УДК 657.1

Л.А. Поливана, канд. екон. наук, доц. *(ДБТУ, Харків)*
О.С. Кравченко, здоб. ОС «магістр» *(ДБТУ, Харків)*
А.І. Давиденко, здоб. ОС «магістр» *(ДБТУ, Харків)*

КІБЕРБЕЗПЕКА ДАНИХ ЯК СКЛАДОВА СТРАТЕГІЧНОГО УПРАВЛІНСЬКОГО ОБЛІКУ

Дані сьогодні є основою для успішного управління, стратегічного планування та стратегічного управлінського обліку в бізнесі. Завдяки ефективному їх використанню керівництво може приймати обґрунтовані рішення, планувати бюджет, оцінювати ринкові тенденції та прогнозувати майбутні результати. Стратегічний управлінський облік дозволяє аналізувати продуктивність бізнес-процесів, ідентифікувати слабкі місця в ланцюжках постачання та управлінні ресурсами, що сприяє підвищенню ефективності роботи. Однак розвиток цифрових технологій і залежність від даних супроводжуються зростаючими кіберризиками, що може впливати на достовірність і доступність інформації для стратегічного управлінського обліку. Кібератаки на бізнес набувають все більшого масштабу та складності, ставлячи під загрозу конфіденційність і цілісність даних, які є основою стратегічного управлінського обліку. Підприємства стикаються з такими загрозами, як хакерські атаки, фішингові розсилки та шкідливе програмне забезпечення, які можуть призвести до значних фінансових збитків та втрати довіри клієнтів.

Як стверджує Bawaneh S.S., безпеку визначають як ступінь захисту від злочинної діяльності, небезпеки, пошкодження або втрати [1, с. 1175]. Питання кібербезпеки зачіпає інтереси не лише державних інституцій, а і приватного сектору та громадянського суспільства. При цьому низький рівень взаємодії органів державної влади, неурядових організацій та приватного сектору, а також відсутність системних нормативних документів, які описували б загрози Україні в кіберпросторі, є наслідком відсутності цілісного обговорення кібербезпекових питань.

Захист інформації на підприємствах має базуватись не на цінності цієї інформації для самого підприємства, а на її значенні для зловмисників, які можуть мати фінансовий інтерес. Інформація стратегічного управлінського обліку, включаючи комерційну таємницю, може бути привабливою для порушників. Очевидно, що питання кібербезпеки повинні бути пріоритетними для всіх підприємств, незалежно від їхнього розміру, складності чи виду діяльності, і мати чітке розуміння серед усіх співробітників.

Alani M.M. визначає загрозу як «потенційне посягання на безпеку, яке існує за наявності обставин, можливостей, дій або подій, що можуть її порушити і заподіяти шкоду» [2, с. 15–16]. Проаналізувавши типи кіберзагроз для бізнесу, ми дійшли висновків, що найбільш актуальними є: фішинг, зловмисне програмне забезпечення (ПЗ) та інсайдерські загрози.

Фішинг- фішинг є одним з найпоширеніших кіберзлочинів, який щороку завдає незліченних фінансових збитків. Його мета - викрасти конфіденційні дані та облікові дані, такі як логін і реквізити кредитної картки, і обманом змусити людей дозволити встановити шкідливе програмне забезпечення. Зловмисне ПЗ - зменшити шкоду від шкідливого програмного забезпечення можна різними способами. Зловмисники розробляють шкідливе програмне забезпечення, щоб отримати постійний доступ до пристрої в підприємстві. Потім ці пристрої використовуються для віддаленого керування, крадіжки даних, виявлення локальної мережі або розсилки спаму з зараженого пристрою. Інфекція є відносно поширеною і може серйозно вплинути на мережу, викрадаючи дані та паролі, сповільнюючи роботу системи або повністю видаляючи файли. Зараджене шкідливим програмним забезпеченням обладнання часто стає непридатним для використання, що завдає шкоди МСП, оскільки вони несуть витрати на заміну обладнання. Шкідливе програмне забезпечення не обмежується одним комп'ютером. Шкідливе програмне забезпечення може швидко поширюватися мережею організації.

Внутрішні загрози - багато людей в організації мають доступ до конфіденційної інформації. Незалежно від того, чи це нинішній або колишній працівник, партнер або підрядник, 25 відсотків витоків даних спричинені внутрішніми загрозами. Зловмисники можуть бути мотивовані жадібністю, або це можуть бути незадоволені працівники, які діють зі злості. У будь-якому випадку, поширення ними конфіденційної інформації може завдати значних фінансових збитків.

