КІБЕРБЕЗПЕКА В УМОВАХ ГЛОБАЛІЗАЦІЇ ЕКОНОМІЧНИХ ПРОЦЕСІВ В ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ

Вальковець А. С.
викладач кафедри економіки та управління бізнесом
Рівненський державний гуманітарний університет

Вступ. / Introductions. Економіка в наш час все більше переходить в цифровий режим, особливо це стало помітно з оголошеною агресією Російської Федерації проти України, коли фізичне існування бізнесу на певній території стало фактично неможливим. Підприємці все більше почали шукати шляхи для трансформації свого виробничого, торгівельного потенціалу в більш гнучке та безпечне середовище. З різким розвитком інформаційних технологій та цифрової економіки постійно відбуваються різноманітні комунікації – з клієнтами, між партнерами через мережі. Тому виникають ризики розголошення комерційної інформації. При цьому деяка інформація є надзвичайно цінною та важливою, оскільки завдяки володінню нею конкретний бізнес має конкурентні переваги та заробляє гроші. Якщо така інформація опиняється в руках сторонніх осіб, то бізнес може опинитися під загрозою. Саме тому захист комерційної інформації є однією з важливих проблем ведення бізнесу.

Мета роботи. / Aim. Метою роботи є дослідження можливостей та потенціалу захисту важливої комерційної інформації від зовнішнього негативного впливу. Кібербезпека стала важливою частиною ведення бізнесу, оскільки від конфіденційності даних залежить і результат роботи того чи іншого підприємства.

Матеріали та методи./Materials and methods. Теоретичні дослідження, пов’язані з питанням захисту конфіденційної інформації, зокрема й комерційної таємниці, проводились наступними фахівцями у цій сфері: А. Маращуком, І. Давидовим, О. Давидюком, В. Дозорцевим, Н. Мироненком, Ю. Назаренком, О. Сергєєвою, О. Підпригорою та іншими.

Як показують опубліковані дані опитування Deloitte провідних світових фінансових компаній, 49% респондентів зафіксували внутрішні інциденти (пов’язані з ІТ-безпекою) за останні 12 місяців. У 31% випадків інсайдери занесли віруси зсередини корпоративної мережі, а з інсайдерськими шахрайством зіткнулися 28% респондентів. 18% організацій стали жертвами витоку приватної інформації клієнтів, а 10% виявили, що інсайдери скомпрометували корпоративну мережу. Організації, які постраждали від внутрішньої витоку, зізнаються, що велика частка загроз є наслідком недолугості або недбалості службовців (людський фактор — 42%, операційні помилки — 37%), а не злого умислу інсайдерів. Правда, 28% стали жертвою ретельно продуманого і професійного шахрайства, а 18% компаній позбулися приватної інформації клієнтів саме через те, що інсайдери цілеспрямовано допустили витік. Щоб не допустити такі інциденти в майбутньому, 80% опитаних фінансових компаній здійснюють моніторинг дій службовців, а 75% вводять різні обмежувальні заходи на використання тих чи інших технологій або пристроїв [1].

За даними дослідницького центру компанії InfoWatch, що спеціалізується на виробництві і продажі систем DLP, за 2012 рік — 42% витоків інформації відбувається ненавмисно по неакуратності або забудькуватості користувачів, внаслідок порушень політик корпоративної безпеки організацій. Більше 40% інформації йде по Інтернет-каналах, і 30% — по мобільних пристроїв. Більше 65% інформації витікає з комерційних підприємств, близько 20% з освітніх і 24% з державних підприємств [2].

Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць [3].

Результати та обговорення./Results and discussion. Захист інформації неможливо регламентувати через різноманітність існуючих інформаційних систем та видів інформації, що обробляється. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства (організації), обсягом конфіденційної інформації та її значущістю. Можна назвати тільки загальні правила:

- створення та експлуатація системи захисту інформації є складною і відповідальною справою, яку мають робити професіонали;
- не слід намагатись організувати абсолютно надійний захист - такого просто не існує. Система захисту має бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації вимірюється не витратами на її організацію, а її здатністю адекватно реагувати на всі загрози;
- заходи із захисту інформації повинні мати комплексний характер, об'єднувати різні засоби;
- систему захисту слід будувати, виходячи з того, що основну загрозу становлять співробітники підприємства (організації, установи) [4].

Сьогодні захист інформації стає однією з галузей, для якої розробляються

спеціальні інструментальні засоби, призначені для генерації тестів, імітації загроз, аналізу текстів програм. Створюються експертні системи для формування вимог до безпеки ІТ та оцінки рівня їх виконання. Однак до захисту інформації повинні залучатись і звичайні користувачі, оскільки цю проблему неможливо вирішити тільки технічними і програмними засобами, людський фактор відіграє важливу роль у забезпеченні конфіденційності.

Висновки./Conclusions. Проблема захисту комерційної інформації набуває особливого значення у сфері економіки, що характеризується підвищеними вимогами до прихованості та оперативності обробки інформації. Захист інформації є життєвою необхідністю функціонування будь-якої системи,

що не можу не зацікавити керівників, які розуміють цінність комерційної таємниці підприємств. Основною програмою захисту комерційної інформації є багаторівнева політика безпеки, яка відображає підхід певного підприємства до захисту своїх інформаційних активів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Деньга С. М. Захист інформації в комп`ютерних інформаційних системах бухгалтерського обліку [Текст] / С. М. Деньга, Ю. О. Верига // Бухгалтерський облік і аудит. – 2004. – № 5. – С. 59-65.

2. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

3. Капіца Ю. Захист комерційної таємниці в Європейських країнах та Україні [текст] / Ю. Капіца // Підприємство, господарство і право. – 2006. № 11. С. 16– 20.

4. Клименко В. Внутрішні загрози інформаційній безпеці організації / В. Клименко // Вісник НБУ. – 2008. – № 5. – С. 62-63.

5. Нікіфоров Г. К. Підприємництво та правовий захист комерційної таємниці [текст] : навч.-практ. посіб. для вищих навч. закл. / Г. К. Нікіфоров, С. С. Нікіфоров. – К. : Олан, 2001. – 208 с.