https://www.sworldjournal.com/index.php/swj/article/view/swj30-01-026
DOI: 10.30888/2663-5712.2025-30-01-026

УДК 334.012.61-022.51:004

INFORMATION THREATS TO SMALL BUSINESS

ІНФОРМАЦІЙНІ ЗАГРОЗИ МАЛОГО БІЗНЕСУ

Kudelskyi Vitalij / Кудельський В.Е.
кандидат економічних наук, доцент
ORCID: https://orcid.org/0000-0002-7252-6533
Leonid Yuzkov Khmelnytsky University of Management and Law /
Хмельницький університет управління та права імені Леоніда Юзькова

Стаття присвячена створенню оптимальних умов для реалізації малого бізнесу. В статті відображено необхідність та потребу забезпечення інформаційної безпеки для малого бізнесу. Досліджено основні причини виникнення інформаційних загроз на малих підприємствах. Запропоновано шляхи уникнення потенційних інформаційних загроз. Досліджено фактори впливу на операційну стабільність джерел інформації малих підприємств. Проведено класифікацію інформаційних загроз для малого бізнесу. Запропоновано заходи для мінімізації інформаційних ризиків в малому бізнесі. Розроблено алгоритм реагування на інформаційну загрозу малого бізнесу.

Ключові слова: *інформація, загроза, інформаційні системи, інформаційні технології, автоматизована інформаційна система, хмарні технології.*

Постановка проблеми. Метою інформатизації на підприємствах малого бізнесу є створення оптимальних умов для задоволення інформаційних потреб та реалізації діяльності бізнесу на основі формування та використання інформаційних ресурсів і сучасних технологій. Досвід інших країн показує, що інформатизація малого бізнесу сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, розвитку наукомістких виробництв та високих технологій, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства. Орієнтація стратегії розвитку підприємства на інформатизацію є передумовою для його ефективної роботи й підвищення конкурентоспроможності. На аналітичне забезпечення управління діяльністю підприємства сьогодні покладено відповідальне завдання підтримувати відповідний рівень ефективності підприємства, функціонування якого здійснюється в умовах глобалізації конкурентного середовища, комунікаційного феномена інформаційних відносин, трансформації економічної реальності внаслідок імплементації технологічних нововведень, поширення науково-технічних розробок, знань, інтелекту.

Огляд літературних джерел. Питання інформаційної безпеки бізнесу досліджені в працях вітчизняних науковців, а саме: Бондарнко В.О., Копитко М.І., Носов В.В., Пономарьов В.П., Пилипенко А.А., Цимбалбк В.Л., Щербина В.М. та інші. Проте враховуючи виклики сучасності та військовий стан в нашій країні питання інформаційної безпеки на малих підприємствах потребує систематизації та додаткових зусиль.

Мета роботи. Метою дослідження є аналіз видів загроз інформаційної безпеки для малих підприємств та розробка алгоритму щодо їх ліквідації.

Основний матеріал дослідження. У сучасних умовах цифрової трансформації тема інформаційної безпеки бізнесу стає все більш актуальною та набуває стратегічного значення. Зростання кількості інформаційних загроз, особливо в контексті воєнних дій, створює нові виклики для підприємств, змушуючи їх адаптуватися до підвищеного рівня ризику. В умовах військових конфліктів інформаційний простір стає ще одним фронтом, на якому відбувається боротьба за інформаційну безпеку. Інформаційні загрози загрожують не лише фінансовій стабільності підприємств, але й їхній репутації та безперервності бізнес-процесів. Найбільш вразливими є малі компанії, які часто не мають достатніх ресурсів для реалізації комплексного захисту.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як стан захищеності критично важливих інтересів громадян, суспільства та держави в цифровому середовищі [5]. З початком повномасштабної агресії Росії питання захисту бізнесу в інформаційному просторі стало ще більш актуальним. За даними Державної служби спеціального зв'язку та захисту інформації України, з 2022 року зафіксовано 796 атак з боку Росії, що втричі перевищує показники попереднього року [2]. Сучасні інформаційні загрози впливають на національну безпеку, економіку та функціонування державних і приватних структур. Це обумовлює потребу у створенні дієвих механізмів захисту, які включають не лише технологічні рішення, але й управлінські стратегії, спрямовані на мінімізацію ризиків та швидке реагування на загрози.

