ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В КОНТЕКСТІ УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВА

К. С. Нікуліна, студентка
І. О. Тарасенко, д.е.н., професор
Київський національний університет технологій і дизайну

Стабільне функціонування, зростання економічного потенціалу будь-якого підприємства в умовах стрімкого розвитку інформаційних технологій та підвищення ролі інформації багато в чому залежить від наявності надійної системи інформаційної безпеки. Це і зумовлює актуальність наукових досліджень за даним напрямом.

Наявність або відсутність необхідної інформації, її збереження і захищеність від стороннього втручання істотно впливає на добробут підприємства. Але з кожним роком все більше зростає кількість вірусів, мережевих атак зловмисників, виникають загрози порушення конфіденційності інформації всередині підприємства, що призводить до фінансових втрат, і часто – досить значних. Вирішення питань захисту даних в сучасних інформаційних системах буде успішним тільки за умови використання комплексного підходу до побудови системи управління безпекою інформації.

Питання управління інформаційною безпекою досліджували такі відомі зарубіжні та вітчизняні науковці як: А. Роберте, В. Хорошко, В. Ящуринський, В. Маричєв, В. Василюк, С. Климчук та ін. Проте поза їх увагою залишилась проблема управління захистом інформації з обмеженим доступом та функціонування субсистеми інформаційного права.

Досвід свідчить, що для зменшення кількості злочинів в інформаційній сфері необхідна цілеспрямована організація процесу захисту інформаційних ресурсів. Найбільший ефект досягається тоді, коли всі засоби, методи і заходи поєднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При цьому функціонування такої системи повинно контролюватися, оновлюватися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов.

Жодна СЗІ не може забезпечити необхідний рівень безпеки інформації без належної підготовки користувачів і дотримання ними усіх установлених правил, спрямованих на її захист.

Систему захисту інформації можна визначити як сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх та зовнішніх загроз.

Створенню СЗІ передує аналіз інформації з виокремленням конфіденційної та тієї, що становить комерційну таємницю.

Відповідно до статті 21 Закону України “Про інформацію” інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Закон України «Про інформацію» не містить чіткого розмежування понять конфіденційної інформації та комерційної таємниці.

Згідно зі 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 і не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить.

Створення ефективної системи інформаційної безпеки неможливе без чіткого визначення загроз інформації, що охороняється. Під загрозами інформації з обмеженим доступом прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного оволодіння інформацією.

У сфері забезпечення інформаційної безпеки можна виокремити такі основні напрями:

1. Розроблення і введення простої системи класифікації ступеня конфіденційності інформації, що обробляється (гриф обмеження доступу). Гриф можна присвоїти за допомогою штампів, спеціальних оцінок, а можна і за допомогою маркування кольором;

2. Встановлення процедури передання конфіденційної інформації від одного співробітника іншому, порядку її обробки і збереження залежно від ступеня таємності (це неминуче призведе до включення до цієї процедури аспектів забезпечення комп'ютерної безпеки, а також порядку ведення діловодства загалом і встановлення правил роботи з конфіденційними документами);

3. Проведення інформування персоналу підприємства про правила поводження з конфіденційною інформацією.

Таким чином, створення системи інформаційної безпеки є масштабною роботою, яка вимагає серйозних зусиль. Це потребує ідентифікації найбільших ризиків, які існують для інформаційної безпеки підприємства, і розробки додаткових заходів щодо забезпечення безпеки, якщо це реально не відобразиться на зростанні самого бізнесу.

Список використаної літератури:

1.Цивільний кодекс України від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – № 40−42. – Ст. 356. Із змінами, внесеними згідно із Законами № 189-VIII від 12.02.2015.

2.Закон України "Про інформацію" від 2 жовтня 1992 року // Із змінами, внесеними згідно із Законами N 2756-VI (2756-17) від 02.12.2010, ВВР, 2011, N 23, ст.160.

3. Гуз А.М. Організація захисту інформації з обмеженим доступом : Підручник / [А.М. Гуз, О.Д. Довгань, А.І. Марущак та ін.; за заг. ред. Є.Д.Скулиша]. – К. : Наук.-вид. відділ НА СБ України, 2011. – 378 с.