УДК 004.056.5

ІНФОРМАЦІЙНА БЕЗПЕКА МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ: ВИКЛИКИ ТА ІНСТРУМЕНТИ ЗАХИСТУ

Назар КІНАЛЬ
Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

В умовах глобальної цифровізації малий та середній бізнес (далі - МСБ) активно інтегрує цифрові технології, хмарні сервіси та мобільні платформи, що суттєво підвищує ефективність бізнес-процесів. Проте цифрове середовище створює нові загрози, пов’язані з кібератаками, витоком інформації, порушенням доступності даних та зловмисними діями третіх осіб. За оцінками експертів Європейського агентства з кібербезпеки (ENISA), МСБ є одним із найбільш уразливих секторів до кібератак через обмежені ресурси та відсутність системного підходу до кіберзахисту [1].

У таких умовах забезпечення інформаційної безпеки стає критично важливим для сталого розвитку, фінансової стійкості та конкурентоздатності МСБ.

Малий та середній бізнес забезпечує основу економіки країни, проте саме він стає ключовою ціллю для кіберзлочинців. За даними NCSC (National Cyber Security Centre), понад 40% усіх кібератак у Європі та Великій Британії спрямовано саме на МСП, оскільки вони часто не мають прописаних політик безпеки, використовують застаріле програмне забезпечення та не проводять навчання персоналу [2].

У контексті України проблема загострюється через значне збільшення державних та кримінальних кібератак на бізнес у період війни.

Таким чином, інформаційна безпека стає не лише технічним, а й стратегічним питанням для збереження життєздатності підприємств.

Основні проблеми забезпечення інформаційної безпеки МСБ можна поділити на три групи.

1. Організаційні проблеми**:** відсутність формалізованих політик інформаційної безпеки; відсутність механізмів контролю доступу; відсутність відповідальних осіб або підрозділів з ІБ; відсутність планів реагування на інциденти; слабкий контроль зовнішніх підрядників.

2. Технічні проблеми: використання застарілого ПЗ та нелегальних програм; неправильне налаштування хмарних сервісів; відсутність шифрування даних; відсутність резервного копіювання; слабкі або повторювані паролі; відсутність мережевого захисту.

3. Людський фактор: За даними Міністерства цифрової трансформації України, до 80% інцидентів виникає внаслідок фішингу або помилок персоналу [3].

Це означає, що навіть найдорожчі системи захисту будуть неефективними без навчання співробітників.

Формування політики інформаційної безпеки є одним із ключових елементів побудови ефективної системи кіберзахисту малого та середнього бізнесу. Наявність такого документу забезпечує структурованість і чіткість у процесах, пов'язаних із доступом до інформаційних ресурсів, використанням корпоративних пристроїв та зберіганням даних. Політика повинна встановлювати вимоги до довжини та складності паролів, регулювати порядок підключення до мережі, визначати рівні доступу до різних категорій інформації та містити інструкції щодо дій персоналу в разі виявлення інциденту. Крім того, документ має містити положення про резервне копіювання, зберігання копій, обмеження щодо використання зовнішніх носіїв та правила роботи з особистими пристроями працівників. Важливою вимогою є регулярний перегляд

політики, оскільки загрози швидко змінюються. Як наголошує ENISA, актуалізація правил і періодичне оновлення заходів безпеки є необхідною умовою ефективного захисту організації [1].

Другим важливим напрямом є впровадження багатофакторної автентифікації (MFA), що суттєво знижує ризик несанкціонованого доступу до облікових записів. Більшість успішних атак здійснюється через викрадення паролів, які можуть бути підібрані автоматичними засобами або отримані внаслідок фішингових кампаній. Використання MFA забезпечує додатковий рівень захисту за рахунок поєднання декількох факторів — знання (пароль), володіння (мобільний токен) або біометричних даних. NCSC підкреслює, що застосування багатофакторної автентифікації дозволяє запобігти до 99% атак на корпоративні та поштові акаунти, що підтверджує її особливу цінність для МСБ, який часто не має інших засобів захисту [2]. З огляду на поширення віддаленої роботи, MFA стає критично важливою частиною інформаційної безпеки.