Інформаційна безпека бізнесу – це сукупність заходів, призначених для захисту інформаційних систем, мереж і даних від кібератак, несанкціонованого доступу та витоку конфіденційної інформації. Вона включає спеціалізоване програмне забезпечення, шифрування, резервне копіювання, контроль доступу, моніторинг мережевої активності та навчання персоналу. Малий бізнес часто стає ціллю кібератак через недостатню увагу до питань інформаційної безпеки. Основні вразливості включають недооцінювання загроз, нехтування навчанням персоналу, використання слабких паролів та ігнорування оновлень програмного забезпечення. Відсутність резервного копіювання даних, офіційної політики безпеки та заходів для захисту мобільних пристроїв значно підвищує ризик компрометації інформаційних систем. Запровадження комплексного підходу до інформаційного захисту, регулярний аналіз ризиків та впровадження сучасних технологій, сприятиме зниженню інформаційних ризиків для малого бізнесу [3].

Кожна українська компанія повинна бути готова до можливих кібератак і заздалегідь оцінити власні вразливості. Ефективна стратегія інформаційного безпеки має бути комплексною та інтегрованою в усі аспекти функціонування підприємства, особливо в умовах повномасштабної війни, що супроводжується значним зростанням кількості хакерських атак, спрямованих на заволодіння критично важливими даними організацій

Інформаційні загрози становлять сукупність факторів і подій, які можуть завдати шкоди діяльності організації, впливаючи на її операційну стабільність, репутацію та безпеку інформаційних активів. Для забезпечення ефективного інформаційного захисту необхідно ідентифікувати ключові типи інформаційних загроз, оцінити їхній вплив на інформаційну безпеку організації (табл. 1).

Для мінімізації інформаційних ризиків у малому бізнесі необхідно впроваджувати комплексні заходи. Насамперед слід провести аналіз рівня інформаційної безпеки, виявити вразливості та оцінити ризики. Важливо регулярно організовувати навчальні заходи для персоналу, проводити тренінги.

Таблиця 1 - Найпоширеніші види інформаційних загроз для малого бізнесу

Вии інформаційних загроз	Характеристика	Наслідки
Зловмисне програмне забезпечення (Malware)	Програми, які містять віруси, трояни, шпигунські модулі, що порушують роботу пристроїв, спотворюють дані.	Витік даних, порушення роботи, фінансові, репутаційні втрати.
Програми-вимагачі (Ransomware)	Шкідливе ПЗ, яке блокує доступ до файлів або систем до сплати викупу.	Втрата даних, фінансові витрати, репутаційні ризики.
Атаки типу «відмова в обслуговуванні» (DDoS)	Перевантаження мережі або серверів, що робить їх недоступними для користувачів.	Збої в роботі сервісів, фінансові втрати через простої.
Соціальна інженерія	Маніпуляції, що змушують людей добровільно передавати конфіденційні дані.	Крадіжка облікових записів, порушення безпеки, фінансові збитки.
Фішинг	Використання обманних методів для викрадення конфіденційних даних через електронні листи або сайти, що маскуються під надійні ресурси.	Компрометація облікових даних, викрадення особистої інформації, фінансові махінації з банківськими рахунками, втрата довіри клієнтів.
Смішинг	Надсилання підроблених SMS із посиланнями на шкідливі сайти або запитами розголосити особисті дані.	Крадіжка конфіденційних даних, розповсюдження шкідливого програмного забезпечення.
Бейтинг	Обман із пропозиціями безкоштовних програм, знижок, купонів.	Завантаження шкідливого ПЗ, компрометація пристроїв.
Тейлгейтінг (піггібекінг)	Фізичне проникнення зловмисника в офіс або на закриту територію.	Компрометація систем, викрадення важливої інформації.
Атаки на ланцюг постачання	Злом підрядників або постачальників для отримання доступу до компаній.	Компрометація даних, порушення роботи ланцюгів постачання.
Ненавмисне розголошення	Випадкове або ненавмисне поширення конфіденційних даних.	Втрати через витік інформації, юридичні та репутаційні наслідки.
Атаки нульового дня	Використання невідомих вразливостей у програмному забезпеченні або пристроях.	Втрати даних, ризик вимог викупу або компрометації систем.
Розвідка сховища	Пошук слабких місць у конфігурації систем для подальшого зламу.	Розголошення критично важливої інформації, значні фінансові збитки.
Витік даних	Несанкціоноване копіювання чи передача даних за межі компанії.	Фінансові, юридичні та репутаційні втрати.
Доступ до інфраструктури через IoT-пристрої	Використання вразливостей інтернету речей (IoT) для проникнення в корпоративні мережі.	Злом мереж, порушення безпеки, втрата контролю над критичною інфраструктурою.

Джерело: згруповано автором [2; 6].

