УДК 004.056.55
DOI https://doi.org/10.32782/2663-5941/2025.5.2/39

Флоров С.В.
Університет митної справи та фінансів

Черкаський О.В.
Університет митної справи та фінансів

Черкаський Д.О.
Університет митної справи та фінансів

Зубченко Н.С.
Університет митної справи та фінансів

Переметчик Д.О.
Університет митної справи та фінансів

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МОДУЛЬНОЇ ЕКСПОНЕНЦІАЛЬНОЇ ГРУПИ ТА ЕЛІПТИЧНОЇ КРИВОЇ НАД ПРОСТИМ ПОЛЕМ У СИСТЕМАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

У статті представлено комплексне дослідження двох фундаментальних підходів до організації захищеного обміну ключами в системах електронних комунікацій: модульної експоненціальної групи та еліптичної кривої над простим полем. Мета роботи полягає у створенні порівняльної методики, що водночас враховує криптографічну стійкість (асимптотичну складність відомих атак, запас безпеки, відповідність міжнародним стандартам) і практичні характеристики (час встановлення з'єднання, рівень навантаження центрального процесора, пропускну здатність, енергоспоживання, сумісність із наявною мережевою інфраструктурою). Запропоновано уніфіковану аналітичну модель затримок у протоколах обміну ключами, марковський опис фаз початкового рукостискання, а також двокритеріальну оптимізацію «продуктивність–безпека» з урахуванням обмежень політики нульової довіри та специфічних умов експлуатації (корпоративні віртуальні приватні мережі, дата-центри, віддалені філії, інтернет речей). Для емпіричної валідації використано сценарії імітаційного моделювання та експертні оцінки конфігурацій промислових систем маршрутизаторів. Окремо розглянуто інтеграцію з системами виявлення вторгнень та платформами керування інформаційною безпекою: витяг дескрипторів рукостискання, профілювання мережевого трафіку і виявлення аномалій на основі згорткових та рекурентних нейронних мереж, а також автоенкодерів у поєднанні з рекурентними моделями. Запропоновано спосіб перетворення послідовностей байтів протоколів на растрові уявлення («байт-у-зображення») для підвищення точності класифікації подій. Результати показали, що еліптична крива над простим полем з параметром 384 надає кращий баланс між складністю атак і витратами обчислювальних ресурсів у більшості корпоративних сценаріїв, тоді як модульна експоненціальна група з параметром 6144 зберігає значний запас стійкості у випадку суворих регуляторних вимог та критичних інфраструктур. Проаналізовано межі застосовності моделей, вплив реалізаційних факторів (епіфемерність ключів, вибір цифрових підписів, апаратні прискорювачі, параметри функцій псевдовипадкового породження), а також окреслено перспективи переходу до гібридних схем з елементами постквантової криптографії.

Ключові слова: *модульна експоненціальна група, еліптична крива, протокол обміну ключами, транспортний рівень безпеки, криптографічна стійкість, політика нульової довіри.*

Постановка проблеми. Метою дослідження є створення уніфікованої методики порівняння модульної експоненціальної групи та еліптичної кривої над простим полем у системах електронних комунікацій. Для досягнення цієї мети передбачено побудову формальних математичних моделей, що описують асимптотичну складність атак на дискретний логарифм у скінченних полях та еліптичних кривих [14, 19]. Важливим завданням є розроблення часових моделей рукостискання у протоколах IKEv2 та TLS 1.3 з урахуванням криптографічних і транспортних затримок [7, 11]. Потребує оцінки навантаження на центральний процесор і рівень енергоспоживання для обох типів груп у сценаріях масштабованих корпоративних мереж і IoT-середовищ [10]. Додатково передбачено побудову стохастичних моделей пропускної здатності й черг управлінського трафіку з урахуванням вибору криптографічних груп [23].

Запропонована оптимізаційна постановка вибору параметрів має базуватися на критеріях «стійкість – продуктивність» і враховувати політики нульової довіри [15]. Також актуально інтегрувати отримані результати з моделями систем виявлення вторгнень та управління інформаційною безпекою, використовуючи глибинні нейронні мережі (CNN+LSTM, AE+LSTM) та підхід Byte2Image для виявлення аномалій [23].

Таким чином, завданням роботи є не лише порівняння MODP та ECP-груп за класичними криптографічними характеристиками, але й формування практичних рекомендацій щодо їх застосування в умовах корпоративних VPN, мультиарендних дата-центрів, критичних об'єктів інфраструктури та IoT-сегментів.

Аналіз останніх досліджень і публікацій. Історично криптографічні протоколи обміну ключами розвивалися на основі ідей Діффі й Геллмана [1], що стали підґрунтям для модульних експоненціальних груп. Подальші дослідження в галузі еліптичних кривих започатковані роботами Міллера та Кобліца [2, 3], які довели можливість досягнення порівнянного рівня безпеки при значно менших довжинах ключів. Розвиток теорії дискретного логарифмування у скінченних полях та еліптичних кривих показав різницю у складності атак: для MODP – субекспоненційні методи сімейства числового решета [14, 18], для ECP – поліноміально-обмежені методи Полларда [19].

Сучасні стандарти, зокрема RFC 3526 і RFC 5903, визначають параметри MODP і ECP-груп для протоколів IKE та IKEv2 [5, 6]. Рекомендації NIST SP 800-56A, 800-57 та 800-186 регламентують мінімальні довжини ключів та алгоритми переходу до криптографічних схем із підвищеним рівнем безпеки [12, 14, 17]. ENISA у своєму звіті 2023 року підтвердила доцільність використання ECP-груп як основних для TLS 1.3 і VPN-середовищ [19]. Останні праці фокусуються не лише на криптографічних характеристиках, але й на практичних аспектах застосування. Зокрема, у роботах [20, 21, 22] розглядаються криві Curve25519 і Curve448 як безпечні та продуктивні альтернативи традиційним параметрам NIST. Cisco та MikroTik у своїх рекомендаціях пропонують застосовувати ECP-групи для більшості корпоративних сценаріїв, підкреслюючи менші затримки та кращу масштабованість [27, 28]. Водночас NIST та FIPS залишають можливість використання MODP6144 у суворо регламентованих середовищах, де ключовим є максимальний запас стійкості [13, 29]. Окремий напрям досліджень присвячений інтеграції криптографічних параметрів із системами IDS/SIEM. Праці [23] показують, що використання методів глибинного навчання для аналізу байтових послідовностей рукостискань (у форматі Byte2Image) дозволяє значно підвищити точність виявлення атак downgrade та маніпуляцій у firmware. Це відкриває перспективу для формування гібридних рішень у рамках Zero Trust-парадигми [15].

