ІНФОРМАЦІЙНА БЕЗПЕКА

Марчук І.В.
Науковий керівник: Гапчак Т.Г., асистент

Анотація. *Висвітлено нагальні проблеми інформаційної політики менеджменту на підприємстві. У статті розглянуто поняття, призначення інформаційної безпеки і методів вдосконалення інформаційного середовища діяльності підприємства в умовах ринкової економіки.*

Ключові слова: менеджмент, інформація, безпека, зовнішнє середовище, внутрішнє середовище, інформаційний простір.

Вступ. Сучасні підприємства різних галузей функціонують в умовах високої складності, невизначеності і динамічності навколишнього соціально-економічного середовища. Зростання рівня інформатизації світового ринку, що дозволяє отримати практично миттєвий доступ до будь-якої ринкової інформації, викликає різке зростання конкуренції між виробниками. Це обумовлює необхідність не лише формування єдиного інформаційного простору, адекватного ринковим механізмам, але й організацію інформаційної безпеки підприємства. Ця діяльність набуває більшої актуальності у зв'язку із поширенням застосування різних способів ворожого конкурентного впливу.

Постановка завдання:

- подати теоретичні особливості інформаційної безпеки підприємств;
- запропонувати основні організаційно-технологічні шляхи формування інформаційної безпеки підприємств.

Метою роботи є вирішення проблем інформаційної безпеки підприємств.

Об'єктом дослідження є стан інформаційного простору підприємств з приводу його безпеки.

Результати дослідження. Господарюючі суб'єкти, надаючи інформацію про свою діяльність, з одного боку, формують певну сферу економічного інформаційного простору, з іншого – кожне підприємство в процесі своєї діяльності використовує значні обсяги різної інформації, як із зовнішнього середовища, так і ту, що генерується всередині самого господарюючого суб'єкта. Саме така інформація становить найбільший інтерес для конкурентів, оскільки володіння нею дозволяє формувати стратегію і тактику цінових і нецінових заходів для боротьби за частку ринку, володіння активами, поширення сфер впливу на клієнтів, фондову боротьбу. Не завжди на цьому конкуренція закінчується. Існують методи «важкої артилерії» в світі бізнесу, особливо на рівні великих компаній.[1, с 37]

Найпоширеніші способи ворожого конкурентного впливу – навмисне доведення до банкрутства, цілеспрямоване зниження вартості підприємства і придбання його активів, боротьба за права власності на стратегічно важливі активи, «купівля» менеджерів підприємства. [2, с 47]

Значною мірою ймовірність інформаційної агресії залежить від передумов для доступу до важливої інформації сторонніх зацікавлених осіб. Варто починати із юридичної основи захисту компанії – скрупульозно розроблених внутрішніх документів (Статут, Положення про органи управління). Часто до цих документів відносяться як до неприємної формальності. Формування ради директорів і правління дозволяє використовувати такий тактичний спосіб, як розумна бюрократизація порядку ухвалення в товаристві рішень. Тобто мова йде про створення на підприємстві таких умов, при яких інформаційний тероризм зводиться до мінімуму. [4, с 41]

Багато агресорів при скуповуванні найцікавіших активів діють за принципом: «Навіщо купувати підприємство, якщо можна купити його менеджмент?». Якщо на підприємстві не побудована дієва система незалежного моніторингу його фінансово-господарської діяльності (інакше кажучи, система економічної безпеки бізнесу, система внутрішнього контролю), реалізувати цей принцип агресорові не так вже й складно.

Система моніторингу традиційно реалізується через створення власної служби поточного моніторингу (служби економічної безпеки) і контрольно-ревізійної служби, до завдань якої відноситься проведення комплексних перевірок дотримання встановлених на підприємствах процедур управління. До цих формувань обов'язково потрібно відділ інформаційної безпеки, а в організаціях, де це неможливо через малі розміри, потрібно доповнити діяльність перерахованих служб функцією інформаційної безпеки. Саме фахівці складають кадрове ядро компанії і багато в чому визначають успіх цього бізнесу. Тому одним з дієвих механізмів захисту бізнесу є створення системи мотивації, що орієнтує менеджмент компанії на зростання ефективності і вартості бізнесу. У західному бізнес-співтоваристві поширені схеми партнерської участі топ-менеджерів і головних фахівців у бізнесі (опціони, механізми відкладеного доходу). Сьогодні ці механізми майже не застосовуються, що свідчить швидше про недостатній розвиток культури корпоративного управління, ніж про принципову неможливість використання цих систем на вітчизняному ґрунті.

Тепер розглянемо, які існують засоби або інструменти, якими реалізовані принципи або механізми безпеки інформації. Наприклад, персонал займається аудитом, який забезпечує облік. Або паролі, що забезпечують аутентифікацію, зберігаються в шифрованому виді, аутентифікація передує, наприклад, дозволу на модифікацію. Виходить, криптографія — засіб захисту паролів, паролі використовуються для механізму аутентифікації, аутентифікація передує забезпеченню цілісності.

