https://doi.org/10.31891/2219-9365-2025-81-56
УДК 004.056:621.317.3:342.738

БУНЯК Віталій
Вінницький національний технічний університет
https://orcid.org/0009–0001–3326–6855
e–mail: vetalbunjak@gmail.com
ЛУКІЧОВ Віталій
Вінницький національний технічний університет
https://orcid.org/0000-0002-3423-5436
e–mail: lukichov.vitalyi@vntu.edu.ua

ЗАХИСТ ДАНИХ У СИСТЕМАХ ОБЛІКУ ЛІЧИЛЬНИКІВ. СУЧАСНІ ТЕХНОЛОГІЇ БЕЗПЕКИ ТА ІНТЕГРАЦІЯ «ДІЇ»

У статті розглядаються сучасні підходи до захисту даних у системах автоматизованого обліку споживання енергоресурсів з акцентом на інтеграцію державних цифрових сервісів, зокрема мобільного застосунку «Дія». Автори аналізують архітектурні рішення, рекомендовані стандартами NIST, та досліджують механізми автентифікації, криптографічного захисту і безпечної передачі інформації, що гарантують конфіденційність, цілісність і доступність даних. У роботі докладно розглянуто можливості впровадження технологій LPWAN, таких як LoRaWAN, як економічно ефективної альтернативи стільниковим мережам для реалізації систем автоматизованого обліку. Особлива увага приділяється оптимізації витрат в українських умовах, де фінансові та інфраструктурні обмеження вимагають застосування адаптивних рішень і гібридних моделей збору даних, що дозволяють мінімізувати операційні витрати без шкоди для безпеки.

Запропоновано використання платформи «Дія» як засобу автентифікації та централізованого контролю доступу до критично важливої інформації. Аналіз практичних кейсів і наукових досліджень дозволяє виокремити основні виклики кібербезпеки, зокрема ризики атак «людина посередині», підробки даних та DoS–атак. У статті наведено рекомендації щодо посилення захисту через впровадження сучасних протоколів шифрування, регулярного аудиту систем і використання резервних каналів передачі даних. Впровадження комплексних заходів дозволить знизити ймовірність успішних кібератак і мінімізувати фінансові та репутаційні збитки. Це сприятиме підвищенню рівня довіри як споживачів, так і державних органів до системи автоматизованого обліку. Крім того, застосування інноваційних технологій забезпечить гнучкість та адаптивність системи до швидко змінюваних кіберзагроз.

Дослідження підкреслює значущість інтеграції державних цифрових сервісів у систему розумного обліку як інструменту модернізації інфраструктури енергетики, підвищення ефективності управління ресурсами та зміцнення довіри споживачів до цифрових технологій. Запропоновані стратегії дозволяють адаптувати міжнародні стандарти до специфіки ринку України, забезпечуючи баланс між високими вимогами до безпеки та економічною доцільністю впровадження інноваційних рішень.

Ключові слова: цифрові сервіси, автоматизований облік, розумні лічильники, NIST, кібербезпека, приватність, «Дія», автентифікація, оптимізація, LPWAN.

BUNIAK Vitalii, LUKICHOV Vitalii
Vinnytsia National Technical University

DATA PROTECTION IN METER METERING SYSTEMS. MODERN SECURITY TECHNOLOGIES AND INTEGRATION OF “DIIA”

This article discusses modern approaches to data protection in automated energy consumption metering systems with a focus on the integration of government digital services, including the Diia mobile application. The authors analyze the architectural solutions recommended by NIST standards and explore the mechanisms of authentication, cryptographic protection, and secure data transmission that guarantee the confidentiality, integrity, and availability of data. The paper discusses in detail the possibilities of implementing LPWAN technologies, such as LoRaWAN, as a cost–effective alternative to cellular networks for the implementation of automated metering systems. Particular attention is paid to cost optimization in the Ukrainian environment, where financial and infrastructure constraints require the use of adaptive solutions and hybrid data collection models that minimize operating costs without compromising security.

The author proposes to use the Diia platform as a means of authentication and centralized control of access to critical information. The analysis of practical cases and scientific research allows us to identify the main challenges of cybersecurity, in particular the risks of man–in–the–middle attacks, data forgery and DoS attacks. The article provides recommendations for strengthening protection through the implementation of modern encryption protocols, regular system audits, and the use of redundant data transmission channels. Implementation of comprehensive measures will reduce the likelihood of successful cyberattacks and minimize financial and reputational losses. This will help increase the level of trust of both consumers and government agencies in the automated metering system. In addition, the use of innovative technologies will ensure the system's flexibility and adaptability to rapidly changing cyber threats.

The study emphasizes the importance of integrating public digital services into the smart metering system as a tool for modernizing energy infrastructure, improving resource management efficiency, and strengthening consumer confidence in digital technologies. The proposed strategies make it possible to adapt international standards to the specifics of the Ukrainian market, ensuring a balance between high security requirements and the economic feasibility of implementing innovative solutions.

Keywords: digital services, automated metering, smart meters, NIST, cybersecurity, privacy, Diia, authentication, optimization, LPWAN.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У всьому світі триває перехід до автоматизованого обліку споживання енергоресурсів. Традиційні лічильники поступово замінюються на «розумні» — такі, що здатні самостійно збирати й передавати дані про споживання через бездротові мережі (GSM, NB–IoT, LoRaWAN тощо). Станом на кінець 2023 року у світі встановлено понад 1,06 млрд розумних лічильників електрики, газу й води, і ця кількість стрімко зростає. В майбутньому очікується, що всі показники лічильників передаватимуться автоматично, без участі людини, використовуючи мережі стільникового зв'язку або технології далекого радіозв'язку малого енергоспоживання.

Автоматизація обліку має очевидні переваги – зручність для споживачів і постачальників, зниження операційних витрат, можливість оперативного моніторингу мереж. Водночас виникають і виклики, головним серед яких є безпека та приватність даних. Детальні дані про споживання енергії можуть містити чутливу інформацію про поведінку користувачів. За профілем електроспоживання можна зробити висновки про розпорядок дня сім'ї, наявність людей у приміщенні, типи пристроїв, що використовуються тощо. Тому питання забезпечення конфіденційності цих даних є надзвичайно актуальним.

З погляду кібербезпеки важливо дотримуватись класичної тріади CIA (Confidentiality, Integrity, Availability): конфіденційність (захист даних від несанкціонованого доступу), цілісність (недопущення несанкціонованих змін інформації) та доступність (безперебійний доступ авторизованих користувачів до даних). Додатковими критеріями, важливими саме для систем обліку споживання, є автентифікація пристроїв і користувачів, а також контроль цілісності повідомлень, що унеможливлює втручання в інформацію під час передачі.

Приватність у контексті систем обліку означає можливість контролю користувачем процесу збору, використання та поширення його персональних даних. Вимоги до надійності включають мінімізацію збоїв, захист від атак і забезпечення точності обліку. Особливу увагу слід приділити проблемі зв'язуваності (linkability) персональних даних (PII), коли зібрана інформація може бути використана для ідентифікації або створення профілів користувачів без їх згоди.

