КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.848
УДК 004.054

Дудикевич Валерій Богданович
д.т.н., професор, професор кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0001-8827-9920
valerii.b.dudykevych@lpnu.ua

Микитин Галина Василівна
д.т.н., професор, професор кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0003-4275-8285
halyna.v.mykytyn@lpnu.ua

Мурак Тарас Євгенович
магістрант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0005-7588-9945
taras.murak.mkbst.2024@lpnu.ua

ІНТЕГРАЛЬНА МОДЕЛЬ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ У ПРОСТОРІ ІНТЕЛЕКТУАЛІЗАЦІЇ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

Анотація. У статті досліджено питання моделей архітектури і безпеки Інтернету речей (IoT) у просторі інтелектуалізації обєктів інфраструктури суспільства. Проведено аналітичний огляд відомих методологій та моделей в розробленні архітектури IoT та створення підходів до забезпечення їх безпеки. Розгорнуто класичну еталонну модель архітектури IoT від Міжнародного союзу електрозв'язку МСЕ-Т за Рекомендаціями 2060, яка структурована складовими у функціональному просторі та в середовищі управління і безпеки. Проаналізовано перший рівень архітектури еталонної моделі від МСЕ-Т — мережу пристроїв, які функціонально взаємодіють з фізичними речами середовища інтелектуалізації на рівні збору та перенесення даних. Розкрито архітектуру еталонної семирівневої моделі від Всесвітнього форуму IoT, якій властиві функції: аналіз даних за критеріями, форматування даних, обробка криптографічних даних, скорочення даних, оцінювання даних за пороговим значенням. Розглянуто модель безпеки IoT на основі архітектури моделі Cisco, яка відобрає взаємозв'язок у просторі «архітектура IoT — безпека» на рівні структури «функціонування IoT — захист». На основі моделі безпеки Cisco створено інтегральну багаторівневу модель безпеки IoT для широкого парку індустріальних об'єктів інфраструктури суспільства, зокрема критичної згідно структури «архітектура IoT — загрози — методи безпеки — технології захисту», яка на рівнях — аутентифікації, авторизації, шифрування, trust-менеджменту, мережевої політики, аналітики безпеки та прогнозування загроз розгортається відповідними алгоритмами і технологіями захисту усіх засобів екосистеми IoT. Розроблено алгоритмічно-програмне забезпечення криптографічного захисту обміну даних на основі симетричного блокового алгоритму автентифікованого шифрування AES-256-GCM заобами мови програмування Python як практичну реалізацію інтегральної моделі безпеки IoT на рівні протоколу OpenVPN і технології UDP.

Ключові слова: інтелектуалізація об'єктів; архітектура Інтернету речей; моделі безпеки; інтегральна багаторівнева модель; автентифікація, шифрування даних; симетричний блоковий алгоритм.

ВСТУП

Сьогодні в світі та в Україні триває розвиток Концепції Індустрії 4.0 [1] у просторі застосування новітніх технологій та методологій їх безпеки для функціонування інтелектуальних об'єктів інфраструктури суспільства, зокрема критичної. Одним з

найбільш актуальних напрямків розвитку інформаційно-комунікаційних технологій є багаторівневі кіберфізичні технології, фізичний простір яких займає Інтернет речей. Інтернет речей — система взаємопов'язаних фізичних обєктів, давачів, виконавчих пристроїв, виконавчих механізмів, мікроконтролерів та програмного забезпечення, що забезпечують відбір/реєстрацію та передавання інформації від різнорідних обєктів інфраструктури, середовища та структури взаємодії «об'єкт — середовище» для її подальшої обробки та аналізу з метою прийнятя управлінського рішення.

Одним з основних векторів розвитку Стратегії Агентства ЄС з питань кібербезпеки (ENISA) і Стратегії кібербезпеки України [2], [3] є безпека інформаційно-комунікаційних технологій, зокрема кіберфізичних, які є ефективним інструментарієм безпечного функціонування інтелектуальних об'єктів. Відповідно актуальним сегментом в методології безпеки кіберфізичних технологій є моделі безпеки Інтернету речей та їх розвиток у просторі використання новітніх підходів для безпечного відбору інформації на рівні давачів та безпечного обміну інформацією між фізичним простором та кібернетичним середовищем на рівні використовуваних протоколів [4].

Відповідно, проблема безпеки Інтернету речей інтелектуальних об'єктів інфраструктури є актуальною в контексті розвитку Концепції Індустрії 4.0 в Україні, особливо у сегменті забезпечення безпечного обміну даними на рівні ідентифікації, аутентифікації, шифрування.

Постановка проблеми. Інтернет речей є однією з найважливіших технологій 21-го століття, яка сьогодні динамічно розвивається як:

- Інтернет всього — об'єднує людей, процеси, дані, технічні пристрої з метою формування необхідного та ефективного інформаційного рівня мережевих з'єднань;
- Промисловий Інтернет — складна самоконфігурована адаптивна система мереж давачів та розумних об'єктів, призначення яких полягає у з'єднанні всіх речей, в тому числі побутових і промислових обєктів;
- Інтернет чого завгодно:
  1) Інтернет людей, кіберфізичні системи та кібер-біологічні системи формують Інтернет речей; Інтернет всього та промисловий Інтернет будуються на базі Інтернету речей і в об'єднанні з розподіленими автоматизованими системами формують Інтернет чого завгодно;
  2) Єдина програмна екосистема, яка підтримує комплекс показів: усіх давачів, системних станів, експлуатаційних умов, контекстів даних. Це вимагає аналізу моделей Інтернету речей, дослідження моделей безпеки та розвитку методології безпеки IoT з врахуванням специфіки індустріального парку інтелектуальних об'єктів інфраструктури та рівнів забезпечення їх безпеки відповідно до комплексу ймовірних загроз і технологій захисту.

