1. Закон України «Про залізничний транспорт» від 10.01.2002 № 2921 – ІІІ.
2. Кулаєв Ю.Ф. Економіка залізничного транспорту: навч. посіб./ Кулаєв Ю.Ф. – Ніжин: ТОВ Видавництво «Аспект-поліграф», 2006. – 232 с.
3. Ансоф И. Стратегическое управление / И. Ансоф; пер. с анг. (науч. ред. и авт. предисл. Л.И. Евенко). – М.: Экономика, 1989. – 519 с.
4. Авдашева С.Б. Теория организации отраслевых рынков / С.Б. Авдашева, Н.М. Разанова. – М.: ИСП «Издательство магистр», 1998. – 360 с.
5. Економічна енциклопедія: у трьох томах. / редкол.: С.В. Мочерний (відп. ред.) та ін. – К.: Видавничий центр «Аркаделія», 2002. – Т. 3 – 952 с.
6. Макаренко М.В. Основи управління економічними процесами на залізничному транспорті України: [монографія] / М.В. Макаренко – К.: КУЕТТ, 2003. – 478 с.
7. Макаренко М.В., Реформування бухгалтерського обліку на залізничному транспорті України/ М.В. Макаренко, Ю.М. Цвєтов, Н.С. Соколовська. – К.: ВАТ ІКТП – Цент, 2002. – 532 с.
8. Перелік робіт і послуг, що належать до основної діяльності залізничного транспорту, затверджений постановою Кабінету Міністрів України від 30.03.2011 р. № 316 // Бухгалтерія, № 22 (957) від 30.05.11 р. – С. 15-17.
9. Стандартизація послуг. Основні положення. ДСТУ 3279 – 95.– [Чинний від 1997-01-01]. – К: Держспоживстандарт України, 1977. – 11 с. – (Національний стандарт України).

651.011.42

Поповенко Н.С., к.е.н., професор,
Полуніна Г.О., магістр,
Одеський Національний політехнічний університет

ІНФОРМАЦІЙНА БЕЗПЕКА НА ПІДПРИЄМСТВАХ МАЛОГО БІЗНЕСУ

Підприємницька діяльність тісно пов’язана з отриманням, накопиченням, зберіганням, обробкою та використанням інформації. Втрата певної інформації може привести підприємця навіть до банкрутства. Разом з тим захисту підлягає не вся інформація, а тільки та, що має цінність для підприємця [1]. При цьому досвід ведення приватного бізнесу напряму впливає на прийняття рішення про захист інформації.

На сучасному етапі розвитку підприємництва конкурентна боротьба неможлива без захисту власної інформації й отримання інформації про конкурентів. Підприємництво й конкуренція взаємно пов’язані, а це означає, що підприємець повинен бути захисником своїх секретів, та в той же час здобувати, купувати чужі секрети, що також захищаються [2]. Така парадоксальна ситуація наявна сьогодні і в малому бізнесі. Для захисту інформаційних потоків підприємцю варто використовувати усі можливі правові й спеціальні заходи.

Внаслідок швидкого розвитку й широкого використання інформаційних технологій й систем при веденні бізнесу, керівники малих підприємств більш серйозно розглядають питання, що пов’язані із забезпеченням інформаційної безпеки, як одним із важливіших напрямів діяльності фірми нарівні із закупівлями, управлінням матеріальними потоками, плануванням виробництва тощо. Заходи, що вживаються для реалізації цього напряму, й бюджет, який виділяється для цього, повинні постійно переглядатись відповідно до наявних потреб й можливостей компанії [3].

Сучасні малі підприємства застосовують інформаційні технології для удосконалення методів роботи, що як наслідок викликає зміни організаційної структури підприємства, розробку нового організаційного зв’язку, який раніше був неможливим. Тому інформаційні технології є досить перспективним та ефективним напрямом для капіталовкладень та потребують захисту й забезпечення надійності роботи. Принципову схема розбудови та взаємодії основних елементів інформаційної системи організації наведено на рис. 1:

Витік інформації із інформаційної системи організації – одна з головних проблем малого бізнесу. В якості причин цього процесу слід виділити:

- крадіжка інформації конкурентами;
- розголос інформації співробітниками що звільнилися або яких звільнили;
- «економія» коштів на захист власної інформаційної системи;
- втрата інформації через слабке володіння комп’ютером, недостатність теоретичних професійних знань в роботі з комп’ютером;

- відсутність «захисту», не кажучи вже про декілька його ступенів.

