УДК 658.5.012.7
DOI 10.31673/2412-9070.2018.042529

В. М. ЧОРНА, аспірантка;
О. М. ТКАЛЕНКО, канд. техн. наук, доцент;
О. В. ПОЛОНЕВИЧ, канд. техн. наук;
О. В. СЕНЬКОВ,
Державний університет телекомунікацій, Київ

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В NFC

Нині спостерігається стрімке впровадження безпроводових технологій у різні галузі суспільного життя. Вони замінюють проводові технології і роблять комунікацію між пристроями набагато зручнішою і простішою для користувача, чому сприяють і відповідні стандарти. Наприклад, стандарт NFC (Near Filed Communication) розвивається разом із такими технологіями, як Wi-Fi, Wi-MAX. У свою чергу, технологію на базі NFC призначено для передавання інформації на невеликі відстані за допомогою мобільних пристроїв. Ця технологія — логічне продовження технологій RFID (Radio Frequency Identification — радіочастотна ідентифікація). NFC підтримує RFID стандарти ISO 14443/mifare, Feli Ca, а також ISO/IEC 18092. Згадані пристрої здатні працювати як в активному, так і в пасивному режимі. Пасивний режим функціонує за тими самими принципами, що й безконтактна картка RFID. Такий режим забезпечує високу автономність портативного пристрою і дозволяє використовувати NFC технологію навіть при вимкненому живленні. NFC можна застосовувати в усіх тих випадках, коли долучаються безконтактні картки, а сумісність із картковими стандартами дає змогу спиратись на існуючу інфраструктуру. Скажімо, мобільна купівля квитків у громадському транспорті — істотне розширення наявної безконтактної інфраструктури; здійснення мобільних платежів — пристрій функціонує як платіжна картка; електронна дошка — мобільний телефон використовується для зчитування RFID міток із вуличних щитів для оголошень, щоб на ходу отримувати інформацію. Незабаром будуть можливі й інші застосування NFC: посвідчення особи; мапи мандрівника; мобільна торгівля; електронні гроші; електронна купівля квитків (авіаквитки, квитки на концерт і т. ін.); електронні ключі — ключі від машини, ключі від дому/офісу, ключі від готельного номера тощо. Існують варіанти криптографії, використовувані в мітках.

Сфери застосування міток розглянуто на конкретних прикладах. З'ясовано, зокрема, як використовується брелок із NFC міткою «Prestigio PKR1». Досліджено проблему захисту інформації та наведено способи її розв'язання. Запропоновано розширити сфери застосування технології NFC упровадженням її в різні телекомунікаційні системи.

Ключові слова: технологія NFC; мітка NFC; технологія RFID; QR код; модуляція; протокол; інтерфейс; криптографія; мобільний пристрій NFC; технологія Wi-Fi.

Вступ

Якщо технологія NFC прийде на заміну здійсненню платежів за допомогою кредитних карток або використовуватиметься для доступу до критично важливих об'єктів, то дані, які передаються, мають бути в якомога більшій безпеці. Один із рівнів безпеки є невід'ємною частиною NFC, оскільки обмін даними відбувається на дуже малій відстані. Але це не означає, що NFC система зовсім позбавлена чутливості до негативних зовнішніх впливів.

Наприклад, не виключається злам NFC системи. Адже за допомогою напрямленої антени з великим коефіцієнтом підсилення, а також високочутливого приймача можна прослухати сигнал NFC на чималій відстані. Утім настільки громіздкий пристрій для зламування навряд вдасться застосувати непомітно.

Загрози безпеці виникають і з інших причин. Наприклад, пошкодити дані неважко, якщо NFC зчитувачу або аналогічному пристрою передати завідомо помилкові дані. Змінювати дані можна й у процесі передавання. Під час такої атаки хакери отримують доступ до даних, що передаються, і змінюють їх перед пересиланням. Такий вид хакерської атаки малоймовірний, але можливий. Найкращим способом захисту даних у таких випадках є їх шифрування. Майже в усіх приймачах NFC для захисту радіоканалу використовується шифрування.

Основна частина

Проблема захисту інформації в NFC полягає в тому, що ця технологія не має власних механізмів безпеки.

Уразливість мобільних пристроїв на базі NFC ілюструють рис. 1–3.