Важливу роль у забезпеченні надійного рівня кіберзахисту відіграє навчання персоналу, яке є одним із найефективніших та найбільш економічно вигідних заходів. Більшість інцидентів інформаційної безпеки спричинена саме людським фактором — необережністю, недостатнім розумінням ризиків або неправильним використанням цифрових інструментів. Працівники повинні проходити навчальні програми, спрямовані на розпізнавання фішингових листів, безпечну роботу в інтернеті та правильне використання корпоративних акаунтів. Також важливо формувати навички безпечного поводження з конфіденційною інформацією, включаючи правила створення паролів, користування хмарними сервісами та обробки документів. Як зазначає Міністерство цифрової трансформації України, систематичне навчання персоналу є найдієвішим способом зменшення ризиків, адже дозволяє усунути основну причину інцидентів — недостатню обізнаність співробітників [3].

Суттєвим елементом кіберзахисту є впровадження сучасних технічних інструментів безпеки, які дають змогу комплексно реагувати на різноманітні загрози. До таких інструментів належать антивірусні рішення нового покоління, що використовують машинне навчання для виявлення невідомих шкідливих програм, міжмережеві екрани (firewall), які контролюють мережевий трафік, та VPN-сервіси, що забезпечують захищені канали зв’язку для працівників, які працюють віддалено. Також важливим є шифрування даних — як на дисках і мобільних пристроях, так і під час передавання інформації. Окрему увагу слід приділити менеджерам паролів та системам моніторингу інцидентів, які дозволяють своєчасно виявляти підозрілу активність у мережі та реагувати на неї до того, як загроза набуде критичного характеру. Для МСБ використання таких інструментів є доступним способом значно підвищити рівень захисту навіть за відсутності великих бюджетів.

Ще одним ключовим аспектом забезпечення інформаційної безпеки є впровадження системи резервного копіювання, що дозволяє зберегти працездатність бізнесу навіть у разі серйозного інциденту, зокрема атаки типу ransomware. Рекомендована міжнародними стандартами схема «3–2–1» передбачає наявність трьох копій даних, розміщених на двох різних носіях, при цьому одна копія має зберігатися офлайн або у захищеному хмарному середовищі. Це гарантує, що навіть якщо основні системи будуть зашифровані, знищені чи недоступні, підприємство зможе швидко відновити свою діяльність. Особливо важливо перевіряти працездатність резервних копій та проводити регулярні тестування відновлення.

Завершальним елементом системи захисту є проведення аудиту інформаційної безпеки та тестування на проникнення. Аудит дозволяє здійснити комплексну оцінку стану захисних заходів, перевірити правильність налаштування програмних рішень, відповідність політик реальним процесам, а також визначити прогалини у захисних

механізмах. Тестування на проникнення, у свою чергу, моделює дії реального зловмисника, що дає змогу оцінити стійкість системи у реальних умовах атаки. Для малого та середнього бізнесу така практика є особливо цінною, оскільки дозволяє виявити критичні вразливості та усунути їх до того, як вони будуть використані у злочинних цілях.

Інформаційна безпека малого та середнього бізнесу є критичним чинником його стійкості в умовах сучасної цифрової економіки. Підприємства мають усвідомити, що кіберзагрози — це реальна й постійна загроза, а не абстрактна можливість.

Незважаючи на обмежені ресурси, МСБ здатні суттєво підвищити рівень кіберзахисту за рахунок впровадження базових, але системних заходів. Комплексний підхід до ІБ — це поєднання політик, технічних інструментів, навчання персоналу та регулярного аудиту.

Саме такий підхід забезпечить стійкість бізнесу, збереже репутацію та підвищить конкурентоспроможність на ринку.

Список використаних джерел:

1. European Union Agency for Cybersecurity (ENISA). *Cybersecurity for SMEs.* URL: https://www.enisa.europa.eu/publications/cybersecurity-for-smes
2. National Cyber Security Centre (NCSC). *Small Business Guide: Cyber Security.* URL: https://www.ncsc.gov.uk/cyberaware/smallbusiness
3. Міністерство цифрової трансформації України. *Рекомендації щодо кіберзахисту бізнесу* URL: https://thedigital.gov.ua/