

УДК 336(477)

Бабенко-Левада В.Г.¹, Цимбал А.С.²

¹канд. екон. наук, доц. НУ «Запорізька політехніка»

²студ. гр.ФЕУ-111 НУ «Запорізька політехніка»

ВПЛИВ КІБЕРБЕЗПЕКИ НА РОЗВИТОК БІЗНЕСУ

Кібербезпека стає не лише важливою, але й критично необхідною для будь-якого сучасного бізнесу. В цифрову епоху, коли даними обмінюються і зберігаються в онлайн-середовищі, забезпечення їх безпеки має пріоритетне значення.

В сучасному світі почали посилювати заходи кібербезпеки. До основних її протидій зловмисним кібератакам відносять:

Захист конфіденційності даних. Бізнеси мають зобов'язання захищати конфіденційні дані клієнтів, партнерів і власну конфіденційну інформацію. Порушення цієї конфіденційності може призвести до великих втрат довіри і фінансових штрафів.

Збереження цілісності даних. Кібератаки можуть призвести до викривлення або втрати даних, що може пошкодити їхню цілісність та достовірність. Це може вплинути на рішення бізнесу, зроблені на підставі цих даних.

Забезпечення доступності інформації. Кібератаки, такі як DDoS-атаки, можуть призвести до відмови в обслуговуванні, що може негативно вплинути на роботу бізнесу та його здатність надавати послуги своїм клієнтам.

Фінансові втрати. Кібератаки можуть призвести до прямих фінансових втрат через крадіжку грошей або шкоду інфраструктурі. Крім того, вони можуть мати і непрямий вплив, знижуючи прибуток через втрату довіри та клієнтів.

Репутаційний ризик. Кібератаки можуть суттєво пошкодити репутацію бізнесу через витік або викривлення даних, а також через відмови в обслуговуванні. Це може мати довготривалий вплив на довіру клієнтів і партнерів.

Україна була сценою кількох значних кібератак, які викликали великі збитки та спричинили серйозні проблеми для урядових установ, бізнесів та громадян. Деякі з найбільш відомих інцидентів включають:

Кібератаки на критичну інфраструктуру. Наприклад, кібератаки на енергетичну систему, телекомунікаційні компанії та інші критичні інфраструк-

турні об'єкти. Ці атаки можуть мати серйозні економічні наслідки та негативно впливати на життя громадян.

Віруси та шкідливе програмне забезпечення. Наприклад, розповсюдження вірусів типу WannaCry, який атакував комп'ютерні системи по всьому світу, включаючи Україну, призвело до значних технічних та фінансових збитків.

Кібератаки на урядові органи та бізнеси. Україна також стала мішенню для кібератак, спрямованих на урядові установи та підприємства. Ці атаки можуть призвести до витоку конфіденційної інформації, фінансових збитків та порушення нормального функціонування. [1]

Нижче перераховано основні методи атак, які в даний час найчастіше використовуються:

Шкідливе програмне забезпечення (ШПЗ) або зловмисне ПЗ - це нелегальне програмне забезпечення, яке незаконно встановлюється у системі. Воно може приховуватися в законних джерелах або прикріплюватися до файлів. ШПЗ може використовуватися для викрадення конфіденційних даних, блокування доступу або шифрування файлів.

Програми-вимагачі - це форма зловмисного ПЗ, яка шифрує файли на комп'ютері та вимагає викуп за їхнє відновлення.

Віруси - це програми, які самовідтворюються та заражають файли та системи, що може призвести до непридатності комп'ютера для використання.

Атаки типу "відмова в обслуговуванні" (DDoS) - це зловмисна кібератака, яка перевантажує мережу хибними запитами, щоб перешкодити нормальному функціонуванню бізнесу.

Фішинг - це атака, яка полягає в імітації законних джерел для отримання конфіденційних даних через електронну пошту, SMS, соціальні мережі тощо.

Внутрішні загрози - це загрози, що виникають зсередини організації. Це можуть бути навмисні дії співробітників або ненавмисні недбалість та помилки.

Досвід компанії BDO в Україні підтверджує необхідність комплексного захисту від цих кіберзагроз, який включає як новітнє обладнання та програмне забезпечення, так і заходи для захисту основних напрямків діяльності компанії. [2]

Компанія може забезпечити собі захист від кібератак, використовуючи комплекс заходів з кібербезпеки. Це включає встановлення надійного антивірусного програмного забезпечення та систем виявлення вторгнень, регулярне оновлення програмного забезпечення, проведення аудитів безпеки, навчання персоналу правилам кібербезпеки, використання багатофакторної автентифікації, міцних паролів та їх періодичну зміну, резервне копіювання та зберігання даних у безпечному місці, а також моніторинг захисту.

Отже, у сучасному світі кібербезпека є ключовим елементом успішного бізнесу і необхідною умовою сталого розвитку. Недбале ставлення до цього питання може призвести до серйозних наслідків, включаючи фінансові втрати та порушення репутації компанії. З іншого боку, вкладання у кібербезпеку дозволить вашій компанії захистити себе від потенційних загроз та підвищить її конкурентоспроможність на ринку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CERT-UA. Computer Emergency Response Team of Ukraine. Режим доступу: <https://cert.gov.ua/articles>
2. LIGA ZAKON. Режим доступу: Захист бізнесу: як убезпечити підприємство від кіберзлочинів? | Think brave (ligazakon.net)