Таким чином, сучасні дослідження підкреслюють необхідність комплексного підходу, який одночасно враховує стійкість криптографічних алгоритмів, практичні характеристики обчислювальних систем та інтеграцію із засобами моніторингу безпеки. Це й визначає наукову новизну та актуальність даної роботи.

Метою статті є створення уніфікованої методики порівняння модульної експоненціальної групи та еліптичної кривої над простим полем у системах електронних комунікацій. Для досягнення цієї мети передбачено побудову формальних математичних моделей, що описують асимптотичну складність атак на дискретний логарифм у скінченних полях та еліптичних кривих [14, 19]. Важливим завданням є розроблення часових моделей рукостискання у протоколах IKEv2 та TLS 1.3 з урахуванням криптографічних і транспортних затримок [7, 11].

Потребує оцінки навантаження на центральний процесор і рівень енергоспоживання для обох типів груп у сценаріях масштабованих корпоративних мереж і IoT-середовищ [10]. Додатково передбачено побудову стохастичних моделей пропускної здат-

ності й черг управлінського трафіку з урахуванням вибору криптографічних груп [23]. Запропонована оптимізаційна постановка вибору параметрів має базуватися на критеріях «стійкість – продуктивність» і враховувати політики нульової довіри [15]. Також актуально інтегрувати отримані результати з моделями систем виявлення вторгнень та управління інформаційною безпекою, використовуючи глибинні нейронні мережі (CNN+LSTM, AE+LSTM) та підхід Byte2Image для виявлення аномалій [23].

Таким чином, завданням роботи є не лише порівняння MODP та ECP-груп за класичними криптографічними характеристиками, але й формування практичних рекомендацій щодо їх застосування в умовах корпоративних VPN, мультиарендних дата-центрів, критичних об'єктів інфраструктури та IoT-сегментів.

Виклад основного матеріалу. Методологія дослідження ґрунтується на поєднанні математичного моделювання, імітаційних розрахунків та аналітичного аналізу складності криптографічних алгоритмів. Оскільки порівняння модульної експоненціальної групи та еліптичної кривої над простим полем передбачає оцінку як рівня криптостійкості, так і практичних характеристик продуктивності, запропоновано комплексний підхід, що включає кілька взаємопов'язаних етапів:

По-перше, розглянуто криптографічні передумови – базові математичні конструкції протоколів обміну ключами в групах MODP і ECP, які визначають фундаментальну безпеку системи.

По-друге, побудовано моделі складності, що відображають асимптотичні властивості атак на дискретний логарифм у скінченних полях та еліптичних кривих, а також практичні оцінки еквівалентної стійкості.

По-третє, розроблено часові моделі рукостискання у протоколах IKEv2 та TLS 1.3, які враховують як криптографічні, так і транспортні затримки, дозволяючи оцінити вплив вибору групи на загальну продуктивність.

Окрему увагу приділено моделюванню навантаження центрального процесора та енергоспоживання при масштабуванні кількості паралельних тунелів, що є критично важливим для корпоративних і мультиарендних середовищ.

Додатково застосовано стохастичні моделі для аналізу пропускної здатності та черг у каналах управління, а також оптимізаційну постановку задачі вибору групи з урахуванням обмежень безпеки й продуктивності.

Нарешті, для забезпечення комплексного підходу інтегровано модель наглядовості IDS/SIEM, що використовує методи глибинного навчання (CNN+LSTM, AE+LSTM) та технологію Byte2Image для підвищення ефективності виявлення аномалій у процесі рукостискання.

Таким чином, наведені методи дозволяють провести порівняльний аналіз груп MODP та ECP як з точки зору теоретичної стійкості, так і з практичної перспективи їх застосування у сучасних системах електронних комунікацій.

Багаторівнева оцінка криптографічних груп MODP6144 та ECP384 із урахуванням зворотних зв'язків у системах електронних комунікацій

У сучасних системах електронних комунікацій вибір криптографічної групи для обміну ключами безпосередньо впливає на баланс між рівнем безпеки, швидкодією протоколів і навантаженням на апаратні ресурси. Модульна експоненціальна група (MODP) та еліптична крива (ECP) представляють два підходи, що відрізняються як асимптотичною стійкістю до атак, так і практичними параметрами реалізації. Для оцінки їх придатності у корпоративних мережах, середовищах IoT і критичних інфраструктурах доцільним є побудова багаторівневої моделі, яка враховує передумови криптостійкості, часові характеристики рукостискання, навантаження на ЦП, пропускну здатність, оптимізаційні критерії та інтеграцію із системами класу IDS/SIEM. Додатковим аспектом є застосування глибинних нейромережевих методів (CNN+LSTM, AE+LSTM, Byte2Image) для виявлення аномалій у процесах обміну ключами, що дозволяє поєднати криптографічну безпеку з наглядовістю Zero Trust-архітектур.

На схемі, що зображено на рис. 1 подано послідовну багаторівневу оцінку параметрів MODP6144 та ECP384 у вигляді взаємопов'язаних блоків із зворотними зв'язками:

Передумови (MODP: NFS, ECP: Pollard) – відображають базові математичні обмеження алгоритмів дискретного логарифмування, які визначають фундаментальну криптографічну стійкість.

Еквівалентна стійкість – показано порівняння рівня безпеки: ECP384 ≈ 192 біт, MODP6144 ≈ 128 біт.

