DOI 10.15276/imms.v16.no1.210
УДК 621.311:004.056

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 210-221

СТАНДАРТИЗАЦІЯ МОДЕЛЕЙ ЗАГРОЗ ДЛЯ СУЧАСНИХ БІЛІНГОВИХ СИСТЕМ ЕНЕРГЕТИКИ З IOT-ТЕХНОЛОГІЯМИ

П.В. Яворський, М.П. Кляп, М.П. Пригара, Т.В. Дитко

ДВНЗ «Ужгородський національний університет»
3, Народна пл., Ужгород, 88000, Україна
Emails: yavorskyi.petro@uzhnu.edu.ua, m.klyap@uzhnu.edu.ua, mykhailo.prygara@uzhnu.edu.ua, taras.dytko@uzhnu.edu.ua

Сучасні білінгові системи енергетичного сектору та IoT-платформ виконують критично важливу функцію обліку послуг, формування транзакцій та обробки великих обсягів даних. Висока концентрація фінансової, персональної та телеметричної інформації робить їх об'єктами стратегічної значимості, де порушення цілісності чи доступності систем може призвести до значних фінансових втрат, зриву інфраструктури та ризиків для безпеки. Розвиток цифрових технологій, хмарних сервісів, API-інтеграцій та IoT-пристроїв створив нові вектори атак, включаючи експлуатацію вразливих конфігурацій, помилки управління доступом, недоліки IoT-протоколів, а також соціальну інженерію та DDoS-атаки, що підвищує цінність транзакцій та масштаби потенційних збитків. У зв'язку з цим кіберстійкість білінгових платформ потребує не лише технічних заходів, а й формування уніфікованої стандартизованої моделі загроз. Таке моделювання дозволяє системно оцінювати ризики, прогнозувати сценарії атак, виявляти ключові вразливості та розробляти багаторівневі механізми захисту, адаптовані до специфіки галузі. Сучасні підходи до моделювання загроз (STRIDE, LINDDUN, MITRE ATT&CK) частково покривають ризики, проте не забезпечують комплексного уніфікованого аналізу саме для білінгових систем. Тому актуальним є створення стандартизованої моделі, що враховує транзакційні особливості, інтеграційні канали, мережеву архітектуру та IoT-пристрої. Запропонована модель передбачає багаторівневий захист даних – від збору телеметрії на IoT-лічильниках до обробки на білінгових серверах. Використовуються криптографічні методи (AES-256, ECC), захищені протоколи передачі, багатофакторна автентифікація, системи моніторингу та виявлення аномалій. Архітектура забезпечує цілісність, автентичність, конфіденційність та стійкість операцій, а стандартизований підхід дозволяє адаптувати систему під різні мережеві та хмарні середовища. Ключові категорії загроз включають порушення конфіденційності, цілісності та доступності даних, а також специфічні ризики білінгу – підміни показників, компрометації IoT-пристроїв, маніпуляцій із тарифікацією та інтеграційними каналами. Об'єднання цих аспектів у єдину модель загроз дозволяє стандартизовано оцінювати вразливості, пріоритезувати ризики та оптимізувати заходи захисту, забезпечуючи безперервність роботи критично важливих систем.

Ключові слова: білінгові системи, моделювання загроз, стандартизація, кібербезпека, енергетика, IoT-пристрої, STRIDE.

Вступ. Сучасні білінгові системи є основою роботи енергетичних компаній, які використовують IoT-пристрої, забезпечуючи автоматизований облік послуг, формування транзакцій і обробку великих масивів даних. Щодня в цій сфері опрацьовуються мільярди записів із платіжною інформацією, персональними даними, телеметрією та критичними технологічними показниками, що робить білінгові платформи об'єктами стратегічної важливості. Порушення їхньої цілісності чи доступності може спричинити значні фінансові втрати, збої в інфраструктурі та ризики для національної безпеки. Розширення цифрової залежності та активне впровадження хмарних технологій суттєво ускладнили ландшафт кіберзагроз. Хмарні сервіси, API-інтеграції, мікросервіси та IoT-пристрої створили нові вектори атак, що включають експлуатацію вразливих конфігурацій, помилки керування доступами, недоліки IoT-протоколів і сучасні методи соціальної інженерії та DDoS-атак. Зростання обсягу

електронних транзакцій додатково підвищує цінність кожної операції та потенційний масштаб збитків від компрометації білінгових процесів. У таких умовах кіберстійкість білінгових систем стає критичною вимогою, яка потребує не лише технічного захисту, а й формування уніфікованої стандартизованої моделі загроз. Стандартизація дозволяє структурувати ризики, уніфікувати підходи до їх оцінювання та забезпечувати відповідність вимогам ISO/IEC 27001, ISO 22301, IEC 62443, OWASP [1] і NIST [2]. Моделювання загроз дозволяє завчасно виявляти ключові вразливості енергетичних систем, прогнозувати можливі сценарії атак і розробляти багаторівневі механізми захисту, адаптовані до специфіки галузі – від атак на критично важливі об'єкти енергетичної інфраструктури до масових компрометацій IoT-пристроїв. Інтеграція цих аспектів у єдину модель загроз забезпечує системний підхід до безпеки та підвищує стійкість цифрової енергетичної інфраструктури.

