УДК: 657.1:004.056.5

Боримська К.П.
к.е.н., доц., докторант кафедри бухгалтерського обліку
Житомирський державний технологічний університет,
м. Житомир, Україна

НАПРЯМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ОБЛІКОВИЙ ВИМІР

Управління сучасним підприємством нерозривно пов'язане з реалізацією концепції інформаційної безпеки. В умовах стрімкого розвитку інформаційно-комп'ютерних технологій й використання переваг мережі Інтернет, не лише полегшується доступ до різних інформаційних ресурсів, а й збільшуються обсяги поширення інформації, забороненої для розголошення, зі статусом комерційної й таємної, зростають витрати суб'єктів господарювання від витоку такої інформації, від зламу інформаційних мереж, рейдерсько-хакерських дій, що знижує не лише рівень прибутковості підприємства, але й надійності й соціальної значущості бізнесу.

За таких умов зростає значення побудови системи інформаційної безпеки підприємства, максимально налаштованої на особливості управління інформаційними потоками сучасних суб'єктів господарювання. Під інформаційними потоками автори розуміють сукупність умов формування, систематизації, руху й використання економічної інформації на мікро- та макрорівнях, яка в цілому в процесі функціонування покликана забезпечити безпеку національної економіки. Концентруючись на мікрорівні, під управлінням інформаційними потоками розуміємо процес реалізації своїх функцій взаємопов'язаних дій (починаючи з визначення потреби в інформації, подальшої її збору, систематизації, руху й використання, та завершуючи зворотнім зв'язком – відтворенням та обміном інформацією). На кожному етапі такого процесу можливі об'єктивні й суб'єктивні втрати інформаційних потоків.

Проф. І.В. Пенькова та асп. О.І. Левченко[1] до неминучих втрат інформаційних потоків на рівні держави відносять: недосконаліть законодавчої бази, низька швидкість і недосконаліть ІК-мереж, висока вартість інформації на міжнародних сайтах; на рівні регіону – відсутність певних повноважень у місцевих органів влади, несвоєчасність інформування регіонів про зміни у законах, висока вартість підводу ІК-мереж; на рівні підприємства – висока вартість ліцензійного програмного забезпечення, несвоєчасність інформування державними інститутами, висока вартість ІК-мереж і комп'ютерного обладнання. Втрати від неефективної діяльності суб'єктів інформаційних потоків (суб'єктивних) дослідники позиціонують наступні: на макрорівні – неузгодженість дій державних інститутів, високі податки, недостатність фінансування НДДКР; на мезорівні – неузгодженість дій інститутів влади різних рівнів, неініціативність керівників, відсутність доступу до ІК-мереж; на мікрорівні – неналагодженість каналів зв'язку та комунікацій, трансакційні витрати неефективних управлінських рішень, несвоєчасна реакція на зміни зовнішнього середовища.

Глобальне дослідження аналітичного центру Info Watch, проведене доц. С.В. Кавуном[2], засвідчило, що за 2011-2012 рр. було зафіксовано 249 інцидентів витоку інформації з обмеженим доступом (витоки охопили більше 100 млн. людей). 29 % витоків інформації здійснюється через мережу (в т.ч. Інтернет), 25 % – через мобільні носії інформації, 14 % – не встановлено, 12 % – через стаціонарний комп'ютер або диск, 9 % – через паперовий документ, по 4 % – через електронну пошту, факс та інше, 3 % – через архівну копію. Для випадкових витоків мобільні носії інформації (CD, DVD, флеш-носії) випереджають витоки через мережу Інтернет (30 % проти 24 %). При цьому за даними світової статистики, втрата тільки 20 % інформації веде до руйнування 65 % підприємств[3].

Вищепредставлені канали витоку інформації реалізуються через такі заходи несанкціонованого доступу: підслуховування, візуальне спостереження, розкрадання, копіювання, підробка, незаконне підключення, перехоплення, фотографування. Тобто із розвитком науково-технічного прогресу не лише удосконалюються засоби матеріального забезпечення ведення бізнесу, але й розширюються технології витоку інформації, як важливого стратегічного ресурсу в конкурентній боротьбі.

За таких умов постає необхідність розробки методичних аспектів побудови адекватної системи захисту інформації на підприємстві, які сприяють реалізації комплексної системи інформаційної безпеки підприємства.

---

[1] Пенькова І.В. Інформаційні потоки в управлінні економічною безпекою держави / І.В. Пенькова, О.І. Левченко // Сучасні перспективи розвитку систем економічної безпеки держави та суб'єктів господарювання: Монографія / За ред. проф. Мігус І.П. – Черкаси: ТОВ «МАКЛАУТ». – Черкаси, 2012. – 636 с. – С. 573

2 Kavun S. Statistical analysis in area of economic and information security. ES INFECO: International research portal of information and economic security, 2011-2012 / [Electronic resource]. – Access mode: http://www.infeco.net

3 Білокомірова Я.М. Інформаційне забезпечення економічної безпеки підприємницької діяльності / Я.М. Білокомірова // Вісник економіки транспорту і промисловості. – 2010. – № 29. – С. 308.

