**International Science Journal of Engineering & Agriculture**
2026; 5(1): 38-47
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20260501.04
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

# Контекстно-орієнтована криптографічна політика для event-driven систем: шифрування за важливістю події

**Ігор Андрущак**
Луцький національний технічний університет, Луцьк, Україна
ORCID 0000-0002-8751-4420

**Олександр Колошко**
Луцький національний технічний університет, Луцьк, Україна
ORCID 0009-0001-9325-9542

**Анотація:** У статті розглянуто підхід до побудови контекстно-орієнтованої криптографічної політики для event-driven систем, у яких обмін даними реалізується через асинхронні події, стріми та журнали (log-based інтеграція). Такі системи генерують величезні обсяги різнорідних подій, що мають неоднакову критичність та вимоги до конфіденційності. У таких архітектурах події часто доставляються за семантикою at-least-once, дублюються при повторах, зберігаються тривалий час у брокерах чи сховищах, передаються між доменами та відтворюються для відновлення стану. Це підсилює ризики компрометації конфіденційності та цілісності, а також створює практичні передумови для помилок використання nonce/IV у режимах аутентифікованого шифрування з приєднаними даними. Основна ідея роботи полягає у формалізації «важливості події» як політичного атрибута, що керує вибором криптографічного профілю (алгоритм шифрування, стратегія nonce, політика associated data, ротація ключів, анти-replay механізми) з урахуванням обмежених ресурсів (час виконання, пам'ять, енерговитрати, накладні байти та мережеві обмеження). Проаналізовано існуючі підходи до класифікації подій та механізми селективного шифрування. Запропоновано модель події та контексту, функцію важливості, модель витрат і модель ризику, а також оптимізаційну постановку «мінімізація витрат за обмеженням ризику» для автоматизованого вибору профілю захисту. Наукова новизна полягає у поєднанні принципів Authenticated Encryption with Associated Data та Attribute-Based Access Control - підходу до політик та ієрархічного керування ключами у єдиній політичній рамці, що враховує характерні для event-driven систем дублікати/ретраї/тривале зберігання подій та запроваджує семантичну цілісність через автентифікацію контексту доставки у складі associated data. Практична значущість полягає у запропонованих шаблонах політик для різних рівнів важливості (L0–L3), а також методикою доменної ізоляції ключів і коротких криптографічних епох, що знижують наслідки компрометації. Розроблено алгоритм динамічного визначення криптографічних параметрів на основі пріоритету події. Показано, що адаптивне шифрування «за важливістю події» дозволяє зменшити криптографічні накладні витрати в потоках високої частоти без деградації безпеки критичних подій, забезпечуючи керований компроміс між ризиком та ресурсами.

**Ключові слова:** event-driven архітектура, контекстно-орієнтоване шифрування, криптографічна політика, класифікація подій, легковагова криптографія, оптимізація шифрування, IoT-безпека

## 1. Вступ

Стрімкий розвиток технологій Інтернету речей, промислової автоматизації та розподілених обчислювальних систем формує нову парадигму обробки інформації, в основі якої лежить архітектура, керована подіями. За даними аналітичних досліджень, понад 72% глобальних організацій використовують event-driven архітектуру для забезпечення

функціонування своїх критичних застосунків [1]. Такі системи характеризуються асинхронною моделлю взаємодії, де компоненти реагують на події в режимі реального часу.

У типовій event-driven системі генеруються мільйони подій різного характеру: від рутинних телеметричних повідомлень сенсорів до критичних сигналів тривоги та команд управління промисловим обладнанням. Кожна з цих подій має власне призначення та рівень конфіденційності [2]. Однак традиційний підхід до криптографічного захисту передбачає застосування уніфікованих алгоритмів шифрування до всього потоку даних незалежно від їхньої природи.

Такий підхід є надмірно витратним для ресурсно-обмежених середовищ, типових для IoT-екосистем. Мініатюрні сенсори та вбудовані контролери мають обмежену обчислювальну потужність та жорсткі обмеження щодо енергоспоживання [3]. Застосування повнорозмірних криптографічних примітивів до кожної події створює непропорційне навантаження на ресурси пристрою та скорочує термін автономної роботи.

Проблема ускладнюється різноманітністю сучасних event-driven систем. В одній інфраструктурі можуть співіснувати пристрої з різними обчислювальними можливостями та різними вимогами до безпеки. Промислові контролери потребують мінімальних затримок, тоді як сенсори моніторингу орієнтовані на енергоефективність [4]. Рутинні телеметричні дані можуть мати низьку конфіденційність та не потребувати повного криптографічного захисту. Водночас команди управління виконавчими механізмами є надзвичайно важливими та вимагають максимального рівня захисту [5]. Ігнорування цієї семантичної різниці призводить до надлишкового захисту некритичних даних.

