УДК 004.056

В.В. Лакіза, канд. екон. наук, доц. *(НУЛП, Львів*)
Ю.В. Литвин, здоб. ОС «бакалавр» *(НУЛП, Львів)*

СУЧАСНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

У світі, де кількість цифрової інформації зростає експоненційно, питання безпеки та конфіденційності відіграють визначальну роль у сучасному бізнесі. Цифрові технології не тільки полегшують спілкування, зберігання та обробку даних, але й вносять безліч можливостей і ризиків для підприємств. У цьому контексті, питання якості захисту цифрової інформації та забезпечення конфіденційності визначає успішність будь-якої компанії. Сучасний бізнес стикається з унікальними викликами у цифровому середовищі. З одного боку, наявність величезних обсягів даних створює безмежні можливості для аналізу, інновацій та покращення взаємодії з клієнтами. З іншого боку, ця значна кількість інформації стає привабливою мішенню для кіберзлочинців, які шукають можливості використовувати дані для шахрайства, крадіжок особистостих даних чи інших злочинних цілей. У даній роботі ми детально розглянемо сучасні підходи до забезпечення безпеки та захисту конфіденційності в цифровому бізнесі.

Як ми згадали раніше, цифрове середовище, в якому ми живемо сьогодні, пропонує безмежні можливості, але разом з тим приносить і величезні загрози для безпеки та конфіденційності. Масштабність цих загроз стала безпрецедентною, охоплюючи всі аспекти нашого життя, від особистих даних до корпоративних інформаційних резервів. Давайте розглянемо масштабність загроз, що загрожують безпеці та конфіденційності в цифровому середовищі:

1) масштабність кібератак – сучасні кібератаки можуть бути величезного масштабу, атакуючи урядові установи, великі корпорації, фінансові установи та навіть критичну інфраструктуру. Атаки масового розмаху, такі як DDoS-атаки, можуть паралізувати навіть найбільш потужні мережі та інтернет-сервіси;

2) масштабність кібершпигунства – як держави, так і окремі злочинці можуть величезними масштабами здійснювати кібершпигунство, отримуючи доступ до конфіденційної інформації, що може включати в себе відомості про виборців, військові плани та комерційні таємниці;

3) масштабність фішингу та соціального інженірингу – кількість

фішингових атак та атак соціального інженірингу зростає експоненційно, злочинці використовують різноманітні методи, щоб отримати доступ до особистих даних користувачів, включаючи е-мейли, паролі та банківські деталі;

4) масштабність загроз в інтернеті речей (IoT) – більшістю пристроїв, які тепер підключені до мережі Internet (від холодильників до автомобілів), загрози в інтернеті речей стають все більш важливими, так як хакери можуть використовувати незахищені IoT-пристрої для здійснення атак та перехоплення інформації;

5) масштабність внутрішніх загроз – не всі загрози є зовнішніми, інсайдери, які мають доступ до важливої інформації, можуть використовувати свій статус для втілення атак, від яких важко захиститися.

За дослідженням Deloitte [1], 90% хакерських операцій зазнають саме критичні дані компаній та ті, що дають їм конкурентну перевагу. Це означає, що традиційні цілі конфіденційності, цілісності та відкритості бізнесу розширюються, а ключовими стають: приватність, безпека та надійність даних.

Візьмімо до уваги IoT, адже прогнозується, що він зросте до 38,7 млрд дол. США в 2023 р. порівняно з 34,2 млрд дол. США в 2022 р. Усе це корелює зі зростанням кількості підключених пристроїв, які потребують надійного захисту. Як результат, у наступному десятилітті мікропрограмне забезпечення безпеки стане більш важливим, аніж будь-коли, саме тому має місце така статистика безпеки пристроїв IoT. На рис. 1 наведено розподіл загроз і проблем безпеки в IoT у всьому світі станом на 2019 р. [2].

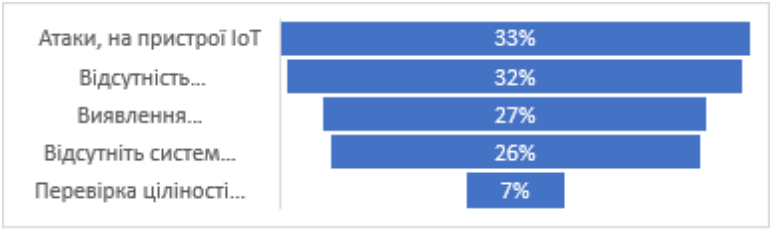

Рис. 1. Загрози та проблеми безпеки в IoT у всьому світі станом на 2019 р.

Як бачимо, статистика є досить приголомшливою, проте не ідеальною. Знаково, що ринок IoT не демонструє жодних ознак сповільнення, аналізуючи попередні роки. Очікується, що до 2025 р. розмір ринку збільшиться, що робить безпечним інвестування в безпеку IoT вже зараз. Отож, у сучасному цифровому ландшафті

компанії відчувають як колосальні можливості, так і величезні загрози, пов'язані з обробкою та зберіганням величезних обсягів даних. Щоби забезпечити безпеку та конфіденційність важливої інформації в онлайн-середовищі, компанії використовують низку передових технологій та стратегій. Нижче ми розглянемо глибокий аналіз найновіших інструментів та підходів, які використовуються для захисту важливих даних:

1) штучний інтелект (ШІ) та машинне навчання (МН) – відіграють важливу роль у виявленні аномальних зразків та попередженні кіберзагроз. Системи ШІ можуть аналізувати поведінку користувачів, виявляти несподівані відхилення від нормальної активності та автоматично виявляти потенційно шкідливі програми;

2) блокчейн-технології – використовуються для створення незмінних та безпечних баз даних. Це забезпечує відсутність можливості маніпуляції даними та забезпечує високий рівень конфіденційності. В бізнесі це може використовуватися для безпечного зберігання контрактів, фінансових транзакцій та особистих даних клієнтів;

3) аутентифікація та авторизація з багаторівневим захистом – сучасні системи аутентифікації включають багаторівневі методи, зокрема двофакторну аутентифікацію, біометричні дані та використання апаратних токенів, що забезпечує подвійний рівень захисту, що ускладнює несанкціонований доступ до системи;

4) аналіз великих даних (Big Data) та передбачення атак – використання аналітики великих даних для передбачення можливих кібератак стає все популярнішим, оскільки алгоритми аналізу великих даних можуть виявляти звичайність у величезних масивах даних та виявляти можливі загрози ще до їхнього виникнення;

5) навчання персоналу щодо кіберзагроз та проведення (соціальний інженіринг, фішинг) – можуть допомогти компаніям створити внутрішні бар'єри перед можливими атаками.

Отже, сучасне забезпечення безпеки та захисту конфіденційності в цифровому середовищі є надзвичайно важливим і складним завданням. Для ефективного забезпечення безпеки та захисту конфіденційності в цифровому середовищі необхідно використовувати комплексний підхід, який включає в себе не лише технологічні рішення, але й організаційні та освітні заходи.

Інформаційні джерела

1. Економічна правда. Цифрова безпека бізнесу: як захиститися. URL: https://www.epravda.com.ua/columns/2021/06/2/674556/

2. Intersog. IoT Security Statistics: 6 Facts. URL: https://intersog.com/blog/iot-security-statistics/