Аналіз останніх досліджень і публікацій. Проблемі безпеки Інтернету речей присвячено багато наукових досліджень як на міжнародному рівні, так і в Україні. Дослідження питань безпеки екосистеми IoT стосуються: підходів, моделей та методологій, апаратного і програмного забезпечення, застосування нейромережевих технологій, вдосконалення криптографічних алгоритмів шифрування, вдосконалення методів захисту мереж і каналів передавання інформації, розвитку комплексних систем безпеки IoT. Розглянемо наукові дослідження в різних сегментах безпеки Інтернету речей, які проводилися на міжнародному рівні. Розвиток підходів до забезпечення безпеки IoT представлено на таких рівнях: в роботі [5] пропонується новий підхід до забезпечення комплексної безпеки пристроїв IoT, що грунтується на реконфігурованому апаратному

механізмі ізоляції та захисту, який працює як динамічна одиниця розділення між пристроями і мережею та аналізує комунікації на наявність шкідливих дій і, на цій основі, запобігає пошкодженню пристрою IoT; в праці [6] розглянуто підхід із використанням апаратних приманок як додаткового захисного рівня від вразливостей апаратного забезпечення IoT, зокрема апаратних троянів. Сегмент апаратної безпеки IoT має свої вектори розвитку. В роботі [7] запропонована підсистема безпеки IoT, яка інтегрує спеціальні апаратні компоненти, включаючи шифрування даних, дешифрування та автентифікацію; її архітектура забезпечує безпечні процеси завантаження та моніторинг виконання програм у реальному часі. В праці [8] розглянуто порівняльний аналіз апаратних механізмів безпеки для оптимального вибору апаратних заходів безпеки в дизайні IoT у просторі довговічності пристроїв на протидію прогресуючим кіберзагрозам. З метою запобігання фальсифікації даних в пристроях IoT та забезпечення профілів безпеки конфіденційності цілісності і автентичності файлів даних в роботі програм IoT в праці [9] проаналізовано апаратну структуру безпеки для пристроїв IoT, зокрема вбудований LUKS (E-LUKS), який розширює можливості LUKS, додаючи методи цілісності та автентифікації на додаток до конфіденційності, яку вже забезпечує LUKS; E-LUKS використовує найсучасніші алгоритми шифрування та хешування. Сегмент захисту мереж IoT має також цікаві аспекти: метод захисту цілісності мережі та конфіденційності даних розглядається на рівні нової структури ідентифікації безпровідних пристроїв на основі згорточної нейронної мережі, що дозволяє автентифікувати пристрої в архітектурі парадигми нульової довіри [10]; застосування криптографічних алгоритмів від прослуховування в мережах IoT [11].

В Україні проводилися наукові дослідження питань безпеки IoT на рівні: моделей, застосування нейронних мереж і штучного інтелекту, захисту безпровідних систем звязку, програмного забезпечення. Розглянемо деякі напрацювання. В праці [12] розглянуто модель безпеки для IoT-пристроїв, яка: враховує обмежені обчислювальні ресурси і мінімальне енергоспоживання, необхідні для ефективного функціонування криптографічних алгоритмів; включає як апаратні, так і програмні рішення для шифрування та управління ключами, з метою мінімізації ризиків компрометації даних. Актуальною є нейромережева модель контролю апаратної сумісності компонентів IoT на основі математичного апарату нейронних мереж [13]. Розгортаються системи виявлення аномалій на основі штучного інтелекту та машинного навчання, які є ефективними для раннього виявлення загроз, зокрема для залізничних мереж IoT [14]. В контексті забезпечення безпечного обміну даними в безпровідних сенсорних мережах Інтернету речей в роботі [15] розглядається метод гомоморфного шифрування та аутентифікації користувачів та їхніх електронних повідомлень. У сегменті програмної безпеки IoT в праці [16] проаналізовано причини програмної вразливості Інтернету речей та визначено складність програмного забезпечення в IoT із зазначенням заходів здатних знизити рівень вразливості, а також запропоновано для проектування програмного забезпечення емулювати поведінку пристроїв Інтернету речей, тобто створити імітатор зовнішнього середовища для серверів.

На основі проведеного аналізу, було встановлено завдання даної роботи:

1) запропонувати інтегральну багаторівневу модель безпеки IoT на основі способів/методів захисту даних;
2) розробити програмну реалізацію криптографічного захисту даних на транспортному рівні IoT на основі — протоколу OpenVPN, технології UDP, симетричного блокового алгоритму автентифікованого шифрування AES-256-GCM засобами мови програмування Python, як одного з ефективних механізмів реалізації безпечного обміну повідомлень між пристроями IoT, що забезпечуватиме високий ступінь конфіденційності та автентифікації.

Метою статті є аналіз моделей Інтернету речей та дослідження методології безпеки IoT на основі моделі Cisco і, на цій основі, побудова інтегральної багаторівневої моделі безпеки IoT для інтелектуальних об'єктів інфраструктури та її практична реалізація на рівні автентифікованого шифрування даних з використанням інструментарію — криптографічного протоколу OpenVPN, технології UDP, алгоритму AES-256-GCM, мови програмування Python.

Завданнями дослідження є:

1. Аналіз еталонних моделей Інтернету речей від Міжнародного електрозв'язку МСЕ-Т та від Всесвітнього форуму;
2. Обгрунтування методології безпеки Інтернету речей на основі моделі Cisco;
3. Побудова інтегральної багаторівневої моделі безпеки IoT для безпечного функціонування інтелектуальних об'єктів;
4. Розроблення алгоритмічно-програмної реалізації автентифікованого шифрування даних згідно запропонованої моделі безпеки IoT на основі: криптографічного протоколу OpenVPN, технології UDP, алгоритму AES-256-GCM, мови програмування Python.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інтернету речей: еталонні моделі, безпека

Еталонна модель Інтернету речей від Міжнародного союзу електрозв'язку МСЕ-Т. Класична модель IoT — це стандартизована еталонна модель IoT від Міжнародного союзу електрозв'язку (МСЕ-Т) описана в Рекомендації Y.2060 [17]. На відміну від більшості відомих еталонних та архітектурних моделей, модель МСЕ-Т деталізує фактичні фізичні компоненти екосистеми IoT. Ця модель є ефективною, оскільки висвітлює усі елементи екосистеми IoT (засоби, сервіси і технології), які повинні бути з'єднані, інтегровані, керовані та надані додаткам. На рис. 1 зображена архітектура класичної еталонної моделі IoT від МСЕ-Т, яка структурована складовими чотирьох рівнів в функціональному просторі та двома міжрівневими складовими в просторі управління і безпеки [18]. Розглянемо функціональні складові багаторівневої еталонної моделі IoT від МСЕ-Т.

