СПІЛКА
АВТОМАТИЗАТОРІВ
БІЗНЕСУ

Нові інформаційні технології управління бізнесом

Збірник тез
VII Всеукраїнської науково-практичної конференції

Київ 2024

СПІЛКА
АВТОМАТИЗАТОРІВ
БІЗНЕСУ

Нові інформаційні технології управління бізнесом

Збірник тез
VII Всеукраїнської науково-практичної конференції

Київ 2024

Збірник тез VII Всеукраїнської науково-практичної конференції "Нові інформаційні технології управління бізнесом". – Київ: Спілка автоматизаторів бізнесу, 2024. – 288 с.

Редакційна колегія:

Мазур Вадим Броніславович**,** Голова "Спілки автоматизаторів бізнесу", Шеремет Ольга Анатоліївна, методист "Спілки автоматизаторів бізнесу", Старцев Олексій Сергійович, методист "Спілки автоматизаторів бізнесу".

Матеріали збірника публікуються у авторській редакції.

©Всеукраїнська громадська організація "Спілка автоматизаторів бізнесу", 2024

Адаптивність та впровадження передових технологій в освітній процес стають ключовими чинниками успіху в цьому напрямку.

Перелік використаної літератури:

1. Освіта і наука України в умовах воєнного стану: інформаційно-аналітичний збірник. – К.: 2023. [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/storage/app/media/zagalna%20serednya/serpneva-konferencia/2023/22.08.2023/Inform-analytic.zbirn-Osvita.v.umovah.voyennogo.stanu-vykl.rozv.povoyen.perspekt.22.08.2023.pdf
2. Coursera. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.coursera.org/learn/os-power-user-ua
3. Udemy. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.udemy.com
4. edX. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.edx.org/learn/operating-systems#b92f28f8-dc0d-59e0-989f-ed7a4504eb8a

Городянська Л.В.
чл.-кор. АЕН України, доцент, к.е.н,
доцент кафедри туризму та готельно-ресторанного бізнесу
Київський національний університет технологій та дизайну

КІБЕРЗАГРОЗИ У МАЛОМУ БІЗНЕСІ В СУЧАСНИХ УМОВАХ

Одним з важливих пріоритетів у повоєнному відновленні економіки України має бути підтримка малого та середнього бізнесу [1]. Характерними ознаками моделей повоєнного відновлення, які передбачають задоволення потреб людини в цифровому середовищі, пов'язані з ризиками кіберзагроз. Такі загрози пов'язані з використанням людиною сучасних інформаційних технологій, Інтернет та інших соціальних мереж. Малий бізнес – це соціально-економічний фундамент держави, на базі якого розвивається суспільство. За даними ООН, тільки у виробничій сфері малі та середні підприємства створюють від 30 % до 70 % національного продукту, забезпечують зайнятість близько 50 % працездатного населення [2]. Мале підприємництво є самостійною інноваційною діяльністю громадян-підприємців на власний ризик з метою отримання доходу. Власники несуть повну відповідальність за результати господарювання, ринок збуту і сімейне володіння справою [3]. За результатами дослідження Комітету Сенату США у справах малого бізнесу і підприємництва, майже 60 % малих підприємств припиняють свою діяльність внаслідок викрадення конфіденційної інформації, а 71 % всіх кібератак відбуваються на підприємствах з чисельністю персоналу менше 100 осіб.

Незадовільний рівень захищеності даних середнього та малого бізнесу в сучасному інформаційному середовищі приваблює хакерів та кіберзлочинців. Пожвавлення ІТ-індустрії та розширення інформаційного простору лише посилює слабкі місця бізнесу, які пов'язані з кібербезпекою. Закон України "Про основні засади забезпечення кібербезпеки України" [4] є одним із базових нормативних документів, який регулює цю галузь на національному рівні. Зокрема, у ст. 10 Закону [4] підкреслено важливість "підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі".

Метою дослідження є узагальнення найбільш привабливих для кіберзлочинців видів інформації суб'єктів малого підприємництва та формування основних напрямів захисту цієї інформації в сучасних умовах.