Концепція контекстно-орієнтованої безпеки передбачає адаптивне застосування механізмів захисту залежно від характеристик оброблюваних даних [6]. Контекст події може включати множину атрибутів: джерело генерації, тип корисного навантаження та рівень поточних загроз.

Легковагова криптографія, стандартизована NIST у 2023-2025 роках, надає ефективні інструменти для захисту ресурсно-обмежених пристроїв [7]. Алгоритми сімейства ASCON забезпечують автентифіковане шифрування з мінімальним споживанням ресурсів. Однак навіть легковагові алгоритми створюють помітне навантаження при обробці високоінтенсивних потоків подій.

Селективне шифрування є перспективним напрямом оптимізації криптографічних систем [8]. Замість уніфікованого захисту всіх даних пропонується концентрувати криптографічні зусилля на найбільш критичних елементах.

Дослідження в галузі контекстно-орієнтованої криптографії активно розвиваються, однак питання динамічної адаптації криптографічних параметрів до характеристик подій у реальному часі залишається недостатньо дослідженим [9]. Таким чином, проблема розробки контекстно-орієнтованої криптографічної політики для event-driven систем є актуальною науковою та практичною задачею.

## 2. Об’єкт і предмет дослідження

Об’єктом дослідження є процеси криптографічного захисту даних у розподілених обчислювальних системах з архітектурою, керованою подіями. Такі системи охоплюють широкий спектр технологій, включаючи промислові мережі автоматизації, інфраструктуру Інтернету речей та телеметричні платформи реального часу.

У event-driven системах події є основною одиницею інформаційного обміну. Кожна подія представляє собою структуроване повідомлення, що містить ідентифікатор типу, часову мітку та корисне навантаження. Потік подій характеризується високою інтенсивністю та нерівномірністю критичності окремих повідомлень.

Криптографічний захист у таких системах має забезпечувати конфіденційність, цілісність та автентичність подій в умовах обмежених обчислювальних ресурсів [10]. Традиційні

підходи до захисту передбачають застосування уніфікованих криптографічних примітивів до всього потоку подій, що є неефективним.

Предметом дослідження є методи та моделі контекстно-орієнтованого криптографічного захисту, що забезпечують адаптивний вибір параметрів шифрування залежно від класу важливості події. Предмет охоплює механізми класифікації подій за рівнем критичності та алгоритми динамічного визначення криптографічних параметрів.

У межах дослідження розглядається формалізація поняття контексту події як сукупності атрибутів, що визначають її важливість та вимоги до захисту. Контекст включає статичні характеристики, такі як тип події та джерело генерації, а також динамічні параметри: поточний стан системи та рівень загроз [11].

Предметна область також охоплює: формалізацію функції важливості події; побудову профілів криптографічного захисту; правила формування associated data для семантичної цілісності; стратегії nonce (у т.ч. misuse-resistance); ієрархічне виведення ключів та ротацію; анти-replay механізми; моделювання витрат і ризику; оптимізаційну постановку вибору профілю.

## 3. Мета та задачі дослідження

Метою дослідження є розробка та обґрунтування контекстно-орієнтованої криптографічної політики для event-driven систем, яка забезпечує адаптивний вибір параметрів шифрування залежно від класу важливості події та дозволяє оптимізувати баланс між рівнем криптографічного захисту та обчислювальними витратами. Дослідження спрямоване на створення методологічної основи для проєктування ефективних криптографічних підсистем у розподілених обчислювальних середовищах, де неоднорідність подій та обмеженість ресурсів унеможливлюють застосування традиційних уніфікованих схем захисту.

Для досягнення мети було передбачено виконання таких задач:

✓ формалізація моделі події та контексту EDA. Визначено набір атрибутів події та параметрів середовища, які впливають на вибір криптографічного профілю, включно з характеристиками доставки (дублікати, повтори, TTL, fan-out);

✓ визначення функції важливості події. Було запропоновано шкалу важливості (L0–L3) та функцію відображення атрибутів події/контексту у числовий або категоріальний рівень важливості;

✓ аналіз загроз для потоків подій. Сформовано модель небезпеки з урахуванням специфіки EDA: пасивне спостереження, активна підміна/ін’єкція, replay, витоки журналів, компрометація брокера, nonce misuse;