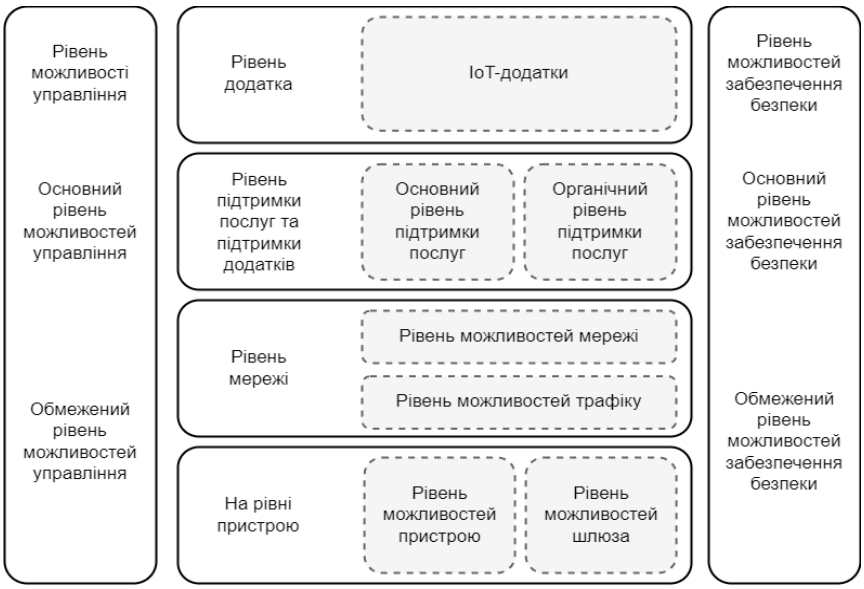

Рис. 1. Класична еталонна модель IoT від МСЕ-Т за Рекомендаціями Y.2060

Рівень пристрою. На рис. 2, адаптованому з Рекомендації Y.2060, зображено мережу пристроїв в моделі МСЕ-Т, в якій сенсорні і виконавчі механізми взаємодіють з фізичними речами у зовнішньому світі. Пристрої збору даних зчитують дані з фізичних речей шляхом взаємодії з пристроями перенесення даних або носіями даних, підключеними до фізичних об'єктів. Ця модель підкреслює відмінність між пристроями перенесення даних і носіями даних. Пристрій переносення даних включає можливість зв'язку і може мати інші вбудовані електронні можливості. Носій даних — це компонент, приєднаний до фізичної речі з метою ідентифікації або інформування. В Рекомендації Y.2060 відзначається, що технології, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Пристрої загального призначення володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT.

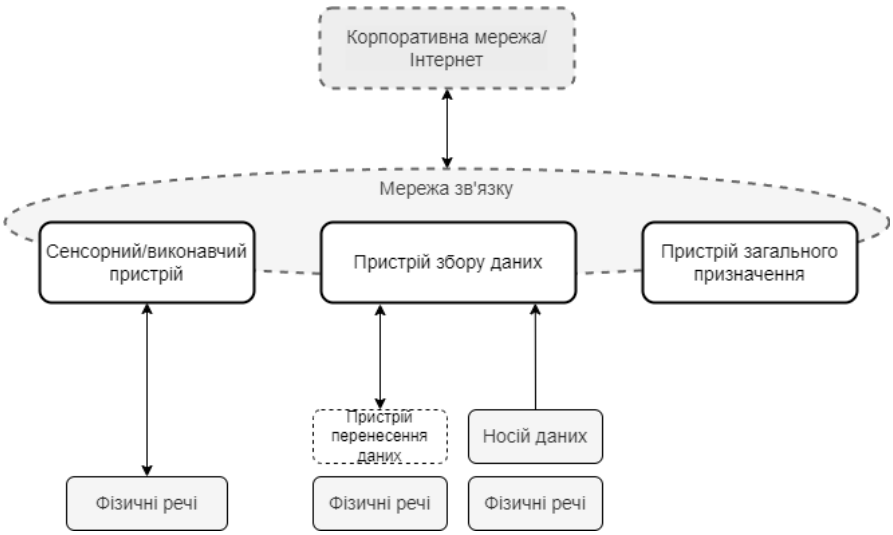

Рис. 2. Типи пристроїв і їх взаємозв'язок з фізичними речами

Рівень мережі виконує дві основні функції — взаємодія пристроїв і шлюзів (можливості мережі) та переносення інформації аплікацій IoT (можливості трафіку), які реалізуються на мережевому і транспортному рівнях моделі OSI.

Рівень підтримки послуг і підтримки додатків — надає можливості для використання додатками функцій спільного опрацювання даних та управління базами даних.

Рівень додатка — складається з додатків, що взаємодіють з IoT-пристроями.

Розглянемо міжрівневі складові еталонної моделі IoT від МСЕ-Т в просторі управління та безпеки.

Рівень можливостей управління – охоплює традиційні функції управління мережею. Серед прикладів загальних можливостей управління за Рекомендаціями Y.2060:

- *управління пристроями* охоплює*:* виявлення пристроїв, аутентифікацію, дистанційне керування і деактивацію пристроїв, налаштування, діагностику, оновлення програмного забезпечення, управління статусом пристрою;
- *управління топологією локальної мережі* реалізує*:* управління налаштуванням мережі;
- *управління трафіком і перевантаженнями* здійснює*:* аналіз навантаження мережі та реалізацію резервного копіювання ресурсів для часових важливих потоків даних.

Рівень можливостей забезпечення безпеки – забезпечує захист, який не залежить від додатків. Серед прикладів загальних можливостей безпеки за Рекомендаціями Y.2060:

- *на рівні програми:* авторизацію, аутентифікацію, захист конфіденційності і цілісності даних програми, захист приватності, аудит безпеки і антивірусний захист;
- *на рівні мережі:* авторизацію, аутентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних;
- *на рівні пристрою:* аутентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності та цілісності даних.

У 2019 році МСЕ-Т оновив Рекомендації Y.2060 на рівні нової серії Y.4460 [19]. Ця рекомендація описує архітектурні еталонні моделі пристроїв для додатків Інтернету речей на основі класифікації пристроїв, визначених потужністю обробки та можливостями зв'язку. Описані архітектурні еталонні моделі також включають функціональні об'єкти пристрою та взаємодію функціональних об'єктів для архітектурної еталонної моделі кожного пристрою. Серед архітектурних еталонних моделей:

- *еталонна модель для LPLC-пристроїв* — з низьким рівнем обробки та низьким підключенням (low processing and low connectivity device);
- *еталонна модель для LPHC-пристроїв* — з низькою обробкою та високою зв'язністю (low processing and high connectivity device);
- *еталонна модель для HPHC-пристроїв* — високої обробки та високого підключення (high processing and high connectivity device).

Еталонна модель від Всесвітнього форуму IoT. Комітет з архітектури Всесвітнього форуму IoT (IoT World Forum, IWF) у складі лідерів індустрії, серед яких IBM, Intel та Cisco в жовтні 2014 року опублікував еталонну модель IoT з метою його просування на міжнародному ринку. Запропонована семирівнева еталонна модель Всесвітнього форуму IoT має такі функції (рис. 3) [20]:

Рис. 3. Еталонна модель Всесвітнього форуму IoT

- *спрощує:* допомагає декомпонувати комплексні системи на більш дрібні частини, щоб кожна з цих частин стала більш зрозумілою;
- *прояснює:* надає додаткові відомості для точної ідентифікації рівнів IoT і створення загальної термінології;
- *ідентифікує:* ідентифікує аспекти, в яких ті чи інші типи обробки оптимізовані в різних частинах системи;

- *стандартизує:* модель забезпечує перший крок до того, щоб постачальники могли створювати стандартизовані продукти IoT, які можуть взаємодіяти один з одним;
- *організовує:* робить IoT реальним і доступним, а не просто концептуальним.

