РІСТ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ ТА КІБЕРБЕЗПЕКА

СОБОЛЄВА Ганна Григорівна,
канд. екон. наук, доцент
ОСАУЛЕНКО Олександр Володимирович,
здобувач вищої освіти
Харківський національний університет
міського господарства імені О. М. Бекетова

Цифровізація економіки робить бізнес більш конкурентним та надає значний ріст та відкриває нові ринки та залучає багато клієнтів, які раніше були недосяжні. Створюються веб сайти та мобільні застосунки, підключається онлайн платежі, впроваджується електронний документообіг, кампанії в соцмережах, підключаються такі технології як Штучний Інтелект та Машинне Навчання для аналізу та управління вашими даними – це все інструменти, для цифровізації.

В цей же час на зворотній “стороні світла” зростають кіберзлочинці. Вони стають вашими клієнтами та починають “вивчати” ваш бізнес. І чим більше ви “оцифрували”, тим більше у кіберзлочинців варіантів для “навчання”. Далі вони починають атакувати спричиняючи великі втрати як фінансові так і іміджеві або призводять, навіть, до закриття бізнесу. Ті випадки, про які ми дізнаємося з ЗМІ, це лише невеличка частина того, що відбувається насправді, і це є проблема. Бізнес не розуміє, що приховування таких атак може спричинити більш тяжкі наслідки, ніж сама атака – втрата довіри, клієнтів, доходів і як наслідок бізнесу. Також не потрібно думати, що кіберзлочинцям цікаві великі корпорації чи компанії, середній бізнес теж під загрозою, бо скоріш за все він менш захищений, а також може бути використаний, в разі успішної атаки, як спосіб проникнення в цифрову інфраструктуру більшої компанії. Поява такого цифрового інструменту економіки, як криптовалюти, допомагають кіберзлочинцям отримувати винагороду за свої дії, анонімізувавши себе.

Запобігти атакам чи мінімізувати втрати після них – це персональна відповідальність як керівників бізнесу так і співробітників. Повинна бути впроваджена програма періодичного навчання та тестування загрозам. Також бізнес повинен мати план дій у разі успішної атаки на його цифрову інфраструктуру. Бізнес повинен розуміти, що ріст цифровізації, а не доходів, як помилково вважають багато керівників, має супроводжуватися і ростом витрат на кібебезпеку.

Не треба забувати і про державні організації, атака на які може спричинити тяжкі наслідки, які можуть загрожувати, навіть, існуванню держави або негативно вплинути на критичні важливі інфраструктурні об’єкти та всю економіку взагалі. Достатньо згадати, як у 2017 році Україна та інші країни в світі, були успішно атаковані хробаком “Petya” через невідому до того часу вразливість Windows. Цю вразливість використали, додавши небезпечний код в оновлення програми M.E.Doc. Згідно звіту, в Україні було

виведено з ладу близько 10% комп'ютерів, а збитки світової економіки сягнули майже 8 млрд. доларів.

Не менш важливу роль кібербезпеки ми почали відчувати в часи великих криз. Коли трапилась пандемія COVID-19, то багато людей в світі відчули, що сучасні цифрові технології дозволяють бізнесу майже не втрачати працездатність і зберігати робочі процеси, перевівши їх в онлайн. Але це відкрило і більше можливостей злочинцям для їхніх атак на інфраструктуру та дані і в цей час кібербезпеці почали приділяти більше уваги ніж будь-коли. Коли відбулося повномасштабне вторгнення Росії в Україну, то той український бізнес, який під час пандемії підлаштувався під зміни, зазнав мінімальних втрат від нападу окупантів. Також для захисту економіки України від кібератак Росії, урядом США був створений проєкт USAID "Кібербезпека критично важливої інфраструктури України", який відіграє важливу роль від початку повномасштабного вторгнення. Він забезпечує державні об'єкти, установи інструментами та експертними знаннями, які необхідні, щоб служби працювали без перерви та збоїв.

