МЕТРИКИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОГРАМ ОБІЗНАНОСТІ З КІБЕРБЕЗПЕКИ ТА УПРАВЛІННЯ ЛЮДСЬКИМ РИЗИКОМ У СУІБ

Скрильник В.Ю., Кононенко І.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах стрімкої цифровізації та загострення кіберзагрози людський фактор залишається первинною мішенню для зловмисників і найменш захищеною ланкою в системі управління інформаційною безпекою (СУІБ) [1, 2]. За даними міжнародних аналітичних досліджень та практичних аудитів, понад 80–90% усіх кіберінцидентів пов’язані з помилками персоналу, маніпуляціями засобами соціальної інженерії або нехтуванням правилами безпеки [1, 3]. Традиційний підхід до навчання обізнаності, який зазвичай обмежується формальним проведенням лекцій або переглядом навчальних модулів задля фіксації «100% охоплення», демонструє вкрай низьку ефективність щодо реальної зміни поведінки співробітників [3, 4]. Недостатність традиційних метрик зумовлена тим, що вони переважно відображають виконання навчальних заходів і рівень знань, але не встановлюють повного зв'язку між навчанням, реальною поведінкою працівників, людським кіберризиком і результативністю СУІБ.

У зв’язку з цим у міжнародних стандартах (ISO/IEC 27001:2022, NIST SP 800-50 Rev. 1) відбулася трансформаційна зміна парадигми: від пасивного підвищення обізнаності до активного «управління людським ризиком» (HRM) [1, 5, 6]. Головною метою HRM є кількісна оцінка, систематичний моніторинг та цілеспрямоване зменшення ризиків, спричинених людською поведінкою. Для забезпечення безперервного вдосконалення СУІБ критично важливо впровадити обґрунтовану систему метрик та кількісних показників (KPIs), які спроможні об’єктивно відображати динаміку поведінкових змін та повернення інвестицій (ROI) у програми безпеки [3, 4].

Метою доповіді є систематизація методологічних підходів до побудови комплексної системи метрик оцінювання ефективності програм обізнаності з кібербезпеки та управління людським ризиком у рамках СУІБ організації.

В межах системи управління інформаційною безпекою недостатньо оцінювати програми обізнаності лише за кількістю проведених тренінгів, відсотком охоплених працівників або результатами тестування знань. Необхідно встановлювати, наскільки навчання змінює поведінку працівників, знижує ймовірність реалізації кіберзагроз, зменшує пов'язані з людським фактором втрати та сприяє досягненню цілей інформаційної безпеки організації.

Для цього доцільно поєднати підходи до оцінювання результативності навчання, вимірювання поведінкових змін, кількісного аналізу ризиків та управління інформаційною безпекою. Результатом має стати не просто набір показників, а ієрархічна система метрик, яка пов'язує навчальні заходи з поведінкою працівників, людським ризиком і результативністю СУІБ.

На основі аналізу сучасних наукових досліджень та практичних напрацювань (зокрема моделей Kirkpatrick, SANS Maturity Model та концепції ELINET) системи метрик програм обізнаності поділяються на чотири ключові групи [3, 4].

1. Метрики участі та доступності вимірюють охоплення аудиторії навчальними матеріалами, відсоток завершення обов'язкових та факультативних модулів (E1), середній час від призначення до проходження курсу (E2) та юзабільність навчальних каналів [3, 4]. Хоча ці показники є необхідними для операційного обліку, вони надають лише опосередковану інформацію і не гарантують безпечної поведінки на робочому місці.

2. Метрики знань та засвоєння оцінюють динаміку зміни рівня знань співробітників за допомогою базового та підсумкового тестування (CKQ), квізів та оцінювання за термінологічними стандартами (наприклад, HAIS-Q, SeBIS) [3, 4]. Зростання рівня знань є передумовою, але не тотожне безпечній дії через наявність розриву між наміром та поведінкою [4].

