Література

1. Стюарт Т.А. Интеллектуальный капитал. Новый источник багатства организаций / Т.А. Стюарт ; пер. с англ. В. Ноздриной. – М. : Поколение, 2007. – 368 с.

2. Кендюхов О.В. Оцінка ефективності управління клієнтським капіталом /О.В. Кендюхов [Електронний ресурс]//Ефективна економіка, 2012. - № 10. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=1493

3. Рябоконь Н.П.До питання формування клієнтоорієнтованості як ключової компетенції компанії. URL: http://www.economy.nayka.com.ua/?op=1&z=4522.

4. Blattberg, R. C., G. Getz, and J. S. Thomas (2001), Customer Equity: Building and Managing Relationships as Valued Assets. Boston, Massachusetts: Harvard Business School Press.

УДК 658.12

Горбашевська М.О.
кандидат економічних наук, доцент кафедри менеджменту

ХАРАКТЕРИСТИКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Ризик є практично у всіх сферах людського життя, тому точно і однозначно сформулювати його визначення неможливо. Ризик у підприємницькій діяльності має самостійне теоретичне і прикладне значення, як невід'ємна частина теорії і практики управління.

Під ризиком інформаційної безпеки розуміється ймовірність (можливість) настання несприятливої події через реалізацію загроз, спрямованих на уразливість інформаційних ресурсів з урахуванням можливих негативних наслідків [1].

Життя сучасної фірми неможливо уявити без добре розвиненої корпоративної системи,
щозабезпечуєпостійнийобмінділовоюінформацієюнезалежновідмісцезнаходженнякористувачів. Забезпечення безпеки діяльності (в широкому сенсі) будь-якої фірми реалізується шляхом створення системи захисту - продуманого комплексу заходів і засобів, спрямованих на виявлення, і ліквідацію різних видів загроз. При цьому кожен об'єкт захисту - будь то процес або засіб – має особливу специфіку, яка і повинна знайти своє відображення в загальній системі безпеки.

Спотворення інформації, необхідної для прийняття відповідальних бізнес-рішень, блокування процесу її отримання від партнерів або співробітників, впровадження в оборот неправдивої інформації, руйнування наявних ресурсів, що містять фінансову, маркетингову або технологічну інформацію, може завдати непоправної шкоди діловій репутації фірми, сприяти прийняттю помилкових рішень, що призводять до значних матеріальних збитків.

Інформація, що обробляється в корпоративних системах, особливо вразлива. Суттєвогопідвищенняможливостінесанкціонованоговикористанняабомодифікаціїданих, введення в оборот неправдивої інформації в даний час сприяють:

- Збільшення обсягів переданої і збереженої в комп'ютерах інформації;

- Зосередження в базах даних інформації різного рівня важливості і конфіденційності;
- Розширення доступу кола користувачів до інформації, що зберігається в базах даних, і до ресурсів обчислювальної мережі;
- Збільшення числа віддалених робочих місць;
- Широке використання для зв'язку користувачів глобальної мережі Internet і різних каналів зв'язку;
- Автоматизація обміну інформацією між комп'ютерами користувачів.

Суб'єкти, дії яких можуть призвести до порушення безпеки інформації, можуть бути як зовнішні: кримінальні структури; рецидивісти і потенційні злочинці; несумлінні партнери; конкуренти; політичні противники. Так і внутрішні: персонал установи; персонал філій; особи з порушеною психікою; спеціально заслані агенти.

Судячи з результатів міжнародного і українського досвіду, дії суб'єктів можуть призвести до ряду небажаних наслідків, серед яких стосовно до корпоративної системи можна виділити наступні:

1) крадіжку: технічних засобів (вінчестерів, ноутбуків, системних блоків); носіїв інформації (паперових, магнітних, оптичних та ін.); інформації (читання і несанкціоноване копіювання); коштів доступу (ключів, паролів, ключової документації та ін.).

2) підміну (модифікацію): операційних систем; систем управління базами даних (СКБД); прикладних програм; інформації (даних), заперечення факту відправки повідомлень; паролів і правил доступу.

3) знищення (руйнування): технічних засобів (вінчестерів, ноутбуків, системних блоків); носіїв інформації (паперових, магнітних, оптичних та ін.); програмного забезпечення (операційних систем, систем управління базами даних, прикладного програмного забезпечення); інформації (файлів, даних); паролів і ключової інформації.