Перелічимо основні засоби (інструменти) інформаційної безпеки:

- персонал — люди, які будуть забезпечувати перетворення в життя інформаційної безпеки у всіх аспектах, тобто розробляти, впроваджувати, підтримувати, контролювати й виконувати;

- нормативне забезпечення — документи, які створюють правовий простір для функціонування інформаційної безпеки;
- моделі безпеки — схеми забезпечення інформаційної безпеки, закладені в дану конкретну інформаційну систему або середовище;
- криптографія — методи й засобу перетворення інформації у вид, що утрудняє або робить неможливим несанкціоновані операції з нею (читання й/або модифікацію), разом з методами й засобами створення, зберігання й поширення ключів — спеціальних інформаційних об'єктів, що реалізують ці санкції;
- антивірусне забезпечення — засіб для виявлення й знищення злобливого коду (вірусів, троянських програм і т.п.);
- міжмережеві екрани — пристрою контролю доступу з однієї інформаційної мережі в іншу;
- сканери безпеки — пристрою перевірки якості функціонування моделі безпеки для даної конкретної інформаційної системи;
- системи виявлення атак — пристрою моніторингу активності в інформаційнім середовищі, іноді з можливістю прийняття самостійної участі в зазначеній активній діяльності;
- резервне копіювання — збереження надлишкових копій інформаційних ресурсів на випадок їх можливої втрати або ушкодження;
- дублювання (резервування) — створення альтернативних пристроїв, необхідних для функціонування інформаційного середовища, призначених для випадків виходу з ладу основних пристроїв;
- аварійний план — набір заходів, призначених для перетворення в життя, у випадку якщо події відбуваються або відбулися не так, як було визначено правилами інформаційної безпеки;
- навчання користувачів — підготовка активних учасників інформаційного середовища для роботи в умовах відповідності вимогам інформаційної безпеки.

Можливо, деякі поняття занадто укрупнені (криптографія), деякі, навпаки, деталізовані (сканери). Основною метою цього списку ставилося показати типовий набір, характерний для підприємства, яке розбудовує в себе службу інформаційної безпеки.

Об'єктивні фактори або цілі інформаційної безпеки забезпечуються застосуванням наступних механізмів або принципів:

- політика — набір формальних (офіційно затверджених або традиційних) правил, які регламентують функціонування механізму інформаційної безпеки;
- ідентифікація — визначення (розпізнавання) кожного учасника процесу інформаційної взаємодії перед тем як до нього будуть застосовані які б то ні було поняття інформаційної безпеки;
- аутентифікація — забезпечення впевненості в тому, що учасник процесу обміну інформацією ідентифікований вірно, тобто дійсно є тим, чий ідентифікатор він пред'явив;
- контроль доступу — створення й підтримка набору правил, що визначають кожному учасникові процесу інформаційного обміну дозвіл на доступ до ресурсів і рівень цього доступу;
- авторизація — формування профілю прав для конкретного учасника процесу інформаційного обміну (аутентифікованого або анонімного) з набору правил контролю доступу;
- аудит і моніторинг — регулярне відстеження подій, що відбуваються в процесі обміну інформацією, з реєстрацією й аналізом визначених значимих або підозрілих подій. Поняття "аудит" і "моніторинг" при цьому трохи різняться, тому що перше припускає аналіз подій постфактум, а друге наближене до режиму реального часу;
- реагування на інциденти — сукупність процедур або заходів, які проводяться при порушенні або підозрі на порушення інформаційної безпеки;
- керування конфігурацією — створення й підтримка функціонування середовища інформаційного обміну в працездатному стані й відповідно до вимог інформаційної безпеки;
- керування користувачами — забезпечення умов роботи користувачів у середовищі інформаційного обміну відповідно до вимог інформаційної безпеки. У цьому випадку під користувачами розуміються всі, хто використовує дане інформаційне середовище, у тому числі й адміністратори;
- керування ризиками — забезпечення відповідності можливих втрат від порушення інформаційної безпеки потужності захисних засобів (тобто витратам на їхню побудову);
- забезпечення стійкості — підтримка середовища інформаційного обміну в мінімально припустимім працездатному стані й відповідності вимогам інформаційної безпеки в умовах деструктивних зовнішніх або внутрішніх впливів.

Аутентифікація сама по собі не може бути метою інформаційної безпеки. Вона є лише методом визначення учасника інформаційного обміну, щоб далі визначити, яка, наприклад, політика відносно конфіденційності або доступності повинна бути застосована до даного учасника.

Структура системи інформаційної безпеки фірми може виглядати як поєднання функцій окремих службових підрозділів. (Рис. 1). Взаємодія із зовнішнім середовищем обов'язково формується по-перше під контролем служби інформаційного забезпечення конкуренції або службовців, які її уособлюють. По-друге, під контролем служби інформаційної безпеки технологічного забезпечення. Ці функції може виконувати інженер програмного і апаратного забезпечення або один із заступників керівника. Додатково варто розглянути інформаційну безпеку фірми в контексті зростання ролі Інтернету у формуванні інформаційного простору фірми. Інфікування комп'ютерів вірусами, троянами, adware і тому подібним шкідливим ПЗ здатна призвести до викрадення конфіденційної інформації, руйнування цінної інформації, виведення з ладу комп'ютерних систем, стрімкого росту витрат на Інтернет (внаслідок неконтрольованої поведінки інфікованої техніки).