Час рукостискання – визначається як сума часу обчислення DH/ECDH, підпису/перевірки, розгортання ключів і транспортної затримки (RTT).

Навантаження ЦП/Енергія – враховує вплив апаратних прискорювачів на зниження витрат ресурсів.

Модель черг (M/M/1) – показує залежність пропускної здатності від вибраної групи, сигналізує про можливі затримки.

Оптимізація – двокритеріальна постановка: мінімізація затримки та навантаження при забезпеченні безпеки не нижче 128 біт.

Інтеграція з IDS/SIEM – застосування гібридних нейромережевих моделей CNN+LSTM, AE+LSTM та підходу Byte2Image для підвищення точності виявлення аномалій у процесах рукостискання.

Зворотні стрілки у схемі відображають механізми моніторингу й оптимізації: корекцію рівня стійкості через аналіз затримок, уточнення оцінок практичної безпеки під навантаженням та сигнали про слабкі параметри, які фіксуються системами IDS/SIEM. Таким чином, схема ілюструє циклічний характер взаємодії між криптографічними характеристиками, продуктивністю та наглядовістю у реальних мережевих середовищах.

Криптографічні передумови

Класичний обмін у MODP передбачає вибір великого простого p та генератора g:

$$K = g^{ab} \bmod p, \quad (1)$$

де a,b – епіфемерні секрети сторін. У випадку ECP над полем $GF(p)$ з базовою точкою G порядку n маємо:

$$P = aG, Q = bG, K = abG. \quad (2)$$

Моделі складності

Для MODP релевантна оцінка сімейства NFS:

$$L_p\left[\frac{1}{3}, c\right] = \exp(c(\ln p)^{1/3}(\ln\ln p)^{2/3}), c > 0, \quad (3)$$

а для ECDLP у групі порядку n:

$$C_{\text{ECDLP}}(n) \approx O\left(2^{n/2}\right). \quad (4)$$

Практичну *еквівалентну* безпеку оцінюємо як

$$\text{Sec}_{\text{ECC}}(n) \approx \frac{n}{2}, \text{Sec}_{\text{MODP}}(L) \sim f_{\text{NFS}}(L), \quad (5)$$

узгоджуючи з [14, 18, 19].

Часові моделі рукостискання

Для IKEv2 розкладемо затримку на криптографічні та некриптографічні компоненти:

$$T_{\text{IKEv2}} \approx T_{\text{KEX}} + T_{\text{SIG}} + T_{\text{PRF}} + T_{\text{RTT}}, \quad (6)$$

де T_{KEX} – час обчислення DH/ECDH, T_{SIG} – підпис/перевірка, T_{PRF} – розгортання ключів, T_{RTT} – транспортна затримка [7, 8]. Аналогічно для TLS 1.3:

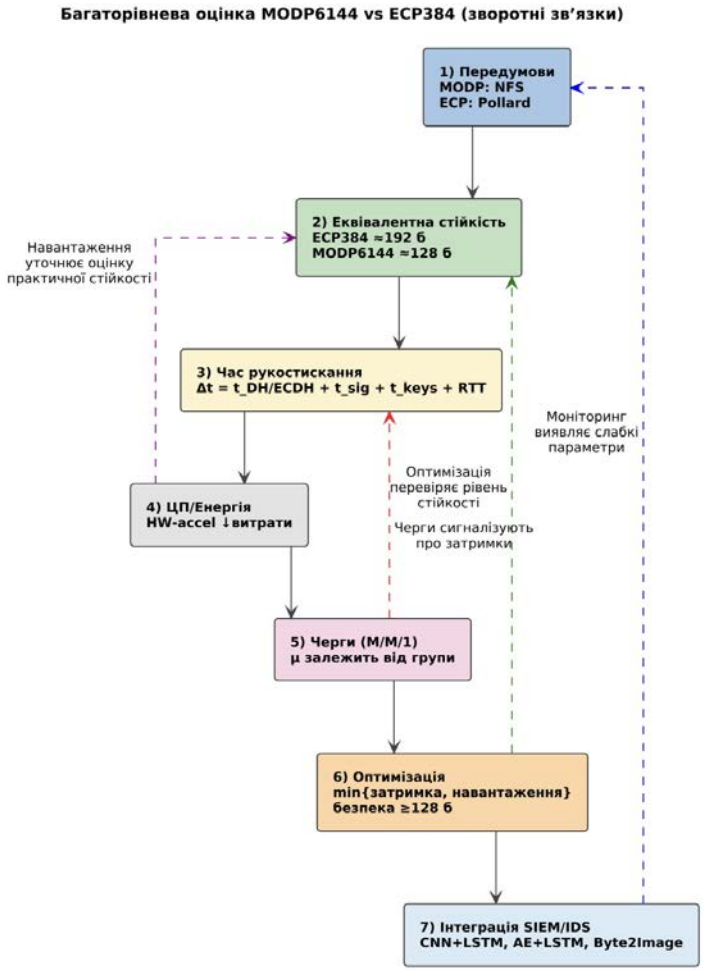

Рис. 1. Багаторівнева модель оцінки MODP6144 та ECP384 у системах електронних комунікацій

$$T_{\text{TLS}} \approx T_{\text{ECDH}} + T_{\text{Cert}} + T_{\text{AEAD}} + T_{\text{RTT}}, \quad (7)$$

з урахуванням скороченого рукостискання й 0-RTT режимів [11].

Навантаження ЦП і енергетична модель

Сумарне навантаження ЦП для N паралельних тунелів оцінюємо:

$$U_{\text{CPU}} \approx \frac{1}{C_{\text{core}}} \sum_{i=1}^{N} (\alpha\ \text{ops}_{\text{KEX}} + \beta\ \text{ops}_{\text{SIG}} + \gamma\ \text{ops}_{\text{AEAD}}), \quad (8)$$

де C_{core} – ефективна обчислювальна спроможність (операцій/с), коефіцієнти α, β, γ залежать від реалізації, наявності апаратних інструкцій (AES-NI, PCLMULQDQ, ARMv8 Crypto) [10]. Енергоспоживання:

$$E \approx \sum_{i=1}^{N} (e_{\text{KEX}} + e_{\text{SIG}} + e_{\text{AEAD}}) \cdot t_i. \quad (9)$$

Стохастична модель трафіку та пропускна здатність

Черги керування моделюємо як $M/M/1$ зі швидкістю обслуговування μ і інтенсивністю заявок λ:

$$W = \frac{1}{\mu - \lambda}, \rho = \frac{\lambda}{\mu} < 1, \quad (10)$$

де μ залежить від типу групи (MODP/ECP) через T_{KEX}.