У цій статті розглянуто можливості інтеграції державних цифрових сервісів України, зокрема застосунку «Дія», у систему обліку споживання ресурсів, з акцентом на забезпеченні приватності даних користувачів. Спочатку проведено огляд типових схем підключення розумних лічильників (за рекомендаціями NIST), далі проаналізовано відомі дослідження щодо їх безпеки. Окремо обговорено українські реалії впровадження таких систем та можливі оптимізації. Основна увага приділяється потенціалу застосунку «Дія» як інструменту для автентифікації, а також питанню його ролі у критичній інфраструктурі.

ОГЛЯД СХЕМ ПІДКЛЮЧЕННЯ ЗГІДНО З NIST

Розумні лічильники зазвичай інтегруються у так звану інфраструктуру розумного обліку (Advanced Metering Infrastructure, AMI) – комплекс, що включає самі лічильники, мережі передачі даних та системи управління даними у постачальника послуг. Відповідно до рекомендацій Національного інституту стандартів і технологій США (NIST), існують різні схеми підключення лічильників у мережу, але всі вони мають забезпечувати надійну двосторонню передачу даних та взаємодію за стандартами. NIST у своїх стандартах робить акцент на дотриманні відкритих протоколів та вимог безпеки при підключенні пристроїв. Зокрема, у рамках NIST Smart Grid концептуально виділено сім доменів (генерація, передача, розподіл, споживачі, оператори, ринки, сервіс–провайдери), між якими відбувається обмін інформацією, і системи AMI відіграють ключову роль у сегменті «споживач–оператор» [2]. Це означає, що лічильник повинен безпечно передавати дані постачальнику (оператору) і, за потреби, отримувати команди (наприклад, щодо тарифів або відключення).

Типова архітектура AMI передбачає, що розумні лічильники можуть передавати дані або безпосередньо до центру обробки через широкомасштабну мережу, або через проміжні шлюзи–концентратори. У першому випадку кожен лічильник оснащується модулем стільникового зв'язку (2G/3G/4G, нині часто LTE Cat M або NB–IoT) і надсилає дані прямо на сервери обліку. У другому випадку використовується локальна мережа – кілька десятків чи сотень лічильників у районі з'єднуються з близьким шлюзом (наприклад, по радіоканалу короткого радіусу або через електромережу PLC), а вже шлюз агрегує ці дані і пересилає їх далі до хмарної платформи обліку. Як правило, більшість сучасних рішень тяжіють до другого варіанту – наявність проміжного концентратора дозволяє використовувати простіші й дешевші пристрої–лічильники, що не потребують потужних передавачів великої дальності [1]. На рис. 1 показано узагальнену схему такої багаторівневої архітектури: лічильники збирають дані, передають їх на шлюз, який пересилає інформацію у хмарне середовище провайдера, де вона аналізується та надається користувачам у вигляді зручних додатків або веб–порталів. Проте зловмисник може втрутитися між лічильниками та шлюзом, підміняючи показники, або перехопити дані між шлюзом і хмарою через атаку Man–in–the–Middle. Також можливий злом серверного додатка, що дасть доступ до всієї системи.

ISSN 2219-9365

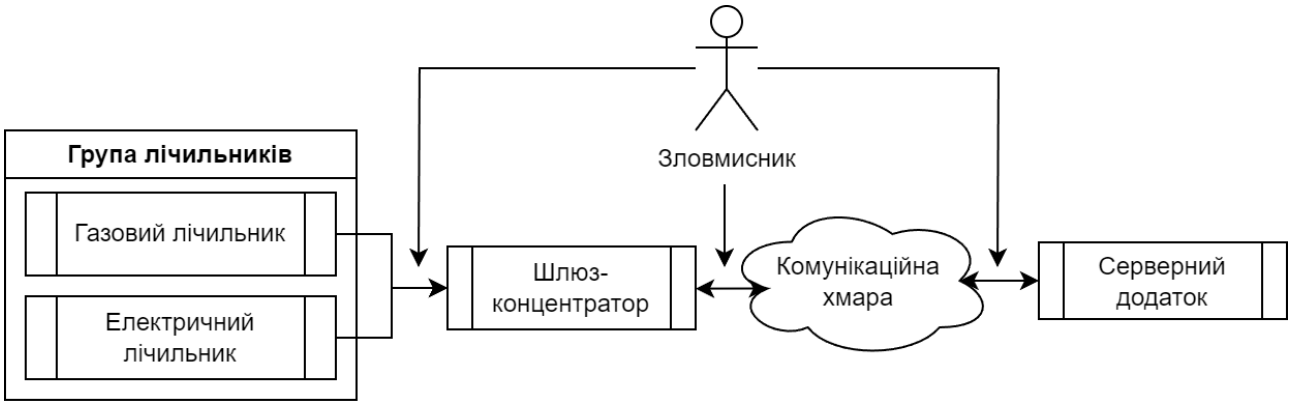

Рис. 1. Типова архітектура системи розумного обліку

Для зв'язку між лічильниками та шлюзами, а також шлюзами і центральною системою, застосовуються різні технології. NIST класифікує їх як дротові та бездротові. Серед дротових рішень традиційними є PLC або виділені канали зв'язку в будівлях. Бездротові рішення поділяються на ті, що працюють у ліцензованих частотних діапазонах (стільникові технології), і безліцензійні. Стільниковий підхід (GSM/3G/4G) забезпечує покриття майже всюди, але може включати значні операційні витрати (SIM–карти, тарифи передачі даних) та залежність від операторів зв'язку. Альтернативою стали LPWAN (Low–Power Wide–Area Network) технології у вільних діапазонах – зокрема, LoRaWAN, Sigfox. NIST дослідив низку таких технологій і відзначив, що LoRaWAN як відкрита технологія з вбудованими засобами безпеки є привабливим вибором для локального розгортання автономної мережі збору даних. Наприклад, LoRaWAN працює в суб–ГГц діапазоні, має дальність у кілька кілометрів, підтримує наскрізне шифрування даних і не потребує підключення до Інтернету для функціонування мережі. Це дозволяє утворити приватну мережу обліку, контрольовану самим підприємством (наприклад, оператором розподілу енергії), що важливо з точки зору безпеки.

На рисунку 2 зображено багаторівневу схему підключення розумних лічильників, де газові й електричні прилади об'єднані в групу та передають дані на шлюз–концентратор за допомогою протоколів Modbus і LoRaWAN. Далі інформація надходить до комунікаційної хмари та серверного додатка через протокол MQTT. Такий підхід забезпечує гнучкість у виборі технологій зв'язку й дає змогу легко масштабувати систему залежно від потреб.