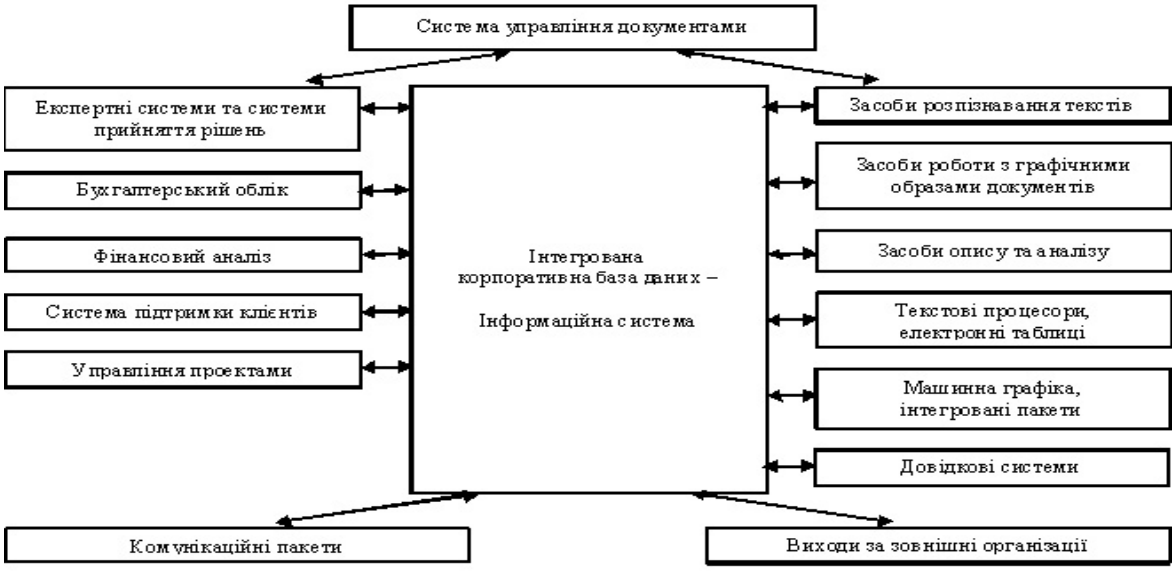

Рис. 1. Інформаційна система організації

Виходячи з вищевикладеного, підприємець має чітко регламентувати доступ до інформації співробітників. При звільненні перевірити цілісність бази даних та змінити паролі.

Підприємці малого бізнесу знають про проблему, але як її вирішити та варто чи її вирішувати, поки що не визначилися. Це може свідчити про їх низьку професійну компетентність в роботі з інформацією.

Знання теорії проблематики захисту інформації дозволить підприємцям правильно організувати її охорону. Для цього кожен підприємець має визначити, яка інформація повинна становити комерційну таємницю та узаконити її у «Переліку відомостей, що складають комерційну таємницю підприємства». До «Переліку» може входити інформація технологічного характеру: конструкторська документація; аналіз технологічних випробувань продукції; «ноу-хау», авторські права й патенти; конструкційні характеристики виробів; унікальні вимірювальні комплекси та прилади, устаткування, обладнання, що використовується на підприємстві.

Практика свідчить, що комерційну таємницю може та повинна мати також така інформація: відомості про укладені контракти та ті, що плануються; відомості про постачальників, реальних та потенційних клієнтах; обзори ринку; маркетингові дослідження, які здійснені спеціалістами фірми; інформація про конфіденційні перемовини.

Частіш за все захист інформації сприймається як забезпечення безперервності внутрішніх бізнес-процесів й безпека обміну даними з клієнтами при використанні інформаційних систем.

З точки зору загроз малий бізнес не суттєво відрізняється від крупного, й вірогідність витоку конфіденційної інформації з невеликої компанії така ж, як і з крупного підприємства. Одначе вартість витоку для малого бізнесу може бути більше, ніж для «гіганта»: що для крупної компанії велика неприємність, то для невеличкої може значити закриття бізнесу взагалі.

Малим фірмам, як і крупним підприємствам, є що захищати:

1. Майже 100% потребують захисту персональних даних.
2. Більш ніж 70% хотіли б забезпечити безпеку клієнтських баз даних.
3. Більш ніж 60% занепокоєні цілісністю даних про фінансовий стан компанії.
4. Ще 50% – за бізнес-плани компанії.

