НАЦІОНАЛЬНА БЕЗПЕКА

Бурлій А.Ю.
студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

КОМЕРЦІЙНА ТАЄМНИЦЯ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В умовах сучасності перед підприємствами гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну таємницю.

Сьогодні в Україні та провідних країнах світу, в умовах посилення суперництва успіх підприємництва, гарантія отримання прибутку все більш залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і конкретну технологію. Це можуть бути далекосяжні технічні рішення, методики робіт, підсумки маркетингових досліджень тощо, які спрямовані на досягнення підприємницького успіху, саме через таку багатомінітність слушним є питання про критерії вибору інформації, яку слід захищати.

Відповідь на це питання дає визначення поняття «комерційна таємниця», яке викладено ст. 505 Цивільного кодексу України: «Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію» [1].

Складовою частиною захисту інформаційної безпеки є забезпечення комерційної таємниці, що в Україні та багатьох промислово розвинутих країнах включає здійснення комплексу заходів, спрямованих на ускладнення витоку інформації, яка захищається.

До такого комплексу належить в першу чергу розробка й прийняття законодавчих актів в інформаційній сфері, що стосуються комерційних секретів (таємниць) підприємств.

При цьому «комерційні секрети» як узагальнююче поняття включає й інші подібні визначення: «ділові секрети», «виробничі секрети», «торгівельні секрети», «комерційна таємниця» тощо, які використовуються в різних країнах. Зокрема, в США під поняттям «ділові секрети» розуміють – різноманітні види технічної інформації (формули, обладнання, методи, техніку і способи виробництва); в Японії – способи виробництва, продажу або іншу інформацію

про технологію та бізнес тощо. Поняття «виробничі секрети» визначено в ФРН – креслення, рецептуру та інші письмові відомості, сукупність виробничого досвіду або інший факт, пов'язаний з виробництвом, в тому числі знання і досвід спеціалістів виробників, комерційні знання та досвід [3]. В Україні під поняттям «комерційна таємниця» можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [1].

Згідно Постанови КМУ № 611 перелік відомостей, які не можуть бути віднесені до комерційної таємниці [2]:

– установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;

– інформація за всіма встановленими формами державної звітності;

– дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

– відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

– відомості, що відповідно до чинного законодавства підлягають оголошенню.

Крім розробки й прийняття законодавчих актів в інформаційній сфері, до заходів охорони комерційної таємниці відноситься:

– створення інструкцій, які регламентують режим використання інформації на конкретних підприємствах та забезпечення реалізації їх вимог;

– здійснення спеціальної перевірки осіб на допуск до роботи із документами, матеріалами й виробами, що містять інформацію з обмеженим доступом;

– використання організаційних, технічних та інших засобів конфіденційної інформації;

– впровадження фізичної охорони об'єктів, на яких безпосередньо зберігаються матеріали;

– здійснення контролю за дотриманням встановленого режиму охорони комерційної таємниці;

– проведення профілактичних заходів тощо.

Для кращого забезпечення захисту комерційної таємниці в інформаційній сфері, слід удосконалюватись. Співпрацювати та переймати досвід провідних країн світу, щоб стати контурентно спроможною країною. Вдосконалювати

законодавство та створювати більш ефективні, доцільні та ненадмірні метоти та засоби захисту таємниці. Також, комерційна таємниця є цілісною і повинно бути недопущення потрапляння секретної інформації до конкурентів чи третіх осіб, що може негативно вплинути на діяльність підприємства.

Список використаних джерел:

1. Цивільний кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України (ВВР). – 2003. – № № 40-44, ст. 356 [Електронний ресурс]. – Режим доступу до тексту: http://zakon3.rada.gov.ua/laws/main/435-15

2. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 09.08.1993 № 611 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/611-93-%D0%BF

3. Клименко П. М. Інформація як об’єкт інтелектуальної власності, що потребує охорони // Недержавна система безпеки підприємництва як суб’єкт національної безпеки України: Зб. Матеріалів наук.-практ. конф., Київ, 16-17 травня 2001 року. – К.: Вид-во Європ. ун-ту, 2003. – С. 283-289.

Клапко О.О.

студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

Сучасні комп’ютерні технології обробки даних істотно підвищили рівень інформаційної безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. Як відомо, на відміну від криптографічного захисту інформації стеганографічні програмні засоби намагаються насамперед приховати сам факт існування конфіденційної інформації.

Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на основі комп’ютерної техніки і програмного забезпечення, становлять предмет вивчення цифрової стеганографії. Актуальність дослідження методів стеганографії невпинно зростає, адже з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу великої кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних [1–5].

Цифрова стеганографія – напрям класичної стеганографії, що полягає у впровадженні додаткової інформації у цифрові об’єкти (контейнери), викликаючи при цьому деякі спотворення цих об’єктів. Ця технологія призначена для організації таємного зв’язку, що є класичним завданням стеганографії, проте останнім часом вона використовується також для захисту інтелектуальної власності [3].