УДК 004.056

**Гарнага В. А.**
**Немировська Д. О.**

# БЕЗПЕКА ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

**Анотація**

*Досліджено тему безпеки Інтернету речей і розглянуто різні аспекти її захисту, важливість впровадження безпеки на різних етапах розробки пристроїв IoT. Також висвітлено різноманітні методи та технології захисту і проаналізовано стандарти і законодавство, спрямовані на покращення безпеки у цій сфері.*
**Ключові слова:** інтернет речей, безпека інтернету речей, методи та технології захисту інтернету речей.

**Abstract**

*The article explores the topic of Internet of Things security and considers various aspects of its protection, the importance of implementing security at different stages of IoT device development. It also highlights various security methods and technologies and analyses standards and legislation aimed at improving security in this area*.
**Keywords:** Internet of Things, Internet of Things security, methods and technologies for protecting the Internet of Things

## Вступ

Інтернет речей описує собою систему взаємопов'язаних фізичних об'єктів, які мають вбудовані технології для взаємодії з навколишнім середовищем. Ці об'єкти можуть автономно обмінюватися даними про свої умови та отримувати інформацію з зовнішнього середовища. Поняття "Інтернет речей" було вперше введено Кевіном Ештоном у 1999 році, який є одним з засновників Центру автоматичної ідентифікації при Массачусетському технологічному інституті [1]. Завдяки таким технологіям ми маємо більшість зручних функцій сьогодення.

## Основна частина

З моменту свого початку Інтернет речей (IoT) пройшов значний шлях розвитку, ставши ключовим елементом сучасного технологічного прориву. Прогнозується, що до 2030 року кількість таких підключених пристроїв перевищить 30 мільярдів, що свідчить про їхню зростаючу популярність. Цей швидкий розвиток є наслідком вдосконалення комунікаційних технологій, таких як 5G, та інновацій у сфері обробки даних, зокрема використання штучного інтелекту та машинного навчання [2].

Згідно з даними Statista, можна відзначити значний розвиток та збільшення популярності Інтернету речей починаючи з 2013 року [3]. Цей період характеризується активним впровадженням таких технологій у повсякденне життя, що сприяло зростанню їх популярності. Зі збільшенням популярності Інтернету речей, ми стикаємося зі зростаючими викликами в області кібербезпеки. Кожен новий метод комунікації між пристроями, чи то через HTTP чи API, відкриває шляхи для хакерів до перехоплення та зловживання даними. Важливо визнати, що захист потрібен не тільки для пристроїв, що підключені до Інтернету, але й для тих, що використовують Bluetooth, оскільки вони також є частиною IoT.

Проблеми, пов’язані з безпекою IoT, такі як можливість віддаленого доступу, відсутність прогнозування в галузі та обмежені ресурси залишаються актуальними. Наприклад, численні точки доступу до IoT пристроїв через Інтернет дають хакерам можливість дистанційно взаємодіяти з ними, використовуючи різні методи. Проблемою є також відсутність уніфікованих методів захисту, що може збільшити ризики в таких секторах, як автомобільна промисловість та охорона здоров’я.

Крім того, слабкі заводські паролі та брак шифрування створюють потенційні вразливості. Багато IoT пристроїв не мають достатньо ресурсів для впровадження складних захисних механізмів, що ускладнює забезпечення їх безпеки. Тому посилення захисних методів та освіта користувачів і виробників щодо ризиків безпеки стає все більш важливим.

Захист систем та пристроїв Інтернету речей є надзвичайно важливим завданням для тих, хто використовує ці технології. Кращі практики безпеки повинні бути враховані на початкових етапах розробки будь-якого пристрою Інтернету речей. Розробники повинні уважно враховувати аспекти безпеки на кожному етапі розробки, забезпечуючи надійний захист пристроїв від потенційних загроз. Використання ідентифікації та аутентифікації за допомогою цифрових сертифікатів допомагає забезпечити безпеку під час обміну даними між пристроями та серверами.