✓ побудова моделі ризику та бюджету безпеки. Визначено метрики ризику підробки, ризики конфіденційності при nonce misuse, та принципи встановлення порогів ризику залежно від важливості;

✓ побудова моделі витрат та оптимізаційної постановки. Формалізовано витрати (час, енергія, пам’ять, накладні байти) і сформулювати задачу вибору профілю як мінімізацію витрат за обмеженням ризику та SLA;

✓ проєктування архітектури політики. Запропоновано механізм PDP/PEP для прийняття рішення та виконання шифрування/перевірки, а також структуру «crypto envelope» для подій;

✓ оцінювання підходу на модельних сценаріях. Показано, як політика змінює накладні витрати та параметри ризику у потоках різної частоти та на різних платформах (edge vs дата-центр), не видаючи ці приклади за емпіричні дані реального розгортання.

Експериментальна верифікація запропонованого підходу передбачає реалізацію прототипу контекстно-орієнтованої криптографічної підсистеми та проведення серії експериментів для оцінки її характеристик.

## 4. Аналіз літератури

Проблематика криптографічного захисту в event-driven системах знаходиться на перетині кількох напрямів досліджень: архітектури систем обробки подій, легковагової криптографії та контекстно-орієнтованої безпеки [1].

Архітектура event-driven систем досліджується в контексті забезпечення масштабованості та реактивності. Confluent визначає event-driven архітектуру як модель, де системи реагують на події в реальному часі [1]. Pietrzak аналізує безпекові виклики та підкреслює необхідність забезпечення цілісності подій [2].

Дослідження IoT-безпеки акцентують увагу на обмеженнях ресурсно-обмежених пристроїв. Систематичний огляд легковагових криптографічних схем виявляє критичну потребу в оптимізації криптографічних примітивів [3]. Традиційні алгоритми часто непридатні для IoT через високі витрати.

У серпні 2025 року NIST опублікував стандарт SP 800-232, що визначає сімейство ASCON як основу для захисту ресурсно-обмежених пристроїв [7]. Стандарт включає ASCON-AEAD128 та ASCON-Hash256.

Порівняльний аналіз легковагових алгоритмів представлений у роботі Ansari та Ali [11]. Результати демонструють суттєві відмінності в характеристиках ASCON, SPECK та AES-128.

Концепція контекстно-орієнтованої безпеки розвивається в контексті захисту розумних речей. Автори описують її як підхід, що враховує бізнес-логіку та поведінку користувачів [6].

Селективне шифрування досліджується переважно для мультимедійних даних [8]. Inshi, Chowdhury та ін. пропонують контекстно-орієнтоване адаптивне рішення для розумних середовищ з використанням машинного навчання [9].

Незважаючи на активний розвиток, виявлено прогалину: відсутня інтегрована модель, що поєднує класифікацію подій з адаптивним вибором криптографічних параметрів.

## 5. Методи досліджень

Дослідження проводилось із застосуванням методу імітаційного моделювання, що дозволяє відтворити поведінку event-driven системи в контрольованих умовах без необхідності розгортання повномасштабної інфраструктури. Такий підхід забезпечує можливість багаторазового повторення експериментів із варіюванням параметрів та отримання статистично значущих результатів.

Архітектура event-driven систем передбачає обмін інформацією через асинхронні повідомлення, що принципово відрізняється від класичної синхронної взаємодії компонентів. Події генеруються різноманітними джерелами - сенсорами, контролерами, користувацькими застосунками - та передаються через брокери повідомлень до споживачів [12]. У процесі передачі події можуть зберігатися у журналах, дублюватися при гарантованій доставці, маршрутизуватися між доменами безпеки. Ці особливості створюють специфічні вимоги до криптографічного захисту, які не враховуються традиційними уніфікованими схемами.

Для формалізації цієї неоднорідності введено поняття рівня важливості події. Класифікація базується на аналізі атрибутів події та поточного контексту системи. До статичних атрибутів належить тип події, що визначає її семантику та потенційний вплив на систему. Службові heartbeat-повідомлення за своєю природою є некритичними, тоді як автентифікаційні події містять чутливі дані облікових записів [13]. Динамічні атрибути включають поточний рівень загроз в системі, що може змінюватися залежно від виявлених аномалій або зовнішніх індикаторів компрометації.