Захист від витоку інформації для малого бізнесу життєво не менш важливий, ніж для крупних підприємств.

Українські компанії сегменту малого бізнесу, як правило, не мають в штаті виділеного офіцера інформаційної безпеки чи служби інформаційної безпеки. Частіше за все процедури, що регламентують ці питання, відсутні. Рішення про покупку продуктів щодо інформаційної безпеки приймають IT-менеджери чи самі директори компаній. При цьому 96% суб'єктів малого

підприємництва обізнані щодо проблеми витоку конфіденційної інформації та про існуючі для вирішення цієї проблеми засоби захисту.

Варто зауважити, що на відміну від великих фірм, малий бізнес не володіє достатніми фінансовими можливостями для того, щоб самостійно забезпечити повний захист своєї комерційної інформації. Малим компаніям потрібна, перш за все, доступна за ціною, легка у бюджетному обґрунтуванні система захисту інформації. Нажаль на сьогоднішній день поки що нема кому зробити таку пропозицію, яка була б адекватна попиту, й зайняти вільну ринкову нішу.

Які ж засоби інформаційної безпеки використовуються малими підприємствами. За даними аналітичної агенції «B2B Research» виявилось, що:

1) 100% компаній малого бізнесу користуються антивірусним захистом;

2) 90% обмежують доступ співробітників до файлів й права співробітників на встановлення програм на робочих машинах;

3) більш ніж 70% компаній обмежують права користувачів на копіювання інформації;

4) близько 20% використовують багатофункціональний інтегрований захист.

У більшості випадків підприємці не мають розуміння про те, що представляє собою спеціалізований засіб захисту від витоків та як саме він захищає конфіденційні данні від витоку.

Цікавим є той факт, що при досить слабкому розумінні саме спеціалізованих систем, IT-менеджери компаній бачать безсумнівні вигоди від їх провадження, а саме:

- спрощення роботи відповідальних за ІБ співробітників,
- моніторинг ситуації з інформаційною безпекою в компанії,
- відсутність інцидентів чи можливість швидкого реагування на них.

Основними факторами, що підштовхують компанії малого бізнесу до придбання інтегрованих рішень захисту інформації, є зростання ризиків та економічне обґрунтування покупки, а також необхідність захисту персональних даних.

Забезпечення інформаційної безпеки – одна з головних задач сучасного малого підприємства. Загрозу можуть представляти не лише технічні збої, але й неузгодженість даних різних облікових систем, що зустрічається чи не у кожній другій компанії, а також необмежений доступ співробітників до інформації. Ключовим у зазначеній проблемі є виявлення й мінімізація інформаційних ризиків [4].

Інформаційні ризики – це небезпека виникнення збитків в наслідок застосування компанією інформаційних технологій. Інакше кажучи, інформаційні ризики пов'язані із створенням, передачею, збереженням та використанням інформації за допомогою електронних носіїв чи інших засобів зв'язку.

Інформаційні ризики можна розділити на дві категорії:

1. Ризики, які викликані витоком інформації й використанням її конкурентами чи співробітниками з метою, що може нашкодити бізнесу.

2. Ризики технічних збоїв роботи каналів передачі інформації, що може призвести до збитків.

Робота щодо мінімізації таких ризиків полягає у попередженні несанкціонованого доступу до даних, а також аварій та збоїв обладнання. Процес мінімізації інформаційних ризиків слід розглядати комплексно: спочатку виявляються можливі проблеми, а потім визначається, якими чином їх можна вирішити. Для цього створюються карти ризиків, здійснюється збір експертних думок тощо.

Виявити найбільш критичні інформаційні ризики можна, якщо відповісти на наступні питання:

– чи здатна компанія контролювати доступ до інформаційних систем, у яких формується й зберігається фінансова звітність;

– чи забезпечені клієнти компанії необхідною інформаційною підтримкою, тобто чи можуть вони у потрібну мить додзвонитися до компанії чи зв'язатися електронною поштою;

– чи зможе компанія у стислий термін інтегрувати наявні технології роботи з інформацією в системи підприємства, що є об'єктом злиття чи придбання;

– чи забезпечений захист інтелектуальної власності компанії та її клієнтів;

– чи має компанія чіткий алгоритм дій у критичній ситуації (у випадку збоїв у роботі комп'ютерних мереж чи вірусної атаки);

– чи відповідає спосіб роботи інформаційних систем загальним задачам компанії.

