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

у попередньому другому півріччі 2023 року. Кількість атак з розповсюдженням шкідливого програмного забезпечення зросла на 40%. Проведені дослідження свідчать, що найсильніше вражаються сайти державних органів, які надають послуги громадянам та обробляють велику кількість даних, потім – фінансовий сектор, засоби масової інформації, IT-компанії та енергетика. Всі ці сектори складають групи ризику, які потребують особливої уваги. Аналітики вважають, що до 2025 року щорічні збитки бізнесу через кібератаки зростуть до 10,5 трлн доларів [1, 2].

Враховуючи це, можна стверджувати, що проблема удосконалення засобів захисту інформації та оцінки їх достатності наразі стає актуальною. Працюючи в напрямку її вирішення, Адміністрацією Державної служби спеціального зв'язку та захисту інформації України у липні цього року було запропоновано «Рекомендації з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації», які описують порядок дій щодо проведення оцінки реалізації базового та цільового профілів безпеки, на базі яких створювалась комплексна система захисту інформації [3].

Окрім розробки законодавчих, нормативних документів та рекомендацій для запобігання порушення та витоку інформації можна виділити також наступні дії, що сприяють захисту інформації саме у бізнесі [4]:

виокремлення всієї конфіденційної інформації, яка підлягає безпосередньо захисту, та її упорядкування згідно з політикою безпеки;

контролювання та оцінювання доступу до конфіденційної інформації та дій, викликаних ним;

безперервний моніторинг руху бізнес-інформації в режимі реального часу;

відстеження та аналіз незвичних поведінок програмних середовищ, що супроводжуються відкритим доступом до інформації, наприклад, під час копіювання даних, завантаженні підозрілих файлів;

обов’язкове оцінювання стану інформаційної безпеки бізнес-партнерів;

захист віддалених розосереджених точок доступу, взаємодіючих з мережею через кінцевих користувачів зі своїми ноутбуками, мобільними пристроями тощо;

шифрування даних, яке дозволяє отримати доступ до конфіденційної інформації та прочитати її тільки тим, хто має ключ дешифрування або знає пароль;

впровадження надійного програмного забезпечення для запобігання витоку інформації;

навчання співробітників своєї організації розпізнавати види кібератак, особливо через спробу отримати конфіденційну інформацію оманливим шляхом (фішингові атаки електронною поштою та атаки з використанням соціальної інженерії).

Елементи комплексної стратегії захисту інформації наведено на рисунку.

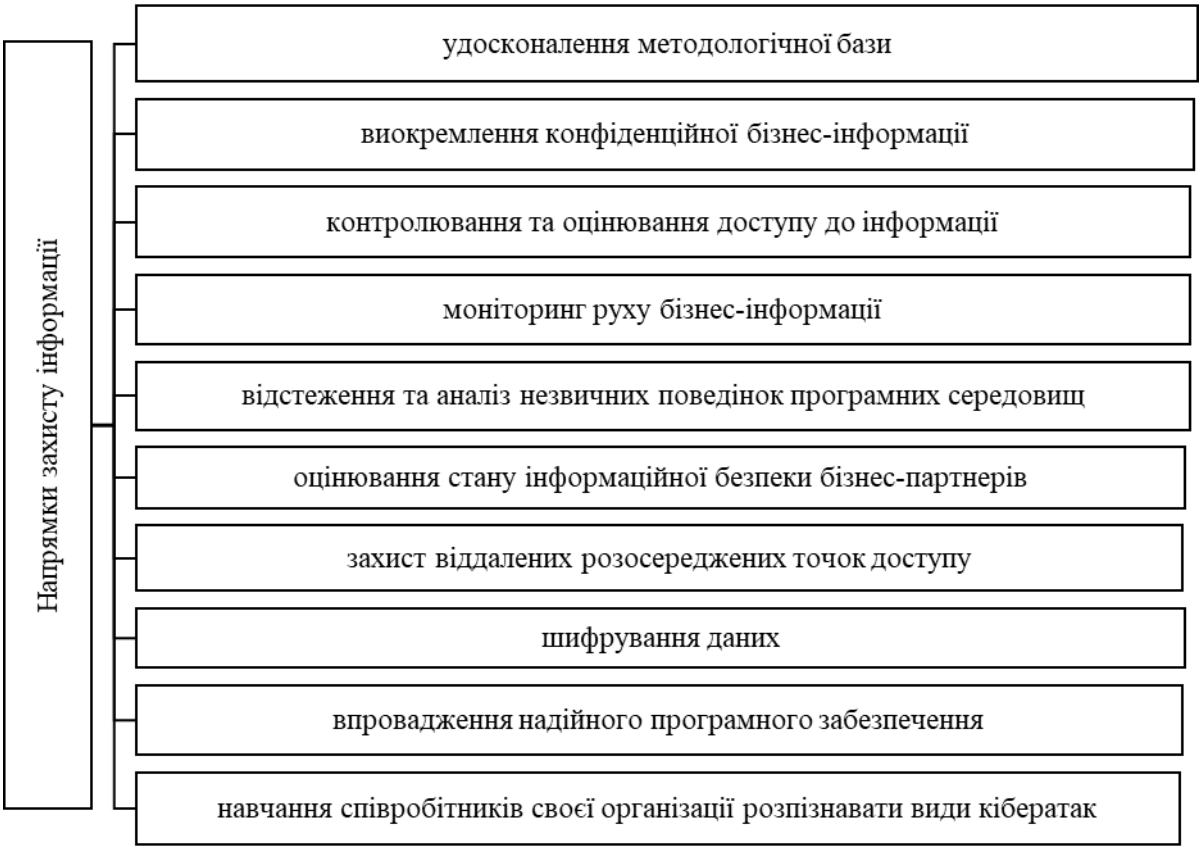

Рис. Напрямки захисту інформації у бізнесі

Діючи за такими напрямками, можна перешкодити кібер-злочинцям отримати конфіденційні дані шляхом їх витоку.

Інформаційні джерела:

1. Кількість кібератак в Україні [Електронний ресурс]. – URL: https://vsviti.com.ua/news/161954.

2. Кібератаки на український бізнес тривають: як захиститися [Електронний ресурс]. – URL: https://www.epravda.com.ua/cdn/cd1/2024/kiberataky_na_biznes.

3. Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/rada/show/v0354519-24#n10.

4. 6 порад як захистити бізнес від витоку даних [Електронний ресурс]. – URL: https:// https://gigatrans.ua/ua/news/6-sposobov-kak-zash-itit-biznes-ot-utechki-dannuh.