2. Наказ Міністерства аграрної політики України ”Про затвердження Методичних рекомендацій з планування, обліку і калькулювання собівартості продукції (робіт, послуг) сільськогосподарських підприємств” N 132 від 18.05.2001 (із останніми змінами від 31.10.2005 Наказу N 589);
3. Методичні рекомендації щодо застосування регістрів журнально-ордерної форми обліку для сільськогосподарських підприємств затверджені Наказом Міністерства аграрної політики України від “ 4 ” червня 2009 р. № 390

***Анжеліка Крутова**, к.е.н., доцент*
Харківський державний університет харчування та торгівлі
м. Харків, Україна

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У РОЗВИТКУ ЕЛЕКТРОННОГО СЕКТОРУ ЕКОНОМІКИ

Зміна світогляду, яка відбулася на межі третього тисячоліття, зумовила революція в області комунікацій та інформації. Твердження Ротшильда про те, що хто володіє інформацією, той володіє світом, сьогодні є справедливим як ніколи. Масова комп’ютеризація, впровадження і розвиток новітніх інформаційних технологій призвели до вражаючих змін технології освіти, бізнесу, промислового виробництва і наукових досліджень. Даний процес супроводжується появою у складі життєво важливих інтересів особистості та суспільства сукупності нових потреб, задоволення яких надійно забезпечить здійснення та можливість прогресивного розвитку всіх суб’єктів соціально-економічних відносин. Звичайно процеси інформатизації різних аспектів людської діяльності вимагають перегляду ключових засад їх безпеки.

Згідно зі статтею 1 ЗУ «Про основи національної безпеки України» безпека визначається, як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам …». Не завжди під «захищеністю … інтересів» малася на увазі також безпека інформаційна. Однак, у сучасних умовах інформаційна сфера розглядається як системоутворюючий чинник життя суспільства і активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України. Інформатизація, яка є визначальним фактором впливу на розвиток суспільно-економічної формації, обумовлює істотну залежність національної

безпеки України від забезпечення інформаційної безпеки і у ході подальшого технічного прогресу така залежність неухильно зростатиме.

Сьогодні проблеми інформаційної безпеки хвилюють практично всіх: силові структури, органи влади, юридичних та фізичних осіб. Однак, особливої актуальності функції інформаційного захисту набувають для підприємств електронної комерції, які окрім інформації суто економічного характеру, що становить комерційну таємницю підприємства, зберігають у своїх базах персональні дані високого ступеня секретності, наприклад, платіжні реквізити своїх покупців. Несанкціоноване одержання такої інформації є найбільш спокусливим для потенційних порушників інформаційної безпеки господарюючого суб'єкта. Законом «Про захист персональних даних» запроваджено, що використання персональних даних власником бази здійснюється у разі створення ним умов для захисту цих даних. Тобто, створення безпечних умов збирання, зберігання та обробки такої секретної інформації покладається на власника бази даних – підприємство електронної комерції і є однією з умов його функціонування.

Законодавство про захист персональних даних складають Конституція України, Закон України «Про захист персональних даних», інші закони та підзаконні нормативно-правові акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України. Однак темпи розвитку інформаційних технологій значно випереджають темпи розробки рекомендаційної і нормативно-правової бази регулюючих документів, що діють на території України. Тому, на наш погляд, рішення питання про розробку на підприємстві ефективної політики інформаційної безпеки пов'язане з проблемою вибору критеріїв і показників захищеності, а також адекватності прийнятих механізмів і ефективності системи інформаційної безпеки.