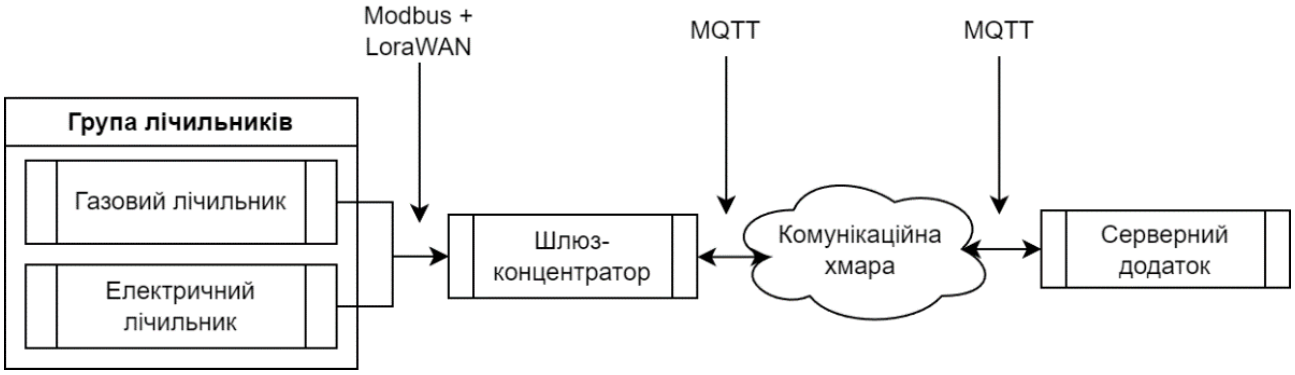

Рис. 2. Приклад архітектури системи обліку споживання

NIST наполягає на використанні відкритих стандартів у побудові AMI, щоб забезпечити інтероперабельність між різними виробниками обладнання. Зокрема, в каталозі стандартів для Smart Grid, опублікованому NIST, присутні вимоги NEMA SG–AMI 1–2009 (стандарт на модернізованість розумних лічильників), профілі протоколів зв'язку (наприклад, IEEE 802.15.4 для бездротових мереж лічильників, ZigBee Smart Energy Profile для домашніх пристроїв), стандарти обміну даними (IEC 62056 / DLMS, ANSI C12.22) тощо [6]. Керуючись цими стандартами, постачальники та комунальні підприємства можуть впроваджувати рішення, що відповідають критеріям безпеки та надійності. NIST також розробив керівництва з кібербезпеки для розумних мереж – зокрема, звіт NISTIR 7628 «Guidelines for Smart Grid Cyber Security», що містить рекомендації щодо архітектури безпеки, захисту комунікацій і приватності користувачів. У цих рекомендаціях наголошується на необхідності забезпечити конфіденційність переданих даних (шифрування), цілісність повідомлень (контроль цілісності, цифрові підписи) та автентифікацію пристроїв при кожному сеансі зв'язку. Таким чином, базові схеми підключення лічильників згідно з NIST включають багаторівневу

архітектуру збору даних (лічильник – локальний шлюз – центр), використання стандартизованих протоколів зв'язку та обов'язкове впровадження криптографічних методів захисту інформації на всіх етапах передачі і зберігання даних [12].

АНАЛІЗ ІСНУЮЧИХ ДОСЛІДЖЕНЬ ПРО СХЕМИ ПІДКЛЮЧЕННЯ NIST

Питання безпеки і приватності в системах обліку споживання привертає увагу наукової спільноти. Багато дослідників аналізували ефективність і вразливості схем, рекомендованих NIST, пропонуючи вдосконалення. Для прикладу стаття «Smart Metering Cybersecurity – Requirements, Methodology, and Testing» розглядає актуальні проблеми кібербезпеки в системах розумного вимірювання енергоспоживання, що є критично важливими в умовах зростаючої інтеграції «розумних мереж». Автори аналізують вимоги до захисту даних, розкривають специфіку сучасних кіберзагроз та підкреслюють необхідність створення комплексних методологій для виявлення та усунення вразливостей у мережах, що забезпечують обмін інформацією між споживачами та постачальниками енергії [12].

Стаття детально розглядає місткість питань кібербезпеки в системах розумного вимірювання, приділяючи особливу увагу аналізу стандартів, що застосовуються в галузі. Серед розглянутих стандартів автори зосереджуються на міжнародних та регіональних нормативних документах, зокрема IEC 62351, який встановлює вимоги щодо безпеки в електроенергетичних системах, а також стандартах, пов'язаних з управлінням інформаційною безпекою, таких як ISO/IEC 27001. Крім того, аналіз включає огляд рекомендацій, запропонованих у керівництвах NIST, що стосуються захисту критичної інфраструктури. Це дозволяє створити комплексну картину вимог до систем розумного вимірювання з точки зору захисту від кіберзагроз, ураховуючи специфіку протоколів обміну даними, методи шифрування та захист від несанкціонованого доступу.

Щодо висновків, дослідники приходять до думки, що забезпечення кібербезпеки в системах розумного вимірювання вимагає багаторівневого підходу, який поєднує технічні, методологічні та організаційні заходи. Особлива увага приділяється питанням приватності: розумні лічильники збирають детальну інформацію про споживання енергії, що може містити конфіденційні дані користувачів. Тому впровадження засад «приватності за замовчуванням» та використання сучасних методів шифрування і безпечних комунікацій є ключовими для збереження довіри споживачів і дотримання нормативних вимог [4].

Також було проведене масштабне дослідження відображене у стандартах NISTIR 7628 було оцінено експертами на предмет відповідності новим викликам. Чан (Aldar Chan) і Чжоу (Jianying Zhou) у своїй роботі відзначили, що керівництво NISTIR 7628 хоча і є всеосяжним, проте не містить детальних інструкцій для новітніх сценаріїв, таких як електромобілі [3].

При підключенні електромобіля до мережі виникають додаткові загрози приватності і безпеки, адже зарядна станція збирає персональні дані (ідентифікатор користувача, платіжну інформацію) та інформацію про місце і тривалість зарядки. Виявлено дві ключові прогалини NISTIR 7628: по–перше, розрив між кібер– і фізичною безпекою – стандарт розглядає їх окремо і не регламентує механізми перевірки відповідності даних реальним подіям, що потенційно відкриває шлях для скоординованих кібер–фізичних атак. По–друге, підхід NIST надто зосереджений на інтересах енергокомпаній і приділяє недостатньо уваги приватності кінцевих користувачів в нових умовах. Зокрема, питання приватності водіїв електромобілів практично не розкрито – хоча сам стандарт застерігає щодо приватності споживачів електроенергії, дані про пересування та зарядку автомобілів уразливі. Таким чином, дослідники звертають увагу, що з появою нових технологій потрібне оновлення схем підключення і політик безпеки [2].

Таблиця 1.

Типові вразливості розумних лічильників згідно класифікації CWE (MITRE)

№ CWE	Назва уразливості	Опис у контексті розумних лічильників
CWE–798	Використання жорстко прописаних облікових даних	Лічильники можуть використовувати вбудовані паролі, які легко виявити та використати зловмисниками.
CWE–284	Неправильний контроль доступу	Недостатньо жорсткий контроль, що дозволяє несанкціонований доступ до даних споживання.
CWE–319	Незахищена передача чутливої інформації	Передача даних без належного шифрування може призвести до перехоплення інформації про споживачів.
CWE–330	Використання недостатньо надійного алгоритму генерації випадкових чисел	Погана реалізація криптографічних функцій дозволяє легко зламати шифрування, що веде до компрометації даних.
CWE–400	Неконтрольоване споживання ресурсів	Вразливість, що дозволяє зловмисникам перевантажити лічильники, спричинивши відмову в обслуговуванні (DoS).
CWE–306	Відсутність автентифікації при критичних функціях	Лічильники без автентифікації можуть дозволити несанкціоноване керування або зміну показників.
CWE–311	Відсутність шифрування чутливої інформації	Дані, що передаються у відкритому вигляді, можуть бути легко викрадені й використані для порушення приватності.
CWE–522	Недостатній захист конфіденційних даних	Дані можуть зберігатися у незахищеному вигляді, що робить їх вразливими до витоків.

