати передачу даних з Телефону на комп'ютер |

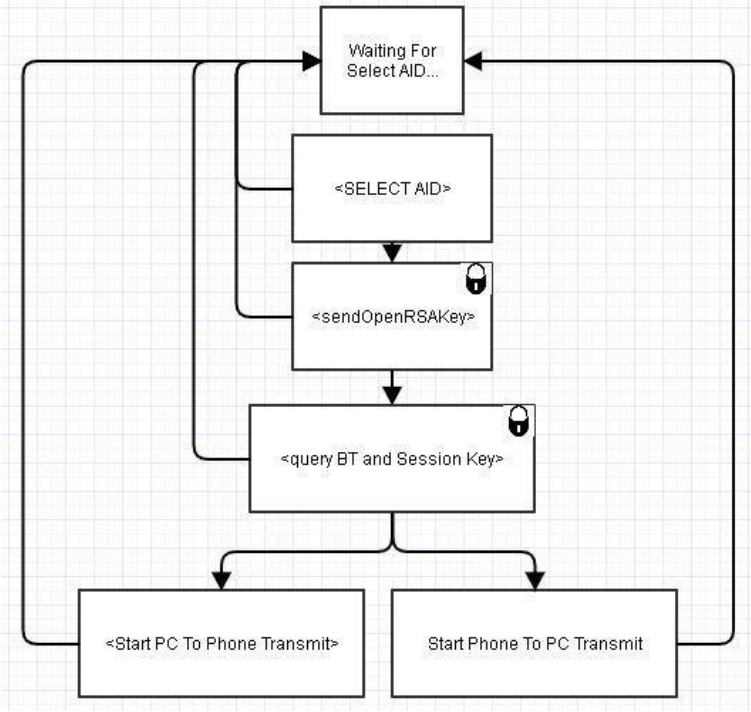


Рисунок 3.4 - Кінцевий алгоритм переходів протоколу обміну NFC-повідомленнями

### 3.2.4. Передача даних за альтернативним каналом

У прототипі в якості альтернативного каналу використовується Bluetooth- з'єднання. Для забезпечення більшої безпеки Bluetooth запускається в режимі прямого з'єднання, тобто з'єднання відбувається за допомогою використання прямої мак-адреси. Широкомовні запити не виконуються.

Крім того, всі дані в Bluetooth-каналі додатково шифруються на сеансовому ключі, що не дозволить зловмиснику зчитати дані з каналу, навіть якщо вдасться провести прослуховування. Схема передавання даних за альтернативним каналом представлена на рис.3.5.

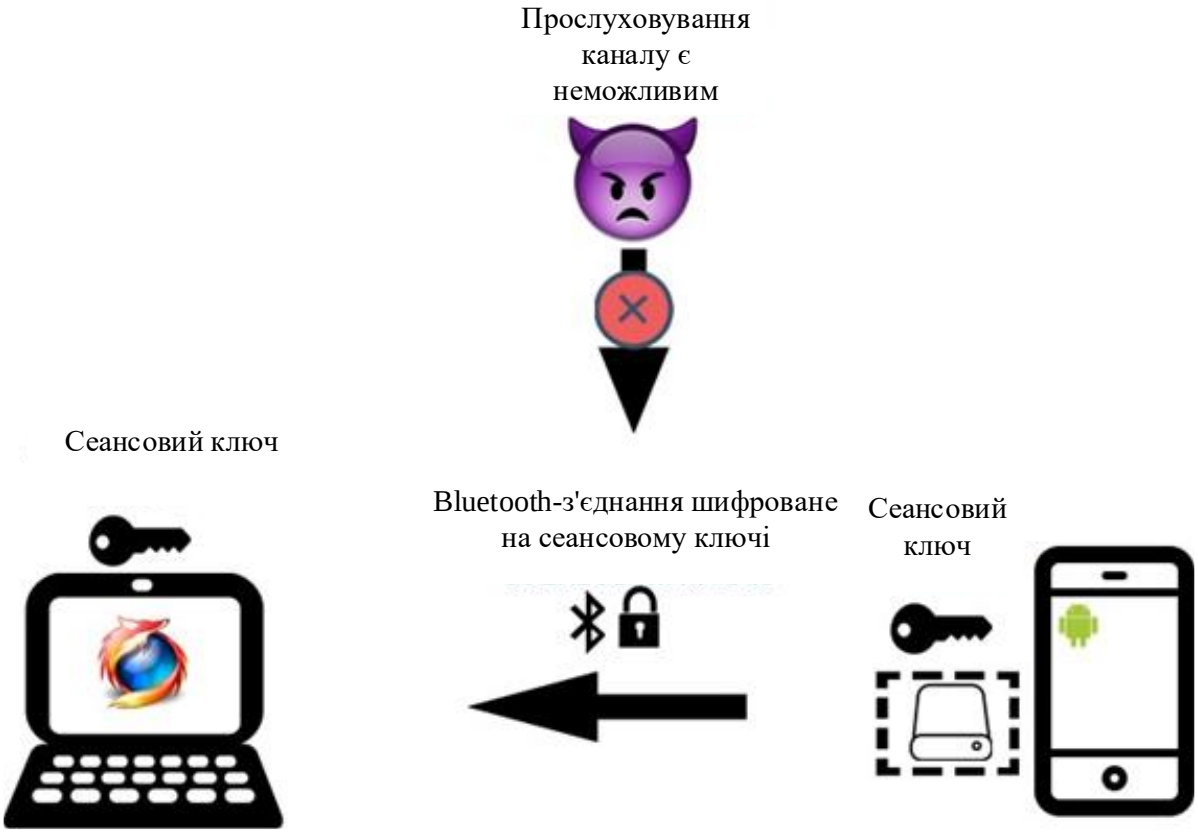


Рисунок 3.5 - Схема передавання даних за альтернативним каналом

Після передачі профілю користувача на комп'ютер, програма-сервер визначає, чи запущений вже браузер Mozilla Firefox і завершує його при необхідності. Потім проводиться розшифровка і парсинг переданого файлу, його переміщення в папку профілів, після цього можна запускати браузер і працювати. Даний етап зображений на рис.3.6.

Користувач може працювати з профілем до тих пір, поки його мобільний телефон знаходиться в полі дії NFC зчитувача. На момент роботи яскравість екрану автоматично забирається на самий мінімальний рівень. Пошук присутності телефону задається в додатку-сервері і за замовчуванням становить близько однієї секунди.

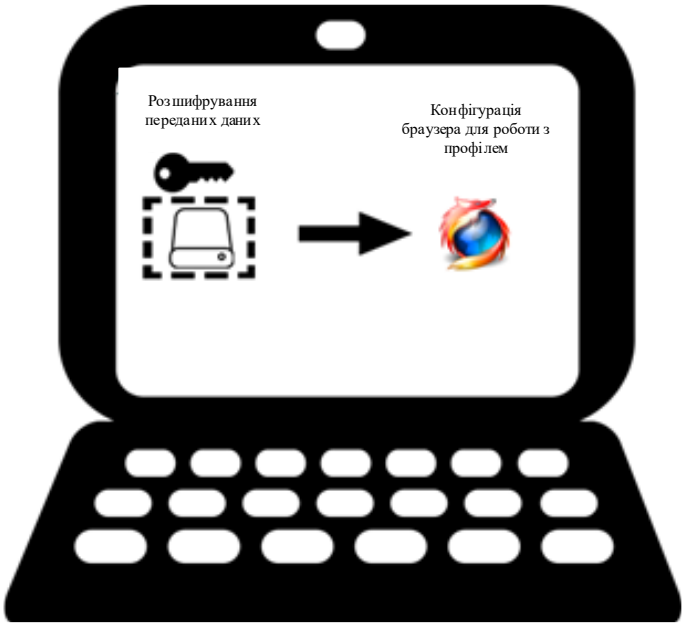


Рисунок 3.6 - Розшифрування переданого файлу та підготовка профілю до роботи

Як тільки телефон пропадає з поля дії зчитувача, виводиться відповідне повідомлення з пропозицією внести телефон назад і продовжити роботу, або вийти з системи і видалити всі дані з комп'ютера.

Окремо варто відзначити, що дані профілю, що репліковуються в цільову систему створюються у вигляді тимчасових файлів, таким чином, при коректному завершенні Java-машини, всі дані будуть коректно видалені.