Необхідно використовувати надійні паролі, багатофакторну аутентифікацію та технології шифрування електронної пошти; варто впровадити системи моніторингу на базі ШІ для оперативного виявлення загроз, обмежити доступ IoT-пристроїв до мережі, здійснювати аудит прав доступу й регулярно створювати резервні копії даних, забезпечити безпечні Wi-Fi-з'єднання для запобігання несанкціонованому доступу. Розробка плану реагування на кіберінциденти сприятиме швидкому відновленню бізнес-процесів, а співпраця з експертами у сфері інформаційної безпеки та постійний моніторинг актуальних загроз дозволять адаптувати захисні механізми до нових викликів [4].

З метою зміцнення інформаційної безпеки українських підприємств малого бізнесу державні органи, зокрема Міністерство цифрової трансформації, у співпраці з профільними установами та міжнародними партнерами, започаткували Програму з інформаційної діагностики бізнесу. Ініціатива покликана допомогти компаніям оцінити стан їхньої інформаційної безпеки та отримати поради для її вдосконалення. У рамках програми підприємства можуть безкоштовно отримати такі послуги: тест на проникнення, який дозволяє імітувати реальні кібератаки для виявлення слабких місць цифрової інфраструктури; тест безпеки застосунку, що допомагає ідентифікувати вразливості програмного забезпечення та пропонує заходи для їх усунення; а також оцінка вразливостей системи інформаційного захисту, яка передбачає комплексний аналіз рівня безпеки IT-інфраструктури компанії [1].

Слід зауважити, що ефективне реагування на інформаційні технології є критично необхідним для гарантування безперервності бізнес-процесів та мінімізації наслідків кіберінцидентів. Впровадження чітко визначеного алгоритму дій дозволяє своєчасно виявляти, аналізувати та нейтралізувати загрози, що виникають у цифровому середовищі (рис. 1).

Всей великий бізнес починався з маленької ідеї-стартапу. З часом розростається-маштабується та стає успішним за умов дбайливого господарського управління. (Mcdonalds – міжнародна мережа швидкого харчування, Viber - застосунок для дзвінків і обміну повідомленнями, Uber –

мережа таксі в різних країнах світу та багато інших). Тому саме малий бізнес де зароджуються божевільні ідеї на перший погляд при умілому управлінському підході переростають у щось грандіозне. Інформаційній безпеці малого бізнесу варто приділяти значну увагу, якій через брак коштів на початкових етапах зародження та кваліфікованих фахівців не приділяється належний інтерес.

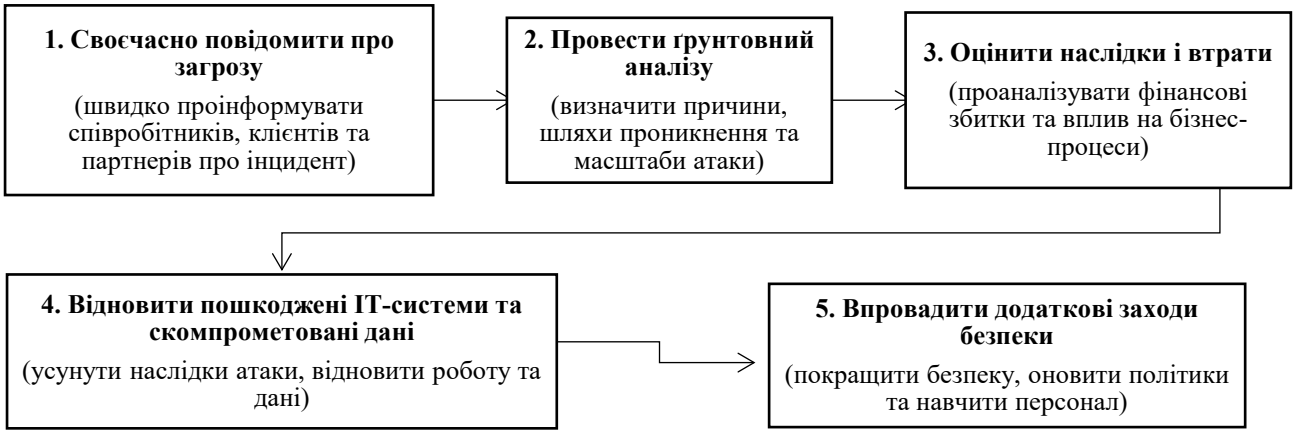

Рис. 1. Алгоритм реагування на інформаційну загрозу малого бізнесу
Джерело: сформовано автором [2].

Отже, аналіз сучасних викликів у галузі інформаційної безпеки малого бізнесу свідчить про необхідність комплексного підходу до захисту інформаційних активів. Зокрема, важливими є впровадження ефективних стратегій захисту, підвищення обізнаності персоналу, використання сучасних систем моніторингу та розробка чітких алгоритмів реагування на інформаційну загрозу. В умовах гібридної війни інформаційна безпека бізнесу стає не лише технічною необхідністю, а й одним із ключових елементів національної безпеки. Ефективний захист передбачає комплексний підхід, який охоплює організаційні, правові та технічні заходи, що дозволять мінімізувати інформаційні ризики. Подальші дослідження у цій сфері повинні враховувати специфічні загрози, що виникають у періоди військових конфліктів, а також сприяти розробці інноваційних підходів до забезпечення інформаційної стійкості та стабільного розвитку бізнесу.