Неможливо уявити успіх малого бізнесу по просуванню товарів (робіт, послуг), пошуку клієнтів по всьому світу, забезпечення внутрішньої комунікації без використання соціальних мереж. Зазвичай, власники малого бізнесу майже не звертають належну уваги на кібербезпеку, що робить такі підприємства ідеальною мішенню для кіберзлочинців. Не зважаючи на вид бізнесу (виробництво, консалтинг чи Інтернет-магазин), бізнес використовує в роботі мережу Інтернет та пов'язані з цим ризики та загрози. Власники бізнесу мають усвідомлювати ці загрози і приділяти належну увагу навчанню співробітників основам кібербезпеки.

Дослідженню проблем наростаючих кіберзагроз присвячено праці таких вчених, як В.Л. Бурячок, Я.Ю. Усов, В.А. Лахно, А.М. Терещук, Т.А. Петренко, R. Abidar, C. Aclaraz, A.J. Jegede, G.I.O. Aimufua, H.O. Salami, A.A.El. Hassani, A.A.El. Kalam, A. Bouhoula, R. Abassi, A.A. Ouahman та інші.

Кіберзлочинці шукають інформацію про бізнес та клієнтів з метою незаконного використання чи пошкодження їх інформаційних ресурсів в незалежності від того, зберігається інформація на серверах чи в хмарах, надсилається електронною поштою чи розміщується в архівах на робочих комп'ютерах співробітників. З метою отримання необхідної інформації, вони знаходять доступ до комп'ютерів, вражають їх вірусами та/або зловмисними програмами [5].

На рисунку наведено основні види інформації, які можуть зацікавити кіберзлочинців в сучасних умовах.

Кіберзлочинці мають багато способів враження персональних комп'ютерів, смартфонів та планшетів з метою незаконного використання інформаційних ресурсів малого бізнесу. За даними Zillya-антивірус [6] активність шкідливого програмного забезпечення в Україні неухильно зростала, і до початку пандемії Covid-19 приріст інфікування пристроїв складав близько 10-15 %.

Зазвичай, малий бізнес стає об'єктом кібератак, оскільки ресурси таких підприємств обмежені. Свідоме розуміння взаємодії між людьми й технологіями в процесі організації бізнесу потребує планування заходів навчання персоналу й набуття ним відповідних фахових компетентностей [7].

Рисунок 1. Види інформації суб'єктів малого підприємництва, які є потенційно цікавими для кіберзлочинців

Сформовано пропозиції щодо створення комплексної програми безпеки, до складу якої мають увійти план дій, спрямований на захист від зовнішнього та внутрішнього впливу на функціонування інформаційної системи підприємства, і комплекс заходів, призначений для захисту конфіденційності, доступності, цілісності даних від внутрішніх і зовнішніх, шкідливих та випадкових загроз [7, с. 111].

Важливо виокремити інформацію, яка є цінною для бізнесу, щоб мати можливість комплексно організувати її захист. Цінність інформації обумовлена наступними критеріями:

- конфіденційна інформація;
- цілісна інформація (інформація не може бути загальнодоступна або втрачена);
- критична інформація про бізнес (наприклад, інформація про продажі, плани реагування на надзвичайні ситуації тощо);
- бухгалтерські записи та первинна інформація, які повинні бути захищеними від несанкціонованих змін (наприклад, контракти, квитанції, договори тощо).

Організація захисту важливої інформації у малому бізнесу передбачає проведення низки наступних дій:

- Визначити цінність інформації; місце, де зберігається важлива інформація; коло працівників, які мають доступ до цінної інформації; можливі загрози для бізнесу.
- Забезпечити захист та обмеження доступу до чутливих систем та інформації; шифрування конфіденційної інформації; можливості вчасного оновлення програмного забезпечення; використання веб-фільтрів та фільтрів електронної пошти; переформатування дисків перед утилізацією.
- Виявити особливості використання антивірусного програмного забезпечення; аналіз журналів, підтримка та відстеження активності для виявлення проблем.

