УДК 005.332.4:[005.92:004.056]

Шопін А. Ю.

Магістр 2 року навчання
факультету обліку і аудиту ХНЕУ

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА

Анотація. Розглянуто сутність безпеки інформації як важливої складової ефективного функціонування підприємств. Досліджено чинники безпеки інформації на підприємстві.

Аннотация. Рассмотрена сущность безопасности информации как важной составляющей эффективнорго функционирования предприятий. Исследованы факторы безопасности информации на предприятии.

Annotation. Considered is the essence of information security as an important prerequisite for efficient company operation. Information security factors were studied.

Ключові слова: інформаційна безпека, підприємництво, захист інформації, безпека підприємницької діяльності, електронна комерція, державна політика.

Ефективна інтеграція вітчизняної економіки у світову може відбутися лише за умови досягнення високого рівня конкурентоспроможності країни, її господарюючих суб'єктів, а також продукції та послуг, що виробляються останніми, на внутрішньому та зовнішньому ринках. Основою конкурентоспроможності є використання сучасної інформаційної технології. Економіка стає більш інформаційно насиченою, питання якісного доступу до інформаційних ресурсів виходить на одне з перших місць у конкурентній боротьбі.

Різні аспекти проблем інформаційної безпеки підприємницької діяльності розглянуто в наукових працях вітчизняних і закордонних дослідників: Домарев В. В, Куркін М. В., Горбатюк О. М., Ткачук Т. М., Савва О. П., Донець Л. І., Ващенко Н. В. Водночас не вистачає досліджень щодо виявлення факторів, які впливають на розвиток інформаційних складових структур безпеки підприємства, відсутня загальновизнана база моделювання процесів розвитку міжнародних відносин крізь призму внутрішньодержавної інформаційної політики.

Метою статті є дослідження основних чинників безпеки інформації на підприємстві, особливості захисту інформації та захисту від інформації, вплив різних чинників, пов'язаних із витоком інформації, на економічну безпеку підприємства.

Сьогодні всі економічно розвинуті країни широко використовують переваги нових інформаційних технологій у виробничій, комерційній та банківській сферах. Електронна комерція охопила весь світ, хоча кількість і поширення електронних засобів у різних країнах є вкрай нерівномірними. Згідно з даними "Доповіді про інформаційну економіку", яка прозвучала на Конференції Організації Об'єднаних Наційу США та Європі – по 200 млн користувачів Інтернет, у Латинській Америці – 30 млн, Африці – 6 млн. Обсяг електронних трансакцій на сьогодні складає сотні мільярдів доларів. Ключову роль тут відіграють "електронні гроші", виникнення яких пов'язують із появою в 1956 р. карток Bankamericard (тепер Visa), а слідом Master Charge (сьогодні MasterCard). Обсяги торгівлі в режимі on-line подвоюються кожні 100 днів. За прогнозами аналітиків, чисельність "електронних комерсантів" у 2013 р. сягатиме 1 млрд осіб. Цей процес не обійшов і Україну, фінансові установи якої отримали доступ до міжнародних платіжних систем. Темпи зростання кількості користувачів Інтернет у нашій державі, на відміну від західних країн, продовжують залишатися високими. Сьогодні їх нараховується близько двох млн. Однак із кожних ста осіб – тільки четверо користуються ресурсом мережі (у США відповідно 25 осіб, а в Європі – 9) [1].

Поняття інформації в загальному вигляді містить ст. 1 Закону України "Про інформацію". Відповідно до ст. 30 цього закону інформація за обмеженим доступом поділяється на конфіденційну та таємну. З приводу складу злочину, що розглядається (підприємницького шпигунства), інтерес становитиме власне конфіденційна інформація [2].

Тривалий час розуміння інформаційної безпеки в наукових та нормативно-правових джерелах ототожнювалося тільки з безпекою інформації, що значно звужувало її сутність. Саме тому з низки питань, присвячених розгляду проблеми забезпечення інформаційної безпеки, найбільш вивченими та дослідженими її аспектами є інформаційна безпека.