Наслідками застосування таких технічних засобів, безпосередньо впливають на безпеку інформації, можуть бути:

1) порушення нормальної роботи: порушення працездатності системи обробки інформації; порушення працездатності зв'язку та телекомунікацій; старіння носіїв інформації та засобів її обробки; порушення встановлених правил доступу; електромагнітний вплив на технічні засоби.

2) знищення (руйнування): програмного забезпечення, ОС, системи управління базою даних (СУБД); коштів обробки інформації (за рахунок кидків напруги); приміщень; інформації (розмагнічуванням, радіацією і ін.); персоналу.

Стихійні джерела, що складають потенційні загрози інформаційній безпеці, як правило, є зовнішніми по відношенню до даного об’єкту, і під ними розуміються, перш за все, природні катаклізми: пожежі; землетрусу; повені; урагани; інші форс-мажорні обставини.

Таким чином, накладання загроз безпеці інформації на модель корпоративної системи дозволяє в першому наближенні оцінити їх небезпеку і методом виключення виділити найбільш актуальні для конкретного об’єкта захисту. Крім того, можна в першому наближенні оцінити обсяги необхідних робіт і вибрати магістральний напрям щодо забезпечення захисту інформації.

Література

1. Авдєєва Є.С., Чернов В.Г., Градусів Д.А. Методика експертної оцінки ризиків при впровадженні корпоративних інформаційних систем, 2010. №4. С. 5-11
2. Авдєєва Є.С., Чернов В.Г. Особливості впровадження КІС на підприємствах. Харків. 2010. №7. С. 176-177

УДК 338.487:659.1
Кислова Л. А.
кандидат економічних наук, доцент кафедри менеджменту

ГАЛУЗЕВИЙ АНАЛІЗ ЯК КЛЮЧОВИЙ КОМПОНЕНТ ПРОЦЕСУ ФОРМУВАННЯ СТРАТЕГІЧНОГО ПЛАНУ

Галузевий аналіз визначає ті характеристики у зовнішньому середовищі компанії, які найбільш суттєво впливають на стратегічне бачення та можливості організації. Сенс у тому, щоб отримати чіткі відповіді у визначені стратегічних питань. Потім ці відповіді будуть використані для чіткого розуміння стратегічної позиції компанії та визначення альтернатив її стратегічним діям.

У моделі «галузевої структури» зовнішнє середовище ототожнюється з галуззю (галузями), в якій діє фірма, тому об'єктом галузевого аналізу виступає галузь економіки у вигляді сукупності підприємств, які виробляють однотипну продукцію або надають схожі послуги та конкурують між собою на споживчому ринку. Галузевий аналіз являє собою структуровану оцінку галузі промисловості, її елементів, учасників і відмінних ознак [1].

Мета проведення галузевого аналізу полягає в дослідженні привабливості галузі та виявленні ринкових сил, які забезпечать підприємству конкурентні переваги. Завдяки цьому аналізу можна зрозуміти галузеву структуру, напрямки її розвитку, унікальні можливості та існуючі загрози, визначити ключові фактори успіху та сформулювати на основі цих факторів ринкові стратегії поведінки [2]. Галузевий аналіз є ключовою первинною ланкою процесу формування стратегічного плану.

Виділяють два напрямки галузевого аналізу:

1) дослідження економічних характеристик, які превалюють в галузі;

2) визначення рушійних сил в галузі.

Розглянемо більш детально виділені напрямки галузевого аналізу. При аналізі галузі та конкурентного середовища, по-перше, важливо визначити превалюючи економічні характеристики галузі:

1) розмір ринку або поле конкуренції (місцеве, регіональне, національне, глобальне);

2) кількість конкурентів, їх відносний розмір та ступінь концентрації конкуренції. В галузі, де фірми займають свої ринкові ніші і не мають великої ринкової частки, спостерігається жорсткіша конкуренція, ніж там, де є лідируюча компанія. У науковій літературі, як правило, виділяють такі типи галузей: *консолідовані галузі* - характеризуються існуванням декількох великих підприємств-виробників, і якщо хоча б одна компанія покидає галузь чи змінює свої стратегічні пріоритети, це призводить до швидкої зміни і перерозподілу конкурентних позицій; *фрагментарні галузі* – характеризуються великою кількістю малих підприємств з високим рівнем диференціації продукту, з вільним входом до галузі і відсутністю ефекту масштабу. Однак, розвиток галузі може призводити до зміни її типу.