Дмитро В. Мироненко

МЕХАНІЗМИ ПОПЕРЕДЖЕННЯ КІБЕРЗАГРОЗ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ

У статті узагальнено наукові підходи до попередження кіберінцидентів, обгрунтовано профілактичні механізми, критичні для зниження економічних втрат. На основі огляду джерел і вивчення кейсів визначено пріоритетні напрями: дисципліна доступів (MFA/принцип найменших привілеїв), керування оновленнями й вразливостями, резервне копіювання з перевіркою відновлення, запобігання витоку даних (DLP) та безперервне навчання персоналу. Показано, що поєднання зазначених заходів із державно-приватною координацією та обміном інформацією про загрози через CERT/CSIRT скорочує простої й масштаб компрометації даних. Зроблено висновок про доцільність комплексного підходу до кібергігієни як практичного інструменту підтримання кіберстійкості критичної інфраструктури України. Застосовано методи структурно-динамічного аналізу, порівняльного аналізу, контент-аналіз та елементи сценарного моделювання.

Кібергігієна в глобальній економіці постає не як суто технічний набір рекомендацій, а як системний інструмент підвищення стійкості держави, бізнесу й суспільства в умовах цифрової взаємозалежності та транскордонних загроз. Для України, яка одночасно інтегрується у світові цифрові ринки й перебуває в середовищі підвищеного ризику, пріоритетність кібергігієни визначається поєднанням економічних і безпекових чинників: безперервність роботи цифрової інфраструктури, довіра до сервісів і транзакцій, захист критичних систем та державних мереж, а також стабільність технологічного сектору прямо залежать від здатності знижувати імовірність інцидентів і обмежувати їх наслідки. Масштаб і еволюція кіберзагроз, у тому числі соціальна інженерія, шкідливе ПЗ, атаки на вебзастосунки, DDoS та використання вразливостей “нульового дня”, підсилюють потребу в переході від фрагментарних заходів до комплексної моделі управління ризиками, що поєднує запобігання, виявлення, реагування та відновлення. Економічний вимір кіберінцидентів – від прямих збитків до втрат довіри, регуляторних санкцій, компрометації інтелектуальної власності й збоїв ланцюгів постачання – робить інвестиції в кіберстійкість не витратами “на IT”, а елементом конкурентоспроможності та економічної безпеки. У практичному вимірі такий підхід передбачає одночасне посилення технічних контролів (зокрема DLP для захисту конфіденційних даних у хмарних та віддалених сценаріях), розвиток культури безпеки через навчання й підвищення обізнаності, а також інституційну й міжнародну взаємодію, без яких неможливі ефективний обмін інформацією, узгодження стандартів і координація дій у протидії кіберзлочинності.

Ключові слова: кібербезпека, кібергігієна, кіберзагрози, ризики, економічна безпека країни, конкурентоспроможність.