

Sofia Kravchenko

Kharkiv National University of
Radio Electronics, Kharkiv, Ukraine

CYBER RESILIENCE OF SMALL AND MEDIUM-SIZED BUSINESSES AS A STRATEGIC MANAGEMENT CHALLENGE

Abstract. The paper examines cyber resilience in small and medium-sized enterprises as a managerial capacity to maintain and restore critical business processes after digital incidents. Based on NIST Cybersecurity Framework 2.0, small-business guidance and ENISA threat reports, a practical sequence of management decisions is proposed: identifying critical processes, mapping digital dependencies, prioritizing risks, establishing baseline controls and testing recovery. Particular attention is paid to connecting technical indicators with business-continuity outcomes. The contribution is a conceptual management framework, not a report of original field measurements.

Keywords: cyber resilience; strategic management; small and medium-sized enterprises; risk management; business continuity.

Софія Кравченко

Харківський національний університет
радіоелектроніки, Харків, Україна

КІБЕРСТІЙКІСТЬ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ЯК ЗАВДАННЯ СТРАТЕГІЧНОГО МЕНЕДЖМЕНТУ

Анотація. Розглянуто кіберстійкість малих і середніх підприємств як управлінську здатність підтримувати критичні бізнес-процеси та відновлювати їх після цифрових інцидентів. На основі аналізу NIST Cybersecurity Framework 2.0, рекомендацій для малого бізнесу та звітів ENISA запропоновано послідовність управлінських рішень: визначення критичних процесів, інвентаризація залежностей, пріоритизація ризиків, мінімальний набір заходів захисту й перевірка відновлення. Обґрунтовано потребу поєднувати технічні метрики з показниками безперервності бізнесу. Робота має концептуально-прикладний характер і не містить неперевіраних емпіричних результатів.

Ключові слова: кіберстійкість; стратегічний менеджмент; малий і середній бізнес; управління ризиками; безперервність бізнесу.

Актуальність проблеми. Цифровізація продажів, обліку, комунікацій і взаємодії з постачальниками перетворює інформаційні системи на основу повсякденних операцій підприємства. Для невеликої компанії збій хмарної платформи, викрадення облікових даних або шифрування робочих файлів може означати не лише витрати на відновлення техніки, а й неможливість прийняти замовлення, провести оплату чи виконати договірні зобов'язання. Водночас ресурси малого та середнього бізнесу для спеціалізованих підрозділів безпеки обмежені. Тому кіберстійкість доцільно розглядати не як закупівлю окремого програмного продукту, а як систему пріоритетів, відповідальності та управлінських рішень.

Мета й методика. Метою роботи є обґрунтування доступної для малих і середніх підприємств моделі керування кіберстійкістю, зорієнтованої на збереження цінності для клієнта. Застосовано аналіз нормативно-методичних документів NIST, зіставлення сучасних характеристик загроз за матеріалами ENISA та концептуальне моделювання управлінського циклу. Запропонована модель є авторською систематизацією рекомендованих практик, а не результатом експерименту на конкретних підприємствах. Вона потребує

адаптації до галузі, законодавчих вимог, масштабу цифрових залежностей і допустимого рівня втрат.

Важливо розмежувати кібербезпеку і кіберстійкість. Перша зосереджується на захисті систем та інформації від загроз, тоді як друга додає здатність зберегти прийнятний рівень функціонування за умов інциденту й відновити діяльність. NIST Cybersecurity Framework 2.0 виокремлює шість взаємопов'язаних функцій: Govern, Identify, Protect, Detect, Respond і Recover (NIST, 2024). Поява управлінської функції Govern особливо важлива для малого бізнесу: власник має визначити, хто приймає рішення, за якими критеріями виділяються кошти та коли технічна проблема переходить у статус бізнес-ризик.

Перший крок – визначення критичних бізнес-процесів. Керівництву пропонується перелічити п'ять–сім процесів, без яких компанія не здатна виконувати основні зобов'язання: приймання замовлень, розрахунки, доступ до клієнтської бази, виробниче планування, комунікація з персоналом. Для кожного процесу слід визначити власника, ключові цифрові сервіси, залежність від підрядників і допустиму тривалість перерви. Так підприємство отримує карту взаємозв'язку між інформаційними активами та грошовим потоком. Відсутність такого зв'язку призводить до ситуації, коли захищають найбільш помітні пристрої, а не найкритичніші для клієнта функції.

Другий крок – формування реєстру кіберризиків. Кожний запис має містити сценарій інциденту, потенційне джерело загрози, уразливий процес, наслідки для бізнесу, поточні заходи і відповідального за реагування. Для первинного ранжування можна застосувати словесну шкалу ймовірності та впливу, уникаючи удаваної точності числових оцінок за відсутності статистики. ENISA (2025, 2026) фіксує різноманітність кіберзагроз для європейських організацій, зокрема атаки з вимогою викупу, порушення доступності сервісів і ризики цифрових залежностей. Водночас загальноєвропейські спостереження не можна механічно переносити на ризик окремої фірми без урахування її контексту.