Режим інформаційної безпеки має охоплювати як організаційні (розробка положення про інформаційну безпеку з визначенням цілей інформаційної безпеки та способів їх досягнення, закріплення рівнів доступу до інформації, в тому числі, з обмеженим доступом (конфіденційної), порядок видачі особистих кодів, карток, паролів доступу до певних ділянок та носіїв інформації, контроль за входом до системи та складання звіту робочого часу, ознайомлення їх з правилами поведінки з конфіденційною інформацією та відповідальністю за її санкціоноване та несанкціоноване розголошення персоналом підприємства), так і програмно-технічні складові (обов'язкове використання засобів ідентифікації і аутентифікації об'єктів та суб'єктів, засобів резервного копіювання, антивірусного та парольного захисту, міжмережевих екранів, шифрування даних і т.д.). Заходи із забезпечення інформаційної безпеки, з одного боку, мають бути спрямовані на охорону конфіденційної інформації (зокрема, усунення «жучків», запобігання несанкціонованому доступу до локальних комп'ютерних мереж тощо), з іншого – забезпечувати пошук даних про конкурентів, партнерів, контрагентів, які слугують запобіганню виникненню можливих ризикових ситуацій в діяльності суб'єкта господарювання, викликаних недобросовісною конкуренцією, рейдерськими схемами захоплення бізнесу тощо.

Крім важливості режимної складової в концепції інформаційної безпеки все ж таки визначальне місце відіграє налагоджена система управління інформаційними потоками сучасних суб'єктів господарювання, основна частина яких формується в системі бухгалтерського обліку, яка, з точки зору забезпечення належного рівня інформаційної безпеки підприємства, виконує подвійну роль. З одного боку – бухгалтерська інформація є основним достовірним, документально підтвердженим, джерелом даних для проведення розрахунків з контрагентами, визначення резервів діяльності підприємства, достатності коштів для придбання програмно-технічних заходів інформаційного захисту тощо. З іншого боку, сама підсистема бухгалтерського обліку в системі управління є фактором загроз інформаційній безпеці суб'єкта господарювання, адже реєстрація в обліку недостовірної інформації, маніпуляції, приховування інформації й шахрайство зі сторони керівництва та головного бухгалтера, отримання доступу до облікової інформації сторонніх осіб, значно знижує рівень захищеності підприємства від можливих законних та незаконних дій суб'єктів як внутрішнього, так і зовнішнього середовища діяльності підприємства.

Так, згідно з опитуванням 250 осіб-представників 100 промислових підприємств, які входять до Українського союзу промисловців та підприємців, проведеним Л.В. Гнилицькою[4], найбільша кількість респондентів (власників та менеджерів) серед загроз, які пов'язані з кругообігом обліково-аналітичної інформації та справляють найсуттєвіший вплив на стан економічної безпеки виробничого підприємства, виділили низьку пристосованість обліково-аналітичних даних до потреб економічної безпеки (30 % власників та 23 % менеджерів) і недостовірність інформації, представленої у звітності контрагентів (27 % власників та 35 % менеджерів).

Крім того, на сьогодні у вітчизняній системі бухгалтерського обліку відсутні законодавчо закріплені організаційно-методичні розробки й рекомендації щодо відображення всіх фактів господарського життя, які мають різний рівень ймовірності виникнення й впливу на господарську діяльність підприємства в умовах невизначеності та ризику підприємницької діяльності.

За таких умов для побудови комплексної системи інформаційної безпеки підприємства, адекватної сучасним умовам господарювання, необхідним виступає ранжування та обґрунтування кожного виду загроз інформаційній безпеці підприємства, яку несуть в собі інформаційні потоки системи бухгалтерського обліку, що обслуговують усі бізнес-процеси сучасного суб'єкта господарювання в умовах ризику та невизначеності, що і слугує перспективою подальших досліджень.

БОРИМСЬКА Катерина Павлівна

К.е.н., доцент, докторант кафедри бухгалтерського обліку Житомирського державного технологічного університету.

Наукові інтереси: 1) проблеми облікового забезпечення фінансово-економічної безпеки підприємства; 2) проблеми побудови системи рахунків бухгалтерського обліку в ретроспективі.

Телефон: (067)365-74-40

E-mail: mavka123@ukr.net

[4] Гнилицька Л.В. Проблеми та шляхи вдосконалення обліково-аналітичного забезпечення економічної безпеки підприємства / Л.В. Гнилицька // Бухгалтерський облік і аудит. – 2011. – № 10. – С. 23.