# 4 СПЕЦІАЛЬНА ЧАСТИНА

В спеціальній частині приведено опис застосунку «SyncManager».

## 4.1 Алгоритм роботи програми

Запускається спочатку адміністративна панель (рис.4.1)

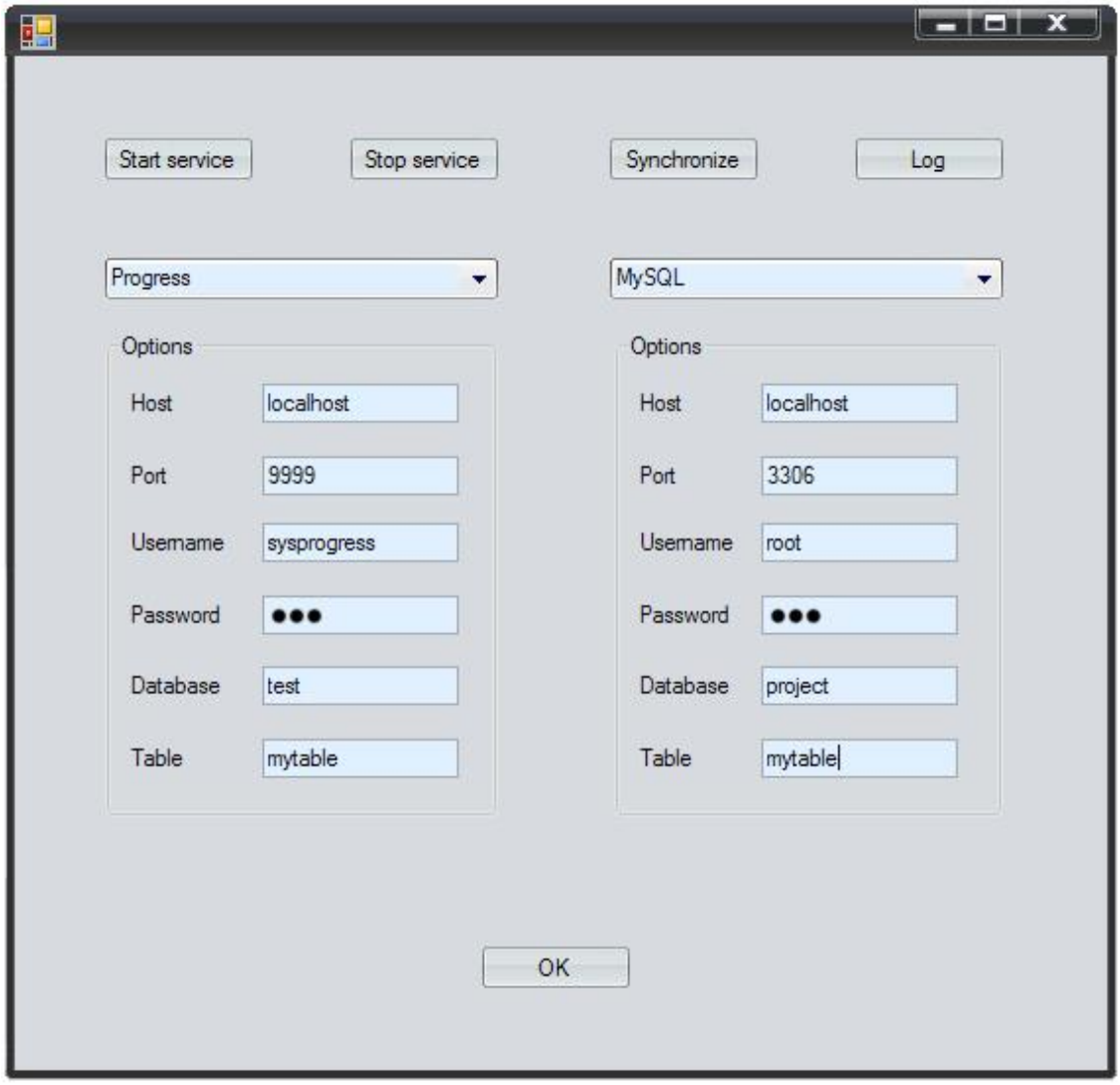


Рисунок 4.1 – Вікно адміністративної панелі

Користувач виставляє всі необхідні настройки з'єднання з базами, дані яких необхідно синхронізувати:

- Host
- Port
- Username
- Password
- Database
- Table

Налаштування записуються в файл. На їх основі автоматично формуються рядки з'єднання, скрипти для створення тригерів. За допомогою тригерів інформація буде заноситися в логи транзакцій таким чином, що в лозі буде зберігатися вже сформована команда для виконання в тій БД, в якій зміни ще не було. Так як бази різнорідні, характеристики у них теж різні. З'єднання ж встановлюється для всіх за однією схемою, ідентично створюються і тригери, але з тими відмінностями, які визначаються при виборі бази даних, яка бере участь в синхронізації. Звідси походить безпосередньо запуск і зупинка сервісу. Якщо з якоїсь причини необхідно змінити налаштування сервісу, то його можна зупинити, змінити конфігурацію і запустити знову. Також програма дозволяє здійснити синхронізація «за вимогою».

## 4.2 Synchronizing Service

Сервіс регулярно (через досить малі проміжки часу) звертається до логам транзакцій до баз, що синхронізуються . Якщо в них зареєстровані нові зміни, то сервіс запускає виконання команди з логу. При цьому відбувається перевірка, не виконувалася чи вже дана команда, і, тільки виключивши можливість дублювання даних, команда виконується. Команди зберігаються в логах в якомусь загальному вигляді, і в залежності від баз даних, що синхронізуються , перетворюються у відповідності з діалектом SQL, прийнятним для конкретної БД.

Труднощі, з якими довелося зіткнутися в ході роботи:

1) Відстеження додавання / зміни / видалення даних в кожній копії даних. Якщо додавання / видалення можна досить надійно синхронізувати, то при модифікації наявних даних виникає проблема "першородність" змін, тобто прийняття рішення про те, яка з змін якого поля є найбільш об'єктивною.

Є такий варіант обробки конфліктів: в лозі транзакцій фіксувати час зміни даних і вважати більш пізні зміни пріоритетними. При спробі видалення неіснуючої записи буде видаватися повідомлення про її відсутність, транзакція - відкочуватися.

2) Об'єктивна модифікація будь-яких лічильників, наприклад, лічильників продукції, що відвантажується. Якщо в обох копіях даних був організований декремент лічильника продукції на 1, при незмінності інших полів запису, то в синхронізованому запису повинен бути зроблений остаточний декремент вже на 2.

3) Проблема зростання складності синхронізації між трьома і більше копіями даних.

4) Необхідно виключати дублювання даних по логам.

5) Різні бази даних підтримують різні діалекти мови SQL, що вимагає індивідуального підходу при формуванні скриптів тригерів і запитів до синхронізуються баз даних. Також це перешкоджає розширенню системи на додаткові види баз даних, але, в силу відносної універсальності додатку, не виключає такої можливості.

### 4.3 Приклад практичної реалізації

Програма виконана на основі технології Windows Forms (Microsoft Visual Studio .Net 2005).

Додаток виконує наступні дії:

- Зчитує настройки з'єднання, назви таблиць, що синхронізуються.
- Заносить конфігураційні дані в файл у форматі XML.
- Визначає структуру таблиць.

- Визначає первинний ключ.
- Створює таблицю, в якій будуть фіксуватися всі зміни.
- Створює тригери на дії над даними.
- Запуск/ зупинка сервісу синхронізації.
- Запускає одноразову синхронізацію.

Налаштування конфігурації наведено на рис.4.2.