Мета дослідження полягає в розробленні уніфікованих та стандартизованих джерел загроз (рис.1) для сучасних білінгових систем у енергетичному та IoT-секторах, що забезпечує комплексне виявлення вразливостей, оцінку ризиків на різних рівнях платформи та формування ефективних заходів кіберзахисту відповідно до міжнародних стандартів.

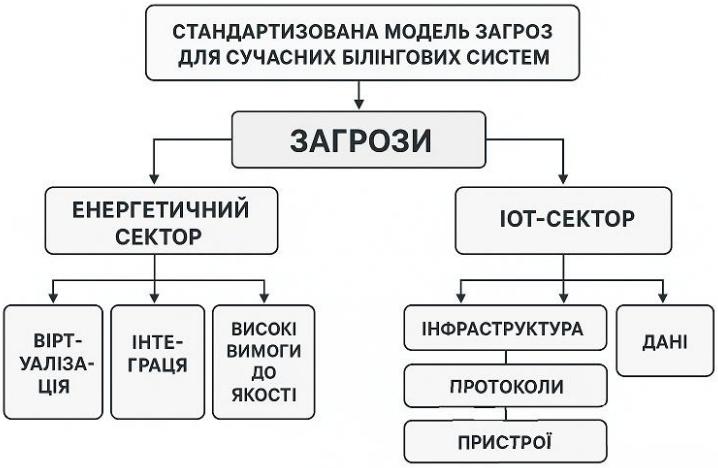

Рис. 1. Стандартизовані джерела загроз для білінгових систем енергетики та IoT

Теоретичні основи дослідження. Білінгові системи виступають ключовими елементами енергетичних операторів та провайдерів IoT-рішень. Вони забезпечують облік наданих послуг, тарифікацію, формування транзакційних записів, обробку платежів і взаємодію з клієнтськими сервісами. Їхня критичність зумовлена високою концентрацією чутливої інформації, яка охоплює персональні дані, детальні показники споживання, параметри мережевої активності та фінансові операції. Це робить білінгові системи об'єктами підвищеного ризику та вимагає застосування чітко визначених моделей загроз.

Основою теоретичного аналізу загроз для таких систем є класичні методи моделювання в інформаційній безпеці [3]. Універсальною та широко застосовуваною є модель STRIDE [4], яка класифікує загрози за шістьма категоріями, такими, як: S – Spoofing (підробка / ідентифікація); T – Tampering (пошкодження / модифікація даних); R – Repudiation (спростування / відмова від дій); I – Information Disclosure (розголошення інформації); D – Denial of Service (відмова в обслуговуванні); E – Elevation of Privilege (підвищення привілеїв), пов'язаними з порушенням конфіденційності, цілісності й доступності інформації. Проте ця модель не враховує специфіку транзакційного білінгу та регуляторні вимоги різних галузей. Інший актуальний підхід – LINDDUN [5] (Linkability (зв'язність), Identifiability (ідентифікація), Non-repudiation (відмова від дій), Detectability (виявлення), Disclosure of information (розголошення інформації), Unawareness (непоінформованість), Non-compliance (невідповідність правилам)) – орієнтований на загрози приватності, що є особливо важливим для енергетичного білінгу

та smart-meter інфраструктури, де дані можуть відображати поведінкові патерни користувача. Значне поширення отримала й модель MITRE ATT&CK [6], яка описує реальні техніки та тактики атак і дозволяє будувати повні сценарії порушення безпеки білінгових систем у контексті сучасних кіберзагроз. Важливим інструментом також є моделювання потоків даних, яке дає змогу виявляти точки потенційного впливу зловмисника у складних багатокомпонентних білінгових архітектурах.

Підґрунтям для моделювання загроз є міжнародні стандарти та галузеві специфікації. До універсальних відносять ISO/IEC 27001 [7] і 27002 [8], що визначають вимоги до побудови систем управління інформаційною безпекою, а також ISO/IEC 27019 [9] для енергетичної інфраструктури та ISO/IEC 30141 [10] для IoT-систем. В енергетичному секторі ключову роль відіграють стандарти DLMS/COSEM та IEC 62056 [11], що визначають протоколи обміну даними лічильників. У сфері IoT важливі рекомендації NIST, ETSI та специфікації безпеки MQTT/CoAP. Попри наявність великої кількості нормативних документів, вони не створюють цілісної та уніфікованої моделі загроз саме для білінгових систем.

Енергетичні білінгові платформи більш вразливі до модифікації даних smart-meter, підміни показників споживання, атак «людина посередині» під час передачі телеметрії та витоку поведінкових профілів користувачів. IoT-білінг характеризується ризиками клонування ідентифікаторів пристроїв, масових телеметричних атак, підробки даних сенсорів та компрометації нестійких до атак протоколів IoT-пристроїв.

Хоч значну кількість галузевих підходів, у сучасних дослідженнях відсутня універсальна, стандартизована та міждисциплінарна модель загроз, яка б охоплювала енергетичні системи з використанням IoT-пристроїв одночасно. Така модель є необхідною для підвищення порівнюваності ризиків, уніфікації засобів кіберзахисту, розроблення галузевих стандартів безпеки та створення узгоджених методів оцінювання вразливостей у критичних білінгових інфраструктурах.

Запропонована схема моделює процес безпечної передачі телеметричних даних від IoT-лічильника до централізованої білінгової системи. Архітектура передбачає багаторівневу модель захисту, яка охоплює формування даних, їх криптографічну обробку, передачу через потенційно незахищене мережеве середовище та подальшу перевірку на стороні серверної інфраструктури (рис.2).