Розроблено чотирирівневу класифікацію важливості. Рівень L0 призначений для публічних даних, розголошення яких не завдає шкоди - наприклад, агреговані метрики продуктивності системи. Рівень L1 охоплює стандартні операційні дані, що потребують базового захисту конфіденційності. Рівень L2 застосовується до інформації підвищеної важливості, включаючи

персональні дані та комерційну інформацію. Рівень L3 зарезервовано для критичних даних - команд управління небезпечним обладнанням, фінансових транзакцій, автентифікаційних токенів. У таблиці 1 наведено їх особливості.

**Таблиця 1.** Специфікація криптографічних профілів

| Рівень | Алгоритм | Ключ | Nonce | Тег | Ротація | Анти-повтор |
|---|---|---|---|---|---|---|
| L0 | ASCON-Hash256 | - | - | 64 | - | Ні |
| L1 | ASCON-AEAD128 | 128 | counter | 128 | 1 год | Ні |
| L2 | ASCON-AEAD128 | 128 | random | 128 | 15 хв | Так |
| L3 | AES-256-GCM-SIV | 256 | SIV | 128 | 5 хв | Так |

Кожному рівню важливості поставлено у відповідність криптографічний профіль, що визначає параметри захисту. Профілі розроблено з урахуванням сучасних стандартів легковагової криптографії [14], зокрема сімейства алгоритмів ASCON, стандартизованого NIST у 2023 році. Для рівня L0 застосовується лише контроль цілісності через криптографічне хешування, що забезпечує виявлення модифікацій без шифрування вмісту. Рівні L1 та L2 використовують автентифіковане шифрування ASCON-AEAD128, що поєднує конфіденційність та цілісність в одній операції. Профіль L2 додатково активує механізми захисту від повторного відтворення повідомлень та скорочує період ротації ключів [15]. Рівень L3 застосовує режим AES-GCM-SIV, стійкий до випадкового повторного використання nonce, та найкоротший період ротації.

Вибір профілю для конкретної події здійснюється алгоритмом, що мінімізує обчислювальні витрати за умови дотримання обмежень на допустимий ризик. Витрати включають затримку виконання криптографічних операцій, енергоспоживання та додаткові байти на кожне повідомлення [16]. Обмеження ризику формулюється як максимально допустима ймовірність успішної атаки на конфіденційність або цілісність даного рівня важливості.

Експериментальна програма включала три серії досліджень. Перша серія порівнювала ефективність трьох стратегій захисту: уніфікованої з максимальним профілем, адаптивної з контекстним вибором та мінімальної з базовим профілем. Друга серія аналізувала вплив класу пристрою на характеристики витрат - від ресурсно-обмежених сенсорів до серверних платформ. Третя серія досліджувала поведінку адаптивної системи при варіюванні рівня загроз від низького до критичного.

## 6. Результати досліджень

Для проведення експериментального дослідження розроблено програмний комплекс мовою Python, що реалізує всі компоненти запропонованої моделі. Код включає класи для представлення подій та контексту, реалізацію функції важливості із налаштовуваними ваговими коефіцієнтами, чотири криптографічні профілі з характеристиками продуктивності, моделі витрат та ризику для трьох класів пристроїв, алгоритм Policy Decision Point із кешуванням рішень, генератор синтетичних потоків подій та модуль візуалізації на базі бібліотеки matplotlib. На рисунку 1 продемонстровано реалізацію обчислення залишкового ризику.

```python
@classmethod
def calculate_risk(cls, profile: CryptoProfile, event: Event) -> float:
    """
    Обчислює залишковий ризик для комбінації профіль-подія

    Returns:
        float: Ризик [0, 1], де 0 - мінімальний, 1 - максимальний
    """
    ctx = event.context
    mitigation = cls.PROFILE_MITIGATION[profile.level]

    # Базовий ризик від типу події
    event_sensitivity = ImportanceFunction.EVENT_TYPE_SCORES.get(
        ctx.event_type, 0.5
    )

    # Розрахунок компонентів ризику
    conf_risk = event_sensitivity * (1 - mitigation["confidentiality"]) * ctx.threat_level
    integ_risk = event_sensitivity * (1 - mitigation["integrity"]) * ctx.threat_level
    replay_risk = (1 - mitigation["replay"]) * ctx.threat_level * 0.5

    # Додаткові фактори ризику
    cross_domain_factor = 1.2 if ctx.source_domain != ctx.destination_domain else 1.0
    fanout_factor = 1 + 0.05 * (ctx.fan_out - 1)

    total_risk = (conf_risk * 0.4 + integ_risk * 0.4 + replay_risk * 0.2) * \
                 cross_domain_factor * fanout_factor

    return min(1.0, total_risk)
```

**Рис. 1.** Обчислення залишкового ризику (авторська розробка).

Порівняльний аналіз стратегій криптографічного захисту проведено на вибірці з десяти тисяч подій, згенерованих відповідно до типового розподілу промислової IoT-системи. Переважну частину потоку становлять телеметричні дані та службові повідомлення, тоді як критичні події виникають значно рідше. Характеристики edge-пристроїв обрано як базовий сценарій, оскільки цей клас обладнання найчастіше виконує функції шлюзу між кінцевими пристроями та хмарною інфраструктурою.

