ефективної реалізації цифрових ініціатив та знижують здатність підприємств адаптуватися до сучасних викликів.

Таким чином, цифрова трансформація для вітчизняних підприємств є не тільки способом підвищити ефективність і конкурентоспроможність, але й необхідністю для адаптації до умов сучасних викликів. Військова агресія, фінансова криза та інфраструктурні втрати створюють додаткові бар'єри для розвитку бізнесу в Україні. В таких умовах цифрові технології допомагають створити нові бізнес-моделі, інтегрувати дистанційне управління, мінімізувати втрати та забезпечити стійкість підприємств в умовах турбулентності. Використання ЗСП дозволяє ефективно планувати фінансові ресурси, адаптуватися до ризиків і забезпечувати стійкий розвиток навіть в умовах економічної невизначеності. Для України, яка перебуває в процесі економічного відновлення та інтеграції у світову економіку, цифрова трансформація є критично важливою, і її успіх значною мірою залежить від ефективності управління фінансовими ресурсами.

Інформаційні джерела:

1. Kaplan R.S., Norton D.P. The Balanced Scorecard: Translating Strategy into Action. Boston (Ma., USA): Harvard Business School Press, 1996. 320 p.

2. Kashchena N., Nesterenko I., Chmil H., Kovalevska N., Velieva V., Lytsenko O. Digitalization of Biocluster Management on Basis of Balanced Scorecard. *Journal of Information Technology Management*. 2023. Vol. 15. Is. 4. P. 80–96. DOI: https://doi.org/10.22059/jitm.2023.94711

3. Пан Л.В. Збалансована система показників (Balanced Scorecard – BSC) як інструмент ефективного управління стратегією організації. URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/8532/Pan_Zbalansovana_systema_pokaznykiv.pdf

4. Кащена Н. Б., Нестеренко І. В., Чміль Г.Л. Стратегічне управління біокластером на засадах ЗСП. *Інфраструктура ринку*. Випуск 71. 2023. С. 135–142. DOI: https://doi.org/10.32782/infrastruct71-24

5. Збалансована система показників (ЗСП, Balanced Scorecard, BSC). KPI MONITOR URL: http://kpi-monitor.com.ua/solutions/balanced-scorecard

КІБЕРБЕЗПЕКА В ХМАРНИХ ІНФРАСТРУКТУРАХ

Тіхонова В.А.
Державний біотехнологічний Університет

Для забезпечення безпечної роботи хмарного сховища (cloud storage, backup) потрібно врахувати що саму хмару можна розглядати як модель зберігання даних, де цифрова інформація зберігається у логічних пулах, а фізичне розміщення відбувається на декількох серверах, не обов'язково розташованих поряд. Адміністрування фізичної інфраструктури належить хостинг-провайдерам, які і відповідають за безпечне збереження даних, забезпечення доступу до них та надійність роботи серверів. Доступ до послуг хмарного сховища надається через вебсервісні інтерфейси (API).

Існують 3 види сховищ: публічна хмара - це модель зберігання даних, де ресурси належать стороннім компаніям(провайдерам), приватна хмара, яка призначена лише для однієї організації та гібридна хмара, яка дозволяє організаціям використовувати переваги обох моделей. Прикладами публічних хмар є Amazon Web Services (AWS), Microsoft Azure та Google Cloud. Ресурси приватної хмари призначені виключно для однієї організації. Такі хмари забезпечують більший рівень контролю та налаштування, але одночасно потребують більших початкових вкладень. Гібридна хмара поєднує в собі елементи публічної та приватної хмар, дозволяючи об'єднувати і спільно використовувати дані та їх додатки. Зазвичай такі віртуальні накопичувачі інтегруються з іншими IT-системами для забезпечення безперебійної взаємодії. Це інтегрування дозволяє отримують кращий контроль над даними, більш гнучке управління IT-інфраструктурою та підвищений рівень безпеки [1].

Зручність та вигідність використання хмарних сховищ пов'язане і з ризиками. В залежності від типів хмарних сховищ можна виділити такі загрози безпеки, як витік інформації, який може статися з широкого спектру причин, від недбалості співробітників до серйозних дій кіберз-злочинців. Наступним у рейтингу є злам інтерфейсу та API (інтерфейсів прикладного програмування). Хоч провайдери пропонують клієнтам зручні інтерфейси для керування своїми ресурсами, що дозволяє легко взаємодіяти з хмарними сервісами та налаштовувати їх під конкретні потреби, але це може створити серйозні загрози для безпеки, тому що API слугують точками доступу до хмарних сервісів, особливо, якщо ці API або інтерфейси мають вразливості.