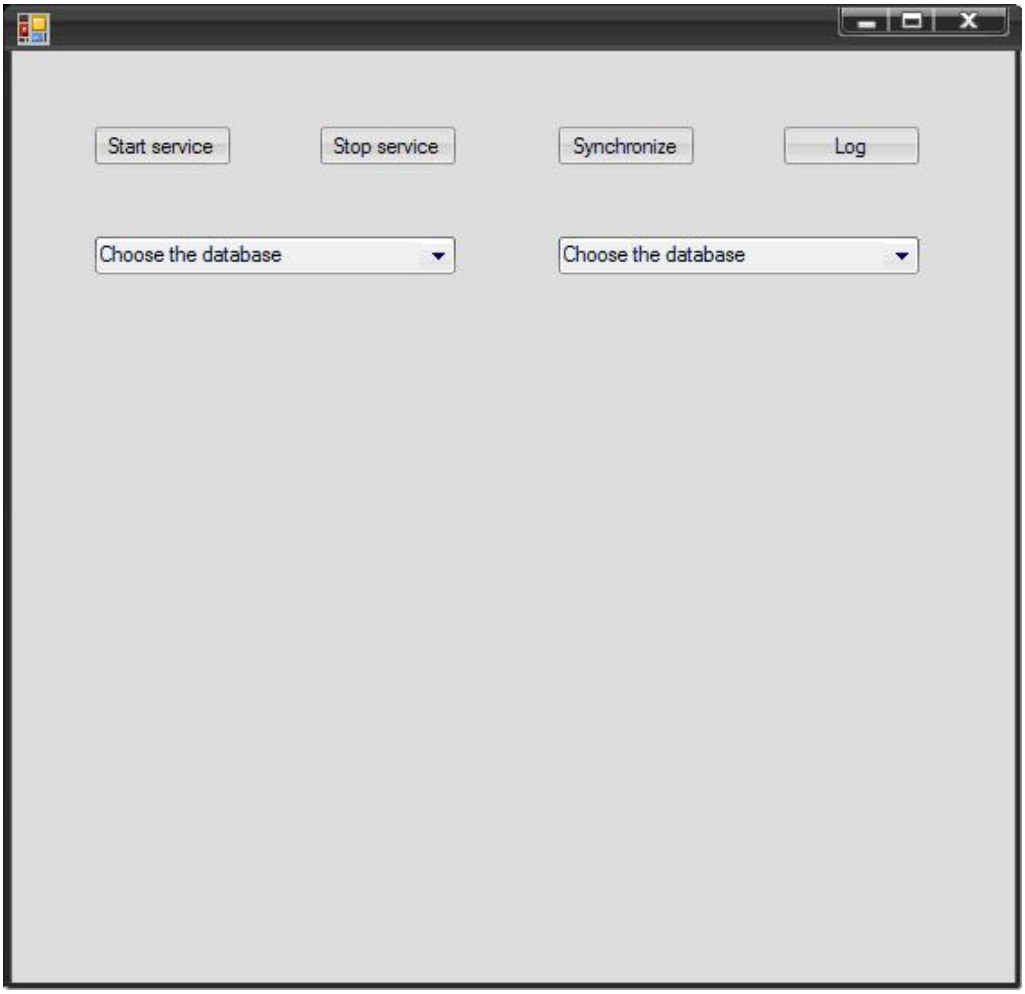


Рисунок 4.2 - Загальне налаштування конфігурації

Для встановлення з'єднання до різних баз потрібна різна інформація. При першому запуску форма має загальний вигляд. Залежно від типу БД, користувач отримує можливість вказати необхідні характеристики з'єднання (рис.4.3)

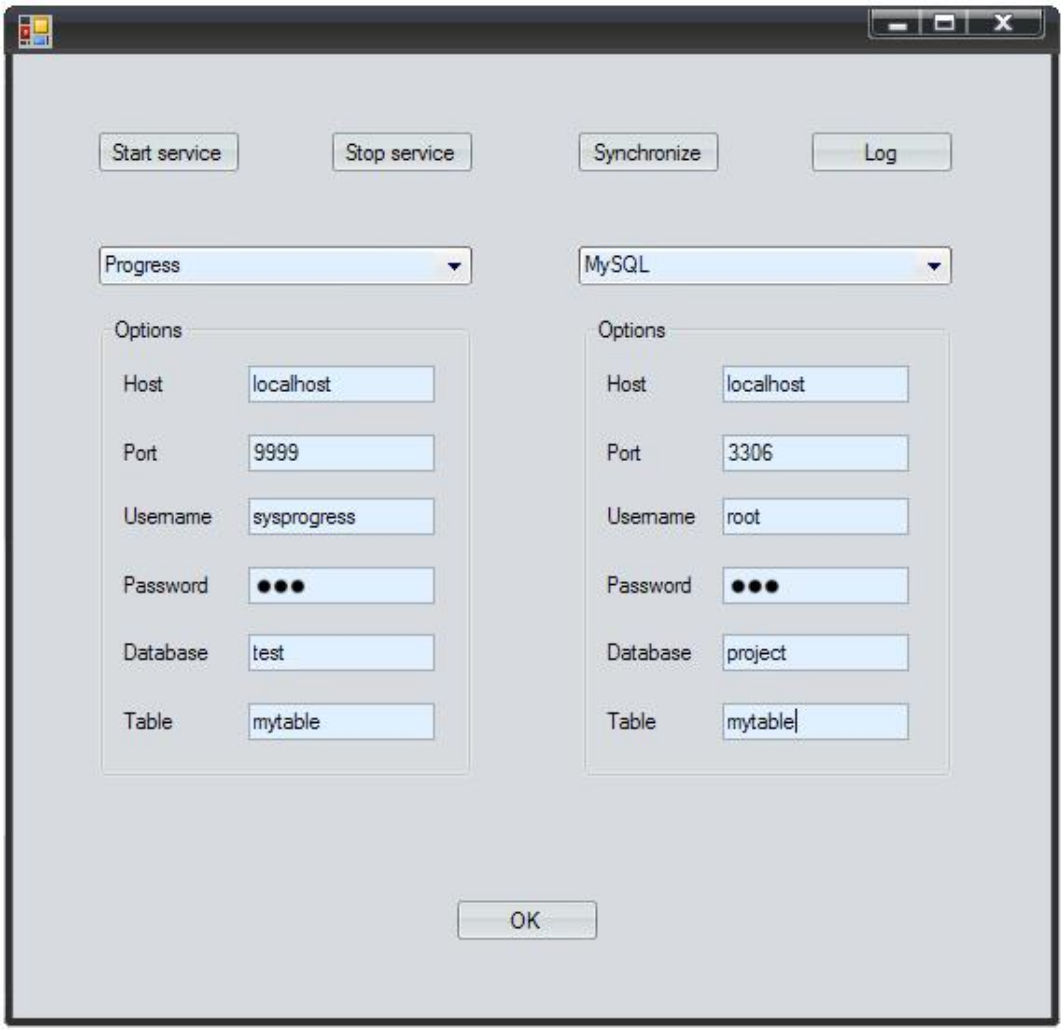


Рисунок 4.3 – Налаштування характеристик з'єднання

1) При натисканні кнопки «ОК» відбуваються такі дії (для кожної бази даних):

- Серіалізація внесених в форму даних
- Зчитування даних (тип бази даних, ім'я таблиці і характеристики з'єднання) з файлу налаштувань
- Формування рядків з'єднання
- Генерація тригерів до даної таблиці
- Створення таблиць змін (логів транзакцій)

2) При натисканні кнопки «Start service» відбувається запускається сервісу синхронізації

# 5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою дипломної роботи є створення захищеного методу реплікації даних використовуючи NFC-технологію, де новим основним шляхом подолання загроз є використання засобів рівня додатків, якими можна домогтися переваг, які не існують на канальному рівні.

## 5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Розробку захищеного методу реплікації даних використовуючи NFC-технологію поділити на декілька етапів, що дозволяє полегшити і структурувати виконання поставленого завдання.

Основні етапи такі:

1. Аналіз існуючих механізмів синхронізації даних і протоколу NFC.
2. Дослідження загроз при передачі даних за допомогою NFC.
3. Дослідження методів захисту від атак на канали NFC.
4. Розробка методу захищеної реплікації профілю користувача.
5. Створення прототипу системи реплікації профілю користувача.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу.

Виконавцем усіх операцій по розробці програмного забезпечення є інженер-програміст.

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та їх час виконання

| № п/п | Назва операції (стадії) | Виконавець | Середній час виконання операції, год. |
|---|---|---|---|
| 1. | Аналіз існуючих механізмів синхронізації даних і протоколу NFC. | розробник | 20 |
| 2. | Дослідження загроз при передачі даних за допомогою NFC. | розробник | 20 |
| 3. | Дослідження методів захисту від атак на канали NFC. | розробник | 30 |
| 4. | Розробка методу захищеної реплікації профілю користувача. | розробник | 40 |
| 5. | Створення прототипу системи реплікації профілю користувача. | розробник | 40 |
| Разом | | | 150 |

Загальні затрати часу на реалізацію даної роботи становить 150 години, найбільш трудомістким є Розробка методу захищеної реплікації профілю користувача та творення прототипу системи реплікації профілю користувача – 40 годин.