Також розглянемо людський фактор як один із видів вразливостей в кібербезпеці. Будь-яка інформаційна інфраструктура, яка навіть має найновіші програмно-технічні засоби захисту, все ще опрацьовується людиною, що дає злочинцям, дуже велику вразливість, яку вони можуть використовувати для своїх цілей через соціальну інженерію. Можна виділити 4 внутрішні загрози – пішаки, гуфи, співучасники, самотні вовки. Розглянемо деякі з них:

Пішак-це працівник, який часто ненавмисно здійснює зловмисні дії через фішинг або соціальну інженерію. Прикладами можуть бути працівники, які ненавмисно завантажують шкідливе програмне забезпечення на робочі станції, або користувачі, які видають себе за працівників служби підтримки і розкривають свої облікові дані третім особам.

Гуфи – дії не зі злим умислом, але навмисне заподіяння шкоди. Не підготовлені або надмірно самовпевнені користувачі вважають, що вони знаходяться поза межами політики безпеки, незалежно від їх компетенції. 95% організацій мають співробітників, які активно намагаються обійти засоби контролю безпеки, і майже 90% інсайдерських атак спричинені недосвідченими користувачами, які не усвідомлюють, якої шкоди можуть завдати їхні дії.

Захист інформації на підприємстві – це ключ до забезпечення безпеки та конфіденційності даних. Узагальнимо найбільш ефективні і поширені заходи захисту:

1. Централізоване зберігання даних (дані треба зберігати в одному місці, контролювати їх обробку та обмежувати доступ співробітників до конфіденційних матеріалів).

2. Голосові канали (використовуйте IP-телефонію, це може запобігти перехопленню розмов і забезпечити конфіденційність інформації, що передається по телефону).

3. Дані про клієнтів (треба використовувати додаток для зберігання даних клієнтів та автоматичного запису інформації про дзвінки, саме це забезпечує конфіденційність і надає адміністраторам доступ до персональних даних клієнтів.

Треба зауважити, що ризики безпеки впливають на бюджетування та фінансовий контроль в стратегічному управлінському обліку.

Після ідентифікації фінансових ризиків, з якими може зіткнутися підприємство в процесі своєї фінансової діяльності, визначення рівня ризику та факторів, що впливають на оцінку ризику, а також виявлення потенційних втрат, пов'язаних з ними, перед підприємство постає завдання розробити заходи з мінімізації фінансових ризиків. Тому фахівці з ризиків повинні визначити найбільш прийнятний спосіб нейтралізації фінансових ризиків і вибрати найбільш відповідний метод їх зниження.

Постійний розвиток стратегій захисту є необхідною умовою для забезпечення безпеки бізнесу в умовах зростаючих кіберзагроз. Сучасні кібератаки стають дедалі складнішими, оскільки зловмисники використовують нові технології та методи, щоб обійти традиційні системи захисту. Стратегія кібербезпеки, яка залишатиметься незмінною, швидко застаріє та стане вразливою, тому підприємствам необхідно регулярно оновлювати свої захисні інструменти та методи. Це включає впровадження нових технологій, таких як штучний інтелект для виявлення аномалій та поведінковий аналіз для передбачення потенційних загроз. Крім того, розвиток стратегій захисту дозволяє бізнесу оперативніше реагувати на нові ризики, включаючи загрози, пов’язані з віддаленою роботою та розширеним використанням хмарних технологій. Такі інструменти, як багатофакторна аутентифікація, сучасні системи шифрування і регулярний моніторинг мережі, сприяють тому, що підприємство залишається на крок попереду кіберзлочинців. Стратегічний управлінський облік також потребує надійного кіберзахисту, оскільки його ефективність залежить від точності й доступності ключових даних для прийняття управлінських рішень. Надійні засоби захисту забезпечують збереження цілісності фінансової інформації та аналітичних даних, на основі яких і розробляються стратегічні плани підприємства.

Інформаційні джерела

1. Bawaneh S.S. Information security for organizations and accounting information systems. A Jordan banking sector case. International Review of Management and Business Research. 2014. Vol. 3. Issue 2. P. 1174–1188.

2. Alani M.M. Elements of Cloud Computing Security. A Survey of Key Practicalities. Switzerland: Springer, 2016. 55p.