КІБЕРБЕЗПЕКА БІЗНЕС-ПРОЦЕСІВ

Проценко Н. М., канд. екон. наук, доц.
Бутенко Т.А., канд. екон. наук, доц.
Синявіна Ю.В., канд. екон. наук, доц.
Державний біотехнологічний університет

На сьогоднішній час формування економіки багато в чому ґрунтується на процесі цифрової трансформації, уявляючи неймовірні можливості та переваги. Технології проникають у всі сфери, змінюючи зовнішнє виробниче середовище діяльності господарства. Тенденції автоматизації процесів, цифрового управління виробництвом дають змогу підвищити коефіцієнт корисної дії праці, зменшити витрати. Проте водночас багаторазово збільшується вразливість виробничих процесів, але це у свою чергу вимагатиме вжиття відповідних заходів. У цьому контексті особливу роль відіграє інформаційна безпека систем.

Потрібно зазначити, що часто виникає плутанина в поняттях «інформаційна безпека» та «кібербезпека», проте сьогодні кібербезпека є сутністю інформаційно-комунікаційних технологій, глобальним завданням якої є захист активів компаній (власників), безпеки додатків, мережевої безпеки, безпеки Інтернету, а також безпеки критичної інформаційної інфраструктури.

На ставлення бізнесу до інформаційної безпеки сильно вплинули пандемія та геополітичні конфлікти.

Внаслідок пандемії безліч компаній були змушені перейти на віддалений формат роботи та змінити свої бізнес-процеси. Як результат, все більше невеликих підприємств зараз зберігають свої найважливіші дані на платформах, які часто є небезпечними. Варто чітко зрозуміти, що наслідки нападів можуть завдати значної шкоди компанії та її прибутку. Наприклад, у Німеччині, за даними федерального об’єднання підприємств цифрової економіки, телекомунікації та нових медіа Bitkom, хакерських атак за рік зазнали 86 % компаній – майже 9 з 10. Bitkom опитало понад 1000 компаній з різних галузей, які стали жертвами хакерських атак: керівники 59 % компаній, які дозволяють працівникам працювати віддалено, повідомили про випадки комп’ютерної безпеки, які відбулися з початку пандемії; 9 % фірм вважають, що кібератаки загрожують їх існуванню [1]. До того же, крім фінансових втрат від хакерських систем, вони загрожують репутаційними ризиками.

Ахім Берг, президент Bitkom, коментуючи поточний розвиток подій, підкреслив, що за результатами злочинних атак багато бізнес-операції були паралізовані, а викрадені дані клієнтів і компаній не тільки завдали шкоди репутації, але й призвели до втрати конкурентоспроможності. Якщо впродовж 2018-2019 рр. сума збитків становила 103 Є мілр на рік, то в наступні роки крадіжки, шпигунство та диверсії завдають економіці Німеччини загальних збитків у 223 Є мілр. щороку [1]. В Україні протягом 2022 року, за даними Державного центру кіберзахисту, 156 атак були спрямовані на комерційні організації. У 2023 р. ця інтенсивність зберігається [2].

Ескалація геополітичних конфліктів у світі серйозно позначилася на «рівні токсичності» кіберпростору. В рази зросла кількість кібератак, проблеми виникли навіть у тих сферах та галузях, які раніше знаходилися осторонь цих процесів через труднощі монетизації атаки. Стабільна регулярність кібератак хактивістів зачіпають практично всі напрямки компаній.

Варто відмітити, доволі часто середній і малий бізнес вважає, що не є привабливим для зловмисників, а отже, не варто витрачатися на фахівців або робити фінансові вкладення у забезпечення кібербезпеки. Проте це велика помилка. Як правило, великі компанії оснащені найновішими засобами захисту від кібератак. Принаймні так вважають шахраї. Тому вони не чіпають великі організації, а йдуть легким шляхом. За статистикою фактично 43 % усіх кібератак спрямовані на малий бізнес [3].

Прискорення цифровізації, спричинене пандемією, геополітичними конфліктами, ставить перед керівниками бізнес-структур нові завдання щодо кібербезпеки. Більшість атак починається з соціальної інженерії, маніпуляції співробітниками. Найслабкіше місце у кіберзахисті будь-якої компанії люди. Злочинці використовують «людський фактор» як найслабшу ланку в ланцюжку безпеки, щоб отримати конфіденційні дані, такі як паролі. Останнім часом такі спроби були зроблені в 41 % опитаних компаній; 27 % опитаних заявили, що з ними зв'язувалися, зокрема, телефоном, а 24 % електронною поштою [1].