Уніфікована стратегія із застосуванням максимального профілю L3 до всіх подій продемонструвала очікувано найвищі показники захищеності. Середній залишковий ризик був найнижчим. Водночас ресурсні витрати виявились значними: кожна подія потребувала в середньому більше часу на криптографічну обробку, споживала більше енергії та додавала службову інформації до розміру повідомлення.

Мінімальна стратегія з профілем L0 характеризувалась протилежними показниками. Затримка скоротилась до 11 мікросекунд, енергоспоживання та накладні витрати суттєво знизилися. Проте зріс залишковий ризик, що є неприйнятним для систем із критичними даними. Фактично, кожна сьома подія потенційно вразлива до компрометації.

Адаптивна стратегія з контекстним вибором профілю посіла проміжну позицію, що відповідає концепції оптимального компромісу. Середня затримка склала 16 мікросекунд - втричі менше за уніфіковану стратегію. Енергоспоживання знизилось до 66 мікроджоулів, накладні витрати - до 22 байтів. Залишковий ризик хоча і перевищує показник уніфікованої стратегії, залишається в межах встановлених порогів для кожного рівня важливості окремо. Всі ці результати показано на рисунку 2. Помітно, що адаптивна стратегія наближається до мінімальної за витратами, водночас забезпечуючи значно кращий захист.

