УДК: 004.056.5:004.67

Василенко В. Ю., канд. наук із соц. ком., старший викладач,
Буряк А. М., здобувачка вищої освіти,
Донецький національний університет імені Василя Стуса, м. Вінниця

БЕЗПЕКА ДАНИХ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ПРОБЛЕМИ ТА ВИКЛИКИ

Анотація. У роботі представлено визначення безпеки даних, виокремлено основні принципи, на яких ґрунтується безпека даних. Висвітлюються актуальність і основні принципи гарантування безпеки даних, зокрема, цілісність, доступність та конфіденційність інформації. Представлені виклики, що виникають у контексті швидкої цифрової трансформації та зростаючої кількості цифрових загроз.

Ключові слова: безпека даних, конфіденційність, кібератаки, епоха цифрової трансформації.

Вступ. У сучасному цифровому світі безпека даних стає надзвичайно актуальним питанням у контексті швидкої цифрової трансформації. Зростаюча кількість цифрових загроз та постійна зміна технологічного ландшафту створюють нові виклики для захисту інформації.

Актуальність. У цифрову епоху, коли обсяги даних постійно зростають, значення безпеки даних стає ще більш критичним. Недостатня захищеність даних може призвести до серйозних наслідків, як-от втрата конфіденційності, втрата довіри клієнтів і партнерів, фінансові втрати та репутаційні проблеми. Тому гарантування безпеки даних стає першочерговим завданням для будь-якої організації, яка бажає успішно функціонувати в цифровому світі, а також для усіх людей загалом, оскільки вони відчувають безпосередні наслідки порушення конфіденційності та втрати доступу до особистої інформації.

Основна частина. Безпека даних – це комплекс заходів та процедур, які забезпечують конфіденційність, цілісність і доступність інформації. Вона спрямована на захист даних від несанкціонованого доступу, крадіжки, пошкодження та втрати. Цей захист стосується будь-якої інформації, що зберігається у цифровому форматі, як-от особисті дані, фінансові записи та корпоративна документація [1].

Є кілька основних принципів, на яких ґрунтується безпека даних:

- Цілісність інформаційних даних – це властивість, яка гарантує, що дані залишаються незмінними у своєму первісному стані та структурі під час зберігання або передачі. Лише користувачі з відповідними правами доступу можуть вносити зміни, видаляти або коригувати дані. Цей принцип також застосовується до осіб з легальним доступом до інформації [2].

• Доступність: доступ інформаційних даних, що перебувають у вільному доступі, має бути забезпечений для легальних користувачів без зволікань та перешкод.

• Конфіденційність інформації ґрунтується на створенні обмеженого доступу до інформаційних ресурсів третіх осіб. Відомості можуть передаватися лише користувачам, які мають право взаємодіяти з цими системами, були ідентифіковані та отримали відповідне право доступу.

• •Авторизація ґрунтується на можливості надання користувачам прав доступу до інформації та ресурсів на основі їхніх ролей і обов'язків. Це забезпечує, що користувачі мають доступ лише до тих даних і ресурсів, які їм необхідні для виконання своїх завдань.

• Достовірність інформації вказує на те, що дані перебувають у власності довіреної особи або законного власника, який є первісним джерелом цих відомостей.

• Прозорість, яка реалізується за допомогою відкритості та зрозумілості політик і процесів безпеки даних для всіх зацікавлених сторін. Це допомагає створити довіру та впевненість у захищеності даних.

Епоха цифрової трансформації, окрім безлічі нових можливостей, несе з собою й нові виклики. Одним із найгостріших із них є безпека даних. Зростання обсягів цифрової інформації робить її об'єктом атак для кіберзлочинців, які постійно вдосконалюють свої методи атак. Основні проблеми безпеки даних в епоху цифрової трансформації виглядають так:

1. Кібератаки. За останні роки відбулося значне зростання кількості та складності кібератак. За даними Cybersecurity Ventures, до 2025 року щорічні збитки від кіберзлочинності можуть сягати 10,5 трильйонів доларів США [3].

Зростає популярність таких атак:

• Фішинг – шахрайські розсилки та вебсайти, що імітують легітимні ресурси для викрадення особистих даних.

• Викрадення даних – несанкціонований доступ до комп'ютерних систем та крадіжка даних.