Точно визначити можливу шкоду від більшості інформаційних ризиків доволі складно, але оцінити їх можливо. Витрати на відновлення роботи інформаційної мережі компанії складаються із заробітної плати IT-спеціаліста за період наладки мережі чи усунення збою, операційних витрат, пов'язаних із зупинкою роботи підприємства, а також із середнього прибутку, який фірма недоотримає за цей час [5].

Як свідчить досвід багатьох українських компаній сегменту малого бізнесу, найбільш успішні стратегії попередження інформаційних ризиків базуються на трьох основних правилах:

1. Доступ співробітників до інформаційних систем та документам компанії повинен бути різним залежно від важливості та конфіденційності змісту документу.

2. Компанія повинна контролювати доступ до інформації й забезпечувати захист уразливих місць інформаційних систем.

3. Інформаційні системи, від яких напряму залежить діяльність компанії (стратегічно важливі канали зв'язку, архіви документів, комп'ютерна мережа), повинні працювати безперебійно навіть у випадку кризової ситуації.

Робота щодо мінімізації інформаційних ризиків розділяється на організаційну й технічну.

Організаційні заходи пов'язані із обмеженням доступу до даних. Для цього вся інформація класифікується на загальнодоступну, для службового користування й секретну. Крім цього, зміст інформаційних потоків можна розділити за призначенням:

- данні, що циркулюють всередині робочої групи (за певним проектом);
- данні, які призначені для виконавців та керівників підрозділів;
- плани стратегічного розвитку.

В результаті утворюється матриця інформаційних потоків, кожному рівню якої відповідає певний рівень доступу.

Ґрунтуючись на зазначених регламентах, кожний керівник малого підприємства може сформувати для своїх підлеглих посадові інструкції й призначає відповідальних за дотримання інформаційної безпеки.

Технічна робота щодо забезпечення інформаційної безпеки полягає у дублюванні важливих функцій, від яких залежить цілісність та збереження інформації, неперервність роботи компанії. З метою мінімізації ризику збоїв, варто використовувати техніку від надійних виробників. Витрати на неї окупуються, бо збиток від простою інформаційних систем за декілька годин багаторазово перевищує їх вартість, а втрата інформації може взагалі паралізувати роботу підприємства.

Забезпечення інформаційної безпеки – це, перш за все, питання ефективності витрачених коштів, враховуючи це, витрати на захист інформації не повинні перевищувати суми можливих збитків [6].

Оскільки будь які витрати на попередження ризиків повинні бути обґрунтованими, необхідно обов'язково розраховувати їх економічну ефективність.

З метою забезпечення необхідного захисту від інформаційних ризиків та контролю безпеки варто здійснити такі заходи:

1. Визначити коло осіб, що відповідатимуть за інформаційну безпеку, створити нормативні документи, в яких будуть описані дії персоналу компанії, що направлені на попередження IT-ризиків, а також забезпечити резервування потужностей для роботи у критичній ситуації.

2. Розробити єдині стандарти інформаційних систем в межах організації, тобто перейти до єдиних звітних форм, а також єдиним правилам розрахунку показників, що будуть застосовуватися у всіх програмних продуктах компанії, які використовуватимуться для цієї мети.

3. Класифікувати данні за ступенем конфіденційності та обмежити права доступу до них.

4. Відслідковувати те, щоб будь які документи, що обертаються всередині організації, створювалися за допомогою систем, централізовано встановлених на комп'ютерах. Установка інших програм повинна санкціонуватися, інакше ризик збоїв та вірусних атак різко зросте.

5. Впровадити засоби контролю, що дозволять відслідковувати стан усіх корпоративних систем: у випадку несанкціонованого доступу система повинна автоматично заборонити вхід чи сигналізувати про небезпеку, щоб персонал міг вжити заходів.

Разом з тим, необхідно підготуватися до наслідків можливих кризових ситуацій та описати дії компанії щодо виходу з кризи. Для цього слід:

- проаналізувати сценарії проникнення сторонніх осіб чи таких, що не мають відповідних повноважень, співробітників компанії до внутрішньої інформаційної мережі, а також здійснити учбові заходи з метою відпрацювання моделі поведінки співробітників, що відповідальні за інформаційну безпеку, в кризових ситуаціях;
- розробити варіанти вирішення проблем, пов'язаних з кадрами, включи вихід із складу компанії ключових співробітників;
- підготувати запасні інформаційні потужності, а також резервні мережі зв'язку.