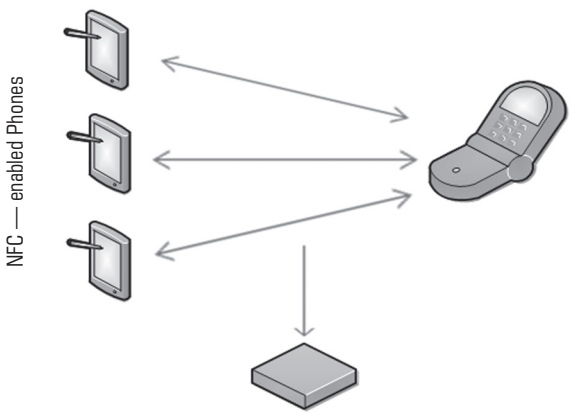

Рис. 1. Схема зламу даних у процесі роботи з NFC

Створення механізмів безпеки повністю покладено на розробників і виробників електронних пристроїв. Якщо смартфон не захищено паролем,

то зловмисник, отримавши до нього доступ, може здійснювати будь-які покупки. Адже використання NFC не вимагає вводу ПІН-коду при оплаті. Саме через це не має сенсу масово застосовувати смартфони з NFC для заміни кредитних карток. Залишаються актуальними проблеми з безпекою трансакцій. Достатньо пройтися в магазині чи ресторані зі зчитувачем у кишені, щоб отримати доступ до інформації та рахунків (див. рис. 1).

А якщо апарат вкрадено або ж загублено, доведеться по черзі блокувати SIM-картку в оператора та платіжну функціональність у банку.

Зауважимо, що на конференції EuSecWest із питань безпеки було презентовано експлойт 0day*, який переконливо довів уразливість технології NFC у мобільних пристроях, про яку вже йшлося. Спеціалістам із безпеки вдалося передати через NFC з'єднання шкідливий файл та отримати повний контроль над приймальним пристроєм. У такий спосіб конфіденційні дані та грошові кошти «жертви» опинилися під загрозою, хоча радіус зв'язку на базі NFC обмежено кількома сантиметрами, ця технологія не гарантує безпеки з'єднання.

Для згаданого нападу зловмисник повинен відправити жертві запит зчитувача та її відповідь, а далі в режимі реального часу передати дані на зчитувальний пристрій. Це робиться для того, аби виконати завдання щодо симуляції володіння смарткарткою жертви.

Проте на практиці така атака надто складна внаслідок жорстких обмежень у часі на відповідь запитуваного пристрою. У деяких випадках, наприклад при виконані обов'язкової процедури антиколізії, може йтися про мікросекундні допуски. Окрім того, через малі відстані взаємодії атаки з використанням ретрансляторів також дуже проблематичні (див. рис. 2).

перебувати під контролем різних осіб при використанні TSM, що його контролює власник SE.

Захищений модуль може зберігати як дані, так і додатки, котрі потребують захисту. Управління даними в захищеному модулі здійснюється через різноманітні канали зв'язку.

Контроль стосовно SE є однією з вагомих причин затримки розвитку технології, оскільки існує кілька базових моделей відповідного контролю. Стільникові оператори вважають, що контроль мають здійснювати тільки вони, і одностайно голосують за єдиний можливий SE, розташований на SIM-картці абонента. Банки, а також усі інші причетні до цих процесів особи не згодні з операторами, обстоюючи свої моделі.

Варто наголосити, що при використанні RFID і NFC актуалізується проблема захисту персональних даних. Справді, технології RFID і NFC мають низку уразливостей, які за відсутності необхідних заходів безпеки полегшують шахраям крадіжку цінної інформації.

Відразу після появи на ринку NFC і RFID в їхній роботі було виявлено неочікувані прорахунки. Зрештою існують певні побоювання стосовно можливостей зчитування та копіювання інформації з таких карток хакерами (див. рис. 3).