Еталонній моделі від Всесвітнього форуму IoT властиві такі операції [20]:

- *аналіз:* аналіз даних за критеріями, що уможливлюють обробку на більш високому рівні;
- *форматування:* зміна даних з метою однакової високорівневої обробки;
- *розархівування/декодування:* обробка криптографічних даних з додатковим контекстом;
- *дистиляція/скорочення:* скорочення та підсумовування даних з метою зменшення обсягу даних і навантаження на трафік в мережі та у високорівневих системах;
- *оцінка:* визначення того, чи становлять дані порогове значення або аварійний сигнал; цей процес повинен включати перенаправлення даних додатковим одержувачам.

Всесвітній форум вважає еталонну модель IoT прийнятою в галузі базовою структурою, спрямованою на стандартизацію концепцій і термінології, пов'язаних з Інтернетом речей.

Безпека Інтернету речей на основі моделі Cisco. Компанія Cisco Systems, розробила фреймворк безпеки IoT на рівні доповнення до еталонної моделі Всесвітнього форуму IoT. На рис. 4 показане середовище безпеки, пов'язане з логічною структурою IoT [20].

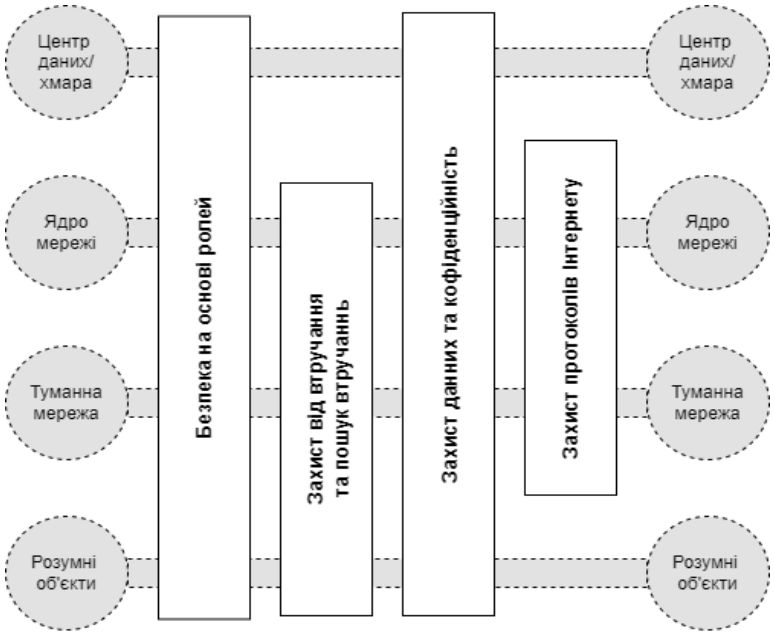

Рис. 4. Модель Cisco IoT та середовище безпеки

Модель Cisco IoT, яка спрощеною версією моделі Всесвітнього форуму IoT, складається з наступних рівнів:

- *«Розумні» об'єкти/вбудовані системи*: включають в себе сенсорні/виконавчі пристрої та інші вбудовані системи на рівні мережі. Ця частина IoT найбільш вразлива. Для цього рівня актуальні аспекти безпеки: профілі конфіденційності, автентичності та цілісності даних, що генеруються сенсорами; захист

виконавчих пристроїв та інших «розумних» пристроїв від несанкціонованого доступу; захист від підслуховування;

- *Туманна/периферійна мережа*: представляє провідні та безпровідні з'єднання пристроїв IoT. Особливостями цього рівня є: реалізація певного обсягу обробки і консолідації даних; велика варіативність мережевих технологій і протоколів, використовуваних різними пристроями IoT; необхідність розроблення та впровадження єдиної політики безпеки.
- *Ядро мережі*: надає алгоритм передавання даних між платформами в центрі мережі та пристроями IoT. Особливістю цього рівня IoT в просторі безпеки є величезна кількість кінцевих вузлів, з якими потрібно взаємодіяти і управляти ними;
- *Центр даних/хмара*: містить платформи для додатків, зберігання даних і управління мережею. Вектором безпеки цього рівня IoT повинен враховувати функціонування величезної кількості окремих кінцевих вузлів.

На основі чотирирівневої архітектури IoT модель Cisco визначає чотири рівні безпеки:

- *Безпека на основі ролей*: системи управління доступом надають права доступу ролям, а не окремим користувачам. Цей інструментарій може використовуватися для управління доступом до IoT-пристроїв і генерованих ними даних;
- *Захист від втручання і виявлення втручань*: ця функція особливо важлива на рівні пристроїв і туманної мережі, але поширюється також і на рівень ядра мережі;
- *Захист даних і конфіденційність*: функції охоплюють всі рівні архітектури IoT;
- *Захист протоколів Інтернету*: захист «даних в русі» від підслуховування і перехоплення важливий для всіх рівнів архітектури IoT.

Інтегральна багаторівнева модель безпеки Інтернету речей інтелектуальних об'єктів

Для забезпечення безпечного функціонування Інтернету речей системи різнорідних інтелектуальних обєктів, необхідно створити інтегральну багаторівневу модель безпеки відповідно до комплексу: технологій екосистеми IoT, ймовірних загроз, відповідних технологій безпеки.

Це дозволить системно підійти до вирішення проблеми безпеки великого індустріального парку об'єктів інфраструктури суспільства в просторі Концепції Індустрія 4.0 за вектором безпечного функціонування IoT з врахуванням:

1) функціональних особливостей об'єктів;
2) усталених методів та засобів захисту.

На основі розглянутої моделі безпеки Cisco для безпечного функціонування IoT доцільно розглянути багаторівневу модель безпеки, яка включає методи безпечного функціонування інтелектуальних об'єктів, що розгортаються на рівні алгоритмів, апаратно-програмних технологій захисту відповідно до компонентів екосистеми IoT — розумних давачів/виконавчих механізмів; систем звязку з давачами; локальних обчислювальних мереж; агрегаторів, маршрутизаторів, шлюзів, пограничних пристроїв; глобальних обчислювальних мереж; хмари, сервісів аналізу даних.