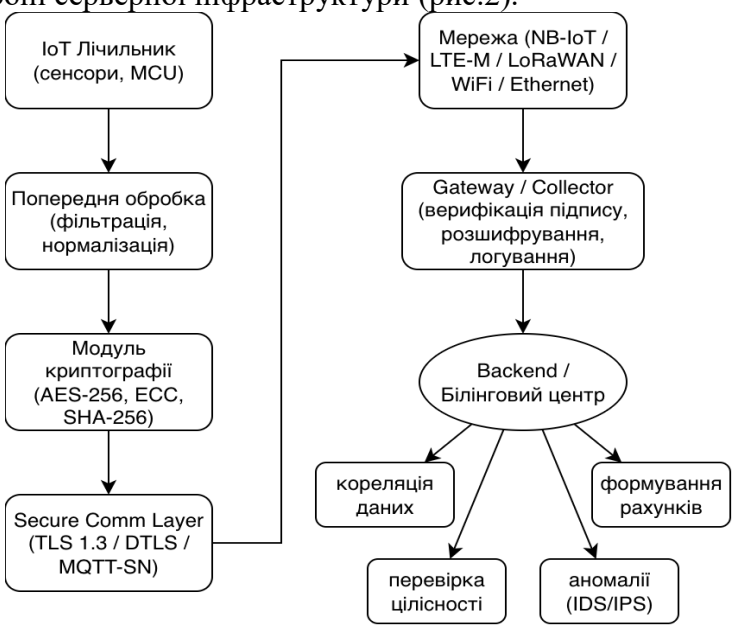

Рис. 2. Архітектурна схема захищеної передачі телеметричних даних IoT-лічильника в білінгову інфраструктуру

На першому етапі лічильник виконує збір та первинну обробку телеметрії. Після цього дані піддаються криптографічному підсиленню шляхом формування MAC-хеша або цифрового підпису, що забезпечує гарантії автентичності та цілісності. Подальше шифрування пакета (наприклад, за допомогою AES-256 або ECC-базованих алгоритмів) запобігає можливості несанкціонованого доступу під час передачі.

Передача даних здійснюється через захищений транспортний рівень – TLS 1.3, DTLS або протокол, який має вбудовані механізми шифрування та захисту (NB-IoT, LTE-M, LoRaWAN). Після доставки пакет надходить на шлюз збору даних, де виконується перевірка підпису, розшифрування та журналювання операцій. На наступному етапі дані передаються до білінгового центру, де додатково працюють системи виявлення вторгнень (IDS/IPS) та алгоритми виявлення аномалій, що дозволяє мінімізувати ризики атак типу man-in-the-middle, replay, підміни або генерації фальшивих значень. Такий підхід створює комплексну багаторівневу модель захисту, яка охоплює цілісність, конфіденційність, автентичність та спостережуваність процесів передачі даних. Архітектура може бути адаптована під різні типи IoT-мереж та рівні енергоспоживання, а також масштабована для інфраструктур, де необхідна висока достовірність телеметричних значень (енергетика, водопостачання, газорозподіл).

Постановка проблеми. Сучасні білінгові системи енергетики та IoT-фахівців функціонують у середовищі зростаючих кіберзагроз, високих вимог до безпеки та ускладненої архітектури. Вони обробляють великі обсяги критичних даних – від тарифікаційних записів і телеметрії до персональних та фінансових відомостей користувачів. Порушення їхньої цілісності або доступності може призвести до фінансових втрат, шахрайства, зриву послуг та підриву довіри споживачів, а в умовах цифровізації критичної інфраструктури ці ризики набувають стратегічного значення.

Попри численні міжнародні стандарти та рекомендації з інформаційної безпеки, наразі відсутня єдина уніфікована модель загроз саме для білінгових систем. Існуючі підходи фокусуються на окремих галузях або описують загальні аспекти захисту, не враховуючи специфіку білінгу. Наприклад, існуючі енергетичні стандарти регламентують інфраструктуру вимірювання та облік споживання, проте не охоплюють специфіку IoT-білінгових систем; загальні рекомендації з безпеки IoT не адаптовані до транзакційної логіки тарифікації. Внаслідок цього оператори застосовують несумісні підходи до моделювання загроз, що ускладнює оцінку ризиків, проведення аудиту та впровадження комплексного кіберзахисту. Додатково відсутність узгодженого термінологічного апарату та структурованої класифікації загроз перешкоджає співставленню ризиків між енергетичними та IoT-білінговими платформами. Це ускладнює формування єдиного стандарту безпеки, інтегрованих систем моніторингу та реагування на інциденти, а також планування розвитку платформ, сертифікацію та дотримання регуляторних вимог. Таким чином постає науково-прикладна проблема – створення уніфікованої моделі загроз, що враховує архітектурні особливості білінгових систем, відповідає міжнародним стандартам і забезпечує стандартизований аналіз, оцінку та мінімізацію ризиків в енергетичній та IoT-інфраструктурі.

