Інформаційні технології забезпечення безпеки електронного бізнесу

Орлик О.В.
кандидат економічних наук, доцент
в.о. зав. кафедри інформаційних систем в економіці
Одеського національного економічного університету

В сучасних умовах найбільшу значимість і поширеність має технологія Інтернет, яка надала підприємствам безмежні можливості в області передачі, розповсюдження та розсилки інформації, дозволила виконувати фінансово-банківські операції, операції з купівлі-продажу товарів, незважаючи на відстані і кордони. Разом з тим, крім позитивного ефекту, деякі особливості даної технології, які допомогли їй поширитися по всьому світу, в той же час створюють сприятливі можливості для багатьох видів злочинної діяльності.

Результатом забезпечення економічної безпеки підприємства є стабільність його функціонування, ефективність фінансово-економічної діяльності, особиста безпека персоналу. Незважаючи на те, що Інтернет забезпечує доступ виробників до максимальної кількості споживачів, дає можливість освоїти велику кількість нових ринків, паралельно виникають питання забезпечення безпеки. З урахуванням цього діяльність із забезпечення економічної безпеки підприємства включає в себе чотири основних напрямки: інформаційне забезпечення комерційної діяльності підприємства в ринкових умовах; захист інтелектуальної власності (в тому числі комерційної таємниці); захист матеріальних і фінансових цінностей; захист персоналу [1, с.90]. За оцінками експертів, витрати на створення системи безпеки підприємства і його оптимальне функціонування можуть досягати 25% витрат на весь процес виробництва [2].

З поширенням мережі Інтернет швидкість і обсяг інформації різко зросли. Кордони сучасного офісу значно розширилися завдяки бездротовим технологіям.

Активне підключення споживачів до мережі Інтернет викликало розвиток електронного бізнесу. Сфери застосування електронного бізнесу різноманітні: електронна торгівля, банківські операції, страхові операції, купівля-продаж різних продуктів, операції на фондовій біржі, IP-телефонія тощо [3]. Банки пропонують послуги управління рахунком і платежі в режимі реального часу. Цілодобово працюють Інтернет-магазини. Інтернет став простим і зручним засобом зв'язку між підприємцями

(business-to-business, B2B), між підприємцями і споживачами (business-to-consumer, B2C), між споживачами (consumer -to-consumer, C2C) та реалізації інших видів електронної комерції.

Перевагами використання підприємствами електронної комерції можна назвати наступні: низька собівартість передачі даних; простота розгортання додатків і управління ними; альтернативний додатковий спосіб ведення бізнесу; недорога рекламна площа; можливість цілодобового доступу; можливість ідентифікувати покупця; розширення ринків збуту товарів та послуг; зростаюча кількість потенційних клієнтів; зменшення часу на отримання відомостей про товар чи послугу; зменшення витрат часу на придбання необхідного товару; інформацію про товар можна представляти в Інтернеті у різному вигляді (текст, графіка, відео, тощо); мінімізація витрат на персонал та оренду приміщень.

Завдяки інформаційним технологіям різко підвищився рівень економічних можливостей у різних галузях виробничої діяльності. Але на сьогодні ситуація з електронним бізнесом залишається досить складною. Це відбувається через невелику ділову активність населення країни, а також через проблеми, пов'язані з організацією безпеки електронного бізнесу, захистом від кіберзлочинності.

З розвитком комп'ютерної техніки та використанням комп'ютерних мереж постає проблема захисту джерел інформації. Будь-яке несанкціоноване вторгнення може призвести до втрати важливої інформації, її секретності, і як наслідок – використання цієї інформації в будь-яких корисливих цілях.

Як вважають експерти, витік 20% комерційної інформації в шістдесяти випадках зі ста призводить до банкрутства підприємства [4].

Швидкий розвиток інформаційних систем загального та спеціального призначення викликав необхідність вдосконалення методів і способів користування – з одного боку, з іншого – методів і засобів захисту від несанкціонованого доступу до інформації.

Підприємства повинні захищати свої активи від випадкового чи злочинного внутрішнього та зовнішнього неправильного використання. Інформація клієнта також повинна бути захищена. Приймаючи рішення про організацію електронного бізнесу, підприємству необхідно бути готовим до того, що використання пластикових карт клієнтами в якості основного платіжного інструменту може спровокувати спроби різного роду комп'ютерних злочинів.

Основні види шахрайських дій зловмисників: придбання товарів і послуг за реквізитами вкрадених пластикових кредитних карток; злам баз даних, що містять інформацію з пластикових карт (відомості про власників пластикових карт, які здійснюють покупки в електронних магазинах); організація шахрайських електронних магазинів [1, с.92].