• Розробка плану реагування на інциденти; планування навчання працівників роботі з електронною поштою та з іншими соціальними мережами.

• Створення резервних копій інформації.

Організація заходів безпеки має бути включена до планів з метою захисту цінної інформації та бізнес-процесів. Адміністрування бізнесу з питань захисту інформаційних активів передбачає планування заходів із забезпечення:

• Веб-безпеки, яка включає захист особистої та ділової інформації, безпечний перегляд Інтернету персоналом підприємства, соціальні мережі, безпеку програмного забезпечення, безпечний хостинг та безпека веб-бізнесу, зловмисне програмне забезпечення, паролі та прохідні фрази, двофакторна аутентифікація.

• Безпеки у місцях продажу (POS), включаючи безпеку електронної пошти (спам, фішинг, безпечне надсилання електронних листів, соціальна інженерія).

• Безпеки даних з урахуванням параметрів резервного копіювання, захищеності у хмарному середовищі, класифікацію та визначення інформації, що потребує особливого захисту та поводження з такою інформацією.

• Безпеки віддаленого доступу з урахуванням основ безпеки віддалених обчислень, особливостей роботи вдома та під час подорожі.

• Захисту мобільних пристроїв.

Клієнти очікують, що їхня особиста інформація теж має бути убезпечена. Підприємства, з якими співпрацює малий бізнес, потребують впевненості в тому, що їх конфіденційна інформація не буде наражатися на кібернетичну небезпеку. Не існує єдиної технології організації бізнесу, особливо в сучасних умовах, коли загроз стає все більше. Захист малого бізнесу потребує чіткої організації процесів виявлення та оперативного реагування на загрози, які неухильно змінюються.

Власники малого бізнесу та найняті працівники не обізнані в усіх видах кіберзагроз, з якими вони можуть зіткнутися, тому особливо важливо дотримуватися плану їх запобігання. Необхідно встановити чіткі і зрозумілі рамки, яких мають дотримуватися співробітники при електронному листуванні або в процесі роботи в мережі Інтернет.

Кібербезпека бізнесу є відповідальністю власника і саме він повинен планувати навчання співробітників з питань кіберзагроз. Самоосвіта та навчання співробітників підприємства є ключовим для уникнення втрат від несподіваної кібератаки.

Висновки: У дослідженні виокремлено види інформації малого бізнесу, які можуть піддаватися кібератакам. Кібератаки можуть спричиняти значні збитки підприємству, які пов’язані з втратою ним клієнтів, зниженням іміджу й конкурентних переваг, та відповідно, прибутку. Разом з цим відбувається зниження вартості бізнесу, штрафні санкції, втрата довіри клієнтів та постачальників та інші негативні наслідки, які руйнують малий бізнес. До важливої інформації, яка цікавить кіберзлочинців, належать: записи клієнтів (включаючи контактну інформацію, історію продажів та паролі); списки контактів клієнтів, співробітників, партнерів; інформацію про працівників (включаючи електронні адреси, паролі); банківську інформацію про компанію та партнерів; номери кредитних карток.

Кібербезпека малого бізнесу передбачає спільні зусилля власника бізнесу та співробітників, які повинні бути підготовленими та реалізувати процедури кіберзахисту і в разі необхідності вміти швидко реагувати на загрози. Власник бізнесу несе відповідальність за впровадження комплексної програми безпеки й організацію навчання співробітників основним протидіям кіберзлочинцям (інструкції, семінари, конференції). Навчання та підготовка співробітників, окрім іншого є однією з найважливіших заходів протидії кіберзагрозам на підприємництві.

Перелік використаної літератури:

1. Мошенець О. Яка модель повоєнного відновлення спрацює в Україні//LB.ua: веб-сайт. 2022. URL: https://lb.ua/blog/olena_moshenets/533342_yaka_model_povoiennogo_vidnovlennya.html (дата звернення: 05.02.2024).