На основі виявлених недоліків Chan та Zhou запропонували низку поліпшень до типової схеми підключення згідно з NIST. Зокрема, йдеться про протокол прив'язки кібер–ідентичності до фізичного пристрою – щоб гарантувати, що дані в системі точно відповідають конкретному реальному об'єкту (наприклад, електромобілю). Це унеможливить ситуації, коли зловмисник міг би подавати фальшиві дані або заряджати крадений автомобіль, обходячи авторизацію. Також пропонується удосконалити механізми аутентифікації користувачів і пристроїв (наприклад, подвійна автентифікація для доступу до зарядної мережі) та впровадити гнучкі рішення для захисту геолокаційних даних, що балансують приватність і відповідальність. Останнє означає, що дані про місцеперебування користувача (наприклад, де і коли він заряджав авто) мають шифруватися і розкриватися лише за наявності обґрунтованої потреби, аби запобігти масовому стеженню [12].

Під час аналізу схем підключення, рекомендованих NIST, важливо враховувати потенційні уразливості, які можуть використовуватися для кібератак на інфраструктуру розумних лічильників (табл. 1). Це дозволяє систематизовано оцінювати ризики та розробляти заходи з їх усунення або пом'якшення.

На всіх етапах життєвого циклу розумних лічильників застосування стандартів класифікації вразливостей, зокрема CWE, дозволяє виявляти та мінімізувати ризики. На етапі встановлення особлива увага приділяється безпечній конфігурації пристроїв, де помилки налаштувань або використання жорстко прописаних облікових даних (CWE–798) можуть стати критичними уразливостями. Під час експлуатації важливо впроваджувати регулярний моніторинг, аудит безпеки та оновлення програмного забезпечення для запобігання таким проблемам, як неправильний контроль доступу (CWE–284) або незахищена передача даних (CWE–319). Нарешті, на етапі утилізації потрібно забезпечити безпечну обробку та знищення даних, адже неналежна утилізація може призвести до витоку конфіденційної інформації (CWE–522) та збереження залишкових вразливостей, що можуть бути експлуатовані [11].

Для комплексного аналізу безпеки важливо розуміти не лише уразливості, але й потенційні загрози, яким можуть піддаватися розумні лічильники. Перелік найтиповіших загроз на основі класифікації MITRE ATT&CK наведено у таблиці 2. Це дозволяє створити чітке уявлення про вектори можливих атак та сприяти розробці відповідних заходів протидії.

Таблиця 2.

Типові загрози для розумних лічильників згідно класифікації MITRE ATT&CK

ID техніки ATT&CK	Назва загрози	Опис у контексті розумних лічильників
T0880	Man–in–the–Middle (MITM)	Перехоплення та зміна даних при передачі між лічильником та сервером
T0803	Підміна ідентифікатора пристрою	Фальсифікація ідентифікаційних даних лічильника для введення в оману системи обліку
T0827	Порушення роботи комунікаційної мережі (DoS)	Атаки, що призводять до недоступності мережі обліку, порушення передачі показів
T0862	Підробка даних	Внесення неправдивих даних у систему для порушення точності обліку
T0846	Віддалене керування пристроями	Отримання несанкціонованого доступу з можливістю відключення або зміни режимів роботи лічильника
T0817	Збір інформації з пристроїв	Несанкціонований збір чутливої інформації (профіль споживання, стан пристрою) з метою її подальшого використання
T0891	Витік конфіденційної інформації	Несанкціонований доступ до персональних даних користувачів, які зберігаються або передаються лічильником
T0858	Експлуатація вразливостей	Використання відомих уразливостей для несанкціонованого доступу до лічильників

Інші дослідження також підтверджують важливість врахування приватності при побудові інфраструктури обліку. Вже згадуваний звіт NISTIR 7628 включає оцінку впливу на приватність (Privacy Impact Assessment), яка показала, що відсутність узгоджених політик приватності та стандартів у різних штатах і компаніях створює значні ризики [10]. Дані споживачів можуть зберігатися у багатьох місцях і передаватися через різні системи, що підвищує їхню вразливість до перехоплення чи випадкового витоку. Тому в наукових роботах пропонуються методи мінімізації обміну надто деталізованими даними – наприклад, агрегація (об'єднання показників кількох домогосподарств для аналітики, щоб ніхто не знав індивідуальних патернів) або диференційна приватність (додавання контрольованого шуму в дані споживання, щоб ускладнити ідентифікацію поведінки окремого користувача). Такі підходи можуть бути інтегровані у схеми підключення, рекомендовані NIST, щоб покращити приватність без суттєвого погіршення корисності даних для енергосистеми.

Отже, аналіз існуючих досліджень демонструє, що базові схеми NIST потребують гнучкого адаптування під нові реалії – з акцентом на поєднанні кібер– і фізичної безпеки та посиленому захисті приватності споживачів. Застосування цих висновків у практиці особливо важливе для країн, що тільки починають впровадження розумних мереж, аби одразу будувати систему обліку з врахуванням найкращих світових напрацювань.

ПРАКТИЧНІ ОБМЕЖЕННЯ ТА ОПТИМІЗАЦІЯ РІШЕНЬ

В Україні впровадження систем автоматизованого обліку споживання лише набирає обертів. Низка пілотних проектів з встановлення розумних лічильників електроенергії, газу та води вже реалізована, проте до масового розгортання поки далеко. Основною причиною є висока вартість сучасних підходів. Розгорнути повномасштабну AMI інфраструктуру – означає замінити мільйони лічильників, обладнати їх модулями зв'язку, налаштувати мережі передачі даних, створити центри обробки та захистити все це відповідно до стандартів. За оцінками, вартість одного розумного електролічильника зі встановленням може сягати $100 і більше; додатково слід врахувати витрати на мережеве обладнання (шлюзи LoRaWAN, базові станції, сервери) або оплату послуг операторів мобільного зв'язку. Для українських обленерго та комунальних підприємств такі інвестиції є суттєвими, особливо в нинішніх економічних умовах. Не дивно, що впровадження сучасних підходів здається дорогим для України, адже навіть у країнах ЄС проекти smart metering підлягають ретельному аналізу витрат і вигод. Наприклад, Євросоюз свого часу поставив ціль замінити 80% лічильників на розумні до 2020 року, але деякі держави відклали ці плани через недостатню економічну доцільність. В Україні ж досі значна частина споживачів використовує застарілі індукційні лічильники, а систематичний дистанційний збір показників відсутній [8].

Ще одним важливим фактором є платоспроможність населення. Враховуючи економічні реалії, значна частина громадян України може бути не в змозі самостійно профінансувати заміну старих лічильників на розумні. Для вирішення цієї проблеми держава започаткувала програму безкоштовної заміни лічильників, яка спрямована на підтримку вразливих категорій населення та покликана частково компенсувати фінансові витрати для громадян[14].

