

# ДОСЛІДЖЕННЯ ЯКОСТІ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ІНТЕРНЕТУ РЕЧЕЙ ІЗ ПІДТРИМКОЮ 5G

Пугач К.О.

Харківський національний університет радіоелектроніки, Україна.

E-mail: [kateryna.puhach@nure.ua](mailto:kateryna.puhach@nure.ua)

---

## Abstract

*The Internet of Things (IoT) is becoming increasingly common in our society as the basis of smart homes and other smart environments. IoT refers to a global network that connects real physical objects with the virtual world. In such an environment, 5G cellular networks play a key role. Distinctive features such as high bandwidth, simple and cost-effective connectivity, etc. make the 5G cellular network an ideal candidate to be used as a backbone network in the future smart environment.*

---

## Вступ

Інтернет речей (ІоТ) стає все більш поширеним у нашому суспільстві як основа розумних будинків та інших розумних середовищ. ІоТ відноситься до глобальної мережі, що об'єднує реальні фізичні об'єкти з віртуальним світом. У такому середовищі стільникові мережі 5G відіграють ключову роль. Такі відмінні риси, як висока пропускна здатність, просте та економічно-ефективне підключення, тощо, роблять стільникову мережу 5G ідеальним кандидатом для використання в якості магістральної мережі у майбутньому розумному середовищі.

## Актуальність завдання

Зростання використання різноманітних пристроїв ІоТ та впровадження технології 5G в сучасних мережах призводять до зростаючої загрози для конфіденційності та безпеки даних. Швидкість передачі даних у мережах 5G дозволяє шпигунам та зловмисникам більше можливостей для злому та несанкціонованого доступу до особистої інформації, що створює необхідність дослідження якості захисту конфіденційності в цьому контексті.

## Об'єкт дослідження

Процеси формування якості захисту конфіденційності інтернету речей із підтримкою 5G.

## Предметом дослідження

Є якість захисту конфіденційності даних, які передаються через мережі 5G, зокрема в контексті вразливостей, які можуть бути використані для несанкціонованого доступу до цих даних.

## Мета дослідження

Є оцінка поточного рівня захисту конфіденційності в мережах 5G з підтримкою ІоТ та ідентифікація проблемних аспектів, які можуть призвести до витоку даних.

## Методи досліджень

базуються на аналізі сучасних стандартів захисту даних у мережах 5G та виявлення їх потенційних вразливостей та на емпіричному дослідженні шляхом збору даних про потенційні загрози та інциденти порушення конфіденційності в мережах 5G.

## Зміст роботи

Незважаючи на те, що проблеми безпеки в сфері інформаційних технологій не нові, використання Інтернету речей (IoT) породжує нові та унікальні проблеми безпеки. Забезпечення безпеки в продуктах та послугах IoT повинно бути головним пріоритетом, оскільки користувачі мають бути переконані в відсутності вразливостей у пристроях IoT та пов'язаних з ними послугах. Особливо це стає важливим з поширенням цієї технології та її інтеграцією в наше повсякденне життя. Недостатньо захищені пристрої та послуги IoT можуть слугувати потенційними точками входу для кібератак та можуть створювати ризик розкрадання даних через недостатній захист потоків інформації.

Взаємопов'язаність пристроїв IoT означає, що недостатньо захищений пристрій, який підключений до Інтернету, може впливати на загальний рівень безпеки та стійкості системи. Ця проблема посилюється через масове впровадження пристроїв IoT з однаковою структурою, здатність деяких пристроїв автоматично підключатися до інших пристроїв і можливість використання їх у незахищеному середовищі.

Оскільки мережі 5G все частіше розгортаються в усьому світі, питання безпеки та конфіденційності стають все більш актуальними. Мережі 5G – це наступне покоління стільникових мереж, які обіцяють вищу швидкість і кращу продуктивність. Але зі збільшенням швидкості та продуктивності з'являються додаткові ризики для безпеки.

Мережі 5G створені для більшої безпеки, ніж їхні попередники, але низка потенційних вразливостей залишається. Серед них доступ до мережі, радіочастотні перешкоди, автентифікація та авторизація пристроїв, конфіденційність даних тощо.

Доступ до мережі становить особливий ризик. Оскільки мережі 5G покладаються на набагато більшу кількість базових станцій, хакерам легше отримати до них доступ.

## Висновок

Дослідження підтвердило значущі проблеми в сфері захисту конфіденційності даних в мережах 5G, але також виділило напрямки для подальших досліджень та розробки ефективних стратегій та методів захисту, які можуть допомогти підвищити рівень кібербезпеки у цих мережах.

## Література

1. Пугач К. О. Проблеми безпеки та захисту конфіденційності Інтернету речей із підтримкою 5G / Катерина Олегівна Пугач. // Міжнародна науково-практична конференція. – 2022. – №5. – С. 23–24.
2. Explained: What is Internet of Things (IoT) and How it Works? [Електронний ресурс] // Appinventiv.. – 2022. – Режим доступу до ресурсу: <https://appinventiv.com/blog/what-is-internet-of-things/>.
3. Інтернет речей (IoT) [Електронний ресурс] // Termin. – 2019. – Режим доступу до ресурсу: <https://termin.in.ua/internet-rechey-iot/>.
4. Ageyev D.V., Evlash D.V. Multiservice telecommunication systems design with network's