Якщо бізнес компанії у багатьох випадках залежить від стану її інформаційних мереж, необхідно назначити відповідального за розробку, впровадження та контроль виконання корпоративних правил, що направлені на зниження інформаційних ризиків.

Обов'язковою умовою успішного ризик-менеджменту в галузі інформаційних технологій є його безперервність. Тому оцінка інформаційних ризиків, а також розробка та оновлення планів щодо їх мінімізації повинні здійснюватися з певною періодичністю. Така робота щодо забезпечення інформаційної безпеки повинна бути комплексною та продуманою.

Література

1. Касперская Н. Защита от утечек информации в малом бизнесе / Н. Касперская. [Електронний ресурс]. – Режим доступу: http://www.rae.ru
2. Аппенянский А.И. Человек и бизнес. Повышение психологической надежности. / А.И. Аппенянский. – М.: Барс, 2005. – 228 с.
3. Смольков Г.В. Предпринимательство и риск: опыт и проблемы / Г.В. Смольков, М.И. Левітан // Социально-политический журнал. – 2008. – №7. – С. 101-108.
4. Мишель М. Управление информационными рисками / М. Мишель // Финансовый директор. – 2010. – № 7. – С. 37-48.
5. Терентьев С. Оценка защищенности информационных ресурсов / С. Терентьєв. [Електронний ресурс]. – Режим доступу: http://www.daily.sec.ru.
6. Белоус Ю. Организация безопасности хозяйствующих субъектов / Ю. Білоус, С. Витновская // Ведомости СПб. – 2006 – № 62 (1589). – С. 52-68.

338.1 *Бакало Н.В., к.е.н., доцент,*
Полтавський національний технічний університет імені Юрія Кондратюка

ІНВЕСТИЦІЙНІ АСПЕКТИ РОЗВИТКУ ПІДПРИЄМСТВ МАЛОГО БІЗНЕСУ

Пошук інвестицій є однією з найскладніших проблем, з якою зіштовхуються підприємці. Інвестори малого бізнесу часто беруть участь в різних виставках або конференціях, на яких підприємці діляться своїми бізнес-ідеями чи досвідом розвитку підприємства. Разом з тим, наразі вони вкрай неохоче надають грошові кошти на розвиток маловідомих підприємств. Активну допомогу в пошуку інвесторів для проектів малого та середнього бізнесу надають різні асоціації підтримки, які забезпечують гарантії, необхідні для отримання позик на розвиток підприємства.

Вагомий внесок у розвиток підприємств малого бізнесу зробили відомі вчені Г. Козаченко, І. Маркіна, О. Виноградова, С. Ніколенко, З. Варналій, Г. Білоусов, В. Сизоненко, С. Реверчук та інші. Разом з тим,низка проблем, пов'язаних з інвестиційними аспектами розвитку керівників малого бізнесу, є недостатньо розробленими.

Реальне сприяння розвитку підприємництва в Україні, передбачає формування зрозумілих та економічно виправданих передумов і правил підприємницької активності. На рівні суспільства, на нашу думку, повинна бути сформована досконала інфраструктура підтримки підприємницької активності.

Тому, за мету статті ми ставимо обґрунтування теоретичних та практичних аспектів пошуку та залучення інвестицій у розвиток малого бізнесу.

Практика господарювання свідчить, в Україні на даний час залишилися, по суті, поодинокі інвестори: банки, венчурні фонди тощо. За великим рахунком, малий бізнес в Україні взагалі не становить інтересу для великих закордонних компаній, окрім вкладень, зроблених особисто. Венчурні фонди та інституційні інвестори (ЄБРР, МФК) взагалі не цікавляться проектами вартістю менше $ 500 тис і не підкріпленими успішною практикою бізнесу.

Проведений аналіз визначив, що зниження інвестицій відбувається нерівномірно: на 41 % зменшився їх обсяг в розвинених країнах і на 39% - до держав з економікою, що розвивається. Найменше (на 2,6%) постраждав Китай, зате в США занепад склав 57%. Рекордсменом за темпами зниження обсягу інвестицій стала Велика Британія – на 92,7%. Інвестиції в Бразилію скоротилися на 49,5%, Індію - на 19%, Росію - на 41,1%. Втім, є й позитив: Німеччина (+40,7%), Африка (+36,2%).

Україна на цьому фоні не показала нічого іншого. Пріоритетними галузями для фондів прямих інвестицій є АПК, харчова промисловість, телекомунікації, енергозбереження та імпортозаміщення,