З погляду економічної доцільності, встановлення автоматичних лічильників є економічно вигіднішим у довгостроковій перспективі. Це дозволяє суттєво знизити витрати на обслуговування, мінімізувати людський фактор при передачі показників, оптимізувати споживання енергії та ефективніше балансувати навантаження в електромережі. Завдяки регулярному автоматичному збору даних можливо швидко реагувати на зміни навантаження та оперативно управляти ресурсами, забезпечуючи стабільність і надійність роботи електромереж.

Окрім вартості, є й інші українські реалії. Інфраструктура зв'язку в сільській місцевості або на околицях міст може бути слабкою – не всюди стабільно працює мобільний інтернет, що потрібен для GSM–модулів у лічильниках. Деякі будинки мають товсті стіни або знаходяться у підвалах, де сигнал поганий (проблема, актуальна і для західних країн, але там більше ресурсів на вирішення, наприклад, встановлення додаткових ретрансляторів). Населення також не однорідно сприймає нововведення – частина українців насторожено ставиться до «пристроїв, що стежать» і має побоювання щодо приватності. Це вимагає проведення роз'яснень та забезпечення прозорості процесів збору даних.

У таких умовах постає питання – як оптимізувати рішення для України, щоб зробити їх економічно доцільними і безпечними? Один з напрямів – використання альтернативних методів передачі даних, що знижують витрати. Наприклад, замість оснащення кожного лічильника дорогим GSM–модемом з SIM–картою, можна застосувати технологію LoRaWAN. Вона дозволяє одному шлюзу покривати тисячі пристроїв у радіусі кількох кілометрів, працює у безліцензійному діапазоні і забезпечує низькі капітальні витрати (CAPEX) та вартість володіння порівняно зі стільниковими рішеннями. В Україні вже є приклади використання LoRaWAN для обліку газу та води – зокрема, пілотні проекти «Кіровоградгазу» та інших компаній продемонстрували успішну передачу показників через мережу Інтернету речей. Такі рішення можуть масштабуватися дешевше, оскільки після встановлення мережі шлюзів комунальне підприємство уникає щомісячних платежів оператору і може обслуговувати велику кількість лічильників [5].

Інший аспект оптимізації – спрощення самих кінцевих пристроїв. Щоби зменшити вартість розумного лічильника, можна мінімізувати на ньому функції безпеки, переклавши частину завдань на рівень шлюзу чи серверу. Наприклад, лічильник може лише шифрувати дані за попередньо записаним ключем і передавати їх далі, а всю складну логіку (керування ключами, автентифікація) виконуватиме потужніший шлюз. Такий розподіл дозволяє застосувати дешевші мікроконтролери у лічильниках, водночас не поступаючись у захищеності системи – за умови, що мережа між лічильником і шлюзом теж захищена (наприклад, LoRaWAN вже має вбудоване шифрування на цьому етапі) [5].

Автоматизовані системи обліку споживання ресурсів можуть передавати покази з різною частотою – від щохвилинної до щомісячної. Частота передачі даних є критичною для оперативного балансування навантаження в електромережах. Передача показників раз на місяць є недостатньо ефективною для оперативного реагування на зміни в електромережах. Оптимальною є передача показників принаймні раз на день або частіше, наприклад, щогодини. Це дозволяє точніше прогнозувати і балансувати навантаження, знижуючи ризики перевантажень і збоїв в мережі.

Для України також актуальне питання – чи варто впроваджувати повністю автоматизовану передачу даних одразу, чи можлива гібридна модель на перехідний період. Одним з альтернативних підходів, які обговорюються, є використання смартфонів споживачів для збору даних. В нашій країні високий рівень проникнення смартфонів та Інтернету, особливо у міських жителів. Тому можна розглянути схему, коли

лічильник оснащений простим модулем ближнього радіозв'язку (наприклад, Bluetooth або NFC), а сам споживач раз на певний період підносить до нього смартфон, на якому спеціальний застосунок (можливо, навіть «Дія») зчитує дані і передає їх через інтернет. Такий підхід суттєво дешевший, адже забирає потребу в далекому модулі зв'язку в кожному лічильнику. Однак він не повністю автоматичний і залежить від дисциплінованості користувача (схожий недолік, як і у ручного введення показників через сайт чи SMS). Проте, як перехідне рішення для малозабезпечених регіонів або поки не створена мережа IoT, це має сенс.

З погляду економічної доцільності, дешевше використовувати автоматичні системи обліку, оскільки вони знижують витрати на обслуговування, зменшують помилки при передачі даних вручну, та забезпечують кращий баланс електромережі. Водночас, частота передачі даних має важливе значення. Передача показників раз на місяць не забезпечує оперативності балансування навантаження в електромережах. Рекомендована частота передачі даних – хоча б раз на день або навіть частіше для більш ефективного моніторингу і керування споживанням.

Важливим аспектом є також кібербезпека. За статистикою, у 2023 році кількість атак на smart meters у світі зросла на 17% порівняно з попереднім роком, зокрема, найбільш поширеними були атаки типу «Man–in–the–Middle» (38%), DoS–атаки (27%) та атаки з підробкою ідентифікаторів пристроїв (19%). Економічні збитки від таких атак можуть сягати десятків мільйонів доларів. Наприклад, у Європі зафіксовано випадок масштабної атаки, що спричинила збитки у розмірі 5 млн євро через перехоплення та підробку даних обліку [13].

Згідно з класифікацією CAPEC (Common Attack Pattern Enumeration and Classification), основні вектори атак на розумні лічильники включають:

- Атаки "Людина посередині" (Man–in–the–Middle, MITM) – зловмисник перехоплює та потенційно змінює дані, що передаються між лічильником і системою збору даних. Це може призвести до викривлення показників споживання або несанкціонованого доступу до конфіденційної інформації.
- Підробка ідентифікаторів пристроїв – атакуючий змінює або підробляє ідентифікаційні дані лічильника, вводячи систему в оману щодо справжності пристрою. Це може дозволити зловмиснику отримати несанкціонований доступ або маніпулювати даними обліку.
- Атаки типу "Відмова в обслуговуванні" (Denial–of–Service, DoS) – зловмисник перевантажує мережу або лічильник надмірною кількістю запитів, що може призвести до збоїв у роботі системи обліку та неможливості збору даних.
- Підробка даних (Data Forgery) – атакуючий вносить фальшиві дані в систему обліку, що може призвести до неправильного нарахування платежів або спотворення статистичних даних.
- Експлуатація вразливостей програмного забезпечення – зловмисник використовує відомі або нові вразливості в програмному забезпеченні лічильника для виконання несанкціонованих дій, таких як отримання доступу до системи або зміна її налаштувань.
- Фізичний доступ до пристрою – отримавши фізичний доступ до лічильника, зловмисник може модифікувати його апаратне забезпечення або підключитися до внутрішніх інтерфейсів для маніпуляції даними або налаштуваннями.

Розуміння цих векторів атак є критичним для розробки ефективних заходів безпеки та захисту інфраструктури розумних лічильників від потенційних загроз. Проте для кращого розуміння структури загроз для розумних лічильників, нижче представлено графік який створено за матеріалами звітів MITRE CAPEC та Enforcement Tracker (ETid–2077) [15]. Він ілюструє розподіл типів кібератак за 2023 рік. Як видно з графіка, найбільш поширеними є атаки типу Man–in–the–Middle (MITM), DoS–атаки та атаки з підміною ідентифікатора пристрою, що вимагає особливої уваги при розробці та впровадженні захисних механізмів (див. рис. 3).