Інтегральна багаторівнева модель безпеки IoT представлена такими рівнями безпеки: аутентифікації; авторизації; шифрування; trust-менеджменту; мережевої політики; аналітики безпеки та прогнозування загроз (рис. 5):

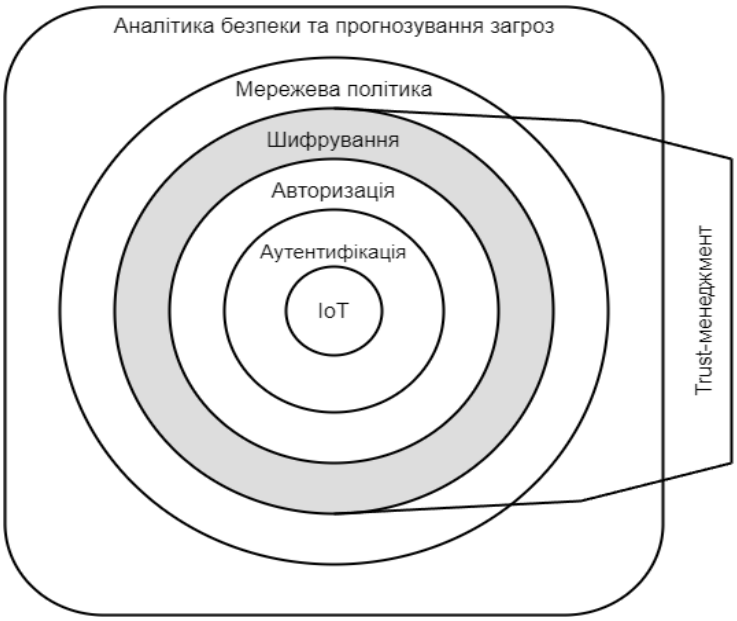

Рис. 5. Інтегральна багаторівнева модель безпечного функціонування Інтернету речей інтелектуальних об'єктів

Рівень аутентифікації. Цей рівень охоплює елементи, які ініціюють доступ і, в першу чергу, ідентифікує пристрої IoT. На відміну від типових корпоративних мережевих пристроїв, для яких ідентифікація може здійснюватися за ідентифікаційними ознаками людини (ім'я/пароль або бейдж), кінцеві пристрої IoT повинні оснащуватися такими методами аутентифікації, які не вимагають втручання людини. До них відносяться: радіочастотні мітки, сертифікати x.509, MAC-адреси кінцевих пристроїв. На рівні хмари IoT ефективно використовується мультифакторна автентифікація, як метод контролю доступу до комп'ютера, в якому користувачеві для отримання доступу до інформації необхідно пред'явити більше одного «доведення механізму аутентифікації», зокрема: пін-код, біометрія або магнітна карта, токен, флеш-пам'ять субєкта [21].

Рівень авторизації. Авторизація управляє доступом до пристрою через структуру мережі. Разом з рівнем аутентифікації він виробляє необхідні параметри для того, щоб дозволити обмін інформацією між пристроями та прикладними платформами, тим самим забезпечуючи роботу IoT-служб.

Рівень шифрування. Перед тим, як дані будуть доставлені до хмарного центру, вони повинні бути зашифрованими на транспортному рівні IoT для досягнення end-to-end шифрування.

Рівень мережевої політики. Охоплює всі елементи, які здійснюють маршрутизацію і транспортування трафіку з кінцевих пристроїв по інфраструктурі — контроль, управління, власне трафік даних.

Рівень аналітики безпеки та прогнозування загроз. Цей рівень включає всі функції, необхідні для централізованого управління пристроями IoT, зокрема охоплює видимість IoT-пристроїв, що забезпечує ідентичність і атрибути кожного з них та уможливлює контроль, включаючи конфігурацію, патчі та оновлення, а також застосування відповідних технологій протидії ймовірним загрозам.

Важливим об'єднуючим рівнем інтегральної моделі безпеки IoT є *trust-менеджмент*. У цьому контексті *trust-менеджмент* означає управління доступом таким чином, щоб два партнери за обміном даними бути впевненими в ідентичності і правах

доступу один одного. Аутентифікаційний компонент концепції довіри реалізує базовий рівень довіри, що доповнюється авторизаційним компонентом.

Інтегральна багаторівнева модель безпеки IoT передбачена для функціонування в просторі «виявлення — блокування — нейтралізація» загроз та прогнозування ризиків з метою протидії їм на рівні структури «витік — модифікація — знищення даних» засобами ІТ-аналітики в режимі реального часу.

Криптографічний захист комунікаційного рівня архітектури IoT на основі симетричного блокового алгоритму AES-256 засобами мови Python

На основі синтезу видів архітектури IoT, можна виділити три основні рівні:

1) *фізичний* — призначений для відбору інформації від комплексу давачів, що взаємодіють з інтелектуальними об'єктами;
2) *комунікаційний* — призначений для передавання інформації в кібернетичний простір з метою подальших дій і прийняття управлінського рішення щодо стану розумного об'єкта;
3) *кібернетичний* — призначений для обробки, аналізу інформації про стан інтелектуальних об'єктів внаслідок їх моніторингу параметрів. Безпечний обмін інформації на комунікаційному рівні IoT забезпечується відповідними технологіями захисту відповідно до ймовірних загроз.

Серед поширених загроз на комунікаційний рівень IoT можна виділити: DOS-атаки, Spoofing-атака, Атака «Man-In-The-Middle». На практиці ефективно застосовують такі технології захисту інформації від загроз на комунікаційний рівень: криптографію, VPN-протоколи, автентифікацію, блокчейн, системи виявлення вторгнень т. і. Серед відомих VPN-протоколів (OpenVPN, WireGuard, IKEv2/IPSec, L2TP/IPSec, PPTP), які управляють створенням і шифруванням VPN-з'єднань, протокол OpenVPN.

OpenVPN має такі особливості: є протоколом з відкритим вихідним кодом, універсальним, сумісним з усіма платформами; фективно використовує технологію UDP (User Datagram Protocol) для безпечного передавання даних між пристроями в мережі IoT та алгоритм AES-256-GCM в режимі Галуа/лічильника для автентифікованого шифрування повідомлень; забезпечує високий ступінь криптостійкості в процесі передавання конфіденційних даних; є одним найнадійніших рішень безпеки екосистеми IoT.

Програмна реалізація симетричного блокового алгоритму автентифікованого шифрування даних AES-256- GCM засобами мови програмування Python. Програмну реалізацію автентифікованого шифрування даних на основі алгоритму AES-256-GCM створено засобами мови програмування Python. Алгоритм AES-256-GCM використовується для програмної реалізації аутентифікованого шифрування даних і дозволяє окрім конфіденційності забезпечити аутентифікацію даних. Алгоритм окрім шифрування генерує тег автентичності і відправляється разом із зашифрованим повідомленням. Отримувач розшифровує повідомлення та порівнює отриманий тег автентичності з очікуваним.

Програмна реалізація складається з сервера та клієнта для імітації взаємодії між кінцевим пристроєм Інтернету речей та сервером обробки данних. Для передавання даних між імпровізованим сервером та клієнтом було використано транспортний протокол UDP через низьку затримку та малу вагу заголовків, що є важливо для малопотужних пристроїв в мережах IoT.

Для генерування серкретного ключа було застосовано протокол Діффі-Хеллмана. Цей протокол використовується для безпечного встановлення секретного ключа між двома сторонами.