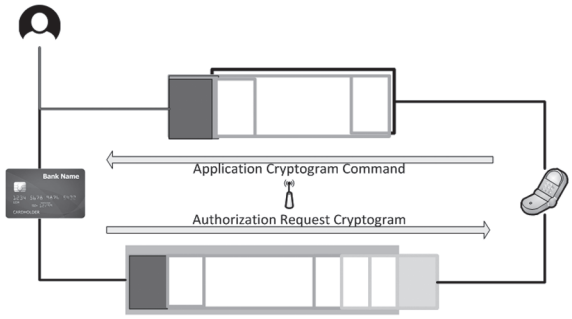

Рис. 3. Процес зчитування інформацій хакерами під час розрахунку за платіж згідно з технологією NFC

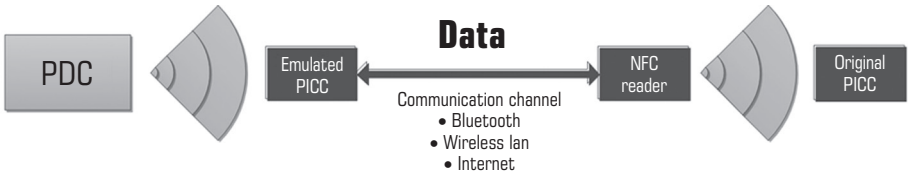

Рис. 2. Схема атаки з використанням ретрансляції (Relayattack)

Якщо технологія NFC прийде на зміну здійсненню платежів за допомогою кредитних карток або слугуватиме для доступу до критично важливих об'єктів, то дані, які передаються, мають бути надійно захищені.

Для захисту інформації застосовується так званий ***захищений модуль*** (*Secure Element* — SE). Ідеться про спеціальну область пам'яті в чіпі, доступ до якої надається тільки виробникам даного чіпа. Згадана область пам'яті може бути розбита на додаткові області (Secure Domain), які можуть

Електронні крадіжки (e-pickpocketing) — це новий термін, що означає вилучення інформації з картки без жодного контакту з нею. А оскільки в основу технології RFID покладено безконтактний зв'язок, сигнали можна зчитувати, перебуваючи навіть поза зоною видимості. Інформацію за допомогою портативного зчитувача може зняти людина, віддалена на кілька метрів від носія інформації. А оскільки інформація зчитується за допомогою електронного сканування (у безконтактному режимі), то рідер сприймає скопійовану картку як оригінал.

Безконтактні RFID-рідери, здатні зчитувати інформацію з кредитної картки на відстані трьох дюймів, можна легко придбати на сайті eBay приблизно за 50 дол. США, а рідери далекого радіуса дії всього лише вдвічі дорожчі.

Інформація, знята з чіпа RFID, може використовуватися для викрадання персональних даних або для здійснення покупок. Це може становити ризик для корпоративної безпеки, а також для недоторканності житла.

З огляду на серйозність проблеми електронних крадіжок пропонуються нові технології забезпечення безпеки RFID-карток. Розглянемо деякі з цих інноваційних методів.

Якщо перевага надається виготовленню обладнання в домашніх умовах (за принципом «зроби сам»), можемо використовувати два матеріали, які заважають проходженню радіосигналів — воду і метал. Теоретично вода має ефективно блокувати радіосигнали, але таке вирішення досить складно втілити в життя. Метал набагато практичніший, тим більш, що такий матеріал, як алюмінієва фольга, можна легко придбати за прийнятною ціною. При цьому аркуша алюмінієвої фольги завтовшки 27 мкм достатньо для блокування сигналів RFID і NFC.

Щоб захистити картку від зчитування, достатньо загорнути її в алюмінієву фольгу, а розгорнути тільки перед використанням. Метод справді ефективний.

Щоб запобігти копіюванню міток RFID і NFC, можна використовувати криптографію. Одноразовий код, який безперервно змінюється після кожного сканування, можна використовувати заради того, аби завадити перехоплювачам фіксувати операції для подальшого відтворення. Навіть якщо шахраям вдасться вкрасти одноразовий код, вони не зможуть ним скористатися.

Для складніших пристроїв можлива автентифікація методом «запит–відповідь» у тих випадках, коли мітка взаємодіє з рідером. У разі такого типу автентифікації рідер видає мітці запит, а мітка, у свою чергу, відповідає секретним цифровим кодом, побудованим на базі симетричної або двоключової криптографії.

Кредитна карта на основі RFID і NFC блокується, якщо вона залишається в кишені або лежить на якійсь поверхні (рис. 4). Тоді шахраї не можуть зчитати її за допомогою портативних сканерів. Це вельми просте й недороге вирішення, яке можна використовувати в процесі виготовлення кредитних карток на згаданій основі.