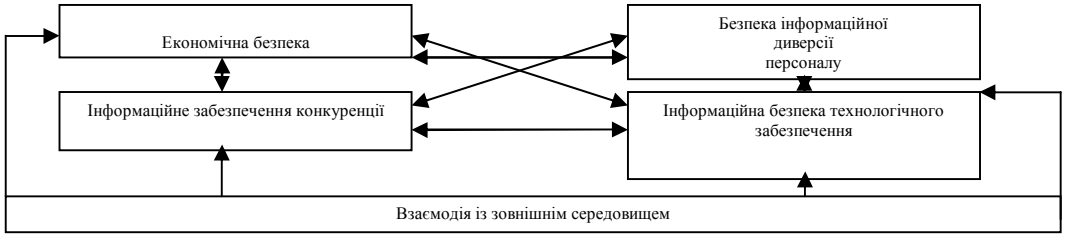

Рис. 1. Структура системи інформаційної безпеки підприємства.

Впровадження Інтернету часто стає фоном, на якому відбуваються негативні процеси всередині колективу установи. Зокрема: марнується робочий час на недоцільне використання Інтернету; виникає напруженість на основі заздрості “непід’єднаних” до “під’єднаних”; виникає роздратування на випадки обмеження доступу до певних служб чи сайтів Інтернету. Виникає ситуація, коли сторонні особи (зокрема родичі та знайомі співробітників) використовують Інтернет, разом з тим різко понижають рівень інформаційної безпеки підприємства. Спрощуються контакти працівників, які є небажаними для підприємства (з конкурентами, перевіряючими органами і т.п.); спрощується доступ працівників до небажаної інформації (компромату на керівництво, служб працевлаштування і т.п.). Провокуються конфлікти із суспільством та державою. Інтернет для підприємства часто стає джерелом нових конфліктів із зовнішнім світом. Природа таких конфліктів лежить у сфері нерегламентованого та безвідповідального використання Інтернету працівниками з подальшою відповідальністю за такі дії усього підпримства. Часто такі конфлікти набувають однієї з наступних форм: відповідальність підприємства перед законом та спільнотою за зловмисні дії працівників (спроби злому, спаму, порушення законів в Інтернет і т.п.); падіння престижу підприємства – через недолугу поведінку співробітників в Інтернет (наприклад некоректні повідомлення на форумах); відповідальність підприємства за певні упущення, які інакше могли б бути прихованими (наприклад, виявлення неліцензійних копій ПЗ при спробі автоматичної реєстрації у виробників); порушення авторських прав (працівники можуть використовувати Інтернет для завантаження неліцензійного ПЗ, баз даних, музики, фільмів, художніх творів). Бездумне впровадження Інтернету здатне завдати значної шкоди репутації та благополуччю підприємства.

Висновки. Система тотальної бюрократизації процедур і жорсткого контролю за їх дотриманням сама по собі не може забезпечити дієвого захисту бізнес-інформації. В основі будь-якої системи управління колективом в бізнесі лежить правильна мотивація його ключових гравців – менеджерів і провідних фахівців. Інформаційна безпека підприємства залежить як від управлінських якостей керівників, так і від досконалості інформаційних потоків на підприємстві і технологічного забезпечення. Окремим фактором впливу є доступ фірми до Інтернету та діяльність служби інформаційної та економічної безпеки підприємства, або менеджерів, які уособлюють ці функції. Важливим фактором небезпеки для підприємств є інфікування комп’ютерів. Інтернет є джерелом різноманітних загроз для комп’ютерної мережі та обладнання підприємства.

Література

1. Нікітін Л. Системний захист компанії від ворожого поглинання. // Фінансовий ринок України. – 2007 р. – №8. –с.35-36.
2. Сердюченко Н. Б. Інформаційне забезпечення підприємств в умовах невизначеності з врахуванням ризику // Економіка та держава. – 2007. - №1. –С. 46 – 47.
3. Гощинський А. Віртуальні кластери як об’єкти інтегрованого маркетингового управління. // Маркетинг в Україні. – 2009 р. – №2. – 47-50 с.
4. Гаман С. М. Формування інформаційного простору підприємства// Інвестиції: пратика та досвід. – 2007. - №16 –С. 40 – 42.
5. Гарбарчук В. І. Інтернет як новий клас інформативних систем і перспективи їх розвитку.// Актуальні проблеми економіки. – 2008 р. - №12(90). – С.192-203.

ІНФОРМАЦІЙНІ СИСТЕМИ АГРАРНОГО МЕНЕДЖМЕНТУ

Понятівський М .С
Науковий керівник: Гапчак Т.Г., асистент

Анотація. *Висвітлено теоретичні аспекти управління в аграрному секторі за допомогою інформаційних систем. У статті розглянуто поняття, суть, призначення управління та його роль в розвитку народного господарства країни.*

Ключові слова. *Управління, інфраструктура, трудові ресурси, сільське господарство, інформаційні*