Функції захисту інформації мають виконуватися у рамках функцій з її збору та обробки, відповідно можна стверджувати, що інформаційний захист є істотною складовою інформаційної системи обліку та становить одну з головних функцій сучасної системи управління. Забезпечення безпеки припускає проведення комплексних заходів, спрямованих, з одного боку, на нейтралізацію або зниження негативного впливу інформаційних загроз на ефективність господарської діяльності, а з іншого – на посилення дії чинників, що підвищують ефективність використання сучасних телекомунікаційних технологій в управлінні. Тому процес розробки політики інформаційного захисту підприємства електронної комерції має включати:

1. визначення цілей політики інформаційної безпеки підприємства;
2. створення ефективної системи управління інформаційною безпекою, яка включає: визначення об'єктів та необхідного рівня захисту, вибір

засобів забезпечення інформаційного захисту та контролю рівня інформаційної безпеки, встановлення відповідальності за порушення інформаційної безпеки;
3. аналіз відповідності проведених заходів інформаційного захисту заявленим цілям;
4. оцінку захищеності інформаційних ресурсів на основі методик управління безпекою, що базуються на обґрунтованій системі показників інформаційної безпеки.

Існує три найуразливіші аспекти електронної комерції – це клієнт, сервер та канали зв'язку. Інформація в процесі комерційної угоди перетікає через канали зв'язку від сервера до клієнта та навпаки. При цьому, на кожному етапі передавання інформації вона може бути пошкодженою, як навмисно, так і випадково.

Основним каналом зовнішнього втручання та порушення інформаційної безпеки сьогодні вважається Інтернет. Тому комерційним підприємствам спеціалісти з безпеки інформаційних технологій (IT-аудиту) зазвичай рекомендують знизити можливість доступу до локальної мережі підприємства. Однак для підприємств, які здійснюють діяльність в електронному секторі економіки, Інтернет є головним каналом зв'язку зі споживачами, постачальниками та іншими бізнес-партнерами. Блокування доступу до мережі є неможливим, бо саме на відкритому доступі до баз даних і базується діяльність підприємств електронної комерції.

Облікові системи підприємств електронної комерції містять великі обсяги конфіденційної та приватної інформації, яка є об'єктом інформаційних загроз. Несанкціонований доступ до облікової інформації підприємства електронної комерції може спричинити катастрофічний ризик втрати даних, порушення їх цілісності або непередбаченого використання. Розголошення облікової інформації підприємства електронної комерції не тільки є шкідливим для комерційної таємниці, а може стати об'єктом фінансових махінації в особливо великих розмірах. Тому безпека та схоронність облікової інформації має бути пріоритетом кожного підприємства, яке виходить на електронний ринок, а основні положення політики інформаційного захисту підприємства електронної комерції, на нашу думку, мають бути зафіксовані в обліковій політиці. Одночасно, необхідно до функцій контролю схоронності активів підприємства віднести завдання контролю схоронності такого виду активів, як інформаційні ресурси. Для цього вважаємо за необхідне розробити систему розрахунку рівня збитку у наслідку можливого інциденту порушення інформаційної безпеки – інтегрованого якісного показника, який комплексно характеризує можливі фінансові збитки, втрату репутації, вірогідність настання громадянської відповідальності та ін.

На нашу думку, ризик інформаційної безпеки слід трактувати як функцію (fR) від трьох параметрів: вірогідності загроз захисту системи (threats – T), ступеня вразливості системи (vulnerability – V) та оціки можливого збитку від порушення безпеки (loss – L).

$$fR = \sum_{t=1} Rt, \tag{1}$$

де t – існуючі види загроз, а Rt – вірогідність настання інциденту певного виду загроз.

Означений інтегрований показник ризику інформаційної безпеки, на нашу думку, має визначатися за схемою (рис. 1). Рівень ризику настання певного виду загроз (природних, техногенних, навмисних та ненавмисних людських) залежить, по-перше, від ступеня вразливості системи, який характеризується мірою несанкціонованої доступності інформаційних ресурсів, які підлягають захисту, як зовні так і всередині підприємства. По-друге, рівень ризику є пропорційним збиткам які може спричинити втрати або пошкодження інформаційних ресурсів фінансовому стану, або репутації підприємства. При цьому, кожен з зазначених параметрів необхідно розглядати в рамках математичної імовірнісної моделі, побудованої на базі експертних оцінок, за наявності достатньої статистичної бази, яка ведеться: а) на державному рівні, б) на рівні громадських та консультаційних організацій, в) на рівні підприємства.