Впровадження кібербезпеки бізнесом не мета, а процес і цей процес має багато стратегій та практик, які можна розділити на три групи: запобігання, виявлення та реакція.

Запобігання – це періодичні навчальні курси всіх співробітників бізнесу, включаючи керівництво, періодичне тестування системи на вразливість, постійне оновлення цифрової інфраструктури згідно рекомендаціям постачальників програмного забезпечення та звітів організацій, які надають послуги з кібербезпеки та аналізують атаки. Це також складання мапи даних, та розділення її на дуже чутливу (секретну), не публічну та публічну. Впровадження надійних сховищ для чутливої та не публічної інформації, дублювання, резервування для відновлення її в разі втрати чи пошкодження від атаки.

Виявлення – це постійний моніторінг та аналіз всіх цифрових інструментів, які впроваджені в компанії, на наявність слідів чи процесів, які вказують на атаку.

Реакція – це дії відповідного департаменту та керівництва, які потрібно виконати, у разі виявлення атаки, втрати чи пошкодження даних, в найкоротший термін, для мінімізація впливу на бізнес, це також публікація звіту про атаку, та які наслідки і який відбувся вплив на бізнес чи дані, що може допомогти іншим компаніям запобігти аналогічним атакам, а також допоможе проінформувати клієнтів про атаку. Додатково повинні бути впровадженні кроки по запобіганню аналогічним атакам в майбутньому.

Отже, не існує кібербезпеки, яка б захистила бізнес від всього на світі, і тому цифровізація економіки повинна відбуватись незважаючи на загрози, в той же час вона повинена бути готова до можливих атак кіберзлочинців та адекватно реагувати на них.

Список використаних джерел:
1.Ляшенко В.І., Вишневський О.С. Цифрова модернізація економіки України як можливість проривного розвитку: монографія / НАН України, Ін-т економіки пром-сті. К.: 2018. 252.
2. Цифровая экономика: 2019: краткий статистический сборник. М.: НИУ ВШЭ, 2019. 96 с.

ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ОПТИМІЗАЦІЇ УПРАВЛІННЯ РЕСУРСАМИ

СТАДНИК Софія Сергіївна,
здобувач вищої освіти
Науковий керівник – ***СЕРЬОГІНА Дар'я Олександрівна,***
канд. екон. наук, доцент,
Харківський національний університет
міського господарства імені О. М. Бекетова

Цифрові технології надають підприємствам нові можливості для оптимізації управління ресурсами. У ході проведеного дослідження було вивчено вплив цифрових технологій на процеси управління ресурсами та їхній внесок у підвищення ефективності та конкурентоспроможності підприємств.

Цифрові технології визначаються як інноваційні інструменти та рішення, спрямовані на забезпечення ефективного управління ресурсами. У результаті аналізу було встановлено, що ці технології дозволяють підприємствам збирати, аналізувати та використовувати дані для оптимізації ресурсів. Вони роблять процес управління більш точним, швидким та адаптивним до змін в бізнес-середовищі.

У використанні цифрових платформ, зокрема систем управління ресурсами (ERP), було виявлено докладний аналіз їхньої ролі в управлінні ресурсами. ERP-системи дозволяють інтегрувати різні аспекти управління, від фінансів до логістики, що полегшує координацію та оптимізацію ресурсів. Досліджено також використання хмарних технологій для зберігання та обробки даних, що робить їх доступними та масштабованими для підприємств різного розміру.

Впровадження аналітики та машинного навчання дозволяє підприємствам передбачати потреби в ресурсах та приймати обґрунтовані рішення. Аналіз великих обсягів даних надає можливість виявляти закономірності та використовувати їх для оптимізації процесів управління ресурсами. Штучний інтелект допомагає підприємствам бути більш адаптивними та реагувати на зміни в реальному часі.

У ході дослідження було виявлено, що автоматизація процесів постачання та логістики через використання цифрових інструментів робить ці процеси більш ефективними та економічними. Internet of Things (IoT) надає