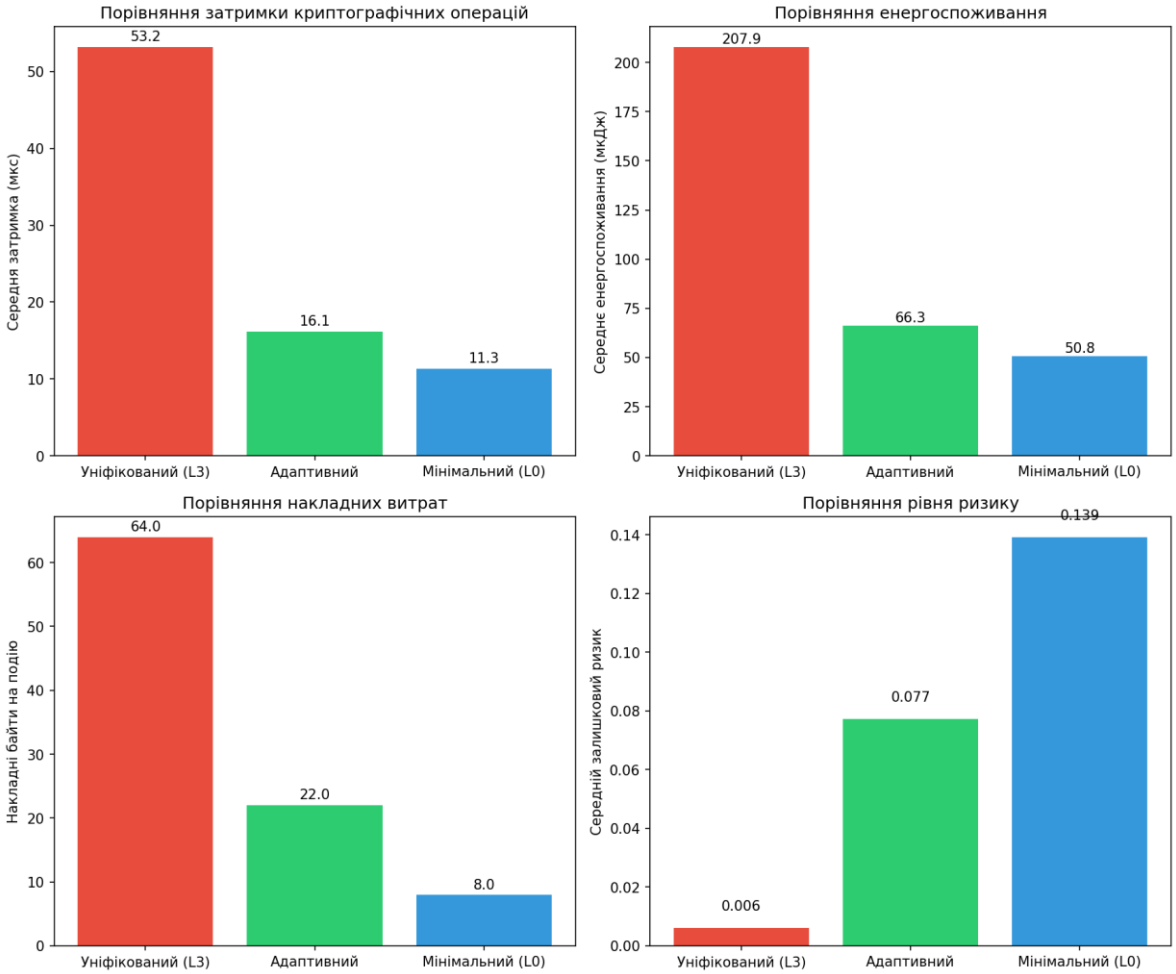


**Рис. 2.** Результати порівняння стратегій захисту (авторська розробка).

Тестування на різних класах пристроїв, як показано на рисунку 3, підтвердило універсальність підходу. Для ресурсно-обмежених пристроїв абсолютні значення затримки та енергоспоживання очікувано вищі через обмежену обчислювальну потужність. Уніфікована стратегія потребує втричі більше часу на подію, як адаптивна. Така економія критично важлива для батарейних IoT-вузлів, де енергетичний бюджет жорстко обмежений.

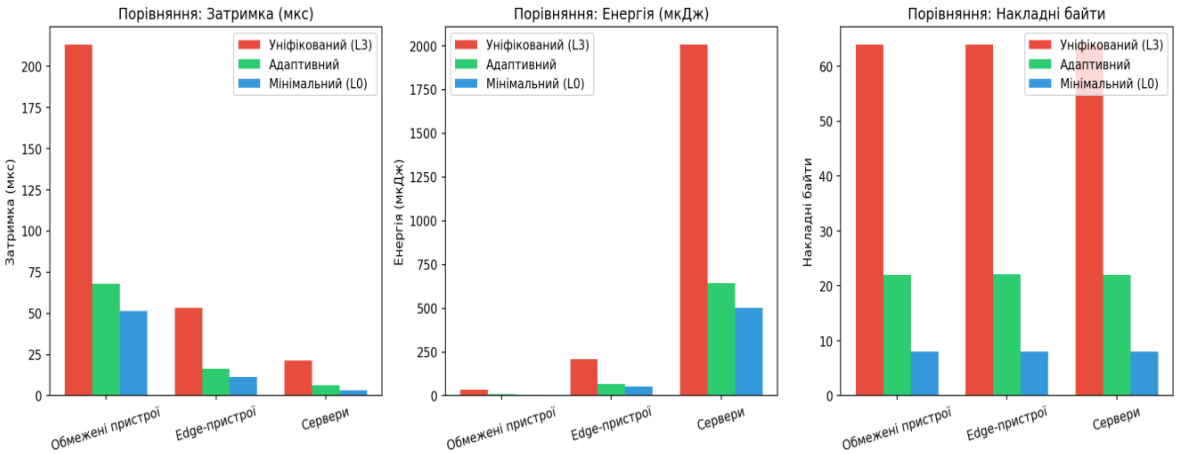


**Рис. 3.** Тестування стратегій на різних класах пристроїв (авторська розробка).

Серверні платформи демонструють на порядок нижчі абсолютні витрати завдяки потужним процесорам та апаратному прискоренню криптографії. Проте відносна економія витрат адаптивної стратегії свідчить про архітектурну перевагу підходу, незалежну від апаратної платформи.

## 7. Перспективи подальшого розвитку досліджень

Отримані результати відкривають декілька напрямків для продовження досліджень у галузі контекстно-орієнтованого криптографічного захисту event-driven систем.

Першим перспективним напрямком є застосування методів машинного навчання для автоматичного налаштування функції важливості. Поточна реалізація використовує експертно визначені вагові коефіцієнти, що потребує ручного калібрування під конкретний домен застосування. Навчання моделі на історичних даних про інциденти безпеки дозволило б автоматично виявляти приховані залежності між атрибутами подій та їх реальною критичністю.

Другий напрямок пов’язаний з інтеграцією запропонованого підходу у існуючі брокери повідомлень. Apache Kafka, RabbitMQ та інші популярні платформи наразі пропонують лише транспортне шифрування на рівні з’єднання. Реалізація контекстно-орієнтованого шифрування на рівні окремих повідомлень потребує розробки плагінів або модифікації ядра брокера. Практична імплементація дозволила б провести випробування на реальних навантаженнях та порівняти теоретичні оцінки витрат з фактичними вимірюваннями.