2. Dykan E. V. DEVELOPMENT OF SMALL BUSINESS IN UKRAINE: PROBLEMS AND WAYS OF SECURITY. Вісник економіки транспорту і промисловості. 2017. № 57. С. 58-65

3. Варналій З. С. Конкуренція і підприємництво: монографія. Київ: Знання України, 2015. 463

с.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.02.2024).
5. Buriachok V., Ageyev D., Zhyltsov O., Skladannyi P. and Sokolov V. Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies. URL: http://ceur-ws.org/Vol-2746/paper3.pdf pp. 23-32.
6. Кіберсвіт: Які загрози очікують на користувачів у 2019 році//Zillya: веб-сайт. URL: https://zillya.ua/kibersvit-yaki-zagrozi-ochikuyut-na-koristuvachiv-u-2019-rotsi (дата звернення: 05.02.2024).
7. Городянська Л.В., Цюкало Л.В.Інформаційна безпека суб'єктів малого підприємництва в умовах цифровізації. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ:ВІКНУ імені Тараса Шевченка, 2021. Вип. 70. С. 105-114. doi:https://doi.org/10.17721/2519-481X/2021/70-11

Грабович І.В.
аспірант
Національний університет "Львівська політехніка"

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МАРКЕТИНГОВОЇ ДІЯЛЬНОСТІ

Зростання ролі штучного інтелекту (ШІ) у бізнесі, зокрема в маркетингу, стає все більш помітним, оскільки компанії розуміють його потенціал для оптимізації та автоматизації процесів та підвищення ефективності діяльності. ШІ вносить значні покращення у велику кількість аспектів маркетингової діяльності, від аналітики та прогнозування до персоналізації стратегій та оптимізації рекламних кампаній.

Штучний інтелект – це концепція нелюдських сутностей (наприклад, комп'ютерів), що володіють інтелектом на рівні людини та виконують інтелектуальні завдання. Загалом, це розумний комп'ютер, який здійснює такі самі розумні операції, як і людина. ШІ має можливість вчитися на досвіді, пристосовуватися до нових даних і виконувати завдання, подібні до людських. Штучний інтелект робить більше, ніж просто надає підприємствам віртуальних особистих помічників – він змінює маркетинг, яким ми його знаємо. Цифрові маркетологи нині мають неймовірну хвилю інформації, що надходить з доступних, просунутих інструментів аналізу даних, забезпечуючи глибоке розуміння не лише споживачів, а й того, що, як і кому продавати [1].

Штучний інтелект у маркетинговій діяльності розглядають як "інструмент, що допомагає підвищити ефективність маркетингових комунікацій. За допомогою штучного інтелекту можна контролювати та управляти процесом реклами, створенням відгуків, аналізувати процес просування та давати рекомендації користувачам" [2]. У маркетингових (споживчих) дослідженнях визначення ШІ використовується для позначення набору інструментів, які можуть підвищити "інтелект" продукту, послуги чи рішення. У більш загальному вираженні штучний інтелекту визначається як "здатність системи правильно інтерпретувати зовнішні дані, навчатися на основі таких даних і використовувати ці знання для досягнення конкретних цілей і завдань через гнучку адаптацію" [3].

Поява мобільних пристроїв зв'язку, портативних комп'ютерів і планшетів, смартфонів, все більш широке використання всесвітньої павутини Інтернет, CRM-системи і соціальних медіа, суттєвим чином впливають на сучасний маркетинг. Комунікації з допомогою цих нововведень допомагають підприємствами рости та розвиватися, знаходити більше споживачів, дозволяють людям швидко знайти детальну інформацію про них. Таким чином, вони повністю змінюють способи взаємодії компаній з їх потенційними клієнтами. Ці нові форми комунікацій практично повністю змінюють уявлення про засоби масової інформації (ЗМІ) і стратегіях просування, які використовують організації [4]. Можливості штучного інтелекту дозволяють підвищити рівень впливу на споживача через персоналізацію реклами, тобто запропонувати покупцю товар, який відповідатиме його вподобанням, потребам, віку, сезону [5]. Особливою відмінністю та перевагою сьогоднішніх цифрових інструментів маркетингу є швидкість, ефективність, персоналізованість та