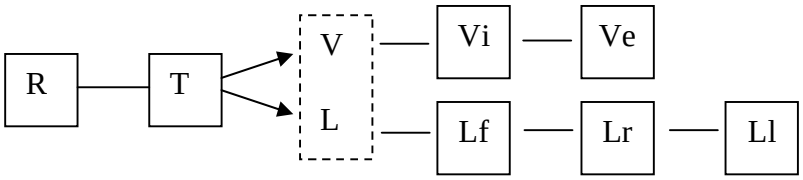

Рис.1. Схема формування інтегрованого показника інформаційного ризику

R – ризик інформаційної безпеки; T – ризик загроз; V – ризики вразливості системи: Vi – внутрішні; Ve – зовнішні; L – ризик збитків: Lf – фінансових; Lr – репутації; Ll – правових

Важливе місце у забезпеченні інформаційного захисту необхідно відводити і використанню засобів зовнішнього контролю. Такі функції можуть взяти на себе спеціалізовані відділи з контролю інформаційних технологій (IT-аудитори). Запровадження незалежної аудиторської перевірки стандартів, процедур та практики інформаційного захисту сприятиме підвищенню рівня захищеності інформаційних ресурсів від втрати, ушкодження або нецільового використання.

Узагальнюючи сказане, необхідно відзначити, що інформаційна безпека електронної комерції характеризується ступенем її захищеності і, отже стійкістю основних бізнес-процесів та інформаційних ресурсів до небезпечних, деструктивних, дестабілізуючих інформаційних дій. Інформаційна безпека визначається здатністю нейтралізувати такі дії. Розробка механізмів забезпечення інформаційної безпеки комерційної діяльності в Україні тісно пов'язана із заходами щодо інформатизації суспільства в цілому. У цих умовах право повинно встати на захист глобальних цінностей. І це, насамперед, стосується добробуту людини та умов функціонування і розвитку суб'єктів підприємницької діяльності. Інформаційну систему не можна регулювати тільки виходячи з інтересів розвитку технологій та інформаційних ресурсів. Охоплюючи всі сфери діяльності інформатизація кидає нові виклики інформаційній безпеці і створює для неї нові загрози. Поодинці комерційні підприємства не зможуть створити ефективну систему інформаційного захисту. Сьогодні настала нагальна потреба у державному контролі та регулюванні правового режиму інформаційної безпеки в основу якого має бути покладений принцип пріоритету людини, особи, суспільства в цілому. Саме таке державне регулювання сприятиме збереженню інформаційних ресурсів підприємства та, відповідно, сприятиме укріпленню довіри до електронної економічної діяльності.

Роман Кулик, *к. е. н., доцент*
Зоряна Островська, *викладач*
Вячеслав Бобівник
Тернопільський національний економічний університет
м. Тернопіль, Україна

РИЗИКИ ОБЛІКОВОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

В умовах ринкової економіки збільшується обсяг інформації, який потрібен менеджерам для управління. Щоб своєчасно прийняти управлінські рішення вони повинні отримувати як зовнішню (ринкові ціни, валютні курси та ін.), так і внутрішню інформацію щодо собівартості продукції (робіт, послуг), прибутку, руху грошових коштів, структури власних та залучених коштів, розрахунків з дебіторами та кредиторами та ін., тобто інформацію, яка продукується обліковою системою. Це підтверджує тезу, що в сучасних умовах бухгалтерський облік виконує не тільки інформаційну, контрольну, аналітичну функції, але і комунікаційну – передачу інформації менеджерам для прийняття управлінських рішень. Інформація бухгалтерського обліку використовується ними для планування та прогно-