351.746.1

Глєбова А.О., к.е.н., доцент,
Бардзік Е., студент,
Полтавський національний технічний університет імені Юрія Кондратюка

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ ПРОЦЕСУ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ РИНКОВИХ ВІДНОСИН

Сьогодні в умовах розвитку ринкових відносин та глобалізації все більшого значення набуває проблема забезпечення інформаційної безпеки підприємства. Без необхідного обсягу і якості інформації не можливий ефективний розвиток підприємницької діяльності і виживання підприємства у конкурентній боротьбі. В сучасних умовах інформаційної насиченості економіки інформація існує вже не як допоміжний ресурс, а як вирішальна складова бізнесу. Інформація набула значення особливого роду товару, що має велику цінність. Цінність інформації визначається, виходячи з її достовірності, своєчасності і доступності. Остання робить інформацію найбільш привабливою, оскільки її конфіденційність визначається встановленим режимом доступу і обмежується колом осіб, які мають право володіти нею [5].

Комп'ютеризація, розвиток телекомунікацій надають сьогодні широкі можливості для автоматизованого доступу до різних конфіденційних, персональних і інших важливих, критичних даних в суспільстві (його громадян, організацій і т. д.). Природньо, люди усвідомлюють появу такого ряду нових ризиків і починають турбуватися про забезпечення необхідної безпеки подібної інформації[6]. Адже, дослідження також показало, що приблизно раз на місяць на підприємствах трапляється один інцидент, який можна віднести до одного з 10 можливих типів загроз. Більше за все відбувається випадків ненавмисної втрати даних через недбалість співробітників – таких інцидентів відбувається 15-20 на рік. Внутрішні зловмисні атаки і шпигунство – 10 випадків на рік, зловживання доступом до інформації – 20 випадків на рік. Якщо говорити про сферу діяльності, то на досліджуваних підприємствах відбувається до 20-30 інцидентів щорічно. Результати дослідження свідчать, що універсального рішення для усунення внутрішніх ризиків не існує. Кожне підприємство має виробити власний комплексний підхід з урахуванням особливостей структури і специфіки діяльності [7].

Висвітленням поняття «Інформаційна безпеки підприємства» займалися Н.В. Ващенко, М.В. Куркіна, О.Ф. Новикова, І.М. Близнюк, О.Р. Братель, В.О. Бондаренко, І.Л. Бучило, М.О. Гуцалюк, О.М. Ляшенко, М.І. Камлик, Г.В. Козаченко, В.П. Пономарьов та ін. Однак, на наш погляд, дана проблема через свою новизну є не в повній мірі розкрита і досліджена, адже інформаційні технології постійно розвиваються і удосконалюються.

Метою статті є дослідження теоретичних та практичних аспектів процесу формування інформаційної безпеки підприємства та визначення шляхів її підвищення ефективності в умовах ринкових відносин.

Людський фактор був і є одним із найбільших ризиків для будь – якого бізнесу, оскільки саме люди створюють системи захисту і самі їх потім використовують. Нині поняття «інформаційна безпека» є одним із важливих складових не тільки економічної безпеки підприємства, але і національної безпеки держави. Адже, всі суб'єкти управління незалежно від галузевої приналежності, виду діяльності та їх функціональних обов'язків використовують інформацію.

Інформаційна безпека підприємства - це захищеність інформації, яку має підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при вступі. Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виведення. Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства в цілісності, захист і гарантування повноти і точності інформації, яка нею видається, мінімізація руйнувань і модифікація інформації, якщо такі трапляються [8].

Сьогодні всі економічно розвинуті країни широко використовують переваги нових інформаційних технологій у виробничій, комерційній та банківській сферах. Це пояснюється тим, що за допомогою традиційних методів неможливо зорієнтуватися в сучасному стрімкому інформаційному потоці й глибоко аналізувати динамічні процеси економічної діяльності підприємств. Найбільш швидко й ефективно розвиваються технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як е-торгівля, е-бізнес, е-уряд тощо [5]. Одночасно виникли нові загрози і перешкоди для електронного бізнесу. На

Першому міжнародному стратегічному конгресі «E-CRIME CONGRESS 2002» у своїй доповіді Віл'ям Барр, віце-президент групи страхових компаній, зокрема, виклав такі факти:

90 % організацій щорічно виявляють порушення інформаційних систем;

80 % з них підтверджують фінансові збитки;

тільки один вірус NIMDA призвів до збитків, що склали понад 1,8 млрд. фунтів;

щорічно викрадається приватної інформації на суму понад 38 мільярдів фунтів [5].