## 5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2019 рік», зокрема статтею восьмою мінімальна заробітна плата у погодинному розмірі становить 25,13 грн. Згідно з Єдиною тарифною сіткою розрядів та коефіцієнтів з оплати праці працівників та організацій окремих галузей бюджетної сфери установ розроблені рекомендовані тарифні розряди, що приблизно відповідають наступним межам погодинної оплати: керівник дипломної роботи – 30,00...50,00 грн./год., інженер-програміст першої категорії– 25,13...30,00 грн./год., консультант – 25,13...30,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (5.1)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує розробник-програміст, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 25{,}13 \cdot 150 = 3769{,}5 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 3769{,}5 \cdot 0{,}15 = 565{,}43 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.3)$$

$$В_{о.п.} = 3769{,}5 + 565{,}43 = 4334{,}93 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%;
- військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0{,}235 \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$В_{с.з.} = 4334{,}93 \cdot 0{,}235 = 1018{,}71 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці наведено у таблицю 5.2.

Таблиця 5.2 – Розрахунки витрат на оплату праці

| з/п | Категорія працівників | Основна заробітна плата, грн. | | | Додаткова заробітна плата, грн. | Відрахування $Ф_{ОП}$, грн. | Всього витрати на плату праці, грн. (6=3+4+5) |
|---|---|---|---|---|---|---|---|
| | | Тарифна ставка, грн. | Кількість відпрацьованих год. | Фактично нарах. з/пл., грн. | | | |
| А | Б | 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | розробник | 25,13 | 150 | 3769,5 | 565,43 | 1018,71 | 5353,64 |

З таблиці розрахунки витрат на оплату праці видно що всього витрати на плату праці становить 5353,64грн.

### 5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{вi} = q_i \cdot p_i \,, \tag{5.5}$$

де: $q_i$ – кількість витраченого матеріалу і–го виду; $p_i$ – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{вi} \,. \tag{5.6}$$

Розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Розрахунки матеріальних витрат

| Найменування матеріальних ресурсів | Один. виміру | Норма витрат | Ціна за один., грн. | Затрати матер., грн. | Транс-портно-заготівель-ні витрати, грн. | Загальна сума витрат на матер., грн. |
|---|---|---|---|---|---|---|
| 1. Основні матеріали | | | | | | |
| Використання мережі Internet | години | 100 | – | 100 | – | 100 |
| Ліцензія Oracle Database Standard Edition на іменного користувача | шт. | 1 | 8653 грн. | 8653 грн. | | 8653 грн. |
| 2. Допоміжні витрати | | | | | | |
| Папір формату А4 | шт. | 160 | 0,5 | 80 | – | 80 |
| Разом: | | | | | | 8833 |

Загальні матеріальні витрати на Internet і ліцензію для розробки застосунку) і папір формату А4 становить 8833 грн.

## 5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S\,, \tag{5.7}$$

де $W$ – необхідна потужність, кВт; $T$ – кількість годин на реалізацію розробки; $S$ – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 1,68грн.

Потужність комп'ютера для створення дипломної роботи – 80 Вт, кількість годин роботи обладнання згідно таблиці 5.1 –150 години.

Тоді,

$$З_в = 0{,}08 \cdot 150 \cdot 1{,}68 = 20{,}16 \text{ грн.}$$

Згідно формули затрати на електроенергію де необхідна потужність множиться на кількість годин на реалізацію розробки і множиться на вартість кіловат-години електроенергії що в висновку дорівнює 20,16 грн.

## 5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їхнього повного відновлення.

Для визначення амортизаційних використовується формула:

$$A = \frac{Б_В \cdot H_A}{100\%}, \tag{5.8}$$

де $A$ – амортизаційні відрахування за звітний період, грн.; $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $H_A$ – норма амортизації.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для даної дипломної роботи засобом розробки є телефон Samsung galaxy s10. Його вартість становить 15000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 15000 \cdot 5\% / 100\% = 750{,}00 \text{ грн.}$$

Оскільки робота виконувалась 150 години, а в місяць є 196 робочих годин, то амортизаційні відрахування будуть становити:

$$A = 1150{,}00 \cdot 150 / 196 = 573{,}94 \text{ грн.}$$

Згідно формули для визначення амортизаційних де $Б_В$ множиться $Н_А$ і ділиться на 100% амортизація розробки становить 573,94 грн.

### 5.6 Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$Н_в = В_{о.п.} \cdot 0{,}2\ldots0{,}6\ , \qquad (5.9)$$

де $Н_в$ – накладні витрати.

Отже, накладні витрати:

$$Н_в = 5353{,}64 \cdot 0{,}2 = 1070{,}73 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 1070,73 грн.

## 5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

| Зміст витрат | Сума, грн. | В % до загальної суми |
|---|---|---|
| Витрати на оплату праці $В_{о.п}$ | 4334,93 | 37,6% |
| Відрахування на соціальні заходи $В_{с.з}$ | 1018,71 | 8,8% |
| Матеріальні витрати $З_{м.в}$ | 8833 | 76,7% |
| Витрати на електроенергію $З_в$ | 20,16 | 0,2% |
| Амортизаційні відрахування $А$ | 573,94 | 5,0% |
| Накладні витрати $Н_в$ | 1070,73 | 9,3% |
| Собівартість $С_в$ | 11516,54 | 100,00% |

Собівартість ($С_в$) роботи розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \, . \quad (5.10)$$

Отже, собівартість роботи дорівнює:

$С_в$ = 4334,93+1018,71+8833+20,16+573,94+1070,73= 11516,54 грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 11516,54грн.

## 5.8 Розрахунок ціни науково-дослідної роботи

Ціну науково-дослідної роботи можна визначити можна визначити за формулою:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ) \quad (5.11)$$

де $P_{рен.}$ – рівень рентабельності, 30 %, *ПДВ* – ставка податку на додану вартість, (20 %).

Звідси ціна на роботу складе:

$$Ц = 11516{,}54 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 17965{,}8 \text{ грн.}$$

Загальний розрахунок ціни програмного продукту становить 17965,8 грн.

## 5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = \frac{П}{C_B}, \quad (5.12)$$

де *П* – прибуток; $C_B$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_в . \quad (5.13)$$

Розраховуємо плановий прибуток:

$$П_{пл} = 17965{,}8 - 11516{,}54 = 6419{,}26 \text{ грн.}$$

# 6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

## 6.1 Охорона праці

В теперішніх умовах, роботодавці мають більше можливостей для оснащення офісних приміщень за всіма необхідними вимогами. Технологічний прогрес, а також не найгірші економічні умови, дозволяють встановити в офісі сучасну комп'ютерну техніку і забезпечити працівника усіма необхідними матеріалами для зручної та продуктивної роботи.

NFC-технологія, описана в даній роботі, може використовуватися у будь-якій компанії, яка має потребу в синхронізації інформації або у корпоративній мережі, робочим місцем користувача можна вважати офіс деякої компанії малого, середнього або великого розміру. Аналіз проведено для працівників які будуть займатися підтримкою баз даних.

Приміщення розташоване на четвертому поверсі в офісній будівлі. Кожне робоче місце обладнане столом (140×75×60 см), стільцем (46×47×50 см) і ноутбуком, на деяких робочих місцях є телефони та принтери.

Під вікнами знаходяться батареї системи опалення. Підлога в приміщенні покрита комерційним лінолеумом. Стіни побілені декоративною побілкою. Стеля побілена розчином крейди.

Кабінет, що розглядається, має 9,2 $м^2$, площі на людину і 29,44 $м^3$ об'єму. Згідно ДСанПіН3.3.2.007-98 в приміщеннях, обладнаних комп'ютерами, площа на одне робоче місце має становити не менше 6,0 $м^2$, а об'єм не менше ніж 20,0 $м^3$, тобто кабінет повністю відповідає вимогам нормативного документу.

До шкідливих і небезпечних факторів, що можуть мати місце при роботі, слід розглянути мікроклімат, освітлення, шум, електробезпеку, пожежну безпеку, а також рівень електромагнітного випромінювання.