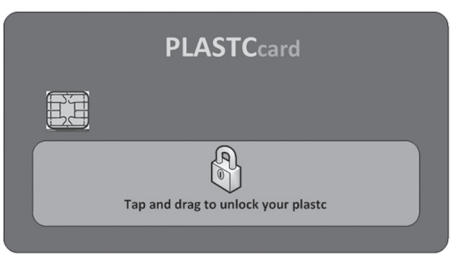

Рис. 4. Універсальна пластикова картка, яка змінює код і блокується, перебуваючи на поверхні або в гаманці

Чинником безпеки використання NFC технології виступає дистанція: ця технологія працює тільки на дуже малих (кілька сантиметрів) відстанях. Отже, помилкове підімкнення практично неможливе. Щоб перехопити NFC сигнал, зловмисникові необхідно бути дуже близько. Окрім того, потрібно підтвердити з'єднання перед передаванням або отриманням даних. Ще один чинник безпеки — шифрування: у телефоні використовуються найсучасніші функції захисту, шифрування та автентифікації для захисту особистої інформації. І, зрештою, управління як гарантія безпеки: функцію NFC можна відімкнути, коли вона не використовується. Але навіть якщо функцію NFC увімкнено, вона автоматично відмикається при блокуванні дисплея телефону.

Розроблено додаток близької взаємодії, поданий мовою C#, що використовує криптографічні засоби з простору імен System. Security. Cryptography. У процесі розробки, налагодження й тестування було задіяно емулятори смартфона на платформі Windows та емулятор NFC (рис. 5).

Як емулятор NFC використовувався екземпляр драйвера близької взаємодії з комплекту драйверів для Windows (WDK). Після установлення комплекту WDK і екземплярів драйвера приклад драйвера близької взаємодії міститиметься в каталозі src\nfp у складі WDK.

Після запуску симулятор виконується у фоновому режимі, тоді як додаток близької взаємодії подається першим планом.

Розроблений додаток є одноранговим, підімкнення відбувається через сокет.

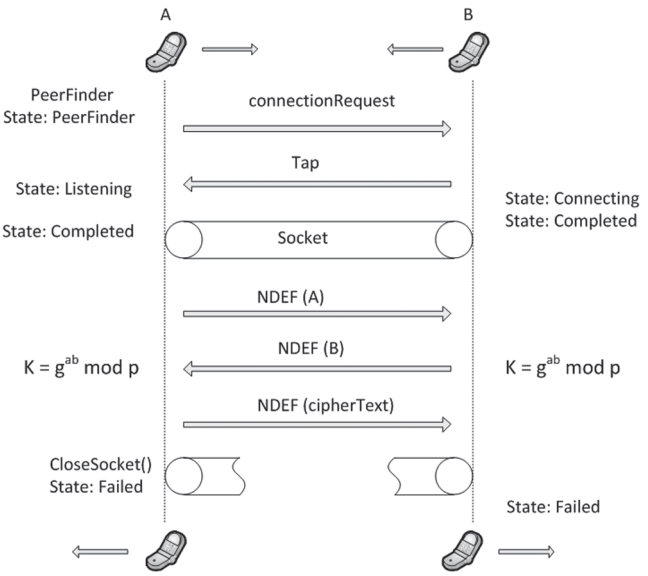

Рис. 5. Схема роботи програми з побудови додатка близької взаємодії

Після установлення загального секрету та формування ключа користувачі обмінюються повідомленнями.

Висновки

Роботу програми подамо як послідовність таких дій.

1. Зближення даних пристроїв.

2. Пошук пристрою класу Peer Finder. Якщо знайдено інший пристрій, то статус змінюється на Peer Found.

3. Знайденому пристрою відправляється connection Request — користувач іншого пристрою отримує запит стосовно згоди на з'єднання.

4. Статус пристрою A змінюється на Listening.

5. Змінюється і статус пристрою B. Статус Connecting означає, що пристрій зазнав дотику і очікується закінчення установлення з'єднання.

6. Після того як з'єднання було встановлено, статус обох пристроїв змінюється на Completed.

7. Створюється сокет за допомогою об'єкта Stream Socket. Із цього моменту жодний пристрій не може знайти справжній пристрій за допомогою Peer Finder, щоб розірвати встановлене з'єднання.

8. На кожному пристрої генеруються вихідні дані для обміну ключами згідно з Діффі–Хелльманом за допомогою класу EC Diffie Hellman Key Derivation Function.