Вразливим пунктом для загрози безпеки даних є вразливість систем у публічних (мультиарендних) середовищах. Щоб уникнути проблем спеціалісти рекомендують регулярно сканувати системи та оперативно реагувати на повідомлення про потенційні загрози. Недбале ставлення до паролів, відсутність шифрування або надання зайвих привілеїв користувачам може створити ризики та допомогти злочинцям легко обійти автентифікацію, що в свою чергу може привести до втрати даних або грошей. Використання спеціальної інженерії в сферах зламу до цього дня залишається однією з поширених загроз. Завдяки різноманітним програмам стає набагато легше отримати доступ до облікових записів клієнтів та їх персональної інформації. Фішинг, або виманювання в користувачів мережі цінних даних, досі є актуальною проблемою, яка пристосовується до прогресу. Хоча хмарні сховища мають багато переваг, питання кібербезпеки залишаються актуальними. Недооцінка ризиків та інші фактори можуть привести до втрат не тільки з боку компанії, але й її клієнтів [2].

Безпека залежить не лише від постачальника послуг, але й від дій самого користувача, та для кращого запобігання та забезпечення цілісності даних можна з допомогою запропонованих правил користування хмарними сервісами: перевірка та шифрування даних, використання захищеного інтернет-з'єднання, застосування спеціалізованих програм для моніторингу даних, захист інтернет-пристроїв і встановлення надійного пароля для адміністрування, постійна увага до фішинг-атак і своєчасне інформування техпідтримки та застосування

багатофакторної автентифікації. Для отримання додаткової інформації про безпеки роботи з хмарними сервісами оприлюднюється за допомогою розроблених додатків, у більшості випадків додається підтримка фахівців компанії. Так, SoftwareOne надає можливість он-лайн консультування .

Основним методом захисту є шифрування даних. Шифрування як криптографічний процес базується на алгоритмічному перетворенні даних з метою приховування інформації та отримання зашифрованого тексту. Воно є оборотним, тобто дозволяє відновити початкові дані. Здійснюється посимвольно і перетворює звичайний текст або повідомлення у форму, яку сторонні особи не можуть прочитати. Ефективність шифрування щодо захисту вмісту нажаль не розповсюджується на приховання метаданих (особа користувача, час чи місцезнаходження). Тому застосовування методів шифрування на всіх етапах обробки та передачі інформації для забезпечення конфіденційності дуже важлива задача [3]. Спосіб шифрування «хмари», тобто перетворення даних у захищений формат перед їх передачею, забезпечує конфіденційність та цілісність даних під час зберігання або передачі. З найрозповсюджених методів шифрування можна виділити AES (Advanced Encryption Standard).

Не менш важливою є функція керування ключами, яка визначає, хто може отримати доступ до даних. Усі ці заходи допомагають запобігти несанкціонованому доступу до конфіденційної інформації навіть у випадку зламу системи або витоку даних, що є дуже зручною функцією [4].

Інформаційні джерела:

1. Найкращі практики захисту хмарних сховищ - вартість рішення з кібербезпеки в Україні / IIT Distribution. URL: https://iitd.com.ua/news/najkrashhi-praktiki-zahistu-hmarnih-shovishh/ (Дата доступу 05.08.2024)

2. Блаженко І. Головні загрози хмарній безпеці та способи захисту. URL: https://galka.if.ua/holovni-zahrozy-khmarniy-bezpetsi-ta-sposoby-zakhystu/ (Дата доступу 27.10.2024)

3. Все, що потрібно знати про шифрування URL: https://safety.rsf.org/ukr/all-you-need-to-know-about-encryption/ (Дата доступу 20.08.2023)

4. What Is Cloud Encryption? Encrypted Cloud Storage Benefits. URL: https://www.zscaler.com/de/resources/security-terms-glossary/what-is-cloud-encryption

СИСТЕМАТИЗАЦІЯ НАПРЯМКІВ ЗАХИСТУ ІНФОРМАЦІЇ У БІЗНЕСІ

Чаговець В.В., канд. екон. наук, доц.
Державний біотехнологічний університет

Поточний рік характеризується суттєвим зростанням кількості кібератак в Україні. За даними Державної служби спеціального зв’язку та захисту інформації України у першому півріччі 2024 року українські об’єкти зазнали російських хакерських атак на 19% більше, ніж у другому півріччі 2023 року. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA у першому півріччі 2024 року зафіксовала 1739 кібератак, що на 276 більше, ніж