Такі атаки можуть призвести до втрати конфіденційних даних, спотворення облікових показників та фінансових збитків як для споживачів, так і для постачальників. Крім того, вони здатні спричинити відмову у наданні послуг, підірвати довіру до системи та ускладнити процеси планування й балансування енергоресурсів.

Прикладом реального інциденту з порушенням безпеки таких систем стала масштабна кібератака в Швеції у 2023 році, яка відбулася через незахищену передачу даних з розумних лічильників. Зловмисники здійснили атаку типу Man–in–the–Middle (MITM), під час якої перехоплювали і змінювали інформацію, що передавалася від лічильників до серверів компанії–оператора. В результаті дані про споживання електроенергії були суттєво спотворені, що призвело до неправильного нарахування вартості енергії для користувачів.

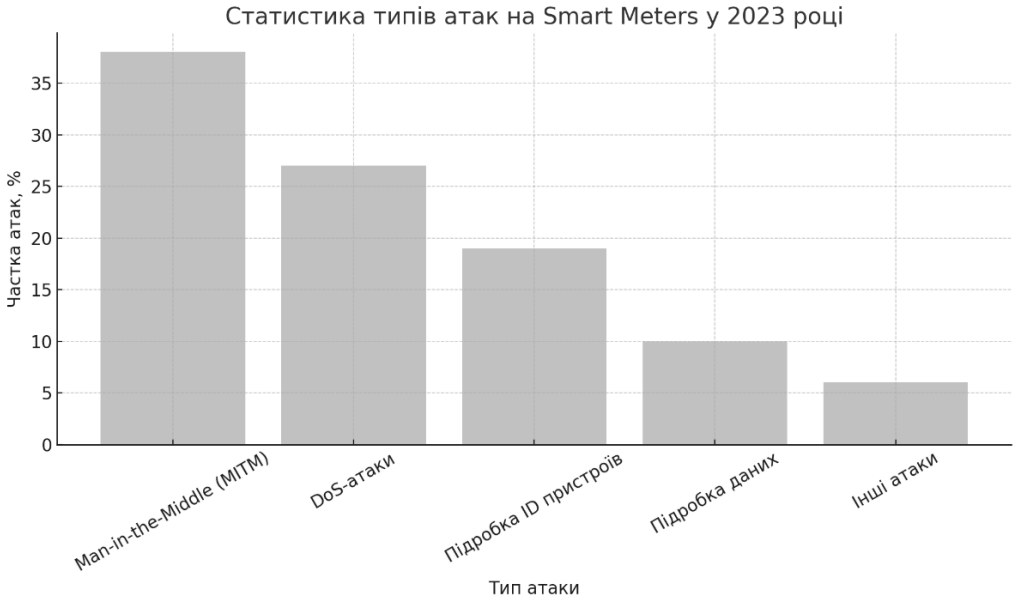

Рис. 3. Статистика типів атак на розумні лічильники за 2023 рік

Такі атаки можуть призвести до втрати конфіденційних даних, спотворення облікових показників та фінансових збитків як для споживачів, так і для постачальників. Крім того, вони здатні спричинити відмову у наданні послуг, підірвати довіру до системи та ускладнити процеси планування й балансування енергоресурсів.

Прикладом реального інциденту з порушенням безпеки таких систем стала масштабна кібератака в Швеції у 2023 році, яка відбулася через незахищену передачу даних з розумних лічильників. Зловмисники здійснили атаку типу Man–in–the–Middle (MITM), під час якої перехоплювали і змінювали інформацію, що передавалася від лічильників до серверів компанії–оператора. В результаті дані про споживання електроенергії були суттєво спотворені, що призвело до неправильного нарахування вартості енергії для користувачів.

Причинами інциденту були недостатні заходи автентифікації та використання незахищених каналів передачі даних. Після розслідування інциденту компанію–оператора було оштрафовано регулятором ЄС за порушення правил захисту персональних даних (GDPR) на суму понад 5 мільйонів євро. Окрім фінансових збитків, оператор зазнав значних репутаційних втрат, оскільки довіра клієнтів і партнерів була суттєво підірвана. Також компанія понесла додаткові витрати на посилення заходів кібербезпеки, впровадження нових протоколів шифрування та оновлення обладнання.

Цей випадок підкреслює важливість дотримання рекомендацій таких стандартів, як NISTIR 7628, які наголошують на необхідності регулярного оновлення протоколів автентифікації, шифрування передачі даних та впровадження багаторівневих механізмів захисту для запобігання подібним атакам [13].

Щодо методів захисту в таких оптимізованих рішеннях – вони теж можуть бути адаптовані під бюджетні реалії. Наприклад, замість впровадження складної інфраструктури PKI для видачі сертифікатів кожному лічильнику (що дорого й потребує кадрових ресурсів), можна використати колективні ключі шифрування на рівні підмережі або захищені канали оператора. Багато українських енергокомпаній вже зараз передають дані телеметрії через закриті APN мобільних операторів (віртуальні приватні мережі) – такий канал вважається достатньо захищеним від зовнішнього втручання, хоч і менш гнучким, ніж повноцінне кінцеве шифрування. У майбутньому, коли з’явиться більше ресурсів, ці рішення можна буде замінити на більш досконалі, але на перших етапах вони дозволяють скоротити витрати і час впровадження [5].

У таблиці 3 систематизовано основні заходи протидії ключовим кібератакам у системах розумного обліку. Таблиця містить опис застосовуваних методів захисту разом з орієнтовними витратами на їх впровадження. Такий підхід дозволяє оцінити не лише технічну ефективність, а й економічну доцільність кожного з заходів, що особливо актуально з урахуванням бюджетних обмежень в Україні.

Підсумовуючи, українські реалії вимагають компромісу між ідеальною моделлю і практично можливим. Сучасні схеми NIST задають високий стандарт безпеки, але для нашої країни критично знайти економічно збалансований підхід. Оптимізація може включати: використання дешевших технологій зв’язку (LPWAN), максимальне залучення існуючих інфраструктур (мобільний зв’язок, смартфони), поетапне впровадження (спершу – у великих містах та для промислових споживачів, пізніше – для населення), а також адаптацію рівня захисту під актуальні загрози.

Таблиця 3.

