Карламов Д. О.
здобувач вищої освіти факультету менеджменту
Науковий керівник: **Полторак А.С.,**
д-р екон. наук, професор
Миколаївський національний аграрний університет,
м. Миколаїв

АНАЛІЗ РИЗИКІВ КІБЕРАТАК НА СУЧАСНОМУ ПІДПРИЄМСТВІ

Проблематика мінімізації рівня кіберзлочинності в Україні є важливим питанням для стабільної діяльності банківського сектору та забезпечення захисту фінансових даних. За останні роки загрози потужних кібератак зростають з великою швидкістю завдяки інтенсивному розвитку технологій [1].

Зловмисники користуються різноманітними технологіями та методами для атак на підприємства, у т. ч. віруси, троянці, фішинг, DDoS-атаки тощо. Це створює великий ризик для підприємств незалежно від їх розміру та галузі функціонування. Сучасні підприємства зберігають значний обсяг конфіденційної та важливої інформації в цифровому форматі. Ця інформація може бути цінною для зловмисників, а її втрата або пошкодження може завдати значної шкоди діяльності підприємства. Виявлено, що кібератаки можуть призвести до значних економічних втрат, включаючи втрату прибутку, витрати на відновлення, втрату клієнтів та репутації. Вони також можуть призвести до штрафів та правових проблем.

Дослідженнями питань протидії кібератакам займаються багато спеціалістів різних сфер діяльності, з-поміж яких М. Ю. Богославський [1, 2], В. Ю. Зубок [3], В. Д. Гавловський [4], Д. О. Маріц [5] та інші.

Існує значна кількість видів кібератак, кожен з яких має свої характеристики та може впливати на сучасне підприємство різними способами. Ось деякі з основних видів кібератак і їх характеристики:

1. Фішинг – атака, під час якої атакуючий видає себе за довірену сторону (переважно через електронну пошту), щоб шахраювати користувачів на відкриття шкідливих посилань або введення конфіденційної інформації. Фішинг може призвести до витрат на відновлення та втрати репутації.
2. Віруси і троянці – програми, які можуть поширювати шкідливий код, що надалі призведе до видалення даних, переривання роботи системи та втрати інформації.
3. DDoS-атаки (атаки з відмовою в обслуговуванні) – це атаки, під час яких атакуючий перевантажує мережу або сервери підприємства з метою їхньої недоступності для легітимних користувачів. Це може вплинути на доступність продуктів і послуг підприємства.

4. Кібершпигунство – процес, спрямований на отримання конфіденційної інформації, такої як комерційні та технічні секрети, патенти, та інші конфіденційні дані. Це може завдати шкоди конкурентному позиціонуванню підприємства.

5. Соціальна інженерія – атака, під час якої атакуючий використовує маніпулювання психологією користувачів, щоб отримати доступ до інформації або систем.

6. Внутрішня загроза – загроза від власних співробітників підприємства, які можуть зловживати своїм доступом або навмисно створювати проблеми.

Для попередження кібератак, а також ефективної боротьби з ними, погоджуємось з думкою В. М. Богуша та В. Л. Бурячка, що для захисту інформації важливою є підготовка спеціалістів, діяльність яких буде пов'язана з протидією кіберзлочинності та зміцненням рівня кібербезпеки особистості, підприємства та держави у цілому [5].

Найбільш цікавими з точки зору сучасних підприємств можуть стати знання, які стосуються: теоретичних основ кібернетичної безпеки, правових та організаційних засад протидії кіберзлочинності, методів та засобів протидії кіберзлочинності, програмного забезпечення систем кібернетичної безпеки, криптографічних механізмів кібернетичної безпеки, кібернетичної безпеки підприємств, основ кібернетичної безпеки держав [5, 6].

Загрози кібербезпеці є постійною реальністю, саме тому підприємства повинні розглядати інвестування в захист даних як вирішальну потребу для збереження успішності та надійності свого бізнесу. Це означає розробку стратегій кібербезпеки, інвестування в сучасні технології, навчання співробітників та постійний моніторинг для виявлення та реагування на потенційні загрози [7, 8].

Доведено, що на сучасному етапі розвитку науки та техніки зміцнення безпеки інформації на підприємстві має ґрунтуватися на принципово новому синергетичному підході. Його впровадження надасть змогу одержати ефект у разі взаємодії обраних профілів безпеки і, як наслідок, проявити якісно нові та невідомі до цього емерджентні властивості системи безпеки.

Односторонні ініціативи з боку підрозділів підприємства можуть забезпечити оперативне реагування на виникаючі ризики, усувати витоки клієнтської інформації, паралельно займатися розробкою нових методів боротьби з кібератаками, залучати менше ресурсів, але з більшим результатом та проводити систематичну профілактику протидії загрозам підприємства [1].

Отже, захист корпоративної інформації та даних на сучасних підприємствах є надзвичайно важливим завданням в умовах постійних кіберзагроз. Кібератаки можуть призвести до серйозних наслідків, включаючи втрату даних, фінансові втрати, репутаційний збиток та юридичні проблеми.

Важливість захисту даних на підприємстві обґрунтовується не лише економічними аспектами, але й суспільною відповідальністю та збереженням довіри споживачів та партнерів.

Список використаних джерел

1. Богославський М. Ю. Дослідження ступеню протидії банківським кібератакам на світовому та вітчизняному рівнях. *Агросвіт.* 2018. № 2. С. 88-92.

2. Богославський М. Ю. Методичні підходи до фінансового заміщення та еластичності в рамках забезпечення протидії кібератакам банку. *Бізнес-навігатор*. 2018. Вип. №1-2. С. 85-88.

3. Зубок В. Ю. Визначення напрямків протидії кібератакам на глобальному маршрутизацію в мережі інтернет. *Електроннне моделювання.* 2018. №5. С. 67-75. DOI: 10.15407/emodel.40.05.067.

4. Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право.* 2019. № 3(30). С. 105-110.

5. Маріц Д. О. “Кібератака” – війна майбутнього. *Інформація і право.* 2015. № 3(15). С. 104-109.

6. Полторак А.С., Баришевська І.В., Мельник О.І., Боднар О.А. Кібернетична безпека банківського сектора в системі фінансової безпеки держави. *Сучасні тенденції розвитку фінансово-кредитної системи: теорія та практика* : колективна монографія; Київ : Центр фінансово-економічних наукових досліджень, 2019. С. 79–83.

7. Полторак А.С., Сухорукова А.Л., Бурковська А.І. Кібербезпека в системі трансформації управління бізнес-організацією. *Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики* : колективна монографія з нагоди 115-річчя Київського національного економічного університету імені Вадима Гетьмана ; за загальною редакцією М. П. Сагайдака, Т. О. Соболєвої. Київ : Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана. КНЕУ, 2021. 378 с. ISBN 978–966–926–399–5 С.158-176.

8. Полторак А. С., Тимошенко Ю. С. Ефективне управління фінансовими ризиками в системі економічної безпеки України. *Агросвіт*. 2015. № 1. С. 34–39.