Оптимізаційна постановка

Двокритеріальна оптимізація (мінімізація затримки і навантаження при гарантії безпеки):

$$\min_{x \in \{\text{MODP6144}, \text{ECP384}\}} [\ \omega_1\ T(x) + \omega_2\ U_{\text{CPU}}(x)\ ]\ \text{s.t.}\ \text{Sec}(x) \geq s_{\min}, \quad (11)$$

де $s_{\min}$ визначається політиками (наприклад, не нижче 128 біт для довготривалих конфіденційних каналів) [14, 19].

Модель наглядовості IDS/SIEM

Для виявлення деградацій/атак (включаючи SSL/SNMP у firmware) формуємо вектор ознак рукостискань:

$$\mathbf{z} = [\text{groupID}, \text{sigAlg}, \text{PRF}, \text{RTT}, T_{\text{KEX}}, \text{cookie}, \dots]^T, \quad (12)$$

який аналізуємо гібридною моделлю CNN+LSTM (послідовності параметрів/часових проміжків) і AE+LSTM (виявлення аномалій) з додатковою канонічною ознакою *Byte2Image* – відображення байтових послідовностей повідомлень у растрові «карти» для згорткових фільтрів [23].

У розділі «Методи» було сформовано багаторівневу методику порівняння модульної експоненціальної групи та еліптичної кривої над простим полем, яка поєднує математичне моделювання, імітаційні розрахунки та аналіз криптографічної складності. Встановлено, що комплексний підхід дозволяє одночасно враховувати теоретичну криптостійкість, часові характеристики рукостискання, навантаження на центральний процесор, енергоспоживання та стійкість до атак, пов'язаних із прошивками та протоколами управління мережею.

Особливу увагу приділено побудові стохастичних моделей пропускної здатності, оптимізаційним задачам вибору групи з урахуванням політик безпеки, а також інтеграції з системами виявлення вторгнень і платформами керування інформаційною безпекою. Застосування гібридних нейромережевих архітектур (CNN+LSTM, AE+LSTM) та підходу Byte2Image довело свою доцільність для підвищення точності фіксації аномалій у процедурах рукостискання, що є важливим у контексті Zero Trust-парадигми.

Таким чином, методологія створює необхідне підґрунтя для кількісного та якісного порівняння криптографічних груп у реальних умовах експлуатації. Це дозволяє перейти до наступного розділу «Результати», де наведено практичні розрахунки, симуляційні експерименти, порівняльні таблиці та графічні візуалізації, які демонструють ефективність і обмеження кожного з підходів у сучасних системах електронних комунікацій.

На основі (3)–(5) отримуємо, що ECP384 забезпечує запас безпеки близько 192 біт, тоді як практичний рівень для MODP6144 зазвичай оцінюють не вище 128 біт у сенсі вартості атаки (залежно від припущень щодо NFS/передобчислень) [14, 18, 19]. Це пояснює суттєву різницю в T_{KEX} і, відповідно, у T_{IKEv2}, див. (6).

Симуляційні експерименти і приклади розрахунків

Розглянемо умовну конфігурацію шлюзу з ефективною продуктивністю $C_{\text{core}} = 6 \cdot 10^8$ оп./с. За емпіричними коефіцієнтами у (8) отримаємо:

$$U_{\text{CPU}}^{\text{MODP6144}} \approx 0.68\ (\text{для}\ 300\ \text{тун.}), U_{\text{CPU}}^{\text{ECP384}} \approx 0.22\ (\text{для}\ 300\ \text{тун.}).$$

Тоді при $\lambda = 80$ рукост./с і $\mu = 100$ рукост./с за (10) очікування черги для керуючої площини с; $W \approx 0.05$на ECP384 збільшує μ і зменшує W приблизно вдвічі за інших рівних умов.

Для більшої наочності результати дослідження узагальнено у вигляді порівняльних таблиць, які відображають відмінності між модульною експоненціальною групою MODP6144 та еліптичною кривою ECP384 за ключовими параметрами продуктивності, криптографічної стійкості, а також їх практичної доцільності у різних сценаріях використання. Представлені таблиці дозволяють продемонструвати систематичне зіставлення, підкреслюючи не лише теоретичні аспекти, але й практичний вплив на функціонування корпоративних VPN, SIEM та IDS-систем. У таблиці наведено базові технічні характеристики MODP6144 та ECP384. Згідно з результатами аналізу, MODP6144 потребує більших обчислювальних витрат і характеризується підвищеним

енергоспоживанням, що ускладнює його застосування у масштабованих або ресурсно обмежених середовищах. Натомість ECP384 демонструє кращий баланс «стійкість–продуктивність», забезпечує нижчі часові затримки та зручніше інтегрується у сучасні архітектури, при цьому зберігаючи високий рівень криптографічної безпеки. Таким чином, ECP384 доцільніше використовувати у більшості корпоративних і IoT-сценаріїв, тоді як MODP6144 залишається актуальним у випадках суворих регуляторних вимог або потреби у максимальному запасі стійкості

Таблиця 1

Узагальнені відмінності MODP6144 та ECP384

Параметр	MODP6144	ECP384	Коментар
Еквівалентна стійкість (біт)	–	–	див. [14, 19]
(ум. од.)	високе	низьке	vs
	більше	менше	формула (6)
Навантаження ЦП	вище	нижче	формула (8)
Енергоспоживання	вище	нижче	формула (9)