Розглянемо алгоритм роботи програмної реалізації шифрування даних. На початку роботи обидві сторони завантажують спільні параметри алгоритму Диффі-Гелмана, які було попередньо згенеровано у вигляді окремого PEM-файлу. Кожен учасник створює власну пару криптографічних ключів: приватний та публічний. Клієнт ініціює з'єднання, надсилаючи серверу свій публічний ключ через UDP-сокет. Сервер у відповідь надсилає свій публічний ключ клієнту.

Далі учасники обчислюють секретний симетричний ключ, який використовується для шифрування даних. Після завершення обміну ключами клієнт відправляє повідомлення, яке шифрується за допомогою AES-256 з унікальним початковим вектором nonce, серверу.

Разом із зашифрованим повідомленням формується тег автентичності, який дозволяє виявити спроби підробки або змінення даних. Клієнт передає на сервер пакет, який містить nonce, зашифровані дані, тег автентичності та, за потреби, додаткові автентифіковані дані (AAD). Сервер приймає ці пакети через UDP, застосовує той самий симетричний ключ і nonce, та намагається дешифрувати повідомлення.

Якщо тег автентичності збігається — повідомлення вважається достовірним і підтверджується сервером. Якщо ж тег не збігається, сервер надає помилку і повідомлення не приймається, що унеможливлює несанкціоновану зміну переданих даних. Основна структура програмного коду включає наступні елементи:

1. Імпорт модулів, які використовуються в програмі:
   - **socket** — приймає UDP-пакети від клієнта, відповідає публічним ключем;
   - **dh** — для роботи з Diffie-Hellman ключами;
   - **default_backend** — використовується для створення криптографічних об'єктів;
   - **HKDF** — ключовивідна функція для обчислення симетричного AES-ключа зі спільного секрету;
   - **hashes** — визначає хеш-функцію (наприклад, SHA256) для HKDF;
   - **serialization** — для кодування та декодування публічних ключів у байтовий формат;
   - **AES** — реалізація алгоритму AES (включає режим GCM).
2. Криптографічний обмін ключами:
   - **generate_key_pair(parameters)** — генерує пару ключів (приватний і публічний) на основі Diffie-Hellman параметрів.
     Використовується як на клієнті, так і на сервері.
   - **derive_shared_key(private_key, peer_public_key)** — обчислює спільний секретний ключ за допомогою власного приватного та отриманого публічного ключа.
     Після цього застосовується HKDF для отримання 256-бітного симетричного ключа AES.
   - **load_dh_parameters()** — завантажує параметри алгоритму Diffie-Hellman з файлу *dh_params.pem*, згенерованого заздалегідь.
3. AES-256-GCM шифрування:
   - **encrypt_message(key, plaintext, aad)** — шифрує текстове повідомлення за допомогою AES-256 у режимі GCM;
   - **decrypt_message(key, nonce, ciphertext, tag, aad)** — дешифрує повідомлення, перевіряючи автентичність за допомогою tag.

На рис. 6 наведено результати шифрування довільних даних з відповідним ключем на основі симетричного блокового алгоритму AES-256-GCM засобами мови програмування Python.

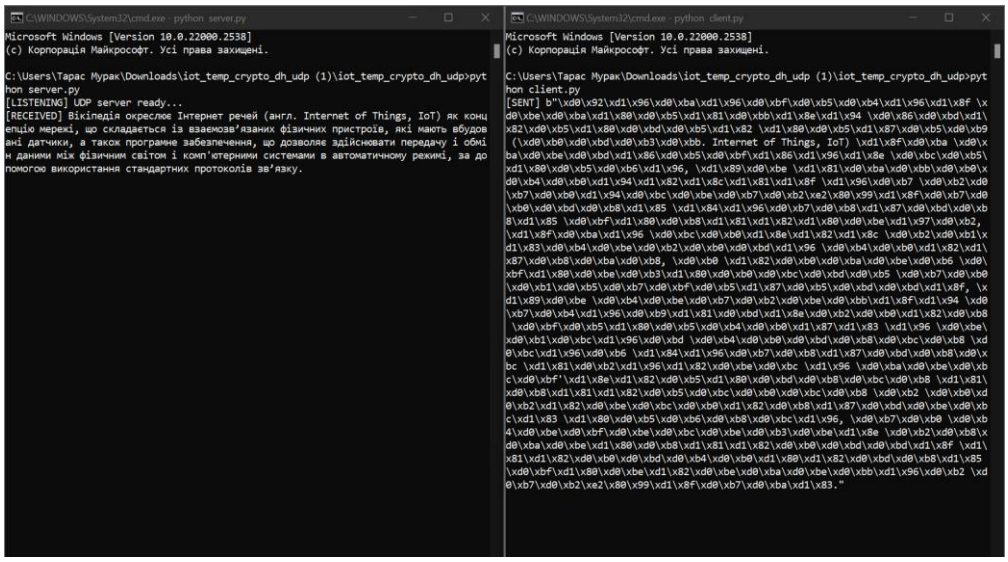

Рис. 6. Скріншот передавання зашифрованого повідомлення від клієнта серверу

Для наочності було захоплено UDP-пакет, щоб побачити, що трафік справді зашифрований (рис. 7).

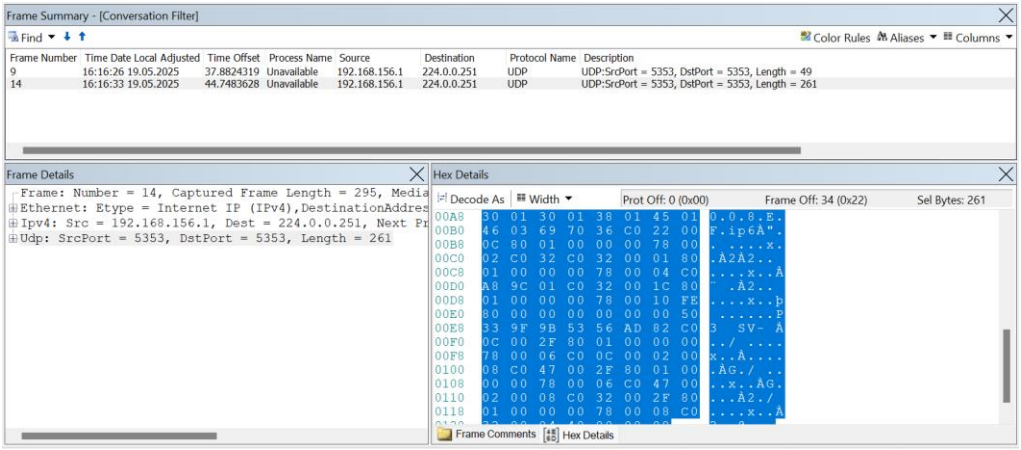

Рис. 7. Вміст перехопленого UDP-пакету

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проаналізовано архітектуру моделей Інтрнету речей від Міжнародного союзу електрозв'язку МСЕ-Т та Всесвітнього форуму IoT та розгорнуто модель IoT Cisco на рівні «архітектура — безпека». Запропоновано інтегральну модель безпеки IoT у просторі «різнорідні інтелектуальні об'єкти — багаторівнева безпека», яка спрямована на протидію ймовірним загрозам технологіями «виявлення — блокування — нейтралізації її» в режимі реального часу. Розроблено програмну реалізацію аутентифікованого шифрування даних на транспортному рівні запропонованої моделі IoT на основі: протоколу UDP, симетричного блокового алгоритму AES-256-GCM, мови програмування Python.

