УДК 658.3: 007

Н.Ю. Захарова

ОСОБЛИВОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ СУЧАСНОГО ПІДПРИЄМСТВА

Мелітопольський державний педагогічний університет імені Богдана Хмельницького

Анотація: *У статті проаналізовано сучасні проблеми забезпечення інформаційної безпеки підприємств. Обґрунтовано важливість формування комплексного підходу до управління інформаційною безпекою в умовах підвищеного ризику та окреслено алгоритм його здійснення на рівні підприємства.*

Ключові слова: інформаційна безпека підприємства; конфіденційність інформації; дезінформація; управління інформаційною безпекою; захист інформації.

Abstract: *The article analyzes modern problems of ensuring information security of enterprises. The importance of forming a comprehensive approach to information security management in conditions of increased risk is substantiated, and an algorithm for its implementation at the enterprise level is outlined.*

Key words: enterprise information security; information confidentiality; disinformation; information security management; information protection.

Забезпечення інформаційної безпеки підприємств є невід'ємною складовою їх загальної системи управління, яка є важливою для досягнення як стратегічних, так і оперативних цілей.

Інформаційну безпеку підприємства можна охарактеризувати як комплекс заходів, процедур та технологій, спрямованих на захист інформації від несанкціонованого доступу, втрати, пошкодження в процесі її обміну, обробки та зберігання.

Важливість систематичної та цілеспрямованої роботи щодо забезпечення інформаційної безпеки посилилась в умовах війни, оскільки інформаційні ресурси можуть бути використані для здійснення кібератак, дезінформації та інших ворожих дій. Великі обсяги важливої конфіденційної інформації, також як і ресурси, стають об'єктом потенційних загроз. В умовах війни, коли загрози можуть бути надзвичайно реальними та різноманітними, захист інформації стає необхідністю для збереження стабільності та функціонування бізнесу.

Крім того, сучасні умови господарювання характеризуються великим обсягом інформації, яка переважно знаходиться в електронному вигляді, що створює додаткові загрози інформаційній безпеці підприємства. Серед іншого зловмисники можуть спробувати отримати несанкціонований доступ до системи або мережі підприємства для викрадення важливої інформації, введення шкідливих програм або розповсюдження шкідливого коду. Несанкціоноване розголошення конфіденційної інформації, такої як плани, клієнтська база даних або фінансові документи, може призвести до втрати конкурентної переваги або порушення довіри клієнтів.

Загалом серед науковців відсутній уніфікований підхід до класифікації загроз інформаційній безпеці підприємства. Нехай В.А., Нехай В.В. пропонують таку їх класифікацію:

– за проявом та наслідками – злочин; шахрайство; хуліганство;

– за типом – програмне; апаратне, інше;

– за метою – оперативні, тактичні, стратегічні;

– за характером виникнення – навмисні, ненавмисні;

– за інформаційними технологіями – об’єкт загроз, методи підготовки загроз, інструментарій загроз, середовище загроз;

– за місцем виникнення – інсайдерські, зовнішні;

– за об’єктом впливу – системні, локальні;

– за причиною виникнення – збої в обладнанні, збої в роботі програмного забезпечення, недосконала архівація даних, несанкціонований доступ [1].

Відзначимо, що за даними, наведеними у Звіті про глобальні ризики 2024 року, 53% опитаних експертів вважають дезінформацію та неправдиву інформацію основними ризиками, поставивши їх на перше місце. За їх оцінкою, дезінформація становитиме найбільший ризик протягом найближчих двох років [2].

Це потребує відповідної реакції збоку суб'єктів господарювання. Вони повинні бути готові не лише реагувати на випадки дезінформації, а й активно працювати над запобіганням її поширенню. Велика увага повинна приділятися аналізу інформації, вдосконаленню системи внутрішньої комунікації, навчанню персоналу та розробці ефективних стратегій протидії дезінформації.

Таким чином, менеджери підприємств повинні акцентувати увагу на формуванні комплексного підходу до управління інформаційною безпекою, що сприятиме забезпеченню захисту інформаційних ресурсів, конфіденційності (обмежений доступ), цілісності (збереження даних) та доступності інформації (обмежений доступ лише для авторизованих).

Управління інформаційною безпекою на підприємстві може здійснюватися на декількох рівнях залежно від потреб, розміру і складності інформаційних потоків та інших чинників. Виділимо такі з них:

- стратегічний рівень передбачає визначення стратегічних цілей, виділення ресурсів і прийняття стратегічних рішень щодо захисту інформації на підприємстві на основі дотримання вимог законодавства та стандартів безпеки;

- тактичний рівень характеризується формуванням конкретних планів дій для виконання стратегічних цілей в сфері інформаційної безпеки й може включати розробку політики, стандартів і процедур безпеки, здійснення аналізу ризиків, планування проєктів з імплементації заходів інформаційної безпеки;

- оперативний рівень передбачає безпосереднє виконання заходів інформаційної безпеки, в тому числі конфігурування технічних засобів захисту, моніторинг систем безпеки, реагування на інциденти та проведення навчання для персоналу.

Ефективність захисту інформації безпосередньо обумовлена взаємодією та координацією зусиль на всіх рівнях управління інформаційною безпекою підприємства.

Характеризуючи алгоритм управління інформаційною безпекою підприємства, можна виокремити наступні етапи:

1. Аналіз потенційних загроз і визначення вразливих місць у системі інформаційної безпеки суб'єкта господарювання з метою ідентифікації всіх можливих джерел ризиків, включаючи технічні, організаційні та людський фактор.

2. Розробка і впровадження політики інформаційної безпеки, яка охоплює різні аспекти захисту даних, включаючи їх збереження, передачу, обробку та доступ у відповідності до поточних стандартів та регулятивних вимог.

3. Забезпечення надійного технічного захисту інформаційних систем, використовуючи сучасні методи шифрування, захист від вірусів, резервне копіювання даних тощо.

4. Проведення регулярного навчання персоналу з питань інформаційної безпеки задля формування вміння реагувати на потенційні загрози, усвідомлення та відповідального ставлення до захисту інформації серед всього персоналу.

5. Здійснення постійного моніторингу інформаційної безпеки підприємства для виявлення потенційних загроз і вчасного реагування на них.

Підвищення заходів безпеки та посилення контролю над доступом до інформації, вдосконалення процедур резервного копіювання та відновлення даних, а також постійне вдосконалення систем захисту від кіберзагроз стають важливими стратегічними завданнями для підприємств в умовах підвищених ризиків. Тільки на основі виконання цих завдань можна забезпечити надійний захист важливої інформації, що сприятиме підвищенню конкурентоспроможності та розвитку бізнесу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf

2. The Global Risks Report 2024. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf?fbclid=IwAR1Nqzbgjn1ORiZIBd_28OM-wGDRj80onykO9x5g7X0ME3UQFl6bGLCqaFE

Захарова Наталя Юріївна, кандидат економічних наук, доцент, завідувачка кафедри управління та адміністрування, Мелітопольський державний педагогічний університет імені Богдана Хмельницького, Запоріжжя, e-mail: nata-zakharova@ukr.net.

Zakharova Natalia U. Candidate of Economic Sciences, Associate Professor, Head of the Department of Management and Administration, Bogdan Khmelnitsky Melitopol State Pedagogical University, Zaporizhzhia, e-mail: nata-zakharova@ukr.net.