Заходи протидії кібератакам у системах розумного обліку

Назва атаки	Пропоновані протидії	Орієнтовна вартість протидії
Man–in–the–Middle (MITM)	– Використання сучасних протоколів шифрування (TLS, AES) – Взаємна аутентифікація пристроїв – Сертифікатне управління та перевірка цілісності	Невисока–середня (може варіюватися від $10 до $100 на пристрій або як частина ПЗ)
Підміна ідентифікатора пристрою	– Захищене завантаження (secure boot) – Використання апаратних модулів безпеки (TPM, HSM) – Цифровий підпис і апаратна автентифікація	Середня (залежно від апаратного забезпечення; можлива інтеграція в процес виробництва)
Атаки типу DoS (відмова в обслуговуванні)	– Впровадження систем захисту від DoS (аналітика трафіку, фільтрація запитів) – Розподіл навантаження та резервування мережевих ресурсів	Відносно висока (від $100 до $1000 на місяць для спеціалізованих анти–DDoS сервісів)
Підробка даних	– Використання цифрових підписів та HMAC для забезпечення цілісності – Регулярний аудит даних та верифікація через контрольні суми	Невисока (зазвичай реалізується програмними засобами)

ПЕРСПЕКТИВИ ІНТЕГРАЦІЇ «ДІЇ» ЯК МЕТОДУ АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ

Платформа «Дія» розроблена з урахуванням сучасних вимог до безпеки інформації. Її архітектура базується на використанні багатофакторної автентифікації, цифрових підписів та криптографічних алгоритмів, що відповідають міжнародним стандартам. Завдяки цьому кожен користувач отримує унікальну цифрову ідентичність, що дозволяє гарантувати підтвердження особистості при доступі до державних сервісів. Такий підхід є ключовим для інтеграції «Дії» в систему обліку споживання, оскільки забезпечує централізоване управління правами доступу та мінімізує можливості несанкціонованого доступу до конфіденційної інформації [9].

Інтеграція «Дії» до існуючих систем обліку споживання можлива завдяки використанню відкритих API та сучасних протоколів зв'язку. При цьому процес автентифікації розбивається на кілька етапів:

– Ініціація сесії: користувач, бажаючи отримати доступ до своїх даних, перенаправляється до платформи «Дія» для проходження процедури автентифікації.

– Підтвердження особистості – використовуючи методи цифрового підпису та багатофакторну автентифікацію (наприклад, підтвердження через BankID або КЕП), здійснюється перевірка особистості.

– Авторизація доступу – після успішного підтвердження користувач отримує токен доступу, який дозволяє йому взаємодіяти із сервісом обліку споживання.

– Логування та моніторинг – всі операції проходять централізоване логування, що забезпечує можливість оперативного моніторингу та аналізу безпеки.

Платформа «Дія» вже стала важливою складовою цифрової інфраструктури України, забезпечуючи доступ до багатьох державних послуг. Водночас її широке застосування супроводжується певними ризиками, серед яких можна виділити централізованість системи, яка потенційно створює єдину точку відмови та привабливу мішень для атак. Важливим аспектом є забезпечення безперервної роботи сервісу, надійності та стійкості до атак типу DDoS, фішинг–атак, підміни ідентифікаційних даних користувачів та витоків персональних даних [9]. Проте «Дія», як і інші сервіси, має напрямки для покращення, як:

– Посилення захисту від атак типу DDoS шляхом впровадження додаткових систем моніторингу трафіку та анти–DDoS сервісів, а також створення резервних каналів доступу.

– Регулярне оновлення криптографічних протоколів та алгоритмів захисту даних, зокрема періодичний аудит криптографічних бібліотек і сертифікація алгоритмів відповідно до сучасних стандартів безпеки.

– Впровадження механізмів постійного моніторингу загроз та аномальної активності на основі штучного інтелекту та машинного навчання, які дозволяють оперативно виявляти та запобігати спробам втручання в систему.

Для забезпечення подальшого розвитку «Дії» важливо не лише підвищувати рівень безпеки, а й оптимізувати наявні технологічні процеси. Це дозволить покращити користувацький досвід, зменшити витрати на інтеграцію та підвищити загальну ефективність системи. Нижче запропоновано кілька напрямків для оптимізації:

– Скорочення часу проходження процедури автентифікації користувачів шляхом оптимізації роботи серверів, застосування більш ефективних алгоритмів криптографічної обробки та впровадження асинхронних механізмів взаємодії з зовнішніми сервісами (наприклад, BankID).

– Спрощення інтеграції сторонніх сервісів завдяки удосконаленню API, включаючи більш детальну документацію, розширення набору доступних методів та підвищення стабільності їхньої роботи.

– Розширення можливостей офлайн–автентифікації, наприклад через використання QR–кодів або NFC–технологій, що забезпечить безперервний доступ до критичних сервісів навіть у регіонах з обмеженим покриттям мережі Інтернет [7].

На рисунку 4 зображено узагальнену схему інтеграції «Дії» у систему розумного обліку. У цій архітектурі користувач автентифікується через «Дію» та отримує доступ до даних лічильників через веб–

інтерфейс, тоді як самі прилади передають покази до шлюзу–концентратора, а далі – до серверного додатка в хмарі.

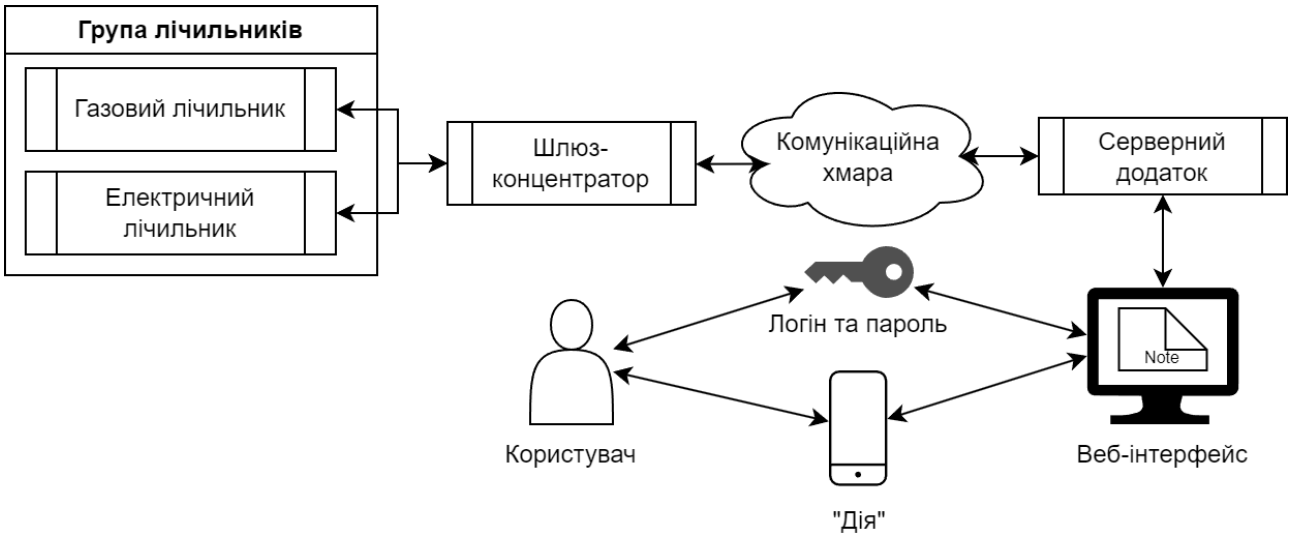

Рис. 4. Схема інтеграції «Дії» у систему розумного обліку

Такий підхід поєднує централізований контроль доступу з ефективним збором і обробкою інформації. Тому інтеграція платформи «Дія» у систему обліку споживання ресурсів дозволяє суттєво підвищити рівень безпеки та конфіденційності, але водночас потребує постійного контролю, оновлення технологій та вдосконалення підходів до захисту інформації.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Цифрова трансформація систем обліку споживання енергоресурсів є неминучою складовою розвитку енергетики і комунального сектору. У статті здійснено аналіз шляхів інтеграції державних цифрових сервісів, зокрема мобільного застосунку «Дія», до інфраструктури розумних лічильників, з акцентом на аспекті приватності даних.