Інформаційна безпека – важлива складова концепції корпоративної безпеки членів Українського союзу промисловців і підприємців (УСПП), що є науково обґрунтованою системою поглядів на визначення основних напрямів, умов і порядку практичного вирішення завдань захисту суб'єктів підприємницької діяльності, що входять до УСПП, від протиправних дій і несумлінної конкуренції [3]. Корпоративна безпека членів УСПП має на меті захист інтересів власників, керівництва, працівників і клієнтів підприємств, матеріальних цінностей, інформаційних ресурсів від внутрішніх і зовнішніх загроз і ризиків.

Під інформаційною безпекою розуміється захищеність інформації і підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури. Завдання інформаційної безпеки зводяться до мінімізації збитку, а також до прогнозування і запобігання таких впливів [4].

Параметри інформаційних систем, які потребують захисту, можна розділити на наступні категорії: забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів. Доступність – це можливість отримання, за короткий проміжок часу, необхідної інформаційної послуги. Під цілісністю розуміють актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни. Конфіденційність – це захист від несанкціонованого доступу до інформації.

Інформаційні системи, перш за все, створюються для отримання певних інформаційних послуг. Якщо отримання інформації за якимись причинами стає неможливим, це шкодить усім суб'єктам інформаційних відносин. З цього можна визначити, що доступність інформації стоїть на першому місці. Цілісність є основним аспектом інформаційної безпеки тоді, коли точність і правдивість будуть головними параметрами інформації. Наприклад, рецепти медичних ліків або набір і характеристики комплектуючих виробів.

Найбільш проробленою складовою інформаційної безпеки в нашій країні є конфіденційність. Але практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем стикається в Україні з великими труднощами. По-перше, відомості про технічні канали просочування інформації є закритими, так що більшість користувачів позбавлена можливості скласти уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перешкоди та технічні проблеми [3].

Інформація на сьогоднішній день є комерційним об’єктом, а отже потребує захисту. Інформаційна безпека заснована не тільки на захисті власної інформації, у тому числі конфіденційної, але й проводить ділову розвідку, інформаційно-аналітичну роботу із зовнішніми й внутрішніми суб'єктами. Інформацію можна продати, купити, імпортувати, фальсифікувати, вкрасти і т. д. Інформація, якою обмінюється людина через машину з іншою людиною чи машиною, може бути важливою і, отже, є предметом захисту. Однак захисту підлягає не будь-яка інформація, а тільки та, котра має ціну, тобто цінна інформація. Цінною ж стає та інформація, володіння якою дасть змогу її дійсному чи потенційному власнику одержати який-небудь виграш: моральний, матеріальний, політичний і т. д. Отже, на перший план виходить проблема і необхідність захисту інформації, що становить комерційну таємницю. Для захисту конфіденційної інформації в установах спеціально створюється служба безпеки, особливості функціонування якої визначаються тим, що на неї покладені обов’язки з організації режимів конфіденційного діловодства; організації допуску співробітників і сторонніх осіб до конфіденційної інформації; організації зберігання, обліку і знищення носіїв конфіденційної інформації; виявлення каналів можливого витоку інформації, їхня нейтралізація; проведення профілактичної роботи і службових розслідувань; протидії технічним засобам промислового шпигунства; проведення спеціальних акцій, спрямованих на створення сприятливих обставин і нормального функціонування власного підприємства; зв’язку зі службами безпеки інших фірм і державних структур; взаємозв’язку із засобами масової інформації [3].

Сучасний діловий світ, представлений головним чином фінансово-інформаційними корпораціями, страждає від інформаційної крадіжки. За даними світової статистики, втрата тільки 20 % інформації веде до руйнування 65 % фірм і компаній. Тому інформаційна безпека є одним із найважливіших показників успішної діяльності організації [5].

Як правило, суб'єктами підприємницького шпигунства є особи, які (або за допомогою яких) реалізують зовнішні загрози інформаційній безпеці суб'єктів підприємницької діяльності (конкуренти, агенти конкурентів, особи, які не мають безпосереднього завдання конкурентів, злочинні елементи, партнери).