Результати та обговорення. Дослідження показало, що сучасні енергетичні білінгові системи з IoT-пристроями вразливі до кіберзагроз через обробку великих обсягів фінансових та телеметричних даних. Класичні моделі загроз (STRIDE, LINDDUN, MITRE ATT&CK) частково покривають ризики, але не забезпечують уніфікованого підходу для білінгу. Розроблена багаторівнева схема захисту телеметрії демонструє ефективність інтеграції криптографії, захищених протоколів та систем виявлення аномалій. Впровадження стандартизованої моделі загроз забезпечує системний підхід до кібербезпеки та підвищує стійкість цифрової енергетичної інфраструктури.

Ключові категорії загроз для білінгових систем. Білінгові системи є високочутливими інформаційними комплексами, що обробляють персональні, фінансові, технічні та транзакційні дані. Через це їхній загрозовий ландшафт формується під впливом

широкого спектра ризиків, що охоплюють традиційні аспекти інформаційної безпеки та галузеві особливості енергетики й IoT-екосистем [12]. Основними групами загроз є порушення конфіденційності, цілісності та доступності, однак у випадку білінгу важливо враховувати також загрози автентичності, непричетності, коректності обліку та захищеності інтеграційних каналів.

Порушення конфіденційності охоплює широкий набір ризиків, пов'язаних із витоком персональних даних абонентів, інформації про платіжні інструменти, історії транзакцій, параметрів споживання та технічної телеметрії. У білінгових системах конфіденційність особливо важлива, адже дані часто містять як фінансову інформацію, так і дані, що характеризують поведінку користувача. В енергетичних системах витік профілів споживання може дозволити зловмисникам робити висновки про присутність користувачів удома чи їх поведінкові звички. У сфері IoT конфіденційність порушується при компрометації вузлів телеметрії, коли облікові дані пристроїв або їхні дані потрапляють до сторонніх осіб. Такі порушення майже завжди створюють підґрунтя для шахрайства, соціальної інженерії або вторинних атак.

Загрози цілісності є критично небезпечними, оскільки вони спрямовані на внесення неправдивої інформації в білінгові записи або маніпуляцію даними, на основі яких формується фінансовий результат. В енергетичних системах атакою може бути фальсифікація показників smart-meter, ін'єкція підроблених даних або підміна пакетів телеметрії. В IoT-білінгу можливими є атаки, пов'язані з генерацією фальшивої телеметрії або клонуванням ідентифікаторів пристроїв, що призводить до неправильного обліку наданих послуг. Зміна API-запитів, ПКС-операцій або сценаріїв тарифікації без належної авторизації призводить до значних фінансових втрат, помилкового нарахування платежів і порушення бізнес-процесів.

Загрози доступності спрямовані на виведення з ладу білінгових платформ або окремих компонентів їхньої інфраструктури. Типовими проявами таких загроз є DDoS-атаки на зовнішні та внутрішні сервіси, перевантаження білінгових процесорів великою кількістю запитів або телеметричних пакетів, блокування доступу до баз даних, порушення роботи дата-центрів або обчислювальних кластерів. У енергетиці та IoT додатковим фактором стають масові атаки на пристрої або шлюзи, які можуть створити штучне перевантаження мережі або ланцюгові відмови.

Окрім традиційних аспектів конфіденційності, цілісності та доступності, білінгові системи мають специфічні категорії загроз. До них належать загрози аутентичності та непричетності, які пов'язані з можливістю підміни користувача, пристрою або джерела даних. Наприклад, у енергетичних системах – це підміна smart-meter, в IoT – клонування пристроїв. Іншим важливим класом є загрози коректності обліку, коли атаки спрямовані не лише на зміну даних, але й на маніпуляцію алгоритмами тарифікації або логікою білінгових процесів, що може створювати значні збитки при масштабному застосуванні. Також вагоме місце займають загрози, пов'язані з інтеграційними механізмами. Білінг практично завжди працює з зовнішніми системами – CRM, OSS, платіжними шлюзами, мережевими вузлами, платформами збору телеметрії та API постачальників. Уразливості в цих інтеграційних каналах, а також недостатня автентичність джерела даних, слабкі механізми шифрування, недостатній контроль доступу або ін'єкційні атаки можуть стати причиною комплексного порушення роботи всієї інфраструктури.

Білінгові системи зазнають впливу широкого спектра кіберзагроз, що охоплюють як класичні аспекти інформаційної безпеки, так і специфічні галузеві ризики. Це обумовлює потребу в комплексній моделі загроз, здатній урахувати різноманіття технологічних платформ, особливості структур даних, сценарії інтеграції та логіку облікових операцій.

Технології та стандарти захисту. Забезпечення безпеки даних у сучасних білінгових системах вимагає застосування комплексного підходу, який поєднує криптографічні технології, механізми контролю доступу, мережевий захист, системи моніторингу та

спеціалізовані галузеві стандарти. Основою побудови такого захисту є вимоги міжнародних стандартів, зокрема ISO/IEC 27001, ISO/IEC 27002, рекомендацій сімейства NIST 800 [13], а також галузевих специфікацій DLMS/COSEM, ETSI та TM Forum, які визначають обов'язкові параметри безпеки для енергетичних та IoT-платформ.