За ДБН В.2.5.-28-2006 (зі змінами 2008 та 2012 року) для роботи в приміщенні використовується суміщене освітлення. Вікна виходять на схід і

захід, розподілені по всьому боковому периметру приміщення і забезпечують природне освітлення.

Загальна площа вікон 24 м$^2$. Використовується також штучне освітлення. Використовуються світильники типів ЛВО10 з лампами Т8 потужністю 18 Вт (забезпечує світловий потік 950 лм) і ЛПО 46-20-002 з лампами ЛБ 20-2 (Т10) потужністю 20 Вт (забезпечує світловий потік 1060 лм). За ДБН В.2.5.-28-2006 світловий потік має складати від 300 до 500 лк, освітлення в приміщенні повністю відповідає вимогам нормативних документів.

Можливими джерелами шуму в даному приміщенні є кулери процесорів. клавіатури і CD-дисководи. Сумарний рівень шуму в приміщенні складає близько 46 дБА (з них 44,3 дБА – шум від кулерів процесорних блоків і 1,5 дБА – шум від клавіатур). Згідно ДСН 3.3.6.037-99 Еквівалентний рівень шуму має становити менше, ніж 50дБА, тобто рівень шуму в приміщенні нижче за допустиму норму.

Основним джерелом ЕМП в приміщенні є ноутбуки, мобільні пристрої, бездротові мережеві адаптери, що працюють у діапазоні частот близько 50Гц.

Робота в даному приміщенні з точки зору фізичного навантаження підпадає під категорію Легка 1а як така, що виконується сидячи і не вимагає фізичного навантаження. Температура повітря підтримується за допомогою кондиціонерів (PANASONIC CS/CU-E28MKD з площею покриття більше 65 м2 і потужністю у режимі охолодження: 7,65 кВт, обігріву: 9,6 кВт відповідно), системи центрального водяного опалення низького тиску і сонячного випромінювання. Використовується загально-обмінна приточно-витяжна система вентиляції з штучною вентиляцією повітря. За допомогою неї повітря в приміщенні організовано подається і видаляється, а також здійснюється його підпір або розрідження. Оскільки робоче місце в приміщенні постійне, то згідно ДСН 3.3.6.042-99 оптимальними умовами мікроклімату для цієї категорії робіт є температура від +22 до +24°С в холодний (від +23 до +25°С в теплий) період року і відносна вологість повітря 40-60%. при цьому швидкість руху повітря не має перевищувати 0,1 м/с.

## 6.2 Безпека в надзвичайних ситуаціях

### 6.2.1 Безпека приміщення

Безпека в приміщенні є важливою складовою безпеки. Для початку потрібно. Електробезпека приміщення відноситься до класу "Без підвищеної небезпеки". В приміщенні використовується трифазна електрична мережа з напругою 220 В і частотою в 50 Гц. Основними джерелами небезпеки ураження електричним струмом в даному приміщенні є дроти від ноутбуків. За умови пробою ізоляції ураження можливе; при дотику до корпусу або з'єднувальних дротів. За умови перевантаження мережі можливе іскріння і пробій ізоляції. Електробезпеку роботи з приладами згідно з Вимогами щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями , затвердженими Наказом міністерства соціальної політики України №207 від14.02.2018 забезпечують такими заходами:

- Для захисту приладів від перенавантажень та коротких замикань використовується запобіжник;
- Для забезпечення електробезпеки в аварійному режимі застосовується захисне заземлення.
- Для захисту мережі використовується мідний провід у поліхлорвініловій ізоляції

Відповідно до ПУЕ-2009 лінія електромережі для живлення ІІК виконується як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення електроприймачів. Заземлення відповідає вимогам НПАОП 40.1-1.21-99 «Правила безпечної експлуатації електроустановок споживачів». Приміщення відповідає вимогам нормативних документів з електробезпеки.

Також потрібно подбати про пожежну безпеку. У приміщенні, що аналізується, виконуються профілактичні заходи згідно з ГОСТ 12.1.004-91 «Пожежна безпека. Загальні вимоги», здійснюються протипожежні заходи, які

визначені Правилами пожежної безпеки в Україні. НПАОП 40.1-31-99 та іншими нормативними документами. Оскільки у приміщенні присутні тверді речовини, що горять, ця лабораторія за НАПБ Б.03.002-2007 відноситься до категорії «В» пожежної безпеки. Можливим джерелом пожежі є загорання ізоляції електрообладнання, яке відбувається внаслідок коротких замикань або перевантаження мережі

Приміщення обладнане сплинктерною системою пожежогасіння в офісі і газовою системою пожежогасіння, що використовує газ хладон, а також димовими пожежними оповіщувачами. Для швидкого сповіщення пожежної охорони при виникненні пожежі в приміщенні використовується електрична пожежна сигналізація автоматичної дії.

Допоміжними засобами гасіння невеликих локальних пожеж в приміщенні є вуглекислотні вогнегасники (ВВ-2), які підходять для тушіння невеликих джерел займання, а також електроустаткування під напругою до 380В. Приміщення відповідає вимогам нормативних документів НПАОП 40.1-1.31-99 і ГОСТ 12.1.004-91.

## 6.2 Розлади здоров'я користувачів, що формуються під впливом роботи за комп'ютером

Для початку варто розглянути зоровий дискомфорт так як це найбільш поширена проблема. Комп’ютерний зоровий синдром (КЗС) – комплекс порушень здоров’я, який може виникати у користувачів персональних комп’ютерів (ПК). Діагноз ставлять, якщо людина, що працює за ПК протягом двох годин, висловлює хоча б дві з десяти скарг:

- головний біль;
- сльозотеча;
- різь;
- туман;
- двоїння;
- свербіж;

- важкість в очах;
- фотофобія;
- миготіння знаків на екрані;
- нудота.

У користувачів ПК дуже поширені кон’юнктивіти і блефарити, патогенетично пов’язані з КЗС.

Синдром розвивається при умові, що робоче місце організовано неправильно – у користувача незручне крісло, відсутні пюпітри для паперів, підставки для ніг та кистей рук, не встановлена висота і нахил монітора відносно очей, відстань від очей до екрана. За таких умов тіло людини при роботі займає вимушене положення: спина статично напружена, шия витягнута, плечі жорстко фіксовані. Напружені м’язи погіршують кровотік у сонних артеріях, а недостатнє кровозабезпечення головного мозку веде до очманіння, появи головного болю. На фоні шийного остеохондрозу з’являється відчуття випирання очних яблук, туману в очах, мушок та райдужних кіл у полі зору. Розвитку КЗС сприяє поганий мікроклімат приміщення, значна загальна іонізація та мікробне забруднення, а також куріння.

Національною радою з наукових досліджень США для стану зорового дискомфорту був уведений термін "астенопія", який означає "будь-які суб'єктивні зорові симптоми чи емоційний дискомфорт, що є результатом зорової діяльності".

Симптоми астенопії були класифіковані на "очні" (біль, печія та різь в очах, почервоніння повік та очних яблук, ломота у надбрівній частині тощо) та "зорові" (пелена перед очима, мерехтіння, швидка втома під час зорової роботи та ін.).

У операторів ВДТ "очні" симптоми трапляються частіше, ніж "зорові", причому частота проявів астенопії вища у жінок, ніж у чоловіків і більше виражена в осіб середнього і старшого віку. Причиною вважається електромагнітне випромінювання від ВДТ.

При роботі з ВДТ основне навантаження припадає на всі елементи зорового аналізатора.

Робота з ВДТ може призвести до розвитку короткозорості, так як у користувачів комп'ютерів, в основному, "працює" ближній зір.

Проаналізувавши зорову роботу операторів ВДТ, М.Танахаші встановив, що через дві години експерименту частота флуктуацій акомодації зменшується, а внесок низькочастотної компоненти підвищується. Це може бути причиною скарг на втому зорового аналізатора. На думку Х. Манер, тривала робота на ВДТ може призвести до розвитку короткозорості, оскільки у користувачів ВДТ головним чином "працює" ближній зір.

За даними Д. Шіді, у 100 пацієнтів із 150, які працювали на ВДТ по шість годин на день протягом чотирьох років, були виявлені проблеми з фокусуванням зору.

