Боднар Мирослав,
здобувач вищої освіти ОС «Бакалавр»
спеціальності «Транспортні технології»
Науковий керівник: **Мушеник І.М.,**
канд. екон. наук, доцент кафедри математичних дисциплін,
інформатики і моделювання
Подільський державний аграрно-технічний університет
м. Кам'янець-Подільський

ІНФОРМАЦІЙНА БЕЗПЕКА ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасні реалії функціонування і ведення бізнесу в епоху інформаційного суспільства приносять нові загрози для економічної безпеки. Міждисциплінарні знання в галузі безпекознавства, права, економіки, менеджменту та інформатики дають можливість вивчити ці ризики і прийняти рішення, які зводять до мінімуму загрози для інформаційної безпеки. В даний час субдисципліна економічної безпеки – інформаційна безпека, відіграє важливу роль у визначенні економікоправових явищ, в тому числі дослідження ризиків, що впливають на сферу безпеки в широкому розумінні. Інформація, що міститься в строгому сенсі цього слова є набагато важливішою і більш цінною, ніж матеріальні ресурси Проте глобальна комп'ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави [3, с. 90].

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій [2].

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;
- відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо [2, с.44].

Захист інформації – галузь науки і техніки, яка динамічно розвивається, пропонує ринку широкий спектр засобів для захисту даних. Проте жоден з них окремо взятий не може гарантувати адекватну безпеку інформаційної системи. Необхідною умовою ефективного захисту є проведення комплексу взаємодоповнюючих заходів.

Комплексне забезпечення інформаційної безпеки автоматизованих систем – це сукупність криптографічних, програмно-апаратних, технічних, правових, організаційних методів і засобів забезпечення захисту інформації при її обробці, зберіганні та передачі з використанням сучасних комп'ютерних технологій [4, с. 433].

Досвід показує, що практично кожне підприємство має антивірусні засоби захисту, системи ідентифікації користувачів, системи управління доступом до інформаційної системи тощо. Тобто потенціал засобів захисту є, але він не реалізується фірмами повністю. Більше того, володіючи складними апаратними засобами захисту інформації, більшість підприємств навіть наполовину не використовують їх потенціал. Переважна більшість вимог стандартів інформаційної безпеки можуть бути реалізовані наявними у фірм засобами захисту.

Сучасне підприємство повинно вміти належним чином розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту

конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію) [1, с. 207].

Сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності.

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов’язані з інформаційними, але і відповідні заходи адміністративного та технічного характеру [3, с. 89].

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами [2, с. 45].

За допомогою вибору відповідних заходів безпеки забезпечується більш ефективне досягнення бізнес-цілей, захищаючи таким чином цілі компанії, її місію, матеріальні і фінансові ресурси, репутацію, правове положення та співробітників. Тому дуже важливо дослідити ризики, пов'язані з безпекою інформації та способи боротьби з такого роду загрозами. У зв’язку із дуже динамічними змінами, які відбуваються в зв'язку з розвитком інформаційних технологій, з'являються нові раніше невідомі загрози. Особливим полем для маневру є розвиток інформаційних технологій, що дозволяє придбати інформацію віддалено, без фізичної присутності в місці зберігання. Це є виклик не тільки для підприємців, які дбають про свої власні інтереси, але й для держави, яка повинна побудувати ефективну правову систему для захисту від шпигунських дій.

Список використаних джерел

1. Близнюк І.М. Інформаційна безпека України та заходи її забезпечення. *Науковий вісник Національної академії внутрішніх справ України.* 2008. № 5. С. 206-214.

2. Мушеник І.М. Моделі оптимізації господарської діяльності підприємств аграрного сектору. Моделювання регіональної економіки. Плай, 2013. №1 (21). С. 39-46.

3. Цимбалюк В.С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації). *Підприємництво, господарство і право.* 2007. № 3. С. 88–91.

4. Ясінецька І.А., Мушеник І.М. Механізми вдосконалення структури інформаційної системи сільськогосподарського землекористування. Science and Practice: Implementation to Modern Society. Proceedings of the 4 th International Scientific and Practical Conference (May 6-8, 2020). Manchester, Great Britain: Peal Press Ltd., 2020. p.430-435.