Нормативні та методологічні засади впровадження ризико-орієнтованого підходу до кіберзахисту

УДК 004.056.55

Володимир Кононович[1], Дмитро Пастухов[2]

Державний університет інтелектуальних технологій і зв'язку,
[1]vl_kononovich@ukr.net, [2]edu.dvpastukhov@gmail.com

Розвиток інформаційно-комунікаційних систем та тотальна цифровізація як державних, так і приватних послуг кардинально змінили ландшафт кіберзагроз. Україна пройшла велику концептуальну трансформацію – відбувається перехід від застарілих комплексних систем захисту інформації (КСЗІ) до сучасних, гнучких та адаптивних ризико-орієнтованих підходів. З огляду на те, що базові системи КСЗІ мали застосовуватись до вересня 2025 року, наразі об'єкти, що підлягають захисту, повинні впровадити нові методології управління безпекою, які відповідають умовам інтенсивної кібернетичної та гібридної війни.

Фундаментальна проблема попередньої парадигми полягала в принципі загрозо-центричного підходу. Класичні системи будували як «рубіжну оборону» – захисту периметру від максимально можливої кількості гіпотетичних загроз, часто без глибокого урахування реальної ймовірності їх виникнення. Такий підхід вимагає значних, часто невиправданих капіталовкладень, що ставить під сумнів економічну доцільність реалізації КСЗІ спираючись на цей принцип. Застарілі методи захисту не здатні протистояти новітнім векторам атак, зокрема тим, що використовують інструменти штучного інтелекту для оптимізації соціальної інженерії та фішингу, де не діють жодні технічні методи захисту.

Новітній, актуальний підхід до безпеки інформації, систем та приватності (рис. 1) закріплені Законом України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» (документ 4336-IX від 27 березня 2025) [1]. Новий підхід описаний у нормативному документі ДСТУ ISO 27005:2023 – побудова КСЗІ на об'єкті повинна спиратись на керуванні ризиками інформаційної безпеки [2].

Математична модель ризико-орієнтованого підходу визначається за наступною формулою оцінки ризику:

$$R = p \times h \tag{1}$$

де R – ризик, p – ймовірність загрози, h – розмір очікуваних збитків.

Розмір збитків, в сучасних умовах гібридних загроз, є комплексною величиною, яка виходить за межі вартості комп'ютерних систем та даних, що зберігаються в них. Він включає у себе також прямі фінансові витрати, репутаційні збитки, когнітивні втрати, штрафні санкції від регуляторів.

Ключовим елементом сучасного підходу є усвідомлення того факту, що досягнення ідеального рівня безпеки є утопією та економічним нонсенсом. Будь-який захід із кіберзахисту – чи то закупівля апаратних брандмауерів наступного покоління, впровадження систем EDR/XDR, інтеграція платформ розвідки загроз, чи то проведення регулярних тренінгів персоналу, має свою

визначену вартість. Завжди слід пам'ятати, що безпека не обмежується суто технічним рівнем захисту інформації, а є тільки її частиною. Не менш важливу роль відіграє когнітивний захист – повинні бути регулярні тренінги, де персонал повинен почати усвідомлювати наявність загроз з боку використання психологічних методик впливу на них для обходу наявних технічних систем захисту інформації [3].

Головним принципом прийняття рішень щодо управління ризиками стає суворе економічне правило: вартість впровадження та підтримки контрзаходів повинна бути меншою ніж можливі фінансові, операційні та репутаційні витрати від реалізації ризику. Якщо вартість захисту перевищує потенційні збитки, єдино правильним та раціональним управлінським рішенням є прийняття цього ризику керівництвом.

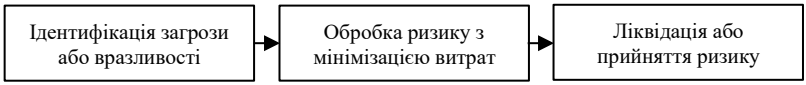

Рис.1. Процес обробки ризику з використанням ризико-орієнтованого підходу

Мінімізація витрат, а під час обробки ризику – пошук необхідних методик захисту, повинен відбуватись циклічно, допоки вартість контрзаходів не буде дешевшою, ніж потенційні витрати. У випадку коли вартість контрзаходу є більшою та його неможливо зменшити – ризик повинен бути прийнятим керівництвом.

На етапі перевірки всієї архітектури на об'єкті, якість побудованих систем захисту інформації можна оцінити завдяки рівню захищеності найслабшої ланки систем безпеки – вся система безпеки залежить від неї.

У якості примітки звернемо увагу на невірний переклад українською назви ДСТУ [2]: «Information security, cybersecurity and privacy». Термін «privacy» перекладено як «конфіденційність», а треба перекладати у даному контексті як «приватність», щоб не вводити читача в оману.

1. Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 13.05.2026).
2. ДСТУ ISO 27005:2023. Інформаційна безпека, кібербезпека та захист приватності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT).
3. Соціальна інженерія та кіберпсихологія: монографія / В. Г. Кононович, С. В. Стайкуца, М. М. Тодорова та ін.; за ред. В. Г. Кононовича, С. В. Стайкуци. Одеса: Астропринт, 2025. 388 с.