9. Обмін згенерованими даними. Дані упаковуються в NDEF повідомлення.

10. Обчислення загального ключа: byte [] z = = Cng Key. Import (bob Public Key, Cng Key Blob Format. Ecc Public Blob).

11. Генерування ключа для алгоритму шифрування: byte [] key = alice. Derive Key Material (z).

12. Шифрування повідомлення через Crypto Stream.

13. Передавання NDEF повідомлення із зашифрованими даними.

Далі можливі два варіанти розриву з'єднання: викликається метод Close Socket, який закриває створений сокет, а після виклику змінна зберігає симетричний ключ шифрування. Для нового обміну даними необхідно заново створити сокет і згенерувати новий ключ. Пристрої віддаляються один від одного. Тоді їхні статуси набувають значення Failed. Сокетні з'єднання розриваються, і змінна, що зберігає симетричний ключ шифрування, очищується. Для нового обміну даними необхідно знову зблизити пристрої і почати виконання програми з методу Peer Finder.

Незабаром практичне застосування NFC може проникнути в усі сфери нашого життя, навіть зовсім несподівані, і це прискорить відшукання способів усунення недоліків, які існують досі.

Список використаної літератури

1. ***Билайн.*** *Бесконтактные платежи: прилажи телефон к турникету — и ты в метро! URL: http://habrahabr.ru/company/beeline/blog/128564/.*

2. ***i-Free.*** *СКУД - NFC и контроль доступа. URL: http://nfc-services.ru/products/skud.*

3. ***Tesa.*** *Технология NFC в электронных замках TESA. URL: http://www.tesa.ru/news/132.*

4. ***Голышко А.*** *Мобильная лавка // Мобильные телекоммуникации. 2011. С. 26–31.*

5. ***Олифер В. Г., Олифер Н. А.*** *Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2006.*

6. ***Потресов С.*** *Билайн: мобильный проездной. URL: http://www.mobile-review.com/articles/2012/bee-nfc-metro.shtml.*

7. ***A Sophisticated*** *RFID Application on Multi-Factor Authentication / J. C. Liou a. o. // Information Technology: New Generations (ITNG), 2011 Eighth International Conference on. IEEE, 2011. С. 180–185.*

8. ***Haselsteiner E., Breitfuss K.*** *Security in near field communication (NFC) // Workshop on RFID Security RFIDSec. 2006.*

9. http://nfcukraine.com/

10. http://www.i-free.com/

Рецензент: канд. техн. наук, доцент **К. П. Сторчак**, Державний університет телекомунікацій, Київ.

В. Н. Чорна, О. Н. Ткаленко, О. В. Полоневич, О. В. Сеньков

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В NFC

В настоящее время наблюдается стремительное внедрение беспроводных технологий в различные сферы жизни общества. Они заменяют проводные технологии и делают коммуникацию между устройствами более удобной и простой для пользователя, чему способствуют и соответствующие стандарты. Например, стандарт NFC (Near Filed Communication) развивается вместе с такими технологиями, как Wi-Fi, Wi-MAX. Технология NFC предназначена для передачи информации на небольшие расстояния, используется преимущественно в мобильных устройствах. Она является логическим продолжением технологий RFID (Radio Frequency Identification — радиочастотная идентификация). NFC поддерживает RFID стандарты ISO 14443 / mifare, Feli Ca, а также ISO / IEC 18092. Устройства могут функционировать как в активном, так и в пассивном режиме. Пассивный режим функционирует по тем же принципам, что и бесконтактная карточка RFID. Такой режим увеличивает автономность портативного устройства, благодаря чему NFC технология работает даже при выключенном питании. NFC приемлема во всех тех случаях, когда применяются бесконтактные карточки, а совместимость с карточными стандартами позволяет использовать существующую инфраструктуру. Например, мобильная покупка билетов в общественном транспорте — расширение существующей бесконтактной инфраструктуры;

мобильные платежи — устройство действует как платежная карточка; электронная доска — мобильный телефон используется для чтения RFID меток с уличных досок для объявлений, чтобы на ходу получать информацию. Возможны и другие приложения NFC в недалеком будущем: удостоверение личности; карты путешественника; мобильная торговля; электронные деньги; электронная покупка билетов (авиабилеты, билеты на концерт и др.); электронные ключи — ключи от машины, ключи от дома/офиса, ключи от гостиничного номера и т. д. Существуют варианты криптографии, используемые в метках. Области применения меток рассмотрены на конкретных примерах. В частности, показано использование брелка с NFC меткой «Prestigio PKR1». Изучена проблема защиты информации и предложены способы ее решения. Предложено расширить сферы применения технологии NFC внедрением ее в различные телекоммуникационные системы.