Запропонована інтегральна багаторівнева модель безпеки Інтернету речей може ефективно застосуватись для побудови комплексних систем безпеки за структурою «інтелектуальний об'єкт — архітектура IoT — загрози — технології безпеки».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Association of Industrial Automation Enterprises of Ukraine. (2018). *Industry 4.0 development strategy*. https://mautic.appau.org.ua/asset/42:strategia-rozvitku-4-0-v3.pdf
2. EU Agency for Cybersecurity. (2021). *International strategy of the EU Agency for Cybersecurity*. https://www.enisa.europa.eu/sites/default/files/all_files/2022-02-16%20ENISA%20International%20Strategy.pdf
3. National Security and Defense Council of Ukraine. (2021). *Cybersecurity Strategy of Ukraine for 2021–2025*.
4. Bobalo, Yu. Ya., Dudykevych, V. B., & Mykytyn, H. V. (2020). *Strategic security of the "object – information technology" system.* National University "Lviv Polytechnic".
5. Hategekimana, F., Whitaker, T. J. L., Pantho, M. J. H., & Bobda, C. (2020). IoT device security through dynamic hardware isolation with cloud-based update. *Journal of Systems Architecture, 109, 101827.* https://doi.org/10.1016/j.sysarc.2020.101827
6. Omar, A. H. E., Soubra, H., Moulla, D. K., & Abran, A. (2024). An innovative honeypot architecture for detecting and mitigating hardware Trojans in IoT devices. *IoT, 5(4),* 730–755. https://doi.org/10.3390/iot5040033
7. Aung, P. P., Aslam, S., & Chong, C. W. (2024). PUF-based lightweight security subsystems for IoT hardware: A concept. *In: Selected Proceedings from the 2nd International Conference on Intelligent Manufacturing and Robotics, ICIMR 2024, Lecture Notes in Networks and Systems, vol. 1316.* Springer. https://doi.org/10.1007/978-981-96-3949-6_31
8. Jasim, W. A., Kwyja, Y. M., Al-Mfarji, A. M. F., & Mohammed, M. (2024). An exhaustive examination of architectural methods for hardware security mechanisms in IoT devices. *Radioelectronics, Nanosystems, Information Technologies, 16(5),* 643–656. https://doi.org/10.17725/j.rensit.2024.16.643
9. Cano Quiveu, G., Ruiz-de-Clavijo-Vázquez, P., & Bellido, M. J. (2021). Embedded LUKS (E-LUKS): A hardware solution to IoT security. *Electronics, 10(23),* 3036. https://doi.org/10.3390/electronics10233036
10. Elmaghbub, A., & Hamdaoui, B. (2024). Domain-agnostic hardware fingerprinting-based device identifier for zero-trust IoT security. *IEEE Wireless Communications, 31(2),* 42–48. https://doi.org/10.1109/MWC.001.2300420
11. Bharathi, R., & Parvatham, N. (2020). Hardware-based physical layer security solutions and algorithms for IoT devices on FPGA platform. *International Journal of Innovative Technology and Exploring Engineering, 9(3),* 2128–2132. https://doi.org/10.35940/ijitee.C8752.019320
12. Rozlomii, I. O., Symoniuk, V. P., Naumenko, S. V., & Mykhailovskyi, P. V. (2024). Security model of interconnected computing devices based on a lightweight encryption scheme for IoT. *Computer-Integrated Technologies: Education, Science, Production, 55,* 191–198. https://doi.org/10.36910/6775-2524-0560-2024-55-24
13. Tymenko, A. V., Shkarupylo, V. V., & Smolii, V. V. (2020). Neural network model for controlling hardware compatibility of IoT system components. *Bulletin of Zaporizhzhia National University. Physical and Mathematical Sciences, (2),* 52–59. https://doi.org/10.26661/2413-6549-2020-2-07
14. Yevdokymov, S. O. (2025). Modeling threats and developing security strategies for protecting IoT railway networks. *Information Technologies and Computer Engineering. Scientific Works of VNTU, (1),* 37–45. http://dx.doi.org/10.31649/2307-5376-2025-1-37-45
15. Lohutova, O., & Belei, O. (2019). Data transmission security for the Internet of Things. *Cybersecurity: Education, Science, Technology, 2(6),* 18. https://doi.org/10.28925/2663-4023.2019.6.618
16. Samoylenko, M. (2020). Security issues in the implementation practice of Internet of Things technology. *Computer-Integrated Technologies: Education, Science, Production, (41),* 198–204. https://doi.org/10.36910/6775-2524-0560-2020-41-31
17. ITU, Telecommunication Standardization Sector of. (2012). *Overview of the Internet of Things (Recommendation ITU-T Y.2060).* International Telecommunication Union. https://www.itu.int/rec/T-REC-Y.2060
18. Zhurakovskyi, B. Yu., & Zeniv, I. O. (2021). *Internet of Things technologies.* Igor Sikorsky Kyiv Polytechnic Institute.
19. ITU, Telecommunication Standardization Sector. (2019). *Architectural reference models of devices for Internet of Things applications (Recommendation ITU-T Y.4460).* International Telecommunication Union. https://www.itu.int/rec/T-REC-Y.4460
20. Cisco Systems. (2014). *The Internet of Things reference model.* https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf

21. Dasgupta, D., Roy, A., & Nag, A. (2017). Continuous Authentication. *In: Advances in User Authentication. Infosys Science Foundation Series().* Springer, Cham, 185-233. https://doi.org/10.1007/978-3-319-58808-7_6

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Valerii Dudykevych
Doctor of Technical Sciences, Professor
Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0001-8827-9920
valerii.b.dudykevych@lpnu.ua

Halyna Mykytyn
Doctor of Technical Sciences, Professor
Professor of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-4275-8285
halyna.v.mykytyn@lpnu.ua

Taras Murak
Master's Student at the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0005-7588-9945
taras.murak.mkbst.2024@lpnu.ua