Робота за комп'ютером характеризується також тим, що постійний напружений погляд на екран монітора зменшує частоту моргання. При цьому погіршується зволоження поверхні очного яблука сльозовою рідиною, яка захищає рогівку ока від висихання, пилу та інших забруднень. Це може призвести до виникнення так званого синдрому Сікка: рогівка висихає і мутніє, і як наслідок — сліпота. Також при напруженій зоровій роботі за ЕОМ можуть бути не лише порушення функції зору, а й виникнення головного болю, посилення нервово-психічного напруження, зниження працездатності.

Наступним значним розладом виступає перенапруження скелетно-мязової системи.

Діяльність користувачів комп'ютерів характеризується тривалою багатогодинною (8 год. і більше) працею в одноманітному напруженому сидячому положенні, малою руховою активністю при значних локальних динамічних навантаженнях, що припадають лише на кисті рук. Такий характер роботи може призвести до появи низки хворобливих симптомів, що об'єднані загальною назвою — синдром довготривалих статичних навантажень (СДСН) . Узагальнюючи статистичні дані можна зробити висновок про те, що СДСН

може проявлятись втомою, скутістю, болем, судомою, онімінням та ін., локалізуватись у різних частинах тіла (шия, спина, руки, ноги та ін.) і виникати індивідуально з різною частотою (ніколи, рідко, епізодично, щоденно).

Робоче положення "сидячи" забезпечується статичною працею значної кількості м'язів, що дуже втомлює. При такому положенні тіла м'язи ніг, плечей, шиї та рук довгий час перебувають у скороченому стані. Оскільки м'язи не розслабляються, в них погіршується кровообіг.

Оператори по введенню даних частіше скаржились на біль у руках, шиї та у верхній частині ніг, тоді як оператори діалогового режиму — на біль спини (частіше у поперековому відділі хребта) та плечового суглоба.

Тривала робота за комп'ютером при неправильному, з фізіологічної точки зору, положенні тіла може викликати такі вади постави, як сутулість, викривлення хребта (сколіоз) та ін.

До найбільш частих симптомів, що характерні захворювань кистей рук належить:

- больові відчуття різної сили у суглобах та м'язах кистей рук;
- оніміння та повільна рухливість пальців;
- судоми м'язів кисті;
- поява ниючого болю в ділянці зап'ястка.

Праця за клавіатурою є інтенсивною динамічною роботою кістково-м’язового апарату кистей, одночасно зі статичним напруженням м'язів передпліччя і плеча. Виконання однотипних фізично неважких рухів кистей, що здаються зовсім необтяжливими можуть призвести до поступових функціональних змін, які непомітно розвиваються протягом кількох років.

Працюючи за клавіатурою, користувачі комп'ютерів з високою швидкістю повторюють одні й ті ж висококоординовані рухи, що виконуються лише кистями. Кожний натиск на клавішу супроводжується скороченням м'язів, при цьому сухожилля ковзають вздовж кісток, внаслідок чого можуть розвинутись запальні процеси, що викликають біль.

За підрахунками дослідників при інтенсивній роботі за клавіатурою протягом робочої зміни на вказівні пальці рук припадає навантаження, яке можна порівняти з навантаженням на ноги після 40-кілометрової прогулянки.

Виникненню захворювань кістково-м'язового апарату кистей сприяє неправильне положення тіла щодо клавіатури, значне відхилення ліктів від тулуба нераціональне взаємоспрямування передпліччя та кисті.

Маніпулюючи "мишею" користувач здійснює мілкі однотипні рухи, в той час як кисть, передпліччя та плече не звикли до таких навантажень. Окрім того, часті випадки, коли поверхня для роботи з "мишею" недостатньо велика, до того ж, розташована у незручному для користувача місці. Все це зумовлює появу неприємних, а згодом і болісних відчуттів у ділянці зап'ястка, у ліктьовому та особливо плечовому суглобах.

Таким чином перенапруження скелетно-м'язової системи, в основному, спричинено:

- нераціональною позою, яка ускладнюється відсутністю урахування
- ергономічних вимог до організації робочого місця;
- однотипними циклічними навантаженнями, що викликані роботою
- за клавіатурою або пристроєм типу "миша";
- обмеженою загальною руховою активністю (гіподинамією).

Розлади центральної нервової системи (ЦНС) є одною з поширених проблем у користувачів ПК.

Виробнича діяльність операторів ВДТ має свої особливості, під впливом яких можуть формуватись розлади здоров'я. До найважливіших факторів, характерних для роботи операторів ВДТ, що впливають на погіршення стану їх ЦНС належать:

- інформаційне перевантаження мозку в поєднанні з дефіцитом часу;
- тривожне очікування інформації, особливо тієї, що викликає необхідність прийняти рішення;
- велике зорове та нервово-емоційне напруження;

- гіподинамія;
- монотонія;
- висока відповідальність за кінцевий результат;
- тривала ізоляція у спілкуванні, зумовлена індивідуальним характером праці за ВДТ.

Під впливом цих факторів виникають зміни у співвідношенні процесів збудження та гальмування в корі головного мозку. При цьому функціональна активність ЦНС знижується, а порушення рівноваги основних нервових процесів все більше спрямовано в бік гальмування. В організмі розвивається втома. В операторів ВДТ більш вираженою є психічна втома, яка виявляється наступними ознаками:

- зниженням здатності концентрувати увагу;
- зниженням сприйняття інформації;
- сповільненням мислення, яке окрім того, певною мірою втрачає гнучкість та широту;
- зниженням здатності до запам'ятовування, важче також згадувати вже відомі речі;
- змінами в емоційному стані (виникають депресії або роздратування, втрата емоційної рівноваги);
- сповільненням сенсомоторних функцій, в результаті чого час реакції оператора збільшується, а рухи стають неточними.

Необхідність обробки великого обсягу інформації в умовах дефіциту часу та високої мотивації праці, є основними причинами розвитку емоційного напруження у операторів ВДТ, що супроводжується активізацією нервової системи й появою в крові біологічно активних речовин, які змінюють діяльність органів кровообігу, дихання, травлення тощо.

Також я би ще хотів виділити ураження шкіри.

В низці наукових праць повідомляється про захворювання шкіри у користувачів комп'ютерів, які проявляються у вигляді папульозної висипки,

свербежу та лущення шкіри, еритеми, перорального та себорейного дерматитів, рожевих вугрів.

Частота шкірних уражень корелюється з низькою відносною вологістю на робочих місцях операторів та частим виникненням електростатичних зарядів. Електростатичне поле, яке генерується дисплеєм комп'ютера, посилює електростатичний заряд на тілі оператора, а відтак зростає електростатичне поле біля нього.

Це сприяє відкладанню аерозольних частинок на обличчі і може у деяких чутливих осіб викликати різноманітні шкірні реакції, залежно від природи забруднених аерозольних частинок.

Підвищення відносної вологості повітря у приміщенні в поєднанні з вилученням килимових покриттів, в яких нагромаджуються статичні заряди, сприяли зниженню шкірних висипань на обличчі. Обладнання заземлення, встановлення сіткового екрана з металевого дроту між дисплеєм і оператором у деяких випадках знижувало частоту захворювань шкіри.

# 7 ЕКОЛОГІЯ

## 7.1 Формування бази статистичних даних в екології

Основою всякої статистичної обробки і оцінки екологічної інформації є збір інформації, що здійснюється методом статистичного спостереження.

Статичне спостереження в екології - це планомірний, науково-організований збір масових даних про екологічні явища і процеси.

Об'єктом спостереження є стан забруднення навколишнього середовища (природних об'єктів) атмосферного повітря, природних водних об'єктів, земель та ґрунтів. Збір даних проводиться не стихійно, а регулярно. Основне завдання статистичного спостереження - отримання вірогідних статистичних даних, які об'єктивно характеризують явища і процеси суспільного життя. Завдання статистичного спостереження зумовлюється завданнями, які ставляться перед дослідженням певних екологічних процесів і явищ і випливають з потреб управління ними.

Програма статистичного спостереження являє собою перелік питань, на які треба одержати відповіді в процесі збирання статистичних зведень щодо кожної досліджуваної одиниці.

Відповіді на питання програми спостереження записуються у документ особливої форми - статистичний формуляр Формуляри мають різні назви: форма первинного обліку або, звітності, акт, бланк, табель, картка (фішка), анкета, опитувальний листок. В формуляр записуються дані по кожному району.