Ключовим напрямом є застосування сучасних криптографічних методів. Шифрування даних у стані спокою та під час передавання є фундаментальною вимогою для захисту білінгової інформації, яка може включати фінансові транзакції, персональні дані споживачів. Найпоширенішим стандартом симетричного шифрування є AES-256 [14], який забезпечує високий рівень стійкості до криптоаналітичних атак і рекомендований NIST для використання в критичних інформаційних системах. Для захисту даних під час передачі використовуються криптографічні протоколи TLS 1.2/1.3 або SSL, що дозволяють забезпечити цілісність і конфіденційність у процесі взаємодії між білінговими сервісами та зовнішніми платформами. Додатковим рівнем безпеки виступають апаратні модулі керування ключами (HSM або KMS), які забезпечують створення, зберігання та ротацію криптографічних ключів у захищеному середовищі, унеможливлюючи несанкціонований доступ до ключового матеріалу навіть у разі компрометації окремих компонентів інфраструктури.

Важливою частиною захисту є побудова надійної системи автентифікації та авторизації. У білінгових системах, що взаємодіють із мільйонами користувачів і тисячами міжсистемних інтеграцій, класичної парольної автентифікації недостатньо. Сучасні платформи впроваджують багатофакторну автентифікацію (MFA), яка може включати SMS- або push-коди, TOTP-додатки, біометричні методи або апаратні токени, зокрема FIDO2-сумісні пристрої. Ці механізми відповідають рекомендаціям NIST SP 800-63 [15] щодо рівнів упевненості в автентифікації та ISO/IEC 29115 [16], які визначають вимоги до електронної ідентифікації та довірчих сервісів. Для міжсервісної взаємодії застосовуються стандартизовані протоколи авторизації, такі як OAuth 2.0, OpenID Connect та SAML, що дають можливість централізовано контролювати доступ і запобігати несанкціонованим API-викликам.

Мережевий захист білінгових платформ є ще одним фундаментальним напрямом забезпечення кібербезпеки. У багатокомпонентних архітектурах, які включають білінгові процесори, хмарні сервіси, бази даних та інтеграційні API, необхідно створювати сегментоване мережеве середовище з використанням брандмауерів нового покоління, систем виявлення та запобігання вторгненням (IDS/IPS), інструментів виявлення аномальної активності та захищених VPN-тунелів. Ці системи здатні своєчасно фіксувати нетипові запити, спроби порушення периметра, а також атаки, спрямовані на маніпуляцію білінговими процесами.

Важливою складовою комплексного захисту є інтегровані платформи моніторингу та реагування, зокрема SIEM-системи та технології SOAR. Вони дозволяють збирати логи подій із різних елементів білінгової інфраструктури, корелювати інциденти та автоматизувати процеси реагування на інциденти. Для білінгових систем, які працюють з високою інтенсивністю запитів, можливість виявляти аномалії на основі поведінкових моделей є критичною для запобігання зловживанням, фальсифікації транзакцій або атак на системи онлайн-тарифікації.

В енергетичних та IoT-платформах додаткову роль відіграють галузеві стандарти. В енергетичних системах протоколи DLMS/COSEM визначають механізми шифрування та автентифікації для smart-meter комунікацій, що забезпечує цілісність і автентичність переданої телеметрії. У сфері IoT важливими є вимоги ETSI EN 303 645, що визначають базові параметри кіберзахисту IoT-пристроїв, зокрема вимоги до оновлення прошивки, унікальних ідентифікаторів, шифрування даних і захисту від маніпуляцій.

Технології та стандарти захисту білінгових систем формують багаторівневий комплекс, який охоплює криптографічні механізми, автентифікацію та авторизацію, мережеву безпеку, моніторинг подій і галузеві стандарти функціонування. Усі ці

елементи мають бути узгоджені в єдиній системі, що забезпечує безперервний і стандартизований захист критично важливих білінгових платформ.

Архітектурні стандарти захисту. Архітектурні стандарти захисту сучасних білінгових систем формуються на основі вимог до високої доступності, безперервності бізнес-процесів і стійкості до кіберзагроз, оскільки енергетичні та IoT-білінгові платформи працюють у режимі реального часу та обробляють великі обсяги транзакцій. Провідною тенденцією є розподілена архітектура, що охоплює декілька незалежних дата-центрів та хмарних сегментів, розташованих у різних географічних регіонах. Такий підхід дає змогу забезпечити стійкість до техногенних аварій, фізичних загроз і кібератак, оскільки кожен із сегментів може виконувати функції резервування та взаємного дублювання. Георознесена інфраструктура дозволяє реалізовувати стратегії безперервності бізнесу з контрольованими показниками RTO та RPO відповідно до міжнародного стандарту ISO 22301 [17], забезпечуючи можливість відновлення повної функціональності системи навіть у разі втрати одного з основних центрів обробки даних.

