Таким чином, впровадження автоматизованих процесів інтеграції та розгортання є критично важливою практикою для підтримки стабільності й масштабованості сучасних вебплатформ. Описані підходи є актуальними для широкого класу застосунків і можуть бути адаптовані відповідно до потреб конкретного проєкту [2]. Трансформація процесів інтеграції та розгортання у цілісну екосистему DevSecOps є критичною умовою для масштабованості вебплатформ. Актуальність дослідження полягає у переході від простого скриптування до створення інтелектуальних систем доставки, що здатні самостійно адаптуватися до навантажень та безпекових викликів.

1. Мачужак А. В. Дослідження методології DevOps для розробки та підтримки веб-застосунків : кваліфікаційна робота магістра. – Тернопіль : ТНТУ, 2023. – 114 с.
2. Спасітєлєва С. О. Безперервна інтеграція та безперервна доставка (CI/CD) як практика безпечної розробки ПЗ // Кібербезпека: освіта, наука, техніка. – 2023. – № 21. – С. 193–210.
3. Evolution of DevSecOps and Its Influence on Application Security: A Systematic Literature Review // MDPI: Applied Sciences. – 2025. – Vol. 13, No. 12. – P. 548–565.
4. Research Directions in Software Supply Chain Security // ACM Transactions on Software Engineering and Methodology. – 2025. – Vol. 34, No. 5. – P. 112–134.

Інструментальні засоби аналізу впливу характеристик комерційних SPAD-детекторів на стійкість протоколу BB84+decoy-state

УДК 004.056.55:535.14

Олексій Пирогов[1], Василь Різак[2]

Ужгородський національний університет,
[1]oleksii.pyrohov@uzhnu.edu.ua, [2]vrizak@uzhnu.edu.ua

QKD вийшов на промисловий рівень: китайська мережа CN-QCN (China Quantum Communication Network) охоплює понад 10 000 км волокна, 145 магістральних вузлів та 20 метромереж у 80 містах [1]. Транскордонний сегмент EuroQCI розгортається з 2026 р. З 20 квітня 2025 р. набрав чинності Закон № 4336-IX про кіберзахист державних інформаційних ресурсів, але не містить вимог до QKD-систем; галузевого стандарту на QKD в Україні немає. Вибір SPAD-детектора критично впливає на максимальну дальність каналу та параметри секретного ключа, але відкритий інструмент аналізу стійкості відсутній.

BB84 [2] із decoy-state розширенням [3] — найпоширеніший протокол комерційних QKD-систем на волокні. Утім, чи здатна така система генерувати секретний ключ і на якій відстані ще зберігається стійкий режим — визначає не протокол, а характеристики SPAD: η_d (квантова ефективність детектування), вакуумний yield Y_0 (зумовлений темновим рахунком), мертвий час, післяімпульсація, похибка оптичного вирівнювання e_{det} — саме вони задають

параметричні межі стійкості. Проте бракує відкритого інструменту для GLLP-розрахунку (Gottesman-Lo-Lütkenhaus-Preskill) [4] з MC-верифікацією та візуалізацією зони стійкості.

Мета роботи — розробити інструментальні засоби, що поєднують аналітичний розрахунок стійкості BB84+decoy-state за GLLP [4], Monte-Carlo верифікацію з реалістичним моделюванням SPAD та інтерактивну параметричну карту $L_{\_max}(\eta_d, Y_0)$ з пресетами комерційних SPAD-модулів 2004–2025.

Реалізація базується на Python (NumPy, SciPy) з GUI на pywebview та 6 пресетами комерційних SPAD. BB84+decoy-state із трьома інтенсивностями (μ, ν, вакуум); загальне пропускання каналу та приймача $\eta_{total} = 10^{(-\alpha L/10)} \cdot \eta_{Bob} \cdot \eta_d$. Q_x та QBER E_x обчислюються стандартними виразами для BB84+decoy-state [3]. Нижня межа однофотонного yield за двома інтенсивностями [3]:

$$Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left[Q_\nu e^\nu - Q_\mu e^\mu \left(\frac{\nu}{\mu}\right)^2 - \frac{\mu^2-\nu^2}{\mu^2} Y_0\right]. \quad (1)$$

Звідки $Q_1^L = \mu\, e^{(-\mu)}\, Y_1^L$; $e_1^U = (E_\nu Q_\nu e^\nu - e_0 Y_0)/(\nu\, Y_1^L)$, де $e_0 = 1/2$. Швидкість секретного ключа за GLLP:

$$R \geq q \cdot \{-Q_\mu f_{EC} h(E_\mu) + Q_1^L \cdot [1 - h(e_1^U)]\}, \quad (2)$$

$q = 1/2$, $f_{EC} = 1{,}16$. L_{max} (де $R = 0$) обчислюємо методом Brent на сітці $\eta d \in [0{,}02;\ 0{,}95]$, $Y0 \in [10^{-9};\ 10^{-3}]$ при $\alpha = 0{,}21$ дБ/км, $\eta Bob = 0{,}45$, $e_{det} = 0{,}033$, $\mu = 0{,}5$, $\nu = 0{,}1$. Формули (1)–(2) асимптотичні (finite-key межі — предмет наступних версій). Monte-Carlo (MC) узгоджується з аналітикою ($|\Delta| \leq 6$ % при $L \leq 100$ км, $5 \cdot 10^7$ імпульсів на точку); для $L > 100$ км точна MC-верифікація потребує $> 10^9$ імпульсів на точку через рідкісну decoy-статистику.