В умовах сучасного світу дуже невеликий відсоток компаній можуть об'єктивно сказати, що ризики інформаційної безпеки для них не є актуальними, мають низький пріоритет. Інформаційні технології стрімко розвиваються і змінюються, у тому числі з'являються нові загрози та небезпеки у кіберпросторі, тому в багатьох компаніях вже прийшли до розуміння що це може торкнутися будь-кого. У компаніях почалося формування ризик-орієнтованого підходу до кібербезпеки, методології оцінки ризиків, раціонального планування бюджету на інформаційну безпеку.

Загрози для бізнесу можуть бути як внутрішніми, так і зовнішніми. Майже кожна компанія має пряму операційну діяльність з Інтернетом: канали комунікацій, інтернет -магазини, хмарні програми тощо. Тому акцент уваги все більше зміщується в бік забезпечення безпеки безпосередньо застосованого програмного забезпечення, веб -порталів та інших ресурсів. Наявність вразливих місць у такому програмному забезпеченні може призвести до різноманітних наслідків від заміни головної сторінки сайту до несанкціонованого доступу до критичної інформації та відповідної шкоди. Розширення спектру атак змушує замислитися про захист від DDOS -атак, щоб забезпечити безперервність бізнес -процесів, фішингових атак, втрата пристроїв зі збереженими паролями, а також захистити рахунки працівників.

Аналіз кібербезпеки стає необхідною складовою стратегії захисту організацій у сучасному цифровому світі і включає кілька етапів, таких як збір інформації про системи, перевірка вразливості, оцінка ризику та соціальна інженерія. Ідентифікація вразливості дозволяє виявити слабкі місця та вразливості в інформаційних системах, які можуть використовуватися зловмисниками. Оцінка ризиків окреслює коло потенційних ризиків для бізнес -

процесів та операційної діяльності компанії. Підвищення ефективності захисту допомагає покращити заходи безпеки для більш ефективної боротьби з загрозами. Аналіз інцидентів дозволяє заздалегідь визначити потенційні загрози та вжити заходів для їх запобігання. Кожен з цих етапів відіграє ключову роль у виявленні проблем та надання рекомендацій щодо підвищення безпеки. Усі ці дії повинні виконуватися з великою швидкістю та з чітким розумінням учасниками їх ролі та функцій. Якісно побудовані процеси управління кібербезпекою дозволяють встановити взаємодію між спеціалізованими підрозділами та інтегрувати окремі процедури та елементи системи кібербезпеки в бізнес-процеси організації.

Дослідження показують, що половина випадків витоку даних відбувається через вину працівників. Тому навчання працівників є однією з головних умов для забезпечення інформаційної безпеки. Навіть у таких елементарних речах, як створення пароля. Як правило, малий бізнес не проводить аудит інформаційної безпеки, не інвестує значні засоби в безпеку і не має кіберінспекції. Проте, один із світових лідерів у галузі рішень щодо захисту корпоративних даних та кібербезпеки для бізнесу, японська компанія Trendmicro в своєму останньому щорічному звіті підкреслила, що організації повинні проводити регулярні аудиту безпеки, щоб переконатися, що їх інфраструктури не мають слабких місця. Експерти також рекомендують постійно оновлювати програмне забезпечення та робити резервні копії своїх даних. Сфера діяльності організації також впливає на формування пакету протидій кіберзловживань. Наприклад, у банківському секторі необхідно запобігати шахрайству при проведенні банківських операцій.

Підводячи підсумки, варто відмітити наступне. Цифрова трансформація це найвпливовіша тенденція бізнесу за останні 5 років і на майбутнє. Однак переважна більшість експертів з інформаційної безпеки впевнена, що проблеми безпеки це найбільші перешкоди для впровадження цифрової трансформації. Тому політика кібербезпеки сьогодні є життєве важливою для формування майбутнього будь -якого підприємства. Створення та підтримка безпечних цифрових середовищ стає все більш важливим. На сьогоднішній час інформаційна безпека спрямована на створення систем та процесів, які виключають можливість неприйнятних процесів для бізнесу. Проникнення кіберзагроз до внутрішньої архітектури не повинене мати жодних можливостей порушувати внутрішні бізнес-процеси та загрожувати функціонуванню, а іноді навіть існуванню організації.

Інформаційні джерела:

1. Internet-Sicherheit. URL: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

2. Український кіберфронт. Мінфін. Спецпроєкт. URL: https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny

3. Cayley Wetzig. 15 Alarming Cybersecurity Facts and Statistics. URL: https://thrivedx.com/resources/article/cyber-security-facts-statistics