Зокрема, з 2009 року дана проблема особливо є актуальною для міжнародних організацій. Адже, на території колишнього СРСР яскравим прикладом атак проти держави стала Естонія - країна з високим рівнем електронних послуг на всьому пострадянському просторі. Саме тут давно і успішно працює електронний уряд. Естонці давно звикли через інтернет оплачувати рахунки оформляти податкові декларації і навіть голосувати на виборах. У 2007 році багато сайтів, серверів і маршрутизаторів Естонії , в тому числі уряду, банків, засобів масової інформації, піддавалися масованим кібератакам, які тривали більше місяця і мали конкретні стратегічні цілі. Незважаючи на те, що аналіз цих подій триває, вони показали уразливість інтернет- інфраструктур як уряду, так і приватного сектора країни та важливість інформаційної безпеки.

Серед найбільш резонансних атак останніх років - злам сайтів сенату США і ЦРУ. У червні 2011- го хакерська група LulzSec зламала базу даних сайту американського сенату і опублікувала внутрішню, хоча і не секретну інформацію. Свою атаку хакери назвали « тренуванням перед більш серйозною справою». Через кілька днів після цього LulzSec атакувала сайт ЦРУ, заблокувавши користувачам доступ до нього. І ці атаки не припиняються у жодній країні світу і ведуться не тільки проти окремих держав, корпорацій, засобів масової інформації, але і проти людей. Прикладом, є останнім часом поява інформації про атаки на інформаційні центри банків у різних країнах світу і інформаційні центри, де міститься вся інформація про громадян (паспортні дані, ідентифікаційні коди, номера кредитних карток тощо). У результаті, за даними світової статистики, втрата тільки 20% інформації веде до руйнування 65% фірм і компаній. Тому інформаційна безпека є одним з найважливіших показників успішної діяльності організації [6].

Інформаційну безпеку підприємства можна охарактеризувати такими основними її складовими: конфіденційністю, цілісністю, доступністю. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час [1].

Для забезпечення ефективної системи інформаційної безпеки підприємства необхідне існування інформаційно-аналітичного підрозділу, що є складовою служби безпеки, функціями якого є захист будь-якої інформації організації, висвітлення стану всередині і поза межами підприємства, вчасно одержувати випереджальну інформацію про життєво важливі для підприємства процеси і знаходити засоби їх оптимального використання [2].

Реалізація інформаційної безпеки включає 5 складових: технічна, організаційна, дозвільна, попереджувальна та правова. Технічна складова відповідає за захист об'єктів підприємства та інформації, за виявлення фактів витікання інформації та неправомірних дій персоналу та сторонніх осіб за допомогою технічних засобів. Організаційна складова має забезпечити належне поводження персоналу із секретною інформацією підприємства. Дозвільна складова здійснює розподіл інформації підприємства за рівнями секретності та визначає ступінь доступу до неї. Для мінімізації ризиків прийняття хибних управлінських рішень, уникнення дезінформації, а також зменшення ймовірності витікання секретної інформації система інформаційної безпеки має включати попереджувальну складову. Правовий захист інтересів підприємства, захист інформації, закріплення прав підприємства щодо комерційної таємниці в установчих документах забезпечує правова складова.

Забезпечення безпеки - це комплексна проблема, для вирішення якої потрібне поєднання законодавчих, організаційних та програмно-технічних заходів. На жаль, законодавча база сьогодні відстає від потреб практики, а наявні закони та укази носять в основному теоретичний характер. Головна мета заходів, що вживаються на організаційно-управлінському рівні, - сформувати програму робіт у галузі інформаційної безпеки і забезпечити її виконання з виділенням необхідних ресурсів і контролем за станом справ. Основою програми є багаторівнева політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів [8].

Використання інформаційних систем веде за собою наявність сукупності ризиків. Загрозу підприємницькій діяльності можуть становити, як зовнішні джерела ризиків, так і внутрішні.

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться: кримінальні структури; потенційні злочинці і хакери; несумлінні партнери; технічний персонал постачальників послуг; представники наглядових організацій і аварійних служб; представники силових структур.

Внутрішні суб'єкти (джерела), як правило, представляють собою висококваліфікованих фахівців у галузі розроблення та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою та основними функціями і принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться: основний персонал (користувачі, програмісти, розробники); представники служби захисту інформації; допоміжний персонал (прибиральники, охорона); технічний персонал (життєзабезпечення, експлуатація).