Третій напрямок стосується розширення моделі загроз з урахуванням специфіки розподілених систем. Поточна модель розглядає атаки на окремі повідомлення, проте не враховує кореляційні атаки на потоки подій, атаки на метадані маршрутизації та часові атаки на виявлення шаблонів комунікації. Формалізація цих загроз та розробка відповідних механізмів захисту підвищить комплексність підходу.

Четвертий напрямок передбачає акселерацію криптографічних операцій на ресурсно-обмежених пристроях. Сучасні мікроконтролери все частіше включають криптографічні співпроцесори, проте їх можливості обмежені фіксованим набором алгоритмів. Дослідження оптимальних стратегій використання апаратних прискорювачів у контексті адаптивного вибору профілю може додатково знизити енергоспоживання та затримки.

Реалізація зазначених напрямків сприятиме переходу від концептуальної моделі до промислово придатного рішення для захисту event-driven систем критичної інфраструктури.

## 8. Висновки

Дослідження контекстно-орієнтованої криптографічної політики для event-driven систем дозволило комплексно проаналізувати взаємозалежність між рівнем криптографічного захисту та ресурсними витратами в системах обробки подій з неоднорідним трафіком. В умовах широкого поширення IoT-платформ, промислових систем автоматизації та розподілених обчислювальних середовищ питання адаптивного вибору криптографічних параметрів набуває особливої важливості.

Запропонована чотирирівнева класифікація важливості подій (L0-L3) разом із відповідними криптографічними профілями дозволяє розділяти захист відповідно до типу даних. Рутинні телеметричні повідомлення та службові heartbeat-сигнали обробляються легковаговими профілями з мінімальними накладними витратами, тоді як критичні команди управління та автентифікаційні події отримують максимальний рівень захисту із застосуванням misuse-resistant алгоритмів та коротких періодів ротації ключів.

Проведений аналіз показав, що традиційний підхід із застосуванням уніфікованого криптографічного захисту є неефективним для event-driven систем, оскільки призводить до надлишкових витрат ресурсів на захист некритичних даних. Запропонована контекстно-

орієнтована політика забезпечує економію часу обробки, зменшення накладних витрат та збільшення пропускної здатності на без компрометації безпеки критичних подій.

Імітаційне моделювання підтвердило принципову ефективність підходу: адаптивне шифрування «за важливістю події» дозволяє зменшувати середні криптографічні накладні витрати для високочастотних некритичних потоків (рівні L0-L1), зберігаючи посилений захист для критичних подій (L3) і дотримуючись заданих порогів ризику на кожному рівні важливості. Отримані результати демонструють керований компроміс між витратами та безпекою, що є особливо важливим для IoT/edge-середовищ, де обчислювальний та енергетичний бюджет обмежений.

Загалом, запропонована контекстно-орієнтована криптографічна політика формує методологічну основу для проєктування криптографічних підсистем у event-driven архітектурах і може бути використана як основа для подальшої практичної інтеграції в брокери повідомлень та промислові EDA-платформи. Подальші дослідження доцільно спрямувати на автоматизоване налаштування функції важливості (зокрема на основі історії інцидентів), експериментальну валідацію на реальних навантаженнях у Kafka/RabbitMQ-подібних середовищах та розширення моделі загроз на кореляційні й метадані-орієнтовані атаки у потоках подіях.

---

**Список літератури:**


1) Confluent. (2024). *What is Event Driven Architecture?* https://www.confluent.io/learn/event-driven-architecture/

2) Pietrzak, S. (2024). *Event-Driven Architectures: An Introduction and Security Challenges. Medium.* https://medium.com/@spietrza/event-driven-architectures-an-introduction-and-security-challenges

3) Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). *Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors, 24(12), 4008*. https://doi.org/10.3390/s24124008

4) Liyanage, M. (2024). *Event Driven Architecture for Large Scale IoT Systems. Medium; Xeynergy Blog*. https://blog.xeynergy.com/event-driven-architecture-for-large-scale-iot-systems-511ea7d8b6cd

5) Zhong, Y., & Gu, J. (2024). *Lightweight block ciphers for resource-constrained environments: A comprehensive survey. Future Generation Computer Systems,* 157, 288-302. https://doi.org/10.1016/j.future.2024.03.054