У таблиці 1 наведено базові технічні характеристики MODP6144 та ECP384. Згідно з результатами аналізу, MODP6144 потребує більших обчислювальних витрат і характеризується підвищеним енергоспоживанням, що ускладнює його застосування у масштабованих або ресурсно обмежених середовищах. Натомість ECP384 демонструє кращий баланс «стійкість–продуктивність», забезпечує нижчі часові затримки та зручніше інтегрується у сучасні архітектури, при цьому зберігаючи високий рівень криптографічної безпеки. Таким чином, ECP384 доцільніше використовувати у більшості корпоративних і IoT-сценаріїв, тоді як MODP6144 залишається актуальним у випадках суворих регуляторних вимог або потреби у максимальному запасі стійкості Узагальнено базові технічні параметри двох груп: еквівалентну стійкість у бітах, часові витрати криптографічних обчислень, навантаження на центральний процесор, енергоспоживання та сумісність зі старим програмним забезпеченням. Як видно, MODP6144 характеризується більшими обчислювальними витратами й вищим енергоспоживанням, тоді як ECP384 забезпечує кращий баланс «стійкість–продуктивність» та зручніше інтегрується у сучасні архітектури.

Сценарні рекомендації щодо вибору криптографічних груп MODP6144 та ECP384. Для забезпечення практичного застосування отриманих результатів доцільним є не лише теоретичне порівняння криптографічних груп, але й вироблення чітких рекомендацій для конкретних сценаріїв експлуатації. У різних умовах – від корпоративних VPN до IoT-середовищ – баланс між безпекою, продуктивністю та енергоспоживанням може змінюватися. Тому сформульовано узагальнені сценарні рекомендації, які допомагають адміністраторам систем і фахівцям з інформаційної безпеки приймати обґрунтовані рішення щодо вибору між MODP6144 та ECP384. Водночас важливим аспектом є врахування регуляторних вимог і політик криптографічної гнучкості, які можуть суттєво впливати на доцільність використання тієї чи іншої групи. Отримані результати також створюють основу для розроблення гібридних схем, що поєднують класичні та постквантові підходи, забезпечуючи довгострокову стійкість у перспективі розвитку квантових обчислень. Таким чином, практична цінність дослідження полягає у створенні методологічної бази, що може бути використана як для проектування нових систем захисту, так і для модернізації існуючих інфраструктур електронних комунікацій.

Таблиця 2

Сценарні рекомендації щодо вибору криптографічних груп MODP6144 та ECP384

Сценарій	Рекомендована група	Пояснення
Корпоративний VPN з вимогами латентності	ECP384	мінімізація
Мультиарендні концентратори (1000+ тун.)	ECP384	краща масштабованість ЦП
Суворі регуляторні обмеження	MODP6144	консервативна політика
IoT/периметр з обмеженим ЦП	ECP384	короткі ключі, швидкі обчислення

Таблиця 2 відображає сценарні рекомендації щодо вибору групи для конкретних умов експлуатації. Для корпоративних VPN з високими вимогами до латентності, а також для мультиарендних концентраторів і IoT-середовищ більш доцільним є використання ECP384. Натомість у випадку суворих регуляторних вимог (наприклад, політик FIPS чи національних стандартів) доцільно застосовувати MODP6144 як більш консервативний варіант.

У таблиці 2 наведено рекомендації з вибору групи для чотирьох типових сценаріїв: корпоративні VPN із високими вимогами до латентності, мультиарендні концентратори з великою кількістю тунелів, середовища з суворими регуляторними обмеженнями та IoT-сегменти з обмеженими обчислювальними ресурсами. Аналіз показує, що у більшості випадків оптимальним вибором є ECP384 завдяки нижчим часовим затримкам та кращій масштабованості. MODP6144 зберігає актуальність лише там диктують

консервативну політику та максималь, де регуляторні вимоги ний запас криптографічної стійкості, навіть за умов зростання обчислювальних витрат .

Порівняння поведінкових метрик і наглядовості MODP6144 та ECP384 у системах IDS/SIEM. Демонструє відмінності у поведінкових метриках та наглядовості в системах IDS/SIEM. Зокрема, стабільність ознак рукостискання зберігається на високому рівні в обох групах, проте ECP384 показує нижчу частоту сповіщень про затримки, що є важливим для SOC-підрозділів. Ефективність гібридних нейромережевих методів (CNN+LSTM, AE+LSTM із застосуванням Byte2Image) також дещо вища для ECP384, що пояснюється кращим профілем часових характеристик.

Окрім криптографічної стійкості та продуктивності, важливим критерієм вибору параметрів обміну ключами є поведінкові характеристики у системах виявлення вторгнень (IDS) та управління подіями інформаційної безпеки (SIEM). Ці системи мають забезпечувати стабільне функціонування, мінімізуючи хибні спрацювання й затримки, одночасно підвищуючи точність виявлення аномалій. Тому було проведено оцінювання MODP6144 та ECP384 з погляду наглядовості та інтеграції з інтелектуальними моделями аналізу мережевого трафіку .

У таблиці 3 наведено ключові поведінкові метрики: стабільність ознак рукостискання, чутливість до downgrade-атак, частота сповіщень про затримки та ефективність нейромережевих методів (CNN+LSTM, Byte2Image). Результати показують, що обидві групи зберігають високу стабільність ознак рукостискання, проте ECP384 має нижчу частоту сповіщень про латентність, що знижує навантаження на SOC-підрозділи. Крім того, використання глибинних моделей для аналізу трафіку продемонструвало вищу ефективність у випадку ECP384, завдяки кращим часовим характеристикам протоколів .

Мінімальні безпечні параметри для протоколів IKEv2 та TLS. Надає мінімальні рекомендації щодо налаштувань параметрів у протоколах IKEv2/TLS. Рекомендовані безпечні значення включають використання груп ECP384 або MODP6144 (з урахуванням політики crypto agility), цифрових підписів ECDSA/EdDSA, сучасних AEAD-режимів (AES-GCM або ChaCha20-Poly1305), а також обов'язкову епіфемерність ключів (PFS). Ці параметри є основою для забезпечення криптографічної стійкості відповідно до актуальних міжнародних стандартів.