Сутність подібних загроз зводиться, як правило, до нанесення того чи іншого збитку підприємству (організації). Прояви можливого збитку можуть бути самими різними: моральний і матеріальний збиток ділової репутації організації; моральний, фізичний чи матеріальний збиток, пов'язаний з розголошенням персональних даних окремих осіб; матеріальний (фінансовий) збиток від розголошення захищеної(конфіденційної) інформації; матеріальний (фінансовий) збиток від необхідності відновлення порушених захищених інформаційних ресурсів; матеріальний збиток (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною; моральний і матеріальний збиток від дезорганізації в роботі всього підприємства [8].

Для протидії інформаційним загрозам має бути розроблений чіткий план, який відображатиме персональну відповідальність кожного працівника, починаючи з технічного персоналу й закінчуючи вищою керівною ланкою. В плані мають визначатися також заходи щодо відновлення інформаційних ресурсів після їх ураження. Ці процедури слід постійно перевіряти. Розробці плану повинен передувати аналіз усіх інформаційних масивів та потоків інформації (як внутрішніх так і зовнішніх). Практика свідчить, що ефективний комплексний аудит є можливим лише за участі сторонньої спеціалізованої організації, яка має відповідну ліцензію на проведення такої діяльності [5].

Нині комісія з питань національної безпеки визначила такі потенційні загрози в інформаційній сфері: відсутність у міжнародного співтовариства об’єктивного уявлення про Україну; інформаційна експансія з боку інших країн; відтік інформації, що містить державну таємницю, а також конфіденційної інформації, що є власністю держави; повільне входження України до світового інформаційного ринку; незбалансованість державної політики та відсутність необхідної інфраструктури в інформаційній сфері [4].

Отже, ми можемо зробити висновок, що зі зростанням науково-технічного прогресу буде зростати і важливість питання інформаційної безпеки громадянина, суспільства, держави. Тобто інформація почала використовуватися як чинник, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав’язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які противорічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [3].

Таким чином ми можемо зробити висновок, що особливо привабливим для скоєння інформаційних злочинів є бізнес-середовище. У цій сфері відбувається значна частина всіх фінансових афер. Злочини скоєні в системі бізнесу є найбільш небезпечними економічними злочинами. Їх негативні наслідки відображаються як на самій бізнес-системі так і на всій фінансовій системі держави.

Для забезпечення інформаційної безпеки підприємства необхідне проведення цілісної державної програми відповідно до Конституції та чинного законодавства України і норм міжнародного права через реалізацію відповідних концепцій і програм, що стосуються національної інформаційної політики України. До інформаційної безпеки підприємства слід також віднести безпечні умови існування інформаційних технологій, які включають питання побудови ефективної інформаційної інфраструктури, захисту інформації, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів. Оптимальним варіантом забезпечення

інформаційної безпеки є дотримання систематичного поєднання правових, організаційних та програмно-технічних методів у процесі управління підприємством.

Література

1. Близнюк І.М. Інформаційна безпека України та заходи її забезпечення / І.М. Близнюк // Науковий вісник Національної академії внутрішніх справ України. – 2008. – № 5. – С. 206-214.
2. Васильчак С.В. Проблеми забезпечення інформаційної безпеки підприємницької діяльності в умовах техноглобалізму [Електронний ресурс] /Васильчак С.В., Гладун Л.Я.// Національний лісотехнічний вісник України .- - Режим доступу://http: archive.nbuv.gov.ua.-Заголовок з титулу екрану.
3. 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.
4. Гуцалюк М.О. Інформаційна безпека України: нові загрози / М.О. Гуцалюк // Бизнес и безопасность. – 2007. – № 5. – С. 2–3.
5. Гуцалюк М.О.Забезпечення інформаційної безпеки підприємницької діяльності [Електронний ресурс] / Гуцалюк М.О.//Юридичний журнал.-2003.-№ 3. - Режим доступу://http://www.justinian.com.ua.-Заголовок з титулу екрану.
6. Прокоф'єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів/Д.М. Прокоф'єва // Український центр інформаційної безпеки.- 2008 - С. 123-128.
7. Результаты исследования IDC по вопросам внутренних рисков[Електронний ресурс] - Режим доступу://http://www.nestor.minsk.by.-Заголовок з титулу екрану.
8. Садердинов А. А. Информациионная безопасность предприятия: Учебное пособие//Садердинов А. А. Трайнев В. А., Федулов А. А. - 2-е изд.—М., Издательско-торговая корпорация «Дашков и К°». – 2005.- С.4-22.
9. Цимбалюк В. С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства/ В. С. Цимбалюк // Підприємництво,господарство і право. – 2007. - №3. - С.88-91.