Література

1 Васильев Г.А., Эриашвили Н.Д., Нагапетьянц Н.А. и др.; Основы маркетинга: Учеб. пособие, Под ред. Проф. Г.А.Васильева. – М.: ЮНИТИ-ДАНА, 2005.- 543 с.
2 Синяева И.М. Маркетинг в малом бизнесе: учеб. пособие для студентов вузов, обучающихся по специальности 080111 «Маркетинг» / И.М. Синяева, СВ. Земляк, В.В. Синяев. − М.: ЮНИТИ-ДАНА, 2006. – 287 с
3 Эклунд Клас. Эффективная экономика. Шведская модель. Пер. со швед. /Авт. предисл. В.В.Попов, Н.П.Шмелев; Науч. ред. А.М.Волков. – М.: Экономика, 1991. – 349 с.
4 Кардаш В. Я. Маркетингова товарна політика : Навч.-метод. посіб. для самост. вивч. дисц. / В. Я. Кардаш.– К.: КНЕУ, 2003.– 250 с.
5 Статистика оптової та роздрібної торгівлі [Електронний ресурс] : Мережа роздрібної торгівлі та ресторанного господарства підприємств на 1 січня 2013 року // Державний комітет статистики України. – Режим доступу : http://ukrstat.org/uk/druk/publicat/kat_u/2013/bl/04/bl_mr_12.zip. – Назва з екрану.
6 Філіп Котлер Основи маркетингу: Санкт-Петербург, 1999.- 523с.

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

Чайковська М.П., к.е.н., доцент
Азєєв А.С.

Одеський національний університет ім. І. І. Мечникова

Вступ. Ефективне управління питаннями інформаційної безпеки здобуває все більше значення для українських компаній у міру їх росту й просування на нові ринки товарів і послуг. Клієнтам важливо знати, що дотримується конфіденційність їх персональних і ділових даних. Інвесторам необхідна впевненість у тому, що бізнес та інформаційні активи компанії захищені. Ділові партнери очікують, що компанія буде функціонувати без збоїв, які можуть бути викликані помилками в роботі інформаційних систем, навмисними або ненавмисними діями персоналу, шкідливим програмним забезпеченням і іншими факторами.

Як правило, головними перешкодами на шляху забезпечення інформаційної безпеки є її невисока пріоритетність при розподілі ресурсів і бюджетні обмеження. Компанії нерідко виділяють єдиний бюджет на задоволення всіх потреб по інформаційних системах (апаратне й програмне забезпечення, зарплата, консультанти й т.п.), що сприяє розвитку тенденції виділяти основну частину коштів на підвищення продуктивності. При цьому нерідко питання інформаційної безпеки залишаються без уваги. Вибіркова й безсистемна реалізація коштів безпеки не зможе забезпечити необхідного рівня захисту. Щоб надійно захистити найважливішу ділову інформацію, компаніям необхідно інтегрувати питання фізичної й інформаційної безпеки в єдиний для всієї організації процес – процес керування інформаційною безпекою підприємства.

Основна частина. Управління інформаційною безпекою – це частина загальної управлінської системи, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу й удосконалення заходів в галузі інформаційної безпеки. Цю систему становлять організаційні структури, політика, дії щодо планування, обов'язки, процедури, процеси й ресурси [1, с.54].

Найбільш значимою метою більшості систем інформаційної безпеки є захист бізнесу та знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав і інтересів клієнтів. У той же час заходи інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну знаннями в компанії, оскільки це може поставити під загрозу розвиток організації.

Система керування інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації й

пов'язаних з нею процесів (створення, введення, обробки й виводу) і ряду інших цілей [2, с.127].

Досягнення заданих цілей можливо в ході розв'язку основних завдань, таких як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки й проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи керування ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролінг інформаційної безпеки на підприємстві [3].