Програму і план статистичного спостереження розробляють органи державної статистики на рівні Міністерства Державного комітету статистики України.

У плані вказують строк проведення спостереження, У плані має бути точно визначена територія, на якій здійснюється спостереження, а також особи і організації, відповідальні за проведення підготовчих робіт.

У статистичний практиці застосовують дві організаційні форми спостереження: звітність і спеціально організовані статистичні спостереження.

Звітність — це форма статистичного спостереження, при якій статистичні дані надходять у статистичні органи у вигляді обов'язкових і таких, що мають юридичну силу звітів про роботу.

За різними ознаками статистичну звітність поділяють на окремі види. Насамперед розрізняють типову і спеціалізовану звітність:

За періодичністю подання звітність буває тижнева, двотижнева, місячна, квартальна, різна; за способом подання - термінова (телеграфна) і поштова. Вид звітності впливає на техніку збору і зведення статистичної інформації.

За порядком проходження звітність поділяють на централізовану і децентралізовану:

Другою за значенням організаційною формою спостереження є спеціально організоване статистичне спостереження. Застосовують його у випадках, коли не можна застосувати звітність або складати звітність нераціонально.

Спеціально організоване статистичне спостереження поєднує в собі такі організаційні форми: а) перепис, б) суцільне і несуцільне обстеження.

Різновид спостереження визначається ознакою групування: охватом одиниць сукупності (суцільне і несуцільне), часом проведення, способом одержання статистичних даних.

При суцільному спостереженні обстеженню і реєстрації підлягають усі без винятку елементи сукупності; при несуцільному спостереженні обліку підлягають не всі елементи сукупності.

Несуцільні спостереження поділяють на такі види: спостереження основного масиву, вибіркове, монографічне і анкетне:

- спостереження основного масиву охоплює переважну частину елементів сукупності, обсяг значень істотної ознаки у яких визначає розмір явища.

- при вибірковому спостереженні також обстежуються не всі елементи сукупності, а певна, випадково відібрана їх частина.

- монографічне спостереження передбачає детальне обстеження лише окремих типових елементів сукупності.

За часом проведення статистичне спостереження поділяють на поточне, періодичне і одноразове.

За способом одержання статистичних даних виділяють: безпосередній облік фактів, документальний облік і опитування респондентів:

- безпосередній облік фактів передбачає безпосередній огляд, перелік, вимірювання, зважування тощо.

- документальний облік ґрунтується на даних різноманітних документів первинного обліку

- опитування респондентів - це таке спостереження, при якому відповіді на питання формуляра записують зі слів респондента.

Різноманітність екологічних явищ потребують поєднання зазначених способів і видів спостереження.

Точність і вірогідність статистичних даних є найважливішою вимогою статистики.

Помилки спостереження - це розбіжність між даними спостереження і дійсним значенням показників. Розрізняють помилки реєстрації і репрезентативності:

Помилками реєстрації називають ті, які виникли внаслідок неправильного встановлення фактів або неправильного їх запису. Вони допускаються випадково - внаслідок дії випадкових причин і спричиняють спотворення даних в той чи інший бік, або систематично, що призводять до значних зміщень загальних підсумків статистичного спостереження. Службові особи, винні у несвоєчасному поданні або перекручені даних державних статистичних спостережень, притягаються до дисциплінарної, матеріальної або кримінальної відповідальності.

Помилки репрезентативності виникають лише в несуцільному спостереженні тому, що відібрана і обстежена частина сукупності не повністю відтворює склад сукупності в цілому.

## 7.2 Джерела шуму і вібрацій та методи їх знешкодження

Шум в навколишньому середовищі – у домашніх чи громадських місцях, на прилеглих до них територіях створюється одиничними чи комплексними джерелами, які знаходяться з зовнішньої чи внутрішньої сторони будівлі. Це насамперед транспортні засоби, технічне обладнання промислових і побутових підприємств, вентиляційні, компресорні установки, різні аерогазодинамічні установки, санітарно - технічне обладнання житлових будівель, електричні трансформатори. Без прийняття відповідних мір по зниженню шуму його рівні можуть значно перевищувати ( на 20-50дБ) допустимі величини. За останні десятиліття спостерігається збільшення шуму в великих містах. Розрахунки показують, що в найближчі 20-30 років рівень шуму на швидкісних магістралях зросте на 7-10 дБ. Високі рівні шуму є в житлових будинках, школах, лікарнях, місцях відпочинку людей і т.д., що призводить до підвищення нервового напруження.

Шуми по характеру спектра поділяється на: широкополосні – мають неперервний спектр шириною більше однієї октави. Наприклад шум в жилій настройці, який виникає при дослідженні турбоактивного двигуна. І тональні, в спектрі яких є чутні дискретні тони, перевищення рівня в одній полосі складає не менше, чим 10 дБ. Наприклад шум осьового вентилятора.

По часовим характеристикам шуми поділяються на постійні, рівень звуку яких міняється а часі не більш чим на 5 дБа, і непостійні, для яких це значення перевищує 5 дБА. Найчастіше шум супроводжується вібрацією.

Технологічне обладнання ударної дії (молоти, преси), потужні енергетичні установки (насоси, компресори, двигуни), рельсовий транспорт підприємств (метрополітен, трамвай), а також залізно дорожній транспорт

відносяться до джерел вібрації, у всіх випадках вібрація розповсюджується по ґрунті і досягає фундаментів громадських і житлових будівель, часто викликаючи звукові коливання. Передача вібрації через фундаменти і ґрунт може спровокувати їх нерівномірну осадку, яка призведе до руйнування розташованих на ній інженерних і будівельних конструкцій. Джерелами вібрацій може бути інженерне обладнання будівель ( ліфти, насосні установки), системи опалення, каналізації, мусопроводів. У всіх випадках вібрація визиває подразнюючу дію, або перешкоду для трудового процесу в громадських будівлях.

Значного ефекту боротьби з комунікаційними шумом і вібрацією можна досягти завдяки обмеженню руху транспорту, своєчасному ремонту поверхні доріг і залізничної колії, модернізації конструкцій потягів, легкових, вантажних автомобілів, автобусів і трамваїв, впровадженню в експлуатацію малошумового обладнання, комунікаційних ліній, створенню захисних бар'єрів, екранів (лісосмуг), використанню природних акустичних бар'єрів, протишумових конструкцій і матеріалів, поліпшенню акустичного фону міст за рахунок об'їзних доріг, своєчасного ремонту і реконструкції автострад, автодоріг.

Захисту людей від шумів і вібрацій у промисловості сприяє використання на підприємствах спеціальних засобів (навушників, прокладок, шоломів), впровадження мало шумових технологій, машин, верстатів, механізмів, автоматів і роботоверстатів у шумовому виробництві, використання у будівництві і реконструкції антивібраційних і протишумових фундаментів, дверей, вікон, звукозахисних екранів, шумопоглинаючих плит, базальтової вати, поліетиленової плівки, ізоляційної піни, поліпшення умов праці (скорочення робочого часу, нормування шуму і вібрації на робочих місцях, в місцях проживання і відпочинку, впровадження системи атестації на шум і вібрацію технологій, обладнання та машин).

# ВИСНОВКИ

Аналіз рівнів реплікації на основі хосту, мережі та контролеру системи зберігання даних показав, що реплікація на основі контролеру системи є одною з найгнучкіших для проведення синхронізації, перевагами якої є: простота використання для одного сховища в простих системах; об'єднання всіх переваг систем реплікації на рівні мережі для просунутих рішень; відсутність необхідності у використанні додаткового обладнання; простота управління однією системою.

Аналіз загроз, що виникають при передачі даних за технологією NFC показав, під час реплікації даних цією технологією можуть бути загрози пов’язані з пасивним прослуховуванням каналів, пошкодженням переданих даних, модифікацією даних, вставки даних та атак типу Relay, проте можна стверджувати, що атака типу «людина посередині» для протоколу NFC є загроз, що виникають при передачі даних за технологією NFC практично нездійсненою.

На основі аналізу загроз, що виникають при передачі даних за технологією NFC, запропоновані методи і шляхи їх усунення, де новим основним шляхом їх подолання є використання засобів рівня додатків, завдяки яким можна домогтися переваг, які не існують на канальному рівні.