3. Поведінкові метрики та показники стійкості відображають реальні дії співробітників під час виконання професійних обов'язків та при моделюванні загрозових ситуацій. Ключовими показниками в цій категорії є [3, 4, 6]:

– Click Rate (P1) та Re-click Rate (P2) - це відсоток співробітників, які переходять за шкідливими посиланнями в базових та повторних фішингових симуляціях;

– Reporting Rate (P3) та Time to Report (P8) - відсоток і медіанний час реагування та повідомлення служби безпеки про підозрілі листи. Зростання даного показника свідчить про трансформацію персоналу у «живі сенсори» кіберзахисту;

– Repeat-Failure Rate (P9) - це частка співробітників, які систематично припустилися помилок, що дозволяє формувати цільові навчальні траєкторії замість загальних покарань;

– Метрики Signal Detection Theory (SDT) - індекс чутливості (P11) та індекс критерію рішення (P12), що визначають здатність диференціювати фішинг від легітимних повідомлень та рівень хибних тривог (P7);

– Confidence Calibration (P13) - оцінка відповідності між суб'єктивною впевненістю співробітника та точністю його дій, що дозволяє виявляти групи з критичним рівнем надмірної впевненості або недовіри до власних дій.

4. Результативні метрики та показники стійкості вимірюють безпосередній вплив на профіль ризику організації та СУІБ у цілому. До них належать кількість інцидентів витоку даних (DLP), спричинених людською помилкою (I8, I12), дотримання політики чистого столу (D2), частка зашифрованих пристроїв (D1), а також показники повернення інвестицій (ROI) та інтеграції процедур обізнаності в загальний регламент управління ризиками [1, 3, 4].

Практичні рекомендації щодо побудови вимірювального каркасу СУІБ. Для побудови дійсно ефективної системи вимірювання людського фактору в СУІБ рекомендується дотримуватися таких принципів [1, 3]:

– використання методології GQM, коли кожен вимірювальний показник повинен формуватися суворо під конкретну бізнес-ціль безпеки та давати відповідь на управлінське питання [3];

– інтеграція невторгливих методів, тобто поєднання пасивного збору логів (DLP, симетричний моніторинг електронної пошти, дані криптографічного захисту) із регулярними симуляціями дозволяє отримати об'єктивну картину без додаткового психологічного навантаження на персонал [4];

– інституціоналізація мережі амбасадорів - розрахунок щільності амбасадорів у підрозділах (C3) та вимірювання кількості звернень співробітників (C1) забезпечує кореляцію між наявністю залучених лідерів та зниженням рівня ризикованої поведінки [3];

– формування єдиного індексу людського ризику - це агрегування вагових показників різних груп метрик у єдиний інтегральний індекс для подання вищому керівництву та раді директорів [3].

Таким чином, управління людським фактором у СУІБ вимагає відходу від формальних кількісних показників відвідуваності на користь цілісної методології вимірювання поведінкових змін та результативності контролів. Саме перехід від оцінювання «скільки навчання проведено?» до оцінювання «як навчання змінило поведінку та наскільки це сприяло зниженню кіберризику?» становить методологічну основу побудови комплексної системи метрик. Впровадження збалансованого каркасу метрик (на основі GQM, SDT та аналізу результативних показників) дозволяє організаціям підвищити стійкість до соціальної інженерії, об'єктивно оцінити повернення інвестицій у програми обізнаності та перетворити персонал із найслабшої ланки на надійну лінію кіберзахисту.

Список літератури

1. Козубцова Л., Ліщина В., Козубцов І. Від обізнаності до управління: концепція людських ризиків в системі кіберзахисту. Кібербезпека: освіта, наука, техніка. 2025. Т. 2, № 30. С. 360–373. URL: https://doi.org/10.28925/2663-4023.2025.30.895 (date of access: 25.10.2026).

2. Сєвєрінов О. В., Черниш В. І., Молчанова М. Є. Управління інформаційною безпекою згідно міжнародних стандартів. Системи управління, навігації та зв'язку. 2011. Вип. 4 (20). С. 250–253.

3. Овчаренко М. Ю., Сєвєрінов О. В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. Проблеми інформатизації : тези доповідей сьомої міжнародної науково-технічної конференції, 13–15 листопада 2019 р. 2019. Т. 1. С. 102. URL: https://openarchive.nure.ua/handle/document/15774.

4. Chaudhary S., Gkioulos V., Katsikas S. Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity. 2022. Vol. 8, no. 1. URL: https://doi.org/10.1093/cybsec/tyac006 (date of access: 25.10.2026).

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO, 2022. 32 p.

6. NIST SP 800-50 Rev. 1. Building a Cybersecurity and Privacy Learning Program. NIST, 2024. 68 p.