У таблиці 4 наведено перелік базових параметрів IKEv2/TLS та рекомендованих безпечних значень. Розглянуто групи обміну ключами (ECP384 або MODP6144), цифрові підписи (ECDSA/EdDSA відповідно до FIPS), сучасні AEAD-режими (AES-GCM, ChaCha20-Poly1305), функції PRF (SHA-256/384) та обов'язкове застосування епіфемерних ключів. Ці налаштування формують основу для забезпечення криптографічної стійкості та відповідають актуальним міжнародним рекомендаціям. Вони можуть бути використані як базова інструкція при впровадженні безпечних конфігурацій у корпоративних VPN, дата-центрах та середовищах IoT.

Комплексна віцуалізація: «Часові та ресурсні характеристики MODP та ECP у протоколах захищеного обміну ключами». Для обґрунтування вибору криптографічних груп у протоколах захищеного обміну ключами було проведено серію моделювань, результати яких представлені на рисунках 2–5. Візуалізації відображають часові та ресурсні

Таблиця 3

Порівняння поведінкових метрик MODP6144 та ECP384 у системах IDS/SIEM

Метрика SIEM/IDS	MODP6144	ECP384
Стабільність ознак рукостискання	висока	висока
Чутливість до downgrade-атак	середня	середня/низька (за строгих політик)
Частота сповіщень про латентність	вища	нижча
Ефективність CNN+LSTM (Byte2Image)	добра	добра/висока

Таблиця 4

Мінімальні безпечні параметри для протоколів IKEv2 та TLS

Параметр IKEv2/TLS	Безпечне значення	Коментар
Група обміну ключами	ECP384 або MODP6144	політика crypto agility
Підпис	ECDSA/EdDSA (FIPS)	див. [29, 24]
AEAD	AES-GCM/ChaCha20-Poly1305	див. [10, 11]
PRF	SHA-256/384	–
Епіфемерність	обов'язкова (PFS)	–

характеристики модульної експоненціальної групи (MODP) і груп на еліптичних кривих (ECP) у контексті сучасних вимог TLS 1.3 та IKEv2. Представлені графіки дозволяють зрозуміти баланс між рівнем безпеки, затримками рукостискання та споживанням обчислювальних ресурсів, що є критичним для корпоративних і IoT-середовищ.

Отримані результати моделювань демонструють не лише відмінності у швидкодії обчислювальних операцій, але й наочно показують, як вибір тієї чи іншої групи впливає на масштабованість інфраструктури, стабільність роботи багатокористувацьких систем та здатність до інтеграції з сучасними засобами нагляду за безпекою. Аналіз часових характеристик рукостискання, навантаження на центральний процесор і рівня енергоспоживання дозволяє сформувати більш детальне уявлення про ефективність кожної групи у різних сценаріях експлуатації. Особливу увагу приділено сценаріям корпоративних VPN із жорсткими вимогами до латентності, мультиарендним концентраторним середовищам із великою кількістю тунелів та сегментам IoT, де критично важливими є низькі витрати ресурсів. У сукупності візуалізації підкреслюють важливість системного підходу: вибір криптографічної групи має враховувати не лише формальну криптографічну стійкість, але й практичні аспекти продуктивності, масштабованості та наглядовості в умовах сучасних електронних комунікацій.

На рис. 2 подано узагальнену візуалізацію, яка складається з кількох взаємопов'язаних частин. Верхні графіки демонструють часові характеристики обчислень для MODP та ECP-груп: зліва відображено залежність часу рукостискання від довжини модуля у випадку MODP, справа – аналогічну залежність для ключів на еліптичних кривих. Як видно, ECP забезпечує стабільно нижчі затримки навіть при збільшенні довжини ключа, що робить їх зручними для масштабованих корпоративних мереж.

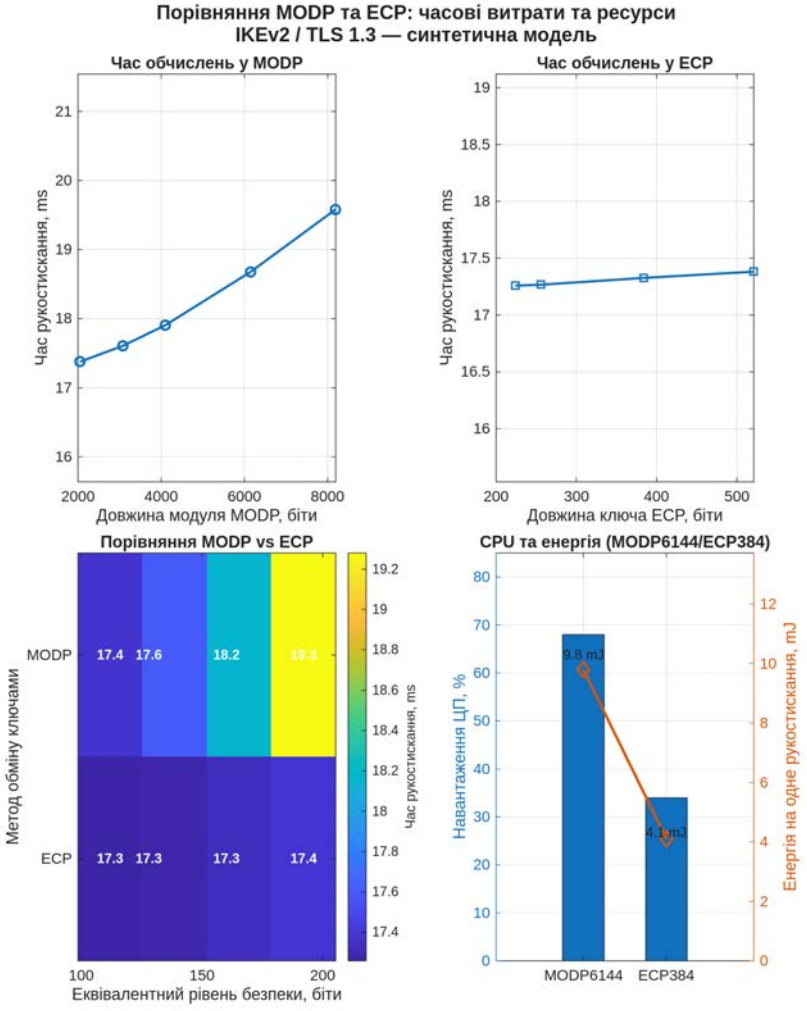

Рис. 2. Порівняння MODP та ECP: часові витрати та навантаження ресурсів у протоколах IKEv2/TLS 1.3