Список використаних джерел

1. Дія. Бізнес. Захист компаній від кіберзагроз: безоплатні послуги для українського бізнесу. *Дія. Бізнес Старт*. URL: https://business.diia.gov.ua/history-of-success/zakhyst-kompanii-vid-kiberzahroz-bezoplatni-posluhy-dlia-ukrainskoho-biznesu.

2. Кібербезпека бізнесу в умовах нестабільності. *PwC*. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.

3. Кравчук В. Проблема захисту кіберпростору малого та середнього бізнесу. *Матеріали XI науково-технічної конференції «Інформаційні моделі, системи та технології»*, Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя. 2023. С. 64-65. URL:https://elartu.tntu.edu.ua/bitstream/lib/44408/2/IMSTT_2023_Kravchuk_V-Cybersecurity_issues_for_64-65.pdf.

4. Кузьменко О.Ю., Маклюк О.В., Чернишова О.О. Кібербезпека бізнесу під час війни. *Економіка та суспільство.* 2022. № 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790/1725.

5. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII станом на 28 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text .

6. Шостак Л.В., Федонюк А.А., Помазун О.О. Особливості кібербезпеки бізнесу в умовах воєнного часу. *Цифрова економіка та економічна безпека*, 2024. №3 (12). С. 121-125. URL:https://evnuir.vnu.edu.ua/bitstream/123456789/25812/1/shostak_fedoniuk_pomazun.pdf.

7. Кучеркова С.О. Використання інформаційних технологій для просування малого бізнесу. Accounting and Finance. 2017. № 1 (75). С. 161-167. URL:http://nbuv.gov.ua/UJRN/Oif_apk_2017_1_20.

8. Саєнсус М.А. Аспекти впровадження інформаційних технологій в малому бізнесі. *Інтелект XXI*.2017.№2.С. 267-272. URL:http://www.intellect21.nuft.org.ua/journal/2017/2017_2/38.pdf.

References:

1. Diia. Business. Protecting companies from cyber threats: free services for Ukrainian business. Diia. Business Start. URL: https://business.diia.gov.ua/history-of-success/zakhyst-kompanii-vid-kiberzahroz-bezoplatni-posluhy-dlia-ukrainskoho-biznesu.

2. Cybersecurity of business in conditions of instability. PwC. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.

3. Kravchuk V. The problem of protecting cyberspace of small and medium-sized businesses. Materials of the 11th scientific and technical conference "Information models, systems and technologies", Ternopil: Ivan Pulyuy Ternopil National Technical University. 2023. P. 64-65. URL: https://elartu.tntu.edu.ua/bitstream/lib/44408/2/IMSTT_2023_Kravchuk_V-Cybersecurity_issues_for_64-65.pdf.

4. Kuzmenko O.Yu., Maklyuk O.V., Chernyshova O.O. Cybersecurity of business during war. Economy and society. 2022. No. 44. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1790/1725.

5. On the Basic Principles of Ensuring Cybersecurity in Ukraine. Law of Ukraine dated 05.10.2017 No. 2163-VIII as of 28 Jun. 2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text .

6. Shostak L.V., Fedoniuk A.A., Pomazun O.O. Peculiarities of Business Cybersecurity in Wartime. Digital Economy and Economic Security, 2024. No. 3 (12). P. 121-125. URL:https://evnuir.vnu.edu.ua/bitstream/123456789/25812/1/shostak_fedoniuk_pomazun.pdf.

7.Kucherkova S.O. Using information technologies to promote small business. Accounting and Finance. 2017. No. 1 (75). P. 161-167. URL:http://nbuv.gov.ua/UJRN/Oif_apk_2017_1_20.

8. Saensus M.A. Aspects of implementing information technologies in small business. Intellect XXI.2017. No. 2. P. 267-272. URL:http://www.intellect21.nuft.org.ua/journal/2017/2017_2/38.pdf.

The article is devoted to creating optimal conditions for the implementation of small business. The article reflects the necessity and need for ensuring information security for small business. The main causes of information threats in small enterprises are investigated. Ways of avoiding potential information threats are proposed. Factors influencing the operational stability of information sources of small enterprises were studied. Information threats to small businesses were classified. Measures were proposed to minimize information risks in small businesses. An algorithm for responding to information threats to small businesses was developed.

Keywords: *information, threat, information systems, information technologies, automated information system, cloud technologies.*