Виділяють чотири стадії реалізації системи керування інформаційною безпекою: формування політики в області ризиків, аналіз бізнес-процесів, аналіз ризиків, формування цільової концепції. І дві стадії подальшого керування ризиками: звіти по ризиках, контроль ризиків.

Представлена на рис. 1. модель інформаційної безпеки – це сукупність зовнішніх і внутрішніх факторів і їх вплив на стан інформаційної безпеки в компанії та на забезпечення збереження ресурсів (матеріальних або інформаційних). Прямокутниками на малюнку представлені зовнішні й внутрішні фактори. Пунктирними стрілками зазначені напрямки керуючого впливу, а суцільними – природнього.

Необхідно чітко розуміти, що слід захищати й від яких погроз. Інформація й матеріальні ресурси, які необхідно захищати, називаються об'єктами захисту. До них ставиться мовна інформація, інформація, збережена й оброблювана за допомогою засобів зв'язку й інформатизації у вигляді різних носіїв інформації, документи на паперових носіях і т.д.

Побудова ефективної системи керування інформаційною безпекою – це не разовий проект, а комплексний процес, наплавлений на мінімізацію зовнішніх і внутрішніх погроз при обліку обмежень на ресурси й час.

Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності (рис. 2). Потім слід визначити поріг ризику – рівень загрози, при якому вона попадає в процес керування ризиками. Потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику.

З погляду процесного підходу систему інформаційної безпеки підприємства можна представити як процес керування ризиками (рис. 2). На даному малюнку показані узагальнені процеси верхнього рівня, а стрілками показані їхні входи й виходи.

Ціль будь-якого бізнес-процесу полягає в створенні виходу для одержання винагороди у вигляді іншого виходу. У цьому випадку виходом є виключення настання ризикової ситуації або мінімізація її наслідків, а винагородою – збереження матеріальних і фінансових ресурсів.