INTEGRAL MODEL OF INTERNET OF THINGS SECURITY IN THE SPACE OF INFRASTRUCTURE OBJECTS' INTELLECTUALIZATION

Abstract. The article explores the issues of architecture models and security in the Internet of Things (IoT) within the context of the intellectualization of societal infrastructure objects. An analytical review of well-known methodologies and models for developing IoT architecture and establishing approaches to ensuring their security is conducted. The classical reference IoT architecture model by the International Telecommunication Union (ITU-T), based on Recommendation Y.2060, is elaborated. This model is structured into components within the functional domain and the environment of management and security. The first layer of the ITU-T reference architecture model is analyzed — the device network, which functionally interacts with physical objects in the smart environment at the level of data collection and transmission. The architecture of the seven-layer reference model by the IoT World Forum is described, featuring such functions as data analysis based on criteria, data formatting, cryptographic data processing, data reduction, and data evaluation based on threshold values. The IoT security model based on the Cisco architecture is considered, reflecting the relationship within the "IoT architecture — security" space at the level of the "IoT functioning — protection" structure. Based on the Cisco security model, an integrated multi-level IoT security model is developed for a wide range of industrial infrastructure objects, including critical ones. This model follows the structure "IoT architecture — threats — security methods — protection technologies" and is deployed at levels of authentication, authorization, encryption, trust management, network policy, security analytics, and threat prediction through corresponding algorithms and protection technologies for all components of the IoT ecosystem. Algorithmic and software tools for cryptographic data exchange protection are developed, based on the symmetric block authenticated encryption algorithm AES-256-GCM, implemented in the Python programming language as a practical realization of the integrated IoT security model at the OpenVPN protocol level using UDP technology.

Keywords: intellectualization of objects; Internet of Things architecture; security models; integrated multi-level model; authentication; data encryption; symmetric block algorithm.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Association of Industrial Automation Enterprises of Ukraine. (2018). *Industry 4.0 development strategy*. https://mautic.appau.org.ua/asset/42:strategia-rozvitku-4-0-v3.pdf
2. EU Agency for Cybersecurity. (2021). *International strategy of the EU Agency for Cybersecurity*. https://www.enisa.europa.eu/sites/default/files/all_files/2022-02-16%20ENISA%20International%20Strategy.pdf

3. National Security and Defense Council of Ukraine. (2021). *Cybersecurity Strategy of Ukraine for 2021–2025*.
4. Bobalo, Yu. Ya., Dudykevych, V. B., & Mykytyn, H. V. (2020). *Strategic security of the "object – information technology" system.* National University "Lviv Polytechnic".
5. Hategekimana, F., Whitaker, T. J. L., Pantho, M. J. H., & Bobda, C. (2020). IoT device security through dynamic hardware isolation with cloud-based update. *Journal of Systems Architecture, 109, 101827.* https://doi.org/10.1016/j.sysarc.2020.101827
6. Omar, A. H. E., Soubra, H., Moulla, D. K., & Abran, A. (2024). An innovative honeypot architecture for detecting and mitigating hardware Trojans in IoT devices. *IoT, 5(4),* 730–755. https://doi.org/10.3390/iot5040033
7. Aung, P. P., Aslam, S., & Chong, C. W. (2024). PUF-based lightweight security subsystems for IoT hardware: A concept. *In: Selected Proceedings from the 2nd International Conference on Intelligent Manufacturing and Robotics, ICIMR 2024, Lecture Notes in Networks and Systems, vol. 1316.* Springer. https://doi.org/10.1007/978-981-96-3949-6_31
8. Jasim, W. A., Kwyja, Y. M., Al-Mfarji, A. M. F., & Mohammed, M. (2024). An exhaustive examination of architectural methods for hardware security mechanisms in IoT devices. *Radioelectronics, Nanosystems, Information Technologies, 16(5),* 643–656. https://doi.org/10.17725/j.rensit.2024.16.643
9. Cano Quiveu, G., Ruiz-de-Clavijo-Vázquez, P., & Bellido, M. J. (2021). Embedded LUKS (E-LUKS): A hardware solution to IoT security. *Electronics, 10(23),* 3036. https://doi.org/10.3390/electronics10233036
10. Elmaghbub, A., & Hamdaoui, B. (2024). Domain-agnostic hardware fingerprinting-based device identifier for zero-trust IoT security. *IEEE Wireless Communications, 31(2),* 42–48. https://doi.org/10.1109/MWC.001.2300420
11. Bharathi, R., & Parvatham, N. (2020). Hardware-based physical layer security solutions and algorithms for IoT devices on FPGA platform. *International Journal of Innovative Technology and Exploring Engineering, 9(3),* 2128–2132. https://doi.org/10.35940/ijitee.C8752.019320
12. Rozlomii, I. O., Symoniuk, V. P., Naumenko, S. V., & Mykhailovskyi, P. V. (2024). Security model of interconnected computing devices based on a lightweight encryption scheme for IoT. *Computer-Integrated Technologies: Education, Science, Production, 55,* 191–198. https://doi.org/10.36910/6775-2524-0560-2024-55-24
13. Tymenko, A. V., Shkarupylo, V. V., & Smolii, V. V. (2020). Neural network model for controlling hardware compatibility of IoT system components. *Bulletin of Zaporizhzhia National University. Physical and Mathematical Sciences, (2),* 52–59. https://doi.org/10.26661/2413-6549-2020-2-07
14. Yevdokymov, S. O. (2025). Modeling threats and developing security strategies for protecting IoT railway networks. *Information Technologies and Computer Engineering. Scientific Works of VNTU, (1),* 37–45. http://dx.doi.org/10.31649/2307-5376-2025-1-37-45
15. Lohutova, O., & Belei, O. (2019). Data transmission security for the Internet of Things. *Cybersecurity: Education, Science, Technology, 2(6),* 18. https://doi.org/10.28925/2663-4023.2019.6.618
16. Samoylenko, M. (2020). Security issues in the implementation practice of Internet of Things technology. *Computer-Integrated Technologies: Education, Science, Production, (41),* 198–204. https://doi.org/10.36910/6775-2524-0560-2020-41-31
17. ITU, Telecommunication Standardization Sector of. (2012). *Overview of the Internet of Things (Recommendation ITU-T Y.2060).* International Telecommunication Union. https://www.itu.int/rec/T-REC-Y.2060
18. Zhurakovskyi, B. Yu., & Zeniv, I. O. (2021). *Internet of Things technologies.* Igor Sikorsky Kyiv Polytechnic Institute.
19. ITU, Telecommunication Standardization Sector. (2019). *Architectural reference models of devices for Internet of Things applications (Recommendation ITU-T Y.4460).* International Telecommunication Union. https://www.itu.int/rec/T-REC-Y.4460
20. Cisco Systems. (2014). *The Internet of Things reference model.* https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf
21. Dasgupta, D., Roy, A., & Nag, A. (2017). Continuous Authentication. *In: Advances in User Authentication. Infosys Science Foundation Series().* Springer, Cham, 185-233. https://doi.org/10.1007/978-3-319-58808-7_6