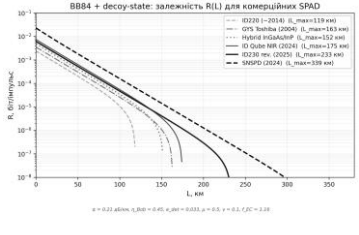

Рис. 1. Межі стійкого режиму QKD-каналу для 6 комерційних SPAD.

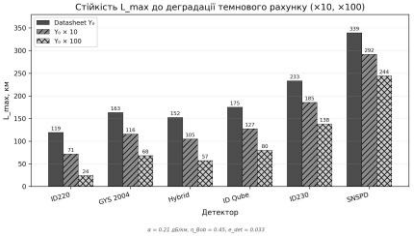

Рис. 2. Стійкість L_{max} до деградації темнового рахунку (×10, ×100).

Параметрична розгортка $L_{max}(\eta_d, Y_0)$ показує, що вакуумний yield обмежує стійкість сильніше, ніж квантова ефективність. Порівняння ID230 та ID Qube ілюструє цей ефект: η_d відрізняється в 1,2×, Y_0 — у 20×, що дає різницю L_{max} у 58 км. Hybrid, попри вищу $\eta d = 20$ %, поступається GYS 2004 (152 проти 163 км) через більший $Y_0 = 2 \cdot 10^{-6}$, що підтверджує визначальну роль темнового рахунку. Аналіз стійкості до деградації Y_0 (Рис. 2) показує: при зростанні

темнового рахунку в 100× ID230 зберігає 138 км (59 % від номіналу), тоді як ID220 — лише 24 км (20 %).

На відміну від NuQKD та OpenQKDSecurity, інструмент орієнтований на інженерну задачу: відкритий код, пресети комерційних SPAD 2004–2025 за публічними datasheet, GLLP+MC та інтерактивна карта $L_{max}(\eta_d, Y_0)$ як критерій вибору детектора.

Інструмент валідовано (MC-аналітика $|\Delta| \leq 6$ % при $L \leq 100$ км). Сучасні SPAD (ID Qube, ID230) забезпечують 175–233 км стійкого QKD-каналу проти 163 км зразка 2004. Результати можуть використовуватись для обґрунтованого вибору SPAD при проектуванні QKD-ланок. Перспектива — розширення інструмента на інші протоколи QKD та finite-key аналіз.

1. Chen H.Z., Li M.H., Wang Y.Z. et al. Implementation of carrier-grade quantum
2. communication networks over 10000 km. npj Quantum Information. 2025. Vol. 11. Art. 137. DOI: 10.1038/s41534-025-01089-8.
3. Bennett C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proc. IEEE Int. Conf. Comput. Syst. Signal Process., Bangalore, 1984. P. 175–179.
4. Lo H.-K., Ma X., Chen K. Decoy state quantum key distribution. Phys. Rev. Lett. 2005. Vol. 94. P. 230504.
5. Gottesman D., Lo H.-K., Lütkenhaus N., Preskill J. Security of quantum key distribution with imperfect devices. Quant. Inf. Comput. 2004. Vol. 4. P. 325–360. arXiv:quant-ph/0212066.

Архітектура системи верифікації відкритих джерел за допомогою OSINT-технологій

УДК 004.056

Олена Пирч[1], Катерина Федоренко[2]

Хмельницький національний університет,
[1]pyrchov@khmnu.edu.ua, [2]katefedorenko8080@gmail.com

В українських реаліях дезінформація має виражений гібридний характер і поєднує психологічні, інформаційні та кіберкомпоненти. Російська збройна агресія проти України супроводжується масштабними інформаційно-психологічними операціями, спрямованими як на внутрішню, так і на зовнішню аудиторію. Основними цілями таких кампаній є підрив довіри до державних інститутів, посилення почуття нестабільності та беззахисності, деморалізація населення, дискредитація Збройних сил України та міжнародних партнерів. Для їх реалізації активно використовуються анонімні Telegram-канали, фейкові акаунти у соціальних мережах, медіаресурси та мережі ботів [1].

Архітектура системи верифікації відкритих джерел побудована як багаторівнева модульна система, у якій кожен рівень відповідає за окремий аспект перевірки допису у відкритому Telegram-каналі на наявність дезінформації. Така структурна організація системи забезпечує не лише логічну послідовність процесу, а й методологічну узгодженість, оскільки кожен модуль