Також важливо захищати мережі IoT від зловмисників завдяки застосуванню заходів безпеки портів, використання антивірусного програмного забезпечення, брандмауерів та систем виявлення вторгнень. Безпека API є критичною для захисту цілісності даних, переданих між пристроями Інтернету речей та внутрішніми системами. Забезпечення взаємодії з API лише авторизованих пристроїв та розробників допомагає уникнути несанкціонованого доступу до даних. Інноваційні підходи до захисту систем та пристроїв Інтернету речей допомагають забезпечити безпеку в доволі швидкозмінному інтернет-просторі та захистити користувачів від потенційних кіберзагроз [4].

В області безпеки Інтернету речей існують численні захисні системи, проте станом на сьогодні уніфікований стандарт безпеки IoT на галузевому рівні відсутній. Втім, впровадження вже існуючих рамок безпеки IoT може бути корисним, оскільки вони забезпечують необхідні інструменти та методики для підприємств, що розробляють та впроваджують IoT-пристрої. Такі рамки пропонуються організаціями, як-от Асоціація GSM, Фонд безпеки IoT, Промисловий консорціум IoT та іншими.

Щодо стандартів та законодавства у сфері IoT, можна виділити наступні ключові моменти:

Вересень 2015: Федеральне бюро розслідувань США опублікувало попередження (FBI Alert Number I-091015-PSA), в якому звернуло увагу на потенційні слабкі місця IoT-пристроїв і надало рекомендації для захисту споживачів.

Серпень 2017: Конгрес США ухвалив закон, який зобов'язує IoT-пристрої, що продаються уряду, відмовитися від заводських паролів, усунути відомі уразливості та мати можливість їх виправлення.

Травень 2018: Загальний регламент про захист даних (GDPR) був прийнятий у ЄС, що стандартизує захист даних і включає IoT-пристрої та їх мережі.

Червень 2018: Конгрес США представив SMART IoT Act, який передбачає дослідження IoT-індустрії та рекомендації для її безпечного розвитку.

Вересень 2018: Законодавчі органи Каліфорнії прийняли закон, що встановлює вимоги безпеки для IoT-пристроїв, які продаються у США.

Лютий 2019: Європейський інститут телекомунікаційних стандартів встановив перший глобальний стандарт безпеки IoT для споживачів.

Січень 2020: Сенат США прийняв DIGIT Act, який вимагає від Міністерства торгівлі створити робочу групу та звіт щодо IoT, включаючи аспекти безпеки та конфіденційності.

Грудень 2020: Екс-президент США Дональд Трамп підписав закон, який доручає Національному інституту стандартів і технологій розробити стандарти кібербезпеки для IoT-пристроїв уряду.

2022 рік: У Великій Британії набув чинності закон, який вимагає від споживчих смарт-пристроїв мати засоби захисту від кібератак [4].

**Висновок**

Інтернет речей - це досить нова технологія, що швидко розвивається, але при цьому вона вносить значний вклад у наше повсякденне життя. Водночас, з розвитком цієї технології відкриваються і різні вразливості, які можуть бути використані зловмисниками для атак на системи та пристрої, що містять їх у своєму складі. Для протидії таким загрозам існують різні методи захисту, які постійно вдосконалюються і повинні впроваджувати на постійні основі для обмеження ризиків пов'язаних з несанкціонованим доступом до таких систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Internet of Things, IoT. *IT-Enterprise – your one-stop platform for digital transformation | www.it.ua*. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (дата звернення: 04.05.2024).
2. Internet of Things (IoT). *Statista*. URL: https://www.statista.com/topics/2637/internet-of-things/#topicOverview (дата звернення: 04.05.2024).
3. IoT devices in use worldwide 2009-2020 | Statista. *Statista*. URL: https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide/ (дата звернення: 04.05.2024).

4. Yasar K., Shea S., Wigmore I. What is IoT Security? | TechTarget. *IoT Agenda*. URL: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security (дата звернення: 04.05.2024).

***Гарнага Володимир Анатолійович*** – к.т.н., доцент кафедри захисту інформації, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: garnaga.volodymyr@vntu.edu.ua

***Harnaha Volodymyr*** - Ph.D., Associate Professor of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

***Немировська Дар'я Олександрівна*** – студентка групи 1БКС-22б, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: nemyrovskadaria@gmail.com

***Nemyrovska Daria Oleksandrivna*** - student of group 1BKS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: nemyrovskadaria@gmail.com