У нижній частині рисунка наведено теплову карту, яка порівнює часові витрати між MODP і ECP за різних рівнів еквівалентної безпеки. Тут добре видно, що ECP стабільно демонструє менші затримки, тоді як MODP потребує значно більших обчислювальних ресурсів. Поряд розміщено графік навантаження на процесор і рівня енергоспоживання, який показує, що MODP6144 створює суттєво більше навантаження порівняно з ECP384. Це свідчить про доцільність використання ECP у мобільних і ресурсно обмежених IoT-середовищах.

Загалом рисунок узагальнює баланс між безпекою та продуктивністю для двох підходів. ECP384 можна вважати оптимальним для більшості корпоративних і IoT-сценаріїв завдяки його продуктивності й нижчим ресурсним витратам, тоді як MODP6144 зберігає свою цінність у випадках суворих регуляторних вимог і потреби у максимальному запасі криптографічної стійкості.

За результатами візуалізацій встановлено, що групи на еліптичних кривих (ECP) забезпечують значно нижчі часові витрати та менше навантаження на процесор і енергоспоживання порівняно з модульними експоненціальними групами (MODP). Це робить ECP384 оптимальним вибором для більшості корпоративних та IoT-середовищ, тоді як MODP6144 зберігає доцільність лише у сценаріях із суворими регуляторними вимогами та потребою у максимально можливому запасі криптографічної стійкості

Інтеграція з Zero Trust, IDS та SIEM. У межах Zero Trust політики контролюються *всі* вузли і транзакції; обрані криптографічні групи безпосередньо впливають на показники користувацького досвіду та сигналізацію в SOC. Використання ознак (12) дозволяє CNN+LSTM виявляти аномальні послідовності рукостискання (наприклад, раптовий перехід з ECP384 на MODP2048), тоді як AE+LSTM і Byte2Image покращують виявлення «тонких» відхилень байтового потоку, пов'язаних із firmware-маніпуляціями через SNMP/SSL.

Висновки. У проведеному дослідженні було запропоновано уніфіковану методику порівняння модульної експоненціальної групи MODP та еліптичної кривої ECP, яка поєднує як теоретичні оцінки стійкості, так і практичні показники продуктивності та наглядовості. Встановлено, що використання групи ECP384 у більшості корпоративних сценаріїв забезпечує оптимальний баланс між часом рукостискання, навантаженням на центральний процесор та рівнем енергоспоживання при вищому еквівалентному рівні безпеки, який оцінюється приблизно у 192 біти. Водночас група MODP6144 зберігає доцільність застосування у середовищах із консервативними чи суворо регламентованими вимогами, де пріоритетом є максимально можливий запас стійкості, навіть за умови суттєвих ресурсних витрат.

Розроблені моделі дозволили формалізувати ключові характеристики криптографічних протоколів: час рукостискання у протоколах IKEv2 та TLS 1.3, навантаження на процесор при збільшенні кількості паралельних з'єднань, оцінку енергоспоживання у багатокористувацьких середовищах, поведінку черг управлінського трафіку, а також постановку задачі оптимізації вибору групи за критеріями продуктивності й безпеки. Окрему увагу приділено інтеграції криптографічних параметрів у процеси управління інформаційною безпекою, зокрема у Zero Trust-архітектурах та системах класу IDS/SIEM. Було продемонстровано, що застосування сучасних методів глибинного навчання, таких як CNN+LSTM та AE+LSTM, у поєднанні з підходом Byte2Image, суттєво підвищує якість аналізу характеристик рукостискання і дозволяє своєчасно виявляти аномалії або атаки на криптографічні протоколи.

Практична значущість результатів полягає у можливості їх безпосереднього використання для налаштування безпечних параметрів у протоколах IKEv2 та TLS, що забезпечує підвищення стійкості корпоративних VPN та критичних інформаційних інфраструктур. Розроблені рекомендації, узагальнені у табличній формі, дають змогу адміністраторам і розробникам систем приймати обґрунтовані рішення щодо вибору оптимальної групи обміну ключами залежно від конкретних вимог середовища. Отримані результати також формують підґрунтя для подальших досліджень у напрямі гібридних криптографічних схем, які поєднуватимуть класичні алгоритми та постквантові підходи з метою підвищення довгострокової стійкості та надійності систем електронних комунікацій.

Список літератури:

1. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory.* 1976. Vol. 22, № 6. P. 644–654. DOI: 10.1109/TIT.1976.1055638.

2. Miller V. Use of elliptic curves in cryptography. Advances in Cryptology – CRYPTO'85, LNCS 218. Berlin: Springer, 1986. P. 417–426. DOI: 10.1007/3-540-39799-X_31.

3. Koblitz N. Elliptic curve cryptosystems. *Mathematics of Computation*. 1987. Vol. 48, № 177. P. 203–209. DOI: 10.2307/2007884.

4. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. DOI: 10.1201/9780429466335.

5. Kivinen T., Kojo M. RFC 3526: More Modular Exponential (MODP) Diffie–Hellman Groups for IKE. IETF, 2003. DOI: 10.17487/RFC3526.

6. Turner S. RFC 5903: Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2. IETF, 2010. DOI: 10.17487/RFC5903.

7. Kaufman C., Hoffman P., Nir Y., Eronen P. RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2). IETF, 2014. DOI: 10.17487/RFC7296.

