# Проекти Європейського Союзу для безпеки Інтернету речей

УДК 004.056:004.738.5:061-1 ЄС Тетяна Мужанова[1], Віталій Тищенко[2]

*Державний університет інформаційно-комунікаційних технологій,*
*[1]muzanovat@gmail.com, [2]tvs5vetal@gmail.com*

Пристрої Інтернету речей (IoT) відіграють ключову роль у забезпеченні стійкості мереж і збереженні конфіденційності й безпеки даних. Але зростаюча тенденція до ускладнення загроз кібербезпеці викликає потребу в більш надійних структурах безпеки для пристроїв і мереж IoT.

Усвідомлюючи нагальність вирішення цієї проблеми, у 2020 році Єврокомісія представила комплексну Стратегію кібербезпеки ЄС для цифрової декади, в якій, зокрема окреслено шлях до поширення Інтернету безпечних речей. Так, Стратегія передбачає формування й дотримання вимог безпеки на внутрішньому ринку продуктів і послуг ЄС, що містять цифрові елементи, в т.ч. IoT, впровадження прозорих рішень безпеки й сертифікації, стимулювання безпечних продуктів і послуг IoT без шкоди для їх продуктивності [1].

На виконання поставлених у Стратегії завдань Єврокомісія започаткувала так званий кластер безпеки проектів IoT, спрямований на усунення недоліків пристроїв і мереж шляхом розробки безпечних і модульних інфраструктур, які можна інтегрувати в нові та існуючі рішення для сфер охорони здоров'я, догляду за людьми похилого віку, виробництва, постачання продуктів харчування, енергетики і транспорту. Цей кластер складається з 8 проектів, на реалізацію яких ЄС передбачив фінансування обсягом 40 млн. євро (приблизно 5 млн. євро кожен) [2].

На рис. 1 показано перелік цих проектів. Розглянемо детальніше призначення кожного з них.


Рис.1. Проекти ЄС щодо безпечного Інтернету речей

*SecureIoT* - це спільний проект компаній у сфері послуг і безпеки IoT, який на основі кількох платформ і мереж розумних об'єктів реалізує низку прогностичних служб безпеки IoT. SecureIoT має забезпечити конкретні механізми збору даних, моніторингу і прогнозних механізмів безпеки, які стануть основою для надання інтегрованих послуг з оцінки ризиків, аудиту нормативної відповідності, а також підтримки для розробників IoT.

Проект *SEMIoTICS* спрямований на розробку керованої шаблонами структури, побудованої на існуючих платформах IoT, щоб забезпечити безпечне й надійне спрацьовування й напівавтономну поведінку в додатках IoT, в т.ч. промислових.

Проект має підтримувати міжрівневу інтелектуальну динамічну адаптацію різнорідних “розумних об’єктів, мереж і хмар, розробляти й інтегрувати розумні програмовані мережі й механізми семантичної взаємодії.

*DevOps ENACT* є спільною ініціативою. Рух DevOps просуває використання набору інструментів розробки ПЗ, які забезпечують якість послуг і одночасно розвиток складних систем, сприяють швидким інноваціям і простоті у використанні. ENACT створив засоби підтримки платформи, давши можливість DevOps розробити надійні рішення для систем IoT з високим рівнем безпеки і стійкості в умовах їх спільного впровадження.

Проект *IoTCrawler* сфокусований на сумісності між платформами, реконфігураційних рішеннях для інтеграції даних і послуг, безпечних алгоритмах з урахуванням конфіденційності й механізмах для сканування, індексування та пошуку в системах IoT.

*BRAIN-IoT* зосереджується на складних сценаріях, де активація й управління спільно підтримуються групою систем IoT. Мета полягає у створенні структури й методології, що підтримує спільну “розумну” поведінку в повністю децентралізованих, комбінованих і динамічних об’єднаннях різнорідних платформ IoT.

Проект *SOFIE* вирішив проблему фрагментації IoT через об’єднання, до якого будь-яка платформа IoT може приєднатися, створивши адаптер. Проект реалізує конфіденційність, забезпечуючи наскрізну безпеку, управління ключами, авторизацію, підзвітність і можливість перевірки.

*CHARIoT* має на меті вдосконалення сучасних технологій IoT шляхом використання методу проектування й когнітивної обчислювальної платформи, що підтримує уніфікований підхід до конфіденційності, надійності й безпеки систем IoT, що сприяє високому рівню безпеки і цілісності промислового IoT.

У рамках проекту *SerIoT* розроблено структуру IoT на основі адаптивної “розумної” програмно-визначеної мережі із захищеними маршрутизаторами, розширеною аналітикою і зручною візуальною аналітикою, оптимізував безпеку на платформах і в мережах у цілісний, багаторівневий спосіб.

Отже, беручи до уваги ключову роль Інтернету речей у забезпеченні стійкості мереж і збереженні конфіденційності й безпеки даних, керівництво ЄС започаткувало кластер безпеки проектів IoT, спрямований на розробку безпечних і модульних інфраструктур IoT. Завдяки використанню модульного підходу з відкритим вихідним кодом, який дозволяє повторно використовувати модулі в інших рішеннях для більш широкого спектру програм, досягнуто значних успіхів у реалізації проектів кластеру.

1. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 (дата звернення: 20.04.2024)
2. Secure solutions for the Internet of Things. URL: https://digital-strategy.ec.europa.eu/en/policies/secure-internet-things (дата звернення: 20.04.2024).