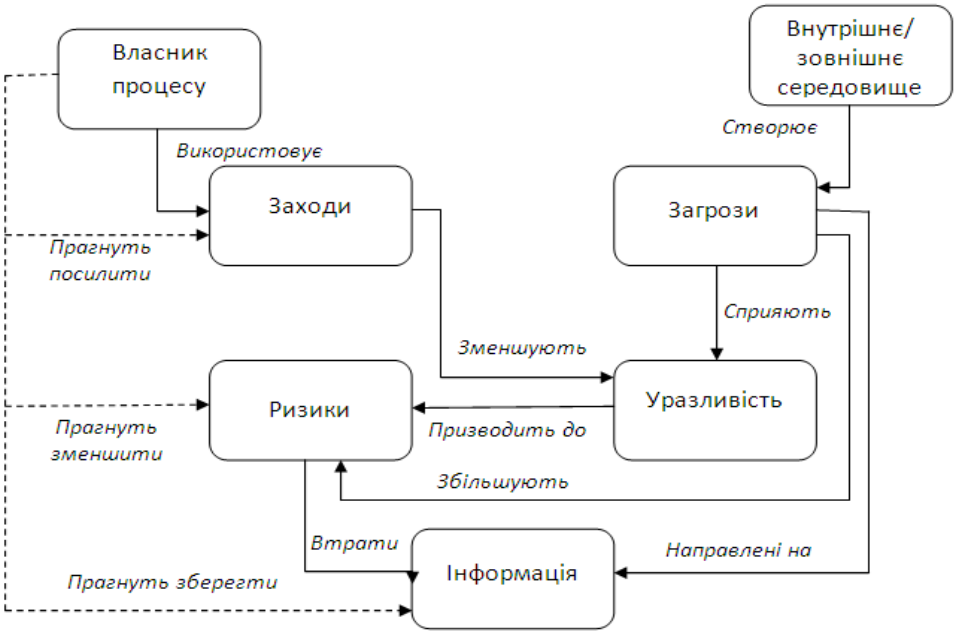

Рис 1. Модель системи інформаційної безпеки підприємства

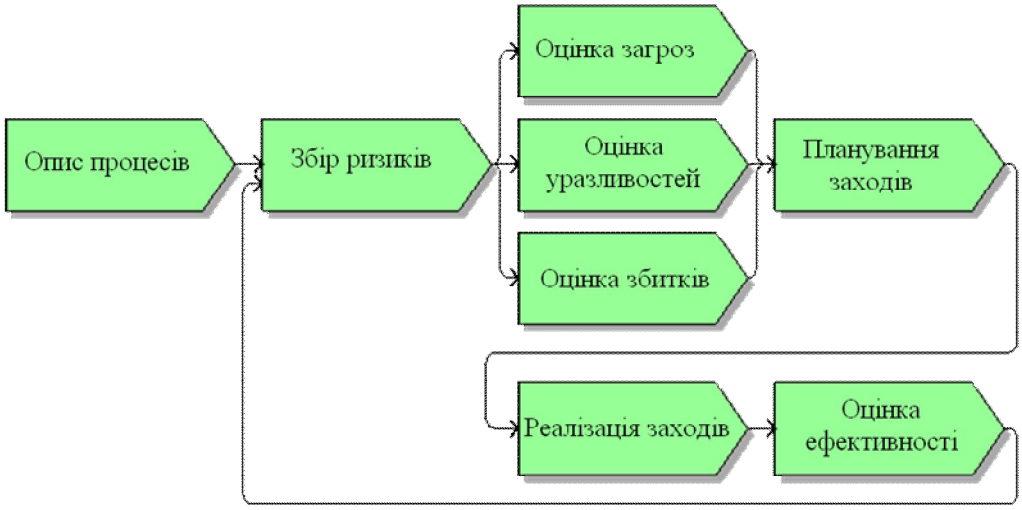

Рис. 2. Модель процесу управління ризиками для системи інформаційної безпеки підприємства

Немаловажна характеристика виходу – його затребуваність стороною, що не є його виробником. Іншими словами, на даний вихід повинен бути попит. Коли існують загрози – існує й попит на захист від них, а виходить, необхідно впроваджувати процес управління ризиками.

Висновки. На закінчення необхідно відзначити, що побудова ефективної системи інформаційної безпеки в компанії – це складний і безперервний процес, від уваги до якого залежить життєздатність бізнесу. Для грамотної побудови такої системи необхідно залучати до участі в їхньому створенні топ-менеджмент компанії, IT-фахівців, консультантів по даній тематиці, технічних фахівців.

Одним з важливих етапів побудови системи інформаційної безпеки є створення ефективного механізму керування доступом до інформації, тобто розв'язок питань як розмежування доступу, так і визначення методів доступу. При цьому необхідно розуміти, що методи доступу до інформації визначаються характеристиками самої інформації й на сьогоднішній день оцінюються для українських умов як: 3-5% структурованої інформації, 5-12% неструктурованої й 80-90% інформації на паперових і інших носіях. Якщо для зберігання й захисту структурованої інформації, а також доступу до неї на сьогоднішній день існують перевірені технології, то у випадку неструктурованої інформації вибір технологій суттєво обмежений, тоді як розв'язок питань керування паперовими архівами може виявитися непростим і витратним.

Хотілося б відзначити, що заходи щодо інформаційної безпеки можуть накладати обмеження, але треба чітко уявляти собі необхідність даних обмежень і намагатися знаходити компроміси.

Література

1 Малюк А.А. Теория защиты информации. – М.:Горячая линия – Телеком, 2012. – 184 с.
2 Петренко С. А. Управление информационными рисками.- М.: Компания АйТи; ДМК Пресс, 2014.- 384 с.
3 Чайковська М.П., Азєєв А.А. Управління системою інформаційної безпеки підприємства на базі ЛСП // М.П. Чайковська, А.А. Азєєв/ Моделювання та інформаційні технології в економіці: Монографія/За ред. Проф. Соловйова В.М. – Черкаси:Брама-Україна, 2014. – с.306-328.