Особливу категорію суб'єктів підприємницького шпигунства становлять співробітники фірми (різновид внутрішніх загроз) – вони можуть діяти як за завданням, так і без завдання конкурентів (останнє найбільш характерно для так званих "ображених співробітників". За даними статистики: 75 % витоку інформації відбувається через співробітників компанії; 25 % витоку інформації – через використання технічних каналів. Серед опитаних 25 % працівників компанії заявили, що є чесними працівниками і за жодних умов не продадуть комерційну таємницю, 25 % працівників компанії готові завжди продавати інформацію, 50 % чинять залежно від обставин. Інформаційні процеси є основою функціонування сучасного суспільства та "провідником", за допомогою якого реалізується взаємодія між суб'єктами ринкових відносин. Їхня відкритість, досить висока розгалуженість породжує проблеми, конфлікти, пов'язані з упровадженням активних наступальних тех-

нологій у світовому інформаційному просторі для того, щоб одержувати переваги в матеріальній і фінансовій сферах [3].

Для ефективної системи інформаційної безпеки підприємницької діяльності безумовно необхідно, щоб на підприємстві існував інформаційно-аналітичний підрозділ, що є складовою служби безпеки, функціями якого є захист будь-якої інформації організації, висвітлення обстановки всередині і за межами підприємства, вчасно одержувати випереджальну інформацію про життєво важливі для підприємства процеси і знаходити засоби їх оптимального використання.

Розглядаючи зміст процесу забезпечення інформаційної складової економічної безпеки підприємства, необхідно виділити такі основні функції інформаційно-аналітичного підрозділу підприємства, належне використання яких необхідне для досягнення належного рівня забезпечення інформаційної складової економічної безпеки підприємства: збирання всіх видів інформації, що стосується діяльності та відповідного її захисту від розповсюдження; аналіз інформації, що отримується; прогнозування тенденцій розвитку наукового і технологічного процесу в сфері технологій діяльності підприємства; оцінювання рівня економічної безпеки підприємства за всіма її складовими загалом, розроблення рекомендацій для його підвищення; інші види діяльності щодо забезпечення інформаційної складової економічної безпеки підприємства.

Отже, для забезпечення інформаційної безпеки підприємницької діяльності необхідна ефективна державна політика, яка передбачає створення загальнодержавної системи інформаційної безпеки. Обов'язковою умовою створення цієї системи є розроблення відповідної нормативної бази, розвиток та вдосконалення системи сертифікації систем та засобів захисту інформації, організація та налагодження виробництва вітчизняних засобів захисту інформації, створення системи підготовки наукових кадрів у галузі захисту інформації. Удосконалення системи підготовки та перепідготовки кадрів для роботи у сфері інформаційної безпеки, врегулювання відносин у галузі використання Internet є одним із важливих напрямів вирішення цих проблем. Створення системи інформаційної безпеки, яка спроможна забезпечити належний рівень її захищеності в умовах постійного вдосконалення можливостей технічних розвідок та засобів ведення інформаційних війн є важливою умовою функціонування підприємницької діяльності.

Наук. керівн. Москаленко Н. О.

Література: 1. Ткачук Т. М. Формування системи інформаційної безпеки бізнесу / Т. М. Ткачук // Бизнес и безопасность. – 2007. – №. 4. – С. 19–23. 2. Про інформацію : Закон України від 02.10.1992 р. [Електронний ресурс]. – Режим доступу : http://www.zakon.rada.gov.ua/. 3. Донець Л. І. Економічна безпека підприємства / Л. І. Донець, Н. В. Ващенко. – К. : Центр наукової літератури, 2008. – 240 с. 4. Савва О. П. Роль інформації в досягненні конкурентоспроможності / О. П. Савва // Вісник КНУТД, 2007. – № 3. – С. 103–111. 5. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 2009. – Вип. 14: Міжнародні відносини. – С. 46–48. 6. Куркин Н. В. Управление экономической безопасностью предприятия : монография / Н. В. Куркін. – Днепропетровск : Изд. АРТ-ПРЕСС, 2004. – 452 с. 7. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ООО ТИД "Диасофт", 2004. – 992 с. 8. Информационный сайт компании "Безопасник". – Режим доступа : http://www.bezopasnik.org/article/index.htm.