Важливою складовою архітектури захисту є використання незалежних комунікаційних каналів, прокладених різними провайдерами або фізично віддаленими маршрутами. Це дозволяє уникати ситуацій, коли вихід з ладу одного каналу стає критичною точкою відмови для всієї білінгової платформи. У середовищах IoT-білінгу також застосовується мультиплексування технологій передачі (LTE-M, NB-IoT, LoRaWAN, Ethernet), що підвищує гнучкість маршрутизації та забезпечує додаткові можливості для обходу перевантажених або недоступних ділянок мережі. Паралельно з цим формуються дублювальні бази даних із застосуванням синхронної або асинхронної реплікації, кластерних конфігурацій і механізмів автоматичного перемикання на резервні вузли. Це критично важливо для забезпечення безперервної роботи модулів тарифікації, маршрутизації транзакцій, формування рахунків і сховищ історичних даних. Системи оркестрації (наприклад, Kubernetes або OpenShift) постійно контролюють стан застосунків, виконують перевірки їхньої працездатності та автоматично перезапускають або переносить контейнери у випадку виявлення аномалій. Захист мережевої інфраструктури вибудовується за принципами сегментації та ізоляції критичних компонентів. Мережа поділяється на зони довіри, між якими встановлюються суворі правила взаємодії, що відповідають підходам стандарта IEC 62443 [18]. Така структура дає можливість мінімізувати горизонтальне поширення атак у разі компрометації одного з компонентів. Для контролю взаємодії між сегментами застосовуються багаторівневі міжмережеві екрани, мікросегментація трафіку на рівні контейнерів або віртуальних машин, а також підхід Zero Trust, який передбачає постійний контроль доступу незалежно від того, де перебуває користувач або сервіс. У середовищах білінгів енергетики додатково впроваджуються вимоги NERC CIP щодо обмеження доступу до критичної інфраструктури, ведення журналів дій операторів і збереження повного трасування операцій.

Централізований моніторинг, що здійснюється через SIEM-системи, є фундаментальним елементом архітектурного захисту. Білінгові платформи генерують значні обсяги журналів, які необхідно агрегувати, аналізувати та корелювати між собою для виявлення аномальних подій. Завдяки інтеграції з системами SOAR можливе автоматичне виконання сценаріїв реагування: блокування підозрілої активності, ізоляція інцидентних вузлів, зміна маршрутів трафіку або запуск процедур аварійного перенесення на резервні середовища. Така автоматизація значно скорочує час реагування на інциденти, що критично для систем, у яких перебої роботи безпосередньо впливають на фінансові операції та якість обслуговування клієнтів.

У комплексі всі ці архітектурні заходи забезпечують відповідність білінгових систем міжнародним нормам IEC 62443, ISO 22301, NERC CIP та ISO/IEC 27001, формуючи стандартизований підхід до моделювання загроз, управління ризиками та забезпечення безперервності операційних процесів. Така структурована архітектура

дозволяє підвищити рівень кіберстійкості та гарантувати стабільну роботу білінгових платформ в енергетичній та IoT-сферах.

Стандартизована модель загроз. Стандартизована модель загроз для сучасних білінгових систем в енергетичній та IoT-сферах має охоплювати комплексну сукупність ризиків, які виникають на всіх рівнях функціонування платформи – від обробки даних і взаємодії з користувачами до мережевих комунікацій, інфраструктури та зовнішніх інтеграцій. Її формування ґрунтується на принципах системного аналізу, врахуванні специфіки предметної області та застосуванні міжнародних рекомендацій STRIDE, OWASP, ENISA та NIST, що дозволяє створити уніфіковану структуру оцінювання загроз для різних типів білінгових середовищ.

На рівні даних до моделі включаються загрози, пов’язані з можливістю витоку персональної, фінансової та транзакційної інформації, підміною або модифікацією критично важливих записів, несанкціонованим доступом до ключів шифрування та порушенням цілісності архівів. Особливої уваги потребує захист баз даних білінгу, оскільки вони містять інформацію про тарифи, облік споживання ресурсів, фінансові операції, ключі доступу до IoT-пристроїв та історію транзакцій користувачів. У системах енергетичного сектору додатковим ризиком є можливість маніпулювання показниками лічильників або втручання у балансування навантажень через зміну даних.

Рівень користувачів охоплює ризики, пов’язані з атаками на механізми автентифікації, соціально-інженерними методами викрадення облікових даних, шкідливими діями внутрішніх співробітників, а також сценаріями підвищення привілеїв. У білінгових платформах, де часто реалізується багаторівневий доступ (оператори, адміністратори, технічні користувачі, сторонні інтегратори), ці ризики посилюються різноманітністю ролей та складністю політик контролю доступу. Недоліки в автентифікації або відсутність багатофакторного захисту призводять до можливості компрометації облікових записів і подальшого впливу на розрахункові модулі, фінансові операції або дані користувачів.

Таблиця 1.

Пріоритезація вразливостей [19-21]

Vulnerability	Component	Likelihood	Impact	Risk
API key exposure	API Gateway	4	5	20
CDR tampering	Rating Engine	3	5	15
Queue flooding	Billing Queue	5	3	15

Мережевий рівень моделі загроз включає DDoS-атаки, сканування відкритих портів, атакування протоколів взаємодії між сервісами, ін’єкційні та інтерцепційні атаки, ботнет-активність, MITM-сценарії, спуфінг та маніпулювання маршрутами трафіку. У сучасних білінгових інфраструктурах, які широко застосовують мікросервісну архітектуру, різноманітні API, контейнеризацію та хмарні сервіси, мережеві загрози стають особливо актуальними, оскільки кожен сервіс відкриває нові потенційні точки входу для атак.

Інфраструктурний рівень охоплює загрози фізичних атак, аварій у дата-центрах, відмов обладнання, збоїв у роботі енергопостачання, пожеж, затоплень, а також ризиків, пов’язаних із хмарними провайдерами, включаючи компрометацію контейнерних середовищ або віртуальних машин. Значна частина білінгових платформ сьогодні розгортається у гібридних або мультихмарних середовищах, що потребує врахування додаткових загроз, пов’язаних з неправильними конфігураціями, недостатнім контролем доступу до хмарних ресурсів і помилками у політиках безпеки. У сфері енергетики

доцільним є врахування загроз, які впливають на критичну інфраструктуру та можуть викликати масові відключення або порушення роботи смарт-мереж.

