Лекція 8

ІНФОРМАЦІЙНА БЕЗПЕКА ФІРМИ ТА ЗОВНІШНЕ ПРЕДСТАВНИЦТВО ФІРМИ

Основні поняття: інформаційна безпека, конфіденційність, криптозахист, ресурси, сайт, потік, IT – продукція, месенджери, маркетплейс, інформаційна мережа.

План

1. Загальні питання інформаційної безпеки
2. Потоки інформації та зовнішній імідж фірми
3. Використання месенджерів
4. IT – продукція та специфіка ринку.

1. Загальні питання інформаційної безпеки

Інформаційна безпека – це стан захищеності інформаційних ресурсів підприємства від несанкціонованого доступу, модифікації, знищення чи розголошення.

Її мета – забезпечення конфіденційності, цілісності та доступності даних, що є базовими принципами міжнародного стандарту CIA-triad (Confidentiality, Integrity, Availability).

Конфіденційність – доступ до інформації мають лише уповноважені особи.

Цілісність – інформація зберігається без змін і спотворень.

Доступність – дані доступні для користувачів тоді, коли вони потрібні.

2. Загрози інформаційній безпеці підприємства

Технічні загрози, а саме - збої обладнання, аварії, знищення носіїв даних.

Програмні загрози, а саме - комп'ютерні віруси, шкідливе ПЗ, хакерські атаки.

Людський фактор, тобто витік інформації через недбалість чи зловмисні дії працівників.

Організаційні загрози, тобто відсутність політики безпеки, неналежний контроль доступу.

3. Засоби забезпечення інформаційної безпеки.

Технічні проблеми, тобто - антивірусні системи, міжмережеві екрани (firewall), системи резервного копіювання.

Організаційні, а саме - розробка політики безпеки, обмеження прав доступу, аудит.

Правові, тобто дотримання законів про комерційну таємницю, захист персональних даних.

Кадрові, тобто навчання персоналу правилам інформаційної безпеки, підписання NDA.

4. Зовнішня інформація у діяльності фірми.

Зовнішня інформація – це дані, які підприємство отримує з навколишнього середовища для ухвалення управлінських рішень.

До неї належать наступні фактори:

- ринкова інформація, тобто дані про конкурентів, ціни, попит і пропозицію;
- державна інформація, тобто законодавчі та нормативні акти, податкова й митна політика;
- фінансово-економічна інформація, тобто курси валют, процентні ставки, умови кредитування;
- соціально-політична інформація, а саме, політична стабільність, міжнародні відносини, соціальні тренди;

Науково-технічна інформація, тобто інновації, патенти, нові технології у галузі.

5. Значення зовнішньої інформації.

Зовнішня інформація є важливим фактором стратегічного менеджменту фірми:

- допомагає адаптуватися до змін середовища;
- забезпечує конкурентні переваги;
- дозволяє мінімізувати ризики;
- підтримує процес стратегічного планування.

6. Взаємозв'язок інформаційної безпеки та зовнішньої інформації.

- надмірна відкритість до зовнішньої інформації підвищує ризики кіберзагроз;
- необхідно поєднувати збір і використання зовнішньої інформації з надійними заходами інформаційної безпеки;
- ефективна система управління інформаційними потоками створює баланс між доступністю та захищеністю даних.

Інформаційна безпека та робота із зовнішньою інформацією – ключові складові сучасного управління підприємством. Без належного захисту даних неможливо зберегти конкурентоспроможність, а без використання зовнішніх джерел інформації – неможливо ухвалювати стратегічні рішення в умовах динамічного ринку.

2. Поняття про криптозахист

1. Визначення.

Криптозахист інформації – це сукупність методів і засобів, що забезпечують захист даних шляхом їх перетворення у вигляд, недоступний для розуміння сторонніми особами.

Основою криптозахисту є криптографія – наука про методи шифрування та розшифрування інформації.

2. Основні цілі криптозахисту:

- конфіденційність – доступ до даних мають тільки уповноважені користувачі;

- цілісність – дані не можуть бути змінені або спотворені непомітно;

- автентифікація – перевірка справжності користувача або джерела інформації;

- невідмовність – неможливість відмовитися від власних дій (наприклад, у фінансових транзакціях).

3. Основні методи криптозахисту.

1. Шифрування, яке буває наступних видів.

- симетричне (один і той же ключ для шифрування й розшифрування). Приклад: AES, DES.

- асиметричне (пара ключів – відкритий та закритий). Приклад: RSA, ECC.

2. Хешування – одностороннє перетворення даних у фіксований код (хеш). Приклад: SHA-256, MD5. Використовується для перевірки цілісності.

3. Електронний підпис – цифровий аналог власноручного підпису, що підтверджує автентичність і цілісність повідомлення.

4. Керування ключами – організація безпечного створення, зберігання, розподілу й відкликання криптографічних ключів.

4. Приклади застосування:

- захист електронної пошти (PGP, S/MIME);

- банківські системи та онлайн-платежі (SSL/TLS);

- електронні документи (цифровий підпис, ЕЦП/КЕП);

- сховище даних та хмарні сервіси;

- M messengers (Signal, WhatsApp – наскрізне шифрування).

5. Виклики криптозахисту:

- кіберзлочинність, а саме - постійні спроби зламати алгоритми;

- квантові обчислення, тобто потенційна загроза для сучасних криптографічних систем;

- людський фактор, тобто слабкі паролі, недбалість у збереженні ключів.

Криптозахист – фундаментальний елемент інформаційної безпеки. Без нього неможливі сучасні фінансові операції, електронна комунікація та захист персональних даних. Це «замок і ключ» цифрової епохи.