Сучасні схеми підключення за NIST. Рекомендації NIST пропонують багаторівневу архітектуру AMI (лічильник – шлюз – сервер) з використанням відкритих стандартів зв'язку та обов'язковим впровадженням засобів кібербезпеки. Це забезпечує інтероперабельність обладнання різних виробників та захист конфіденційності даних споживачів шляхом шифрування і автентифікації на кожному етапі. NIST також наголошує на врахуванні приватності в розумних мережах, проводячи оцінки впливу на приватність та розробляючи принципи (GAPP, OECD), які мають лягти в основу політик обробки даних.

Аналіз наукових праць показав, що навіть при дотриманні стандартів NIST лишаються потенційні вразливі місця. Зокрема, досвід з електромобілями висвітив необхідність тіснішої інтеграції фізичної та кібербезпеки – щоб система достовірно відображала події в реальному світі і протидіяла комбінованим атакам. Крім того, необхідно розширити рамки приватності – нові типи даних потребують нових підходів до їх захисту. Дослідники пропонують удосконалені протоколи і методи (додаткова автентифікація, шифрування з врахуванням контексту), які можуть бути імплементовані поверх існуючих схем NIST без їх радикальної зміни. Таким чином, базові принципи NIST залишаються актуальними, але їх практична реалізація має еволюціонувати разом із технологіями і загрозами.

Для України повномасштабне впровадження класичної AMI за західними зразками є фінансово та організаційно складним. Необхідно шукати компромісні рішення, які дозволять досягти основної мети (автоматизація обліку) меншим коштом. До таких рішень віднесено використання дешевших технологій зв'язку (LoRaWAN та інші LPWAN, що вже довели свою ефективність і низьку вартість впровадження), поетапне розгортання інфраструктури з концентрацією на пріоритетних сегментах, а також залучення самого споживача до процесу збору даних (через смартфони, додатки). Альтернативні методи захисту – такі як VPN–канали операторів або групове шифрування – можуть тимчасово замінити складніші, але дорогі рішення, щоб забезпечити базовий рівень безпеки. При цьому важливо не втрачати з поля зору приватність – навіть спрощені системи повинні мінімізувати збір зайвих персональних даних і забезпечувати прозорість для користувача.

Використання «Дії» як засобу автентифікації дозволить державі значно прискорити впровадження розумних лічильників, адже цей підхід забезпечує зручність для користувачів та централізований контроль

над доступом до чутливої інформації. Однак інтеграція такого роду ставить перед платформою «Дія» нові вимоги: вона повинна забезпечувати безперервну роботу, мати резервні плани на випадок збоїв і відповідати найвищим стандартам кібербезпеки. Враховуючи успішний досвід «Дії» під час пікових навантажень і її ключову роль у наданні державних сервісів у надзвичайних ситуаціях (наприклад, під час воєнного часу, коли через «Дію» здійснювалися виплати та надавалися послуги переміщеним особам), такі виклики є цілком вирішуваними.

На основі проведеного аналізу негативного впливу атак на системи розумного обліку, а також з урахуванням економічних та технічних аспектів впровадження заходів безпеки, можна виділити наступні рекомендації для підвищення безпеки та стабільності роботи систем:

– Використовувати надійні механізми шифрування та автентифікації на всіх рівнях передачі й зберігання даних, забезпечуючи належний захист від атак типу «Людина посередині» та інших загроз.

– Проводити регулярний аудит безпеки та оновлення ПЗ, включаючи тестування на проникнення, аби своєчасно виявляти й усувати вразливості.

– Застосовувати принцип мінімізації даних, зменшуючи ризики несанкціонованого розголошення та витоку конфіденційної інформації.

– Впроваджувати резервні механізми та розподіл навантаження (зокрема, анти–DDoS рішення) для підвищення надійності та безперервності роботи систем.

– Забезпечувати багаторівневий моніторинг (мережевий, системний, прикладний) і централізоване логування, що дозволить оперативно реагувати на інциденти та покращувати загальний рівень безпеки.

Отже, інтеграція державних цифрових сервісів і систем обліку споживання є багатообіцяючим напрямом, який здатен вирішити одразу кілька завдань: модернізувати інфраструктуру, підвищити ефективність енергопостачання, забезпечити приватність і безпеку даних громадян.

References

1. IoT Analytics. (2024). Smart electricity meter market 2024: Global adoption landscape [Electronic resource] / IoT Analytics Research Blog, February 21, 2024 – Access mode: http://iot–analytics.com.
2. NIST (2010). Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid [Electronic resource] / NISTIR 7628, National Institute of Standards and Technology, 2010 – Access mode: http://everycrsreport.com.
3. Chan, A., & Zhou, J. (2013). On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628 [Electronic resource] / IEEE Communications Magazine, 51(1), 58–65. – (Analysis of the shortcomings of NISTIR 7628) – Access mode: http://phys.org.
4. Phys.org (2013). Cybersecurity: Plugging smart grid weaknesses [Electronic resource] / A*STAR, June 5, 2013. – (News based on Chan & Zhou) – Access mode: http://phys.org.
5. Wirepas. (2024). The hidden costs of cellular technology in smart metering: A wake–up call [Electronic resource] / Wirepas Blog, March 27, 2024. – (GSM vs LPWAN cost issues) – Access mode: http://tsapps.nist.gov.
6. ELKO Group (2018). Smart Building starts with migration to Smart Metering [Electronic resource] / ELKO News, February 27, 2018. – (LoRaWAN NAS solution, CAPEX reduction) – Access mode: http://elkogroup.com.
7. Karachyna, O. (2022). What's Wrong with Diia? [Electronic resource] / Electronic Ukrainian Mutual Prosperity (Analytical overview). – Access mode: http://eump.org
8. Ukraine Business News. (2021). Data risk of Diia app mitigated by no data storage [Electronic resource] / UBN Tech, 29 June 2021. – Access mode: http://ubn.news
9. Ministry of Digital Transformation. (2023). Diia – the ecosystem of e–services [Electronic resource] / Official website/presentation materials of the Diia platform – Access mode: https://thedigital.gov.ua/news/tag/%D0%94%D1%96%D1%8F.
10. NIST. (2019). Considerations for Managing IoT Cybersecurity and Privacy Risks [Electronic resource] / NISTIR 8228, 2019. – (General principles of IoT risk management) – Access mode: https://csrc.nist.gov/pubs/ir/8228/final.
11. MITRE. (n.d.). CWE [Electronic resource]. – Access mode: http://cwe.mitre.org
12. Smart Metering Cybersecurity – Requirements, Methodology, and Testing. [Electronic resource]. – Access mode: https://www.mdpi.com/1424–8220/23/8/4043
13. ETid–2077. (n.d.). [Electronic resource]. – Access mode: https://www.enforcementtracker.com
14. RBC. (n.d.). Programme of free replacement of meters [Electronic resource]. – Access mode: https://www.rbc.ua/news/programa–bezkoshtovnoyi–zamini–lichilnikiv–1701824839.html.
15. MITRE CAPEC. (n.d.). Common Attack Pattern Enumeration and Classification [Electronic resource]. – Access mode: https://capec.mitre.org