• Атаки типу «відмова в обслуговуванні» – перевантаження серверів або мереж з метою блокування доступу до них.

2. Вразливість програмного забезпечення – не всі програмні продукти й системи захищені від вразливостей, оскільки розробники програмного забезпечення не завжди приділяють належну увагу кібербезпеці. Саме тому вразливості в програмному забезпеченні можуть бути використані кіберзлочинцями для проникнення в комп'ютерні системи та крадіжки даних.

3. Недостатня обізнаність. Багато людей не знають про кібербезпеку і не вживають заходів для захисту своїх даних. Саме тому необхідно проводити інформаційні кампанії з кібербезпеки для підвищення обізнаності людей про ризики та способи захисту даних. Важливо навчити людей використовувати надійні паролі, двофакторну автентифікацію та інші заходи захисту даних.

4. Відсутність єдиних стандартів. Відсутність єдиних стандартів у сфері кібербезпеки створює складнощі у захисті даних на міжнародному рівні. Різні країни та організації мають власні вимоги до кібербезпеки, що ускладнює процес захисту інформації, яка передається між ними. Для ефективного захисту даних та гарантування безпеки в цифровому середовищі важливо розробити та впровадити єдині глобальні стандарти кібербезпеки [3].

Виклики безпеки даних в епоху цифрової трансформації є складними та багатогранними. Для їх вирішення необхідний комплексний підхід, який включає в себе технологічні рішення, організаційні заходи та підвищення обізнаності персоналу.

Визначимо виклики безпеки даних в епоху цифрової трансформації:

Постійно мінливі загрози. Кіберзлочинці постійно вдосконалюють свої методи, тому важливо бути в курсі нових загроз та адаптувати заходи захисту даних. Важливо мати план реагування на інциденти кібербезпеки, щоб мінімізувати шкоду від кібератак. Зростає популярність хмарних сховищ, тому важливо використовувати надійні методи захисту даних у хмарному середовищі.

Конфіденційність даних. Зростає кількість законів про захист даних, тому важливо відповідати всім чинним законам, щоб захищати конфіденційність даних. Зростає кількість випадків викрадення особистих даних, тому важливо вживати заходів для їх захисту.

Безперервність роботи. Зростає кількість кібератак, які призводять до перебоїв в роботі. Важливо мати план відновлення після катаклізмів, щоб відновити роботу в найкоротші терміни після кібератаки.

Компетентність персоналу. Важливо мати кваліфікованих фахівців з кібербезпеки та навчати персонал основам кібербезпеки і правилам захисту даних.

У світі цифрової трансформації безпека даних стає ключовим питанням, яке вимагає уваги та дієвих заходів. Лише шляхом спільних зусиль уряду, бізнесу та громадськості можливо забезпечити захист наших даних та зберегти їх конфіденційність у цифровому світі.

Висновки. В епоху цифрової трансформації безпека даних стає надзвичайно важливою. Зростання обсягів цифрової інформації призводить до збільшення кібератак, які загрожують конфіденційності, цілісності та доступності даних. Щоб ефективно захищати інформацію, потрібно дотримуватися основних прин-

ципів безпеки даних, як-от цілісність, доступність, конфіденційність та достовірність. В епоху цифрової трансформації безпека даних стає критично важливою з огляду на постійне зростання кіберзагроз і важливості захисту інформації для успішного функціонування організацій та особистих даних користувачів. Нові виклики безпеки даних, як-от зростання кібератак, вразливість програмного забезпечення, недостатня обізнаність користувачів та відсутність єдиних стандартів, вимагають комплексного підходу до захисту інформації. Важливо бути в курсі нових загроз, мати плани реагування на інциденти кібербезпеки, дотримуватися законодавства про захист даних, мати плани відновлення після кібератак та навчати персонал правилам кібербезпеки.

Список використаних джерел

1. Захист даних. *Інтрасистемс.* URL: https://www.intrasystems.ua/solutions/informacyna-bezpeka/zahyst-danyh/ (дата звернення: 06.05.2024).

2. Інформаційна безпека: види загроз і методи їх усунення. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 06.05.2024).

3. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics. URL: https://cybersecurityventures.com/cybersecurity-almanac-2023/ (дата звернення: 06.05.2024).