З урахуванням виявлених слабких і сильних сторін існуючих каналів, проведеного аналізу загроз та методів їх подолання, був запропонований новий метод реплікації, заснований на використанні технології NFC в якості каналу установки сеансового ключа на основі чого запропоновано використовувати канал NFC для реалізації тимчасової реплікації профілю користувача.

В спеціальній частині приведено опис застосунку «SyncManager».

В розділі "Обґрунтування економічної ефективності" було розраховано економічну доцільність даного дослідження.

У підрозділі "Охорона праці" розглянуто вимоги щодо охорони праці в приміщеннях та їх оснащення. У підрозділі "Безпека життєдіяльності" описано безпеку приміщень та розлади здоров'я користувачів, що формуються під впливом роботи за комп'ютером.

В розділі "Екологія" описано формування бази статистичних даних в екології. Також розглянуто джерела шуму і вібрацій та методи їх знешкодження.

# БІБЛІОГРАФІЯ

1. J.Padgette, K. Scarfone, L.Chen. Guide To Bluetooth Security. 2012. URL: http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121_Rev1.pdf/.

2. R.Kilani, K.Jensen. Mobile Authentication with NFC enabled Smartphones. 2012. URL: http://ojs.statsbiblioteket.dk/index.php/ece/article/download/21229/18718.

3. Information technology - Telecommunications and information exchange; between systems — Near Field Communication — Interface and Protocol (NFCIP-1). 2004. URL: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnu m ber=56692.

4. Near Field Communication - Interface and Protocol (NFCIP-1). 2013. URL: http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf.

5. E.Haselsteiner, K.Breitfuß.Security in Near Field Communication (NFC). URL: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-20Security%20in%20NFC.pdf.

6. Relay Attacks in EMV Contactless Cards with Android OTS Devices. URL: https://conference.hitb.org/hitbsecconf2015ams/wp-content/uploads/2014/12/D1T1- R.-Rodriguez-P.-Vila-Relay-Attacks-in-EMV-Contactless-Cards-with-Android- OTS-Devices.pdf.

7. Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema. 2013. URL: http://resources.infosecinstitute.com/near-field- communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

8. Gerhard P. Hancke, Markus G. Kuhn. An RFID Distance Bounding Protocol. 2005. URL: https://www.cl.cam.ac.uk/~mgk25/sc2005-distance.pdf /

9. W. Diffie, M.E. Hellman. New directions in cryptography.1976. URL: https://www- ee.stanford.edu/~hellman/publications/24.pdf/

10. Host Card Emulation. URL: https://developer.android.com/guide/topics/connectivity/nfc/hce.html/

11. Profile Folder. URL: http://kb.mozillazine.org/Profile_folder_-_Firefox

12. Android Security Tips. URL: https://developer.android.com/training/articles/security-tips.html/

13. Біячуев Т.А. Безпека корпоративних мереж. Навчальний посібник / під ред. Л.Г.Осовецкого - СПб .: СПбГУ ИТМО, 2004. - 161 с. ;

14. Лапонін О.Р. Криптографічні основи безпеки. - М .: "Інтернет-університет інформаційних технологій - ІНТУІТ.ру", 2009. - 389 с .: іл. ;

15. Блек У. Інтернет: протоколи безпеки. Навчальний курс. - СПб .: Пітер, 2001. - 288 с .: іл. ;

16. Лапонін О.Р. Криптографічні основи безпеки. - М .: "Інтернет-університет інформаційних технологій - ІНТУІТ.ру", 2004. - 320 с .

17. Вихорев С. В., Кобцев Р. Ю. Як дізнатися - звідки напасти або звідки виходить загроза безпеці інформації // Захист інформації. Конфідент, № 2, 2002. ;

18. Обчислювальні системи, мережі та телекомунікації: Підручник. - 2-е вид., - М .: Фінанси і статистика, 2003. ;

19. Галатенко В.А. Стандарти інформаційної безпеки. - М .:"Інтернет-університет інформаційних технологій - ІНТУІТ.ру", 2004. - 328 с.: іл.;

20. Wireless LANs - - Security measures. I. Mouchtaris, Petros. II. Title TK5105. 59. A54 2007 005.8- -dc22;

21. Рошан Педжман, Ліері Джонатан. Основи постороения бездротових локальних мереж стандарту 802.11. : Пер. з англ. - М .: Видавничий дім «Вільямс», 2004. -304 с.;

22. Максим М. Безпека бездротових мереж / Меріт Максим, Девід Поліно; Пер. з англ. Семенова О.В. - М .: Компанія АйТі; ДМК Пресс, 2004.-288с.;

23. Goodman M. International Dimensions of Cybercrime // S. Ghosh and E. Turrini (eds.), Cybercrimes: A Multidisciplinary Analysis. Berlin, Heidelberg, 2010.

24. Осипенко А.Л. Сетевая компьютерная преступность. Омск, 2009. The Economic impact of cybercrime and cyberspionage. Center for Strategic and International Studies July 2013 Report.

25. Малюк А.А. "Информационная безопасность. Концептуальные и методологические основы защиты информации"/ Малюк А.А. –М.: Гарячая линия- Телеком, 2004. -280с.

26. Хорошко В.А.Методы и средства защиты информации/ Хорошко В.А., Чекатков А.А. - К.: Юниор, 2003. - 504с.

27. Ленков С.В. Методы и средства защиты информации. В 2-х томах, Том 2. Информационная безопасность / Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. – К.: Арий, 2008. – 344 с.

28. Двухфакторна аутентифікація google. [Електрон. ресурс].- http://www.google.com/intl/ru/landing/2step/

29. Управління інформаційною безпекою сучасних ІКСМ на базі стандартів ISO. [Електрон. ресурс].- http://www.rusnauka.com/22_PNR_2010/Informatica/70334.doc.htm

30. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты"/ Домарев В.В. – К.: ООО "ТИД "ДС", 2002 – 688 с.

31. За подвійною бронею [Електрон. ресурс]. – https://xakep.ru/2013/02/18/60139/

32. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98

33. Грибан В. Г., Негодченко О. В. Охорона праці : навчальний посібник . -2-е видання. Київ: Центр учбової літератури, 2018.- 280 с, ISBN 978-966-364-832-3

34. Запорожець О. І., Протоєрейський О. С., Франчук Г. М., Боровик І. М. Основи охорони праці підручник Київ: Центр учбової літератури, 2017. - с.264, ISBN 978-617-673-423-9

35. М. С. Одарченко, А. М. Одарченко, В. І. Степанов, Я. М. Черненко. Основи охорони праці: підручник/ – Х. : Стиль-Издат, 2017. – 334 с. ISBN 966-7885-84-4

36. Охрана окружающей среды: учеб. для техн. спец. вузов./ С.В. Белов, Ф.А. Барбинов, А.Ф. Козьяков и др. ; под ред. С.В.Белова М.: Высшая школа, 1991.- 319с. ISBN 5-06-000665-1.

37. Васійчук В.О., Гончарук В.Є., Качан С.І., Мохняк С.М.Основи цивільного захисту: Навч. посібник / В.О. Васійчук, В.Є Гончарук, С.І.Качан, С.М. Мохняк.-Львів:Видавництво Національного університету "Львівська політехніка", 2010.-417с

38. Білявський Г. О. Основи екології: підручник для студ. вищих навч. закладів / Г. О. Білявський, Р. С. Фурдуй, І. Ю. Костіков. К. : Либідь, 2004. - 408 с. ISBN 966-06-0289-8.

39. Запольський А.К. Основи екології: підр. для студ. техн. технол. спец. вищ. навч. закл. / А. К. Запольський, А.І. Салюк; за ред. К.М. Ситника. К.: Вища школа, 2001.- 358с. ISBN 966-642-059-7.

40. Тарасова В.В. Екологічна статистика // Київ: «Центр учбово\ї літератури», 2008 ро.-391с.

41. Бедрій Я. І.; Джигирей В. С.; Кидисюк, А. І. та ін. Основи екології та охорона навколишнього природного середовища: навч. посіб. для студ. вищих навч. закладів // за ред. В. С. Джигирей ; Український держ. лісотехнічний ун-т, Львівський електротехнікум зв'язку. - Л. : [б.в.], 1999. - 239 с. Альтернативна назва : Екологія та охорона природи. - ISBN 5-7763-2641-9.

# ДОДАТКИ