Інтеграційні загрози стосуються взаємодії білінгових платформ з зовнішніми сервісами, API, платіжними шлюзами, IoT-платформами, сторонніми системами моніторингу, CRM та ERP. Типовими є API-атаки, експлуатація вразливостей у сторонніх бібліотеках, порушення цілісності передавання даних, підміна запитів, а також загрози, пов'язані з некоректною фільтрацією трафіку між зовнішніми та внутрішніми модулями. У системах IoT-білінгу окреме значення мають ризики компрометації вбудованих пристроїв, прошивок, протоколів MQTT та CoAP, що прямо впливають на точність збору показників і коректність нарахувань.

Об'єднання всіх перелічених складових у єдину стандартизовану модель загроз дає змогу комплексно оцінювати ризики, створювати уніфіковане середовище для аналізу вразливостей та визначати пріоритетні напрями захисту. Використання принципів STRIDE забезпечує структуровану класифікацію загроз за типами впливу – підміна, підробка, розкриття інформації, відмова в обслуговуванні, ескалація привілеїв, порушення цілісності. Дотримання рекомендацій OWASP гарантує актуальність моделі для сучасних веб- і API-орієнтованих білінгових систем. Такий підхід дозволяє сформувати узгоджену архітектуру безпеки, що однаково ефективно працює в енергетичних та IoT-середовищах, забезпечуючи належний рівень кіберзахисту та стійкість критичних процесів білінгу.

Висновки. Стандартизація джерел загроз для білінгових систем у сферах енергетики та IoT є невід'ємною складовою формування надійної та стійкої інфраструктури сучасних цифрових сервісів. Враховуючи стрімке зростання обсягів даних, інтенсивність транзакційних процесів і взаємодію систем у розподілених середовищах, саме уніфікований підхід до моделювання загроз дозволяє забезпечити системність аналізу, прогнозованість ризиків та ефективність реалізації захисних механізмів. Використання міжнародних стандартів, таких як ISO/IEC 27001, 27005, NIST SP 800-30, OWASP ASVS, MITRE ATT&CK та актуальних рекомендацій ENISA, створює методологічну базу, яка спрямовує організації на впровадження найкращих світових практик щодо кібербезпеки критичних платформ. Це не лише підвищує рівень взаємної сумісності архітектур і процедур безпеки, а й забезпечує можливість незалежного аудиту, коректного оцінювання захищеності та формування обґрунтованих технічних вимог для розробників та операторів білінгових систем.

Сучасні білінгові рішення є багаторівневими й часто включають локальні, хмарні, гібридні та периферійні компоненти, що формує додаткові вектори атак і збільшує складність забезпечення їх кіберстійкості. Відповідно, стандартизована модель загроз надає можливість комплексно оцінити потенційні ризики, починаючи від неправомірного доступу та маніпуляцій із транзакційними потоками і завершуючи глибшими загрозами, такими як компрометація модулів білінгу, викривлення показників споживання енергії або втручання у процеси тарифікації IoT-пристроїв. Чітке структурування загроз забезпечує формування погоджених сценаріїв реагування, оптимізацію політик доступу, правильну побудову криптографічного контуру та застосування механізмів багатофакторної автентифікації, що суттєво знижує можливість успішних атак на критичні компоненти систем.

Одним із ключових результатів стандартизації є можливість впровадження безперервного моніторингу загроз із використанням автоматизованих систем виявлення аномалій, кореляції подій, поведінкового аналізу та адаптивних механізмів реагування. У поєднанні з георезервуванням інфраструктурних елементів, розподіленими механізмами відновлення та цифровими сертифікаційними платформами це створює стійку екосистему, здатну функціонувати навіть у разі масштабних кібератак або збоїв на окремих вузлах мережі. Важливо також, що стандартизація сприяє підвищенню прозорості взаємодії між різними суб'єктами ринку – постачальниками послуг,

операторами інфраструктури, аудиторами, регуляторами та виробниками енергетичного обладнання.

Узагальнюючи, можна стверджувати, що стандартизація моделей загроз виступає фундаментом для розвитку захищених білінгових платформ, які відповідають вимогам кібербезпеки сучасного цифрового суспільства. Вона забезпечує ефективне управління ризиками, підвищує рівень довіри користувачів і бізнесу до критичних сервісів, формує основу для впровадження інновацій і зміцнює загальну кіберстійкість галузей, у яких точність, безперервність і безпека обробки даних мають вирішальне значення.