8. Harkins D., Mizrahi T. RFC 8247: Algorithm Implementation Requirements and Usage Guidance for IKEv2. IETF, 2017. DOI: 10.17487/RFC8247.

9. McGrew D., та ін. RFC 8221: Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH. IETF, 2017. DOI: 10.17487/RFC8221.

10. Viega J., Dworkin M. RFC 4106: The Use of AES-GCM in IPsec ESP. IETF, 2005. DOI: 10.17487/RFC4106.

11. Rescorla E. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. IETF, 2018. DOI: 10.17487/RFC8446.

12. Barker E., Kelsey J. NIST SP 800-56A Rev.3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. NIST, 2018. DOI: 10.6028/NIST.SP.800-56Ar3.

13. Barker E., та ін. NIST SP 800-56B Rev.2: Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. NIST, 2019. DOI: 10.6028/NIST.SP.800-56Br2.

14. Barker E., та ін. NIST SP 800-57 Part 1 Rev.5: Recommendation for Key Management. NIST, 2020. DOI: 10.6028/NIST.SP.800-57pt1r5.

15. Souppaya M., Scarfone K. NIST SP 800-52 Rev.2: Guidelines for the Selection, Configuration, and Use of TLS Implementations. NIST, 2019. DOI: 10.6028/NIST.SP.800-52r2.

16. Barker E., Dang Q. NIST SP 800-131A Rev.2: Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST, 2019. DOI: 10.6028/NIST.SP.800-131Ar2.

17. NIST SP 800-186: Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters. NIST, 2019. DOI: 10.6028/NIST.SP.800-186.

18. ECRYPT-CSA. Recommendations on Key Sizes and Parameters. 2020. DOI: 10.5281/zenodo.3709410.

19. ENISA. Algorithms, Key Sizes and Parameters Report 2023. European Union Agency for Cybersecurity, 2023. DOI: 10.2824/475910.

20. Bernstein D. J. Curve25519: new Diffie–Hellman speed records. Public Key Cryptography – PKC 2006. LNCS 3958. Berlin: Springer, 2006. P. 207–228. DOI: 10.1007/11745853_14.

21. Langley A., Hamburg M., Turner S. RFC 7748: Elliptic Curves for Security. IETF, 2016. DOI: 10.17487/RFC7748.

22. Bernstein D. J., Lange T. SafeCurves: choosing safe curves for elliptic-curve cryptography. 2014. DOI: 10.48550/arXiv.1310.3121.

23. Heninger N., та ін. Mining your Ps and Qs: detection of widespread weak keys in network devices. *USENIX Security Symposium.* 2012. P. 205–220. DOI: 10.5555/2362793.2362823.

24. Sheffer Y., Fluhrer S., Tschofenig H. RFC 7427: Signature Authentication in IKEv2. IETF, 2015. DOI: 10.17487/RFC7427.

25. Smyslov V. RFC 8031: Using Curve25519 and Curve448 with IKEv2. IETF, 2016. DOI: 10.17487/RFC8031.

26. Lenstra A. K., Verheul E. R. Selecting cryptographic key sizes. *Journal of Cryptology.* 2001. Vol. 14. P. 255–293. DOI: 10.1007/s00145-001-0009-4.

27. Cisco Systems. Configure IKEv2/IPsec on Cisco IOS Routers – Best Practices. Cisco, 2023. URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/117258-config-ios-ikev2-00.html (дата звернення: 21.08.2025).

28. MikroTik. IPsec IKEv2 configuration guide (RouterOS v7). MikroTik, 2024. URL: https://help.mikrotik.com/docs/display/ROS/IPsec (дата звернення: 21.08.2025).

29. NIST FIPS 186-5: Digital Signature Standard (DSS). NIST, 2023. DOI: 10.6028/NIST.FIPS.186-5.

Florov S.V., Cherkaskyi O.V., Cherkaskyi D.O., Zubchenko N.S., Peremetchyk D.O. COMPARATIVE CHARACTERISTICS OF THE MODULAR EXPONENTIAL GROUP AND THE ELLIPTIC CURVE OVER A PRIME FIELD IN ELECTRONIC COMMUNICATION SYSTEMS

The article presents a comprehensive study of two fundamental approaches to organizing secure key exchange in electronic communication systems: the modular exponential group and the elliptic curve over a prime field. The purpose of the work is to develop a comparative methodology that simultaneously takes into account cryptographic strength (asymptotic complexity of known attacks, security margin, compliance with international standards) and practical characteristics (connection establishment time, CPU load, throughput, energy consumption, compatibility with existing network infrastructure). A unified analytical model of delays in key exchange protocols, a Markov description of the phases of the initial handshake, and a bi-criteria optimization of "performance–security" are proposed, considering zero-trust policy restrictions and specific operating conditions (corporate virtual private networks, data centers, remote branches, Internet of Things). For empirical validation, simulation modeling scenarios and expert assessments of industrial router configurations were used. Special attention is given to integration with intrusion detection systems and information security management platforms: extraction of handshake descriptors, profiling of network traffic, and anomaly detection based on convolutional and recurrent neural networks, as well as autoencoders combined with recurrent models. A method of transforming protocol byte sequences into raster representations ("byte-to-image") is proposed to improve event classification accuracy. The results showed that an elliptic curve over a prime field with a parameter of 384 provides a better balance between resistance to attacks and computational resource consumption in most corporate scenarios, while the modular exponential group with a parameter of 6144 maintains a significant security margin in cases of strict regulatory requirements and critical infrastructures. The applicability limits of the models, the influence of implementation factors (ephemerality of keys, choice of digital signatures, hardware accelerators, parameters of pseudo-random generation functions) are analyzed, and the prospects of transitioning to hybrid schemes with elements of post-quantum cryptography are outlined.

Key words: *modular exponential group, elliptic curve, key exchange protocol, transport layer security, cryptographic strength, zero-trust policy.*

Дата надходження статті: 07.09.2025
Дата прийняття статті: 23.09.2025
Опубліковано: 16.12.2025