ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ВИКЛИКИ ТА СТРАТЕГІЇ

Жорняк А.С., здоб. ОС «бакалавр»
Харківський національний університет радіоелектроніки
Науковий керівник – канд. екон. наук, доц. **Н.О. Бірченко**
Державний біотехнологічний університет

У сучасному цифровому світі, де дані є одним з найцінніших активів підприємств, інформаційна безпека стає життєво важливою складовою діяльності будь-якого підприємства. Вона стала критично важливою для сучасних підприємств у зв'язку зі зростанням кількості кіберзагроз та потенційних ризиків порушення конфіденційності, цілісності та доступності даних. Поглиблене розуміння сутності та ролі інформаційної безпеки на рівні підприємства дозволить ефективно впроваджувати стратегії та заходи для захисту даних та забезпечення стійкості бізнес-процесів.

Інформаційна безпека підприємства – це комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також на захист від кіберзагроз, внутрішніх та зовнішніх атак.

Потапюк Л.М. та Потапюк І.П. зазначають, що «інформація є предметом і результатом праці управлінського персоналу, сукупністю даних про стан управляючої та керованої підсистем і зовнішнього середовища. Чим повніше і достовірніше інформація, чим оперативніше і якісніше її опрацьовано, тим вище обґрунтованість і потенційна ефективність управлінських рішень і дій» [1].

Захисту підлягає будь-яка інформація, що має цінність для підприємства. У першу чергу, це стосується інформації, що становить комерційну таємницю. Вона може включати в себе унікальні технології, процеси виробництва, або інші секрети, які дозволяють підприємству відзначитися на ринку та здобути конкурентну перевагу. Деякі аспекти комерційної таємниці можуть підлягати захисту за законодавством про інтелектуальну власність, що дозволяє підприємству контролювати їхнє використання та отримувати користь від їхнього володіння. Комерційна таємниця також може включати в себе дані про клієнтів та їхні угоди, що допомагає підприємствам підтримувати та розширювати свою клієнтську базу тощо.

Забезпечення інформаційної безпеки підприємства супроводжується різноманітними викликами, а саме:

1) Кіберзагрози та кібератаки: підприємства стикаються з низкою кіберзагроз, включаючи віруси, троянські програми, фішингові атаки та інші види зловмисного програмного забезпечення. Кібератаки можуть призвести до втрати даних, порушення діяльності підприємства та збитків;

2) Недбалість персоналу: людський фактор може бути слабким ланцюгом у системі інформаційної безпеки. Недостатня інформаційна грамотність персоналу, втрата або крадіжка пристроїв, неправильне використання паролів – усе це може стати причиною порушення безпеки даних;

3) Загрози зсередини: інсайдерська загроза від співробітників або колишніх співробітників також є серйозним викликом для інформаційної безпеки. Необхідно відстежувати доступ до конфіденційної інформації та реагувати на будь-які підозрілі дії.

Для забезпечення інформаційної безпеки підприємства необхідно розробити та дотримуватися наступних стратегій:

1) Розробка політики інформаційної безпеки: підприємства повинні розробити і впровадити політику інформаційної безпеки, яка включає в себе правила щодо захисту даних, доступу до них, а також процедури реагування на інциденти.

2) Постійне навчання та освіта персоналу: підприємства повинні інвестувати в навчання свого персоналу з питань інформаційної безпеки, щоб забезпечити їхню свідомість про потенційні загрози та навички захисту.

3) Використання технологій безпеки: підприємства повинні використовувати сучасні технології безпеки, такі як файрволи, антивірусне програмне забезпечення, системи виявлення вторгнень та шифрування даних.

4) Аудит та моніторинг безпеки: постійний аудит та моніторинг системи інформаційної безпеки допомагають вчасно виявляти потенційні загрози та вразливості.

Отже, забезпечення інформаційної безпеки підприємства є складним завданням, проте воно є критично важливим для збереження конкурентоспроможності та довіри клієнтів. Шлях до успіху полягає в поєднанні правильної стратегії, технологій та свідомого відношення персоналу до питань безпеки.

Інформаційні джерела

1. Потапюк Л.М., Потапюк І.П. Інформаційна безпека як складова економічної безпеки підприємства. URL: https://core.ac.uk/download/pdf/214871049.pdf