Третій крок – добір контрольних заходів за очікуваними втратами. Для підприємства з обмеженим бюджетом стартовими пріоритетами можуть бути багатофакторна автентифікація для критичних облікових записів, своєчасне оновлення систем, мінімізація надлишкових прав, окремі резервні копії та навчання персоналу розпізнавати шахрайські повідомлення. Посібник NIST для малого бізнесу акцентує саме на практичному початку управління ризиками, а не на одночасному виконанні всіх можливих заходів (Eliot, 2024). Економічна логіка інвестицій у захист передбачає зіставлення витрат з очікуваним скороченням потенційних втрат; як показали Gordon і Loeb (2002), найбільша вразливість активу сама по собі не гарантує найвигіднішого напрямку інвестування.

Четвертий крок – план дій під час інциденту. Підприємству потрібен короткий документ із контактами відповідальних осіб, порядком відключення уражених облікових записів, альтернативними каналами зв'язку, правилами фіксації подій та процедурою інформування клієнтів і партнерів, якщо це необхідно. План має враховувати можливість, що основна електронна пошта чи корпоративний месенджер будуть недоступні. Для мікропідприємства достатньо чіткої схеми прийняття рішень, перевіреної в настільному тренуванні, а не

громіздкого регламенту, який ніхто не читає. Власник процесу повинен знати, як продовжити обслуговування клієнтів у тимчасовому ручному режимі.

П'ятий крок – кероване відновлення. Захист резервних копій має оцінюватися разом із можливістю реально відновити потрібні дані та сервіси. Доцільно визначити цільовий час відновлення бізнес-функції та припустимий обсяг втрати даних, а потім перевіряти ці параметри під час вправ. Наприклад, наявність копії бухгалтерської бази не вирішує проблему, якщо для її відновлення немає відповідного програмного забезпечення, ключів доступу або підготовленого співробітника. У моделі запропоновано після кожного тренування оновлювати реєстр ризиків і переглядати пріоритети бюджету.

Організаційні ролі й постачальники. Кіберстійкість не може бути делегована лише системному адміністратору або зовнішньому ІТ-підряднику. Керівник визначає прийнятний ризик, фінансовий працівник оцінює можливі простої, власники процесів описують наслідки для клієнтів, а технічний спеціаліст добирає засоби захисту. У договорах із цифровими постачальниками доцільно передбачати порядок повідомлення про інциденти, відповідальність за копії даних, можливість експорту інформації та умови переходу до іншого сервісу. Особливої уваги потребують спільні облікові записи й ситуації, коли доступ до критичних систем контролює лише одна особа.

Показники результативності. Для управлінського перегляду пропонується компактна панель: частка критичних сервісів із перевіреним сценарієм відновлення; частка привілейованих облікових записів із багатофакторною автентифікацією; прострочені критичні оновлення; час виявлення і локалізації навчального інциденту; тривалість недоступності основної бізнес-функції. Показники необхідно аналізувати у динаміці, а не використовувати як самодостатній рейтинг. Наприклад, зростання кількості зареєстрованих інцидентів інколи може свідчити про кращу систему виявлення, а не про погіршення захищеності.

Пріоритетність упровадження. На початковому етапі керівнику доцільно затвердити власників критичних процесів, перелік цифрових залежностей і мінімальний план реагування. Далі – усунути очевидні концентрації ризику, перевірити резервне копіювання та провести коротке тренування персоналу. На етапі зрілості – запровадити періодичний перегляд показників, аудит ризиків підрядників і бюджетування на основі можливих бізнес-наслідків. Послідовність не є універсальним стандартом, однак допомагає уникнути характерної помилки, коли витрати на технології передують визначенню цілей і відповідальності.

Обмеження підходу. Запропонована схема не замінює юридичного аналізу вимог до персональних даних, галузевих нормативів або спеціалізованого тестування захищеності. Самооцінка компанії може не виявити прихованих уразливостей, а економічні оцінки простоїв залежать від якості внутрішніх даних. Ефективність моделі доцільно перевіряти через порівняльні кейс-дослідження підприємств схожого профілю, документуючи початковий стан, витрати на контрольні заходи й результати тренувального відновлення, але не приписуючи пропонованій моделі непідтвердженого причинного ефекту.

Висновки. Кіберстійкість малого та середнього бізнесу є складовою стратегічного менеджменту, оскільки визначає здатність підприємства виконувати зобов'язання за умов цифрових порушень. Запропонований цикл "критичні процеси – ризики – контрольні заходи – реагування – відновлення – перегляд" поєднує практики NIST із бізнес-орієнтованими показниками. Його основний результат – перехід від фрагментарного захисту окремих пристроїв до усвідомленого управління безперервністю створення цінності. Подальшим завданням є апробація моделі на підприємствах різного масштабу та секторів.

СПИСОК ДЖЕРЕЛ

1. Eliot, D. (2024). NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide (NIST SP 1300). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.1300>.
2. European Union Agency for Cybersecurity. (2025). ENISA Threat Landscape 2025. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>.
3. European Union Agency for Cybersecurity. (2026). ENISA Threat Landscape 2026. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026>.
4. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. <https://doi.org/10.1145/581271.581274>.
5. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>.