Список літератури

1. Лях І. М., Кіш Ю.В. Сучасні стандарти забезпечення інформаційної безпеки мобільних та Web-застосунків на прикладі OWASP TOP 10. *Національна безпека у фокусі викликів глобалізаційних процесів в економіці» XVI Міжнародна наукова Інтернет-конференція*. 2023. С. 41–44
2. Kaur J., Canto A. C., Kermani M. M., Azarderakhsh R. A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. arXiv, 2023. DOI: 10.48550/arXiv.2304.06222
3. Sulaiman N. S., Fauzi M. A., Wider W., Rajadurai J., Hussain S., Harun S. A. Cyber–information security compliance and violation behaviour in organisations: *A systematic review. Social Sciences*. 2022. No.11(9). DOI: 10.3390/socsci11090386
4. Mauri L., Damiani E. Modeling threats to AI-ML systems using STRIDE. *Sensors*. 2022. No.22(17). DOI: 10.3390/s22176662
5. Sion L., Van Landuyt D., Wuyts K., Joosen W. Robust and reusable LINDDUN privacy threat knowledge. *Computers & Security*. 2025. V.154. DOI: 10.1016/j.cose.2025.104419
6. Al-Sada B., Sadighian A., Oligeri G. Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. *IEEE Access*. 2024. No. 12, DOI: 10.1109/ACCESS.2023.3344680
7. ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems. Requirements. URL: https://www.iso.org/standard/27001
8. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/standard/75652.html
9. ISO/IEC 27019:2024. Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry. URL: https://www.iso.org/standard/85056.html
10. ISO/IEC 30141:2018. Internet of Things (IoT). Reference Architecture. URL: https://www.iso.org/standard/88800.html
11. IEC 62056-6-1. URL: https://webstore.iec.ch/en/publication/67916
12. Лях І.М., Кляп М.П., Шумило Н.Я., Ціпіньо А.Ю. Безпека IoT-протоколів як виклик для міжнародного співробітництва. *Наука і техніка сьогодні*. 2025. № 7(48). С. 1669-1681. https://doi.org/10.52058/2786-6025-2025-7(48)-1669-1681
13. NIST. Special Publication 800-series General Information. URL: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
14. Mohammed Z. K., Mohammed M. A., Abdulkareem K. H., Zebari D. A., Lakhan A., Marhoon H. A., Martinek R. A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Applied Soft Computing*. 2024. V.158. DOI: 10.1016/j.asoc.2024.111588
15. NIST. Special Publication 800-63. Digital Identity Guidelines. URL: https://www.nist.gov/identity-access-management/projects/nist-special-publication-800-63-digital-identity-guidelines
16. ISO/IEC 29115:2013. Information technology. Security techniques. Entity authentication assurance framework. URL: https://www.iso.org/standard/45138.html

17. ISO 22301:2019. Security and resilience. Business continuity management systems. URL: https://www.iso.org/standard/75106.html
18. ISA/IEC 62443 series of standards. Security for industrial automation and control systems. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
19. Kabenge J. Vulnerability Management: Towards better vulnerability prioritisation, an automated proof of concept 2024 URL: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-242844
20. He J., Chen H. H., Yang K., Gao T., Cao Z. Automated Spam Call Traceback: Two Efficiency Enhancement Approaches. *IEEE Network*. 2025. DOI: 10.1109/MNET.2025.3591651
21. Yaegashi R., Hisano D., Nakayama Y. Queue allocation-based DDoS mitigation at edge switch. *IEEE International Conference on Communications Workshops*. 2021. P. 1-6. DOI: 10.1109/ICCWorkshops50388.2021.9473582

STANDARDIZATION OF THREAT MODELS FOR MODERN ENERGY BILLING SYSTEMS WITH IOT TECHNOLOGIES

P.V. Yavorskyi, M.P. Klyap, M.P. Prygara, T.V. Dytko

Uzhhorod National University
3, Narodna Square, Uzhhorod, 88000, Ukraine
Emails: yavorskyi.petro@uzhnu.edu.ua, m.klyap@uzhnu.edu.ua, mykhailo.prygara@uzhnu.edu.ua, taras.dytko@uzhnu.edu.ua

Modern billing systems in the energy sector and IoT platforms perform a critically important function of service accounting, transaction processing, and handling large volumes of data. The high concentration of financial, personal, and telemetry information makes them strategically significant targets, where violations of system integrity or availability can lead to substantial financial losses, infrastructure disruptions, and security risks. The development of digital technologies, cloud services, API integrations, and IoT devices has created new attack vectors, including exploitation of vulnerable configurations, access management errors, weaknesses in IoT protocols, as well as social engineering and DDoS attacks, which increases the value of transactions and the potential scale of damage. In this context, the cyber resilience of billing platforms requires not only technical measures but also the development of a unified, standardized threat model. Such modeling enables systematic risk assessment, attack scenario forecasting, identification of key vulnerabilities, and the development of multi-layered protection mechanisms tailored to the specifics of the industry. Modern threat modeling approaches (STRIDE, LINDDUN, MITRE ATT&CK) partially address risks but do not provide a comprehensive, unified analysis specifically for billing systems. Therefore, the creation of a standardized model that considers transactional features, integration channels, network architecture, and IoT devices is highly relevant. The proposed model provides multi-layered data protection—from telemetry collection on IoT meters to processing on billing servers. Cryptographic methods (AES-256, ECC), secure transmission protocols, multi-factor authentication, and monitoring and anomaly detection systems are employed. The architecture ensures integrity, authenticity, confidentiality, and operational resilience, while the standardized approach allows adaptation of the system to different network and cloud environments. Key threat categories include violations of data confidentiality, integrity, and availability, as well as billing-specific risks—meter reading tampering, IoT device compromise, manipulation of tariffing, and integration channels. Combining these aspects into a single threat model allows standardized vulnerability assessment, risk prioritization, and optimization of protective measures, ensuring the continuous operation of critical systems.
Keywords: billing systems, threat modeling, standardization, cybersecurity, energy sector, IoT devices, STRIDE.