Виділяють декілька складових елементів захисту електронного бізнесу:

− інженерно-технічний захист інформації призначений для пасивної і активної протидії за допомогою комплексів технічних засобів;

− програмно-математичний захист інформації призначений для захисту цінної інформації, що обробляється і зберігається в комп'ютерах, локальних мережах і різних інформаційних системах;

− організаційний захист інформації містить заходи, що спонукають персонал дотримуватися правил захисту цінної інформації підприємства. Ці заходи складають 50-60% в структурі більшості систем захисту інформації. Це пов'язано з низкою факторів, а також з тим, що важливою стороною організаційного захисту інформації є підбір, розстановка і навчання персоналу, який буде здійснювати на практиці принципи і методи захисту [4].

Зміст складових елементів захисту, методи і засоби захисту повинні регулярно змінюватись з метою запобігання їх розкриття.

При цьому впроваджуються наступні механізми безпеки: шифрування, електронний цифровий підпис, контроль доступу, забезпечення цілісності даних, забезпечення аутентифікації [3].

Шифрування служить завданням дотримання конфіденційності інформації, що передається. Шифрування передбачає оборотне перетворення інформації з метою приховування від неавторизованих осіб, з наданням в той же час доступу до даної інформації авторизованим користувачам, які мають певний аутентичний ключ.

Електронний цифровий підпис (ЕЦП) призначений для захисту електронного документа від підробки. Особливість ЕЦП полягає у тому, що він ґрунтується на алгоритмах криптографічного захисту інформації і накладається за допомогою особистого ключа – спеціального коду, відомого тільки особі, яка підписала документ. Дійсність ЕЦП перевіряється за допомогою відкритого ключа – коду перевірки. Цей код робить неможливим підробку ЕЦП автора електронного документа, але надає можливість перевірити його справжність.

Контроль доступу – функція системи, що забезпечує технологію безпеки, яка дозволяє або забороняє доступ до певних типів даних, засновується на ідентифікації суб'єкта, якому потрібен

доступ, і об'єкта даних, що є метою доступу. Доступ до захищеної інформації повинен бути обмежений, щоб тільки особи, які мають право доступу, могли отримувати цю інформацію.

Комп'ютерні програми і в багатьох випадках чужорідні комп'ютери за допомогою локальної мережі, Інтернету, бездротових технологій можуть отримати секретну інформацію, яка їм не призначена. Тому, складність механізмів контролю доступу повинна бути в паритеті з цінністю інформації, тобто чим більш важливою або цінною є інформація, тим складнішими повинні бути механізми контролю доступу до неї.

Цілісність даних означає, що дані не були змінені при виконанні будь-яких операцій над ними, будь то передача, зберігання і відображення.

Забезпечення аутентифікація передбачає проведення процедури перевірки автентичності іншої сторони: перевірка справжності користувача шляхом порівняння введеного їм пароля з паролем, збереженим в базі даних користувачів; підтвердження справжності електронного листа шляхом перевірки цифрового підпису листа з відкритим ключем відправника тощо.

Основними заходами протидії комп'ютерним злочинам також є: контроль роботи розробників комп'ютерних систем, захист від несанкціонованого доступу до системи, профілактика від комп'ютерних вірусів, ретельність підбору персоналу, виключення випадків ведення особливо важних робіт тільки однією людиною, охорона об'єктів безпеки, установка резервних систем електроживлення, оснащення приміщень кодовими замками і сигналізацією тощо. Основними характеристиками кожного заходу є вартість захисту та економічний ефект використання.

Отже, з розвитком комп'ютерних інформаційних технологій загострилася проблема комп'ютерних злочинів, які можуть завдати підприємству як фінансових, так і інформаційних втрат. Головне в організації бізнесу – не тільки грамотно використовувати наявну інформацію, але і забезпечити її якісний захист всіма доступними засобами.

Література:

1. Дробышева, В.Г. Роль и место информационных технологий в системе экономической безопасности государства [Текст] / В.Г. Дробышева, А.П. Черноиванов // Социально-экономические явления и процессы. – 2011. – №3-4. – С. 87-93.

2. Козивкин, В. В. Экономическая безопасность промышленного предприятия[Електронний ресурс] / В.В. Козивкин. – Режим доступу \www/ URL: http://secandsafe.ru/pravovaya_baza/blogi/ekonomicheskaya_bezopasnost/ekonomicheskaya_bezopasnost_promyshlennogo_predpriyatiya. – Заголовок з екрана, доступ вільний, 08.10.2016.

3. Будянский, П. С. Роль информационных технологий в современной экономике [Електронний ресурс] / П.С. Будянский. – Режим доступу \www/ URL: http://economyar.narod.ru/budjnskii.pdf. – Заголовок з екрана, доступ вільний, 08.10.2016.

4. Павлов, А. П. Информационные технологии экономической безопасности бизнеса [Електронний ресурс] / А.П. Павлов, А. В. Колосов // Мир науки. Научный Интернет журнал. – 2013. – Вып. 1. – Режим доступу \www/ URL: http://mir-nauki.com/PDF/02EMN113.pdf. – Заголовок з екрана, доступ вільний, 08.10.2016.