6) Sylla, T., Chalouf, M.A., Krief, F., Samaké, K. (2020). *Towards a Context-Aware Security and Privacy as a Service in the Internet of Things.* https://doi.org/10.1007/978-3-030-41702-4_15

7) Turan M., McKay K., Kang J., Kelsey J., Chang D. (2025). *Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions*. https://doi.org/10.6028/NIST.SP.800-232

8) Lookabaugh, T., & Sicker, D. C. (2004). *Selective encryption for consumer applications. IEEE Communications Magazine,* 42(5), 124–129. https://doi.org/10.1109/mcom.2004.1299355

9) Inshi, S., Chowdhury, R., Ould-Slimane, H., & Talhi, C. (2023). *Secure Adaptive Context-Aware ABE for Smart Environments. IoT,* 4(2), 112-130. https://doi.org/10.3390/iot4020007

10) Shujaa W., Alanzi M., Sankaranarayanan S. (2025). *Enhancing IoT security through blockchain integration.* Frontiers in Computer Science. 7:1670473. https://doi.org/10.3389/fcomp.2025.1670473

11) Ansari, S.A., Ali, S. (2025). *A systematic review of lightweight cryptographic schemes for security and privacy in IoT. Discov Computing 28, 266*. https://doi.org/10.1007/s10791-025-09755-3

12) Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). *Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology,* 34(3). https://doi.org/10.1007/s00145-021-09398-9

13) Alzubaidi, A., & Kalita, J. (2016). *Authentication of Smartphone Users Using Behavioral Biometrics. IEEE Communications Surveys & Tutorials,* 18(3). https://doi.org/10.1109/comst.2016.2537748

14) Khan, S., Ferreira Lopes martins, P. A., Sousa, B., & Pereira, V. (2025). *A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems. ACM Computing Surveys,* 58(1), 1–37. https://doi.org/10.1145/3757734

15) Menon, R. (2024). *The Impact Of Adaptive Encryption Algorithms On Cloud Data Confidentiality.* In International Journal of Scientific Research & Engineering Trends. http://doi.org/10.5281/zenodo.17800103

16) Xu, Z., Zhou, W., Han, H. et al. (2025). *A secure and scalable IoT access control framework with dynamic attribute updates and policy hiding. Sci Rep 15*, *11913*. https://doi.org/10.1038/s41598-024-80307-3

# Context-aware cryptographic policy for event-driven architectures: encryption based on event importance

**Igor Andrushchak**
Department of Software Engineering, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0000-0002-8751-4420

**Oleksandr Koloshko**
Department of Software Engineering, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0009-0001-9325-9542

**Abstract:** The article discusses an approach to building a context-oriented cryptographic policy for event-driven systems in which data exchange is implemented through asynchronous events, streams, and logs (log-based integration). Such systems generate huge volumes of heterogeneous events with varying criticality and confidentiality requirements. In such architectures, events are often delivered according to the at-least-once semantics, duplicated when repeated, stored for a long time in brokers/repositories, transferred between domains, and reproduced to restore the state. This increases the risks of compromising confidentiality and integrity, and also creates practical prerequisites for nonce/IV usage errors in authenticated encryption modes with attached data. The main idea of the work is to formalize the «importance of an event» as a policy attribute that guides the choice of a cryptographic profile (encryption algorithm, nonce strategy, associated data policy, key rotation, anti-replay mechanisms) taking into account limited resources (execution time, memory, energy consumption, overhead bytes, and network constraints). Existing approaches to event classification and selective encryption mechanisms are analyzed. A model of events and context, an importance function, a cost model, and a risk model are proposed, as well as an optimization problem of "minimizing costs under risk constraints" for automated selection of a protection profile. The scientific novelty lies in combining the principles of Authenticated Encryption with Associated Data and Attribute-Based Access Control approach to policies and hierarchical key management in a unified policy framework that takes into account the duplicates/retries/long-term storage of events characteristic of event-driven systems and introduces semantic integrity through authentication of the delivery context as part of associated data. The practical significance lies in the proposed policy templates for different levels of importance (L0–L3), as well as the methodology for domain isolation of keys and short cryptographic epochs, which reduce the consequences of compromise. An algorithm for dynamic determination of cryptographic parameters based on event priority has been developed. It is shown that adaptive encryption «by event importance» reduces cryptographic overhead in high-frequency streams without degrading the security of critical events, providing a manageable trade-off between risk and resources.

**Keywords:** event-driven architecture, context-aware encryption, cryptographic policy, event classification, lightweight cryptography, encryption optimization, IoT security.