Ключевые слова: технология NFC; метка NFC; технология RFID; QR код; модуляция; протокол; интерфейс; криптография; мобильное устройство NFC; технология Wi-Fi.

V. M. Chorna, O. M. Tkalenko, O. V. Polonevich, O. V. Senkov

FEATURES OF INFORMATION PROTECTION IN NFC

At present, the implementation of wireless technologies in various applications is being observed. They replace advanced technologies and make communication between devices more convenient and easy for the user. Near Filed Communication (NFC) is evolving with technologies such as Wi-Fi, Wi-MAX. This technology is designed to transmit information over short distances. NFC technology is used on mobile devices. It is a logical continuation of RFID technologies (Radio Frequency Identification). NFC supports RFID standards ISO 14443 / mifare, Feli Ca as well as ISO / IEC 18092. Devices can operate in both active and passive modes. The passive mode operates according to the same principles as the non-contact RFID card. This mode increases the autonomy of the portable device and allows you to use the NFC technology even when the power is off. NFC can be used in all cases where contactless cards are used, and card standard compliance allows the use of existing infrastructure. For example, mobile purchase of tickets in public transport is an extension of the existing non-contact infrastructure; mobile payments — the device acts as a payment card; Electronic Board — A mobile phone is used to read RFID tags, from outdoor bulletin boards to get information on the go. Also, other NFC applications in the future may include: Identity; traveler's card; mobile trade; electronic money; electronic purchase of tickets (air tickets, concert tickets, and others); electronic keys — car keys, home / office keys, hotel room keys, etc. There are variants of cryptography that are used in the labels. The scope of the labels is examined on specific examples using the NFC Prestigio PKR1 keychain. The problem of protection of information is studied and ways of its solution are proposed. It is proposed to expand the scope of application of NFC, introducing it into various telecommunication systems.

Keywords: NFC technology; NFC tag; RFID technology; QR code; modulation; protocol; interface; cryptography; NFC mobile device; Wi-Fi technology.

УДК 004.62

Є. С. ТИХОНОВ, аспірант;
В. В. ЖЕБКА, канд. техн. наук;
А. П. БОНДАРЧУК, доктор техн. наук, доцент,
Державний університет телекомунікацій, Київ

ВИКОРИСТАННЯ СТАТИСТИЧНИХ І АНАЛІТИЧНИХ МЕТОДІВ ДЛЯ РОЗВ'ЯЗАННЯ ПРОБЛЕМ «ВЕЛИКИХ ДАНИХ»

Аналіз великих даних дедалі частіше стає популярною практикою, яку впроваджують численні організації, маючи на меті створення цінної інформації з величезних обсягів даних. Великі дані пропонують принципово нові можливості, а також виклики для статистиків. Адже використовуючи дані, ми стикаємося з багатьма супутніми проблемами, такими як висока вартість обладнання, неструктурованість масивів даних, що заважає негайно знаходити потрібну інформацію, блискавична швидкодія — опрацювання мільярдів гігабайт. У статті розглянуто статистичні та аналітичні методи боротьби з «поганими» даними.

Ключові слова: великі дані (big data); аналітика; аналіз великих даних; дискретизація; статистичні методи.

Вступ

Великі дані являють собою ті чи інші відомості в масовому (стосовно обсягу, інтенсивності та складності) масштабі, опрацювання яких перевершує можливості стандартного програмного забезпечення у плані управління та аналізу. Пошукові системи в інтернеті (наприклад, Google і YouTube) та інструменти соціальної мережі (скажімо, Facebook і Twitter) генерують щодня мільярди даних про суспільну активність. Ці дані включають у себе текстовий контент — структурований, напівструктурований або неструктурований, мультимедійний контент (відео, аудіо) на безлічі платформ. Щодня людство виробляє близько 2,5 квантилійних байт даних (2,5 мільярда гігабайт), переважно (до 90%) неструктурованих [1].