Корнієнко Наталія Яківна
Таврійський державний агротехнологічний університет імені Дмитра Моторного (м. Мелітополь)
Науковий керівник: к.е.н., доцент Ілляшенко К.В.

ІНФОРМАЦІЙНА БЕЗПЕКА БУХГАЛТЕРСЬКИХ ДАНИХ

З огляду на те, що в той час як економічний потенціал усе більшою мірою визначається рівнем розвитку інформаційної структури, пропорційно зростає потенційна уразливість економіки від інформаційних впливів. Хакерські атаки, віруси-вимагачі, промислове шпигунство, крадіжка персональної інформації – все це стало невід'ємною частиною ризиків для діяльності підприємств. А повністю автоматизована форма бухгалтерського обліку з підключенням до мережі стає одним з основних джерел подібної уразливості.

Швидке вдосконалювання інформатизації, проникнення її в усі сфери суспільства та держави викликали крім безсумнівних переваг і появу ряду суттєвих проблем. Однією з них стала необхідність захисту підприємства від імовірних інформаційних небезпек.

Формування інформаційного суспільства опирається на новітні інформаційні, телекомунікаційні технології та технології зв'язку. Саме нові технології призвели до бурхливого поширення глобальних інформаційних мереж, що відкривають принципово нові можливості міжнародного інформаційного обміну. Формування інформаційного суспільства концептуально та практично означає формування нового світогляду, в якому дуже важливе значення буде мати безпека від інформаційних загроз.

З урахуванням того, що об'єктом інформаційної безпеки є підприємство, зміст поняття «інформаційної безпеки» буде полягати у захищеності інтересів власника даного підприємства, що задовольняють за допомогою інформації, або пов'язаних із захистом від несанкціонованого доступу тих відомостей, які представляються власникові досить важливими. Інтереси проявляються через об'єкти, здатні служити для їхнього задоволення, і дії, що вживають для володіння цими об'єктами. Відповідно, інтереси, як об'єкт безпеки, можуть бути представлені сукупністю інформації, здатної задовольняти інтерес власника, і його дій, спрямованих на оволодіння інформацією або приховування інформації. Ці складові об'єкта інформаційної безпеки і захищаються від зовнішніх і внутрішніх загроз [1, с.188].

Слід зауважити, що застосування інформаційних технологій є одним з важливих факторів, що визначають конкурентоздатність підприємств. Однак поряд з очевидними перевагами, такими як автоматизація виробничих і обліково-аналітичних процесів, доступність електронних розрахунків, швидкість обробки інформації для прийняття управлінських рішень, використання інформаційних технологій привносить нові істотні

ризики [2, с. 20].

Питання інформаційної безпеки при веденні бухгалтерського обліку з використанням комп'ютерних технологій доцільно розглядати у двох аспектах: запобігання зловживань чи ненавмисних порушень працівниками підприємства (внутрішній аспект) та створення належної інформаційної безпеки для запобігання несанкціонованому доступу, пошкодженню комп'ютерних програм чи даних вірусами, комп'ютерному саботажу (зовнішній аспект) [3, с.232].

Превентивні механізми запобігання втрат та перекручень облікової інформації повинні базуватися на комплексних, взаємопов'язаних методиках і процедурах виявлення, аналізу ризиків для інформаційної системи обліку підприємства, розробках контрольних технологій щодо управління безпекою облікової інформації [4, с.126].

У теперішній час найбільшу питому вагу в цій групі заходів у системах обробки обліково-звітної інформації складають спеціальні пакети програм або окремі програми, які включаються до складу програмного забезпечення з метою реалізації завдань щодо захисту інформації. Технологічні засоби інформаційної безпеки – це комплекс заходів, які органічно вбудовуються в технологічні процеси перетворення даних.

Можливі методи зниження інформаційного ризику для кожної одиниці стандартні і можуть бути використані в обліково-аналітичній діяльності [5, с.121]:

- прийняття ризику – визнання потенційних втрат прийнятними;
- запобігання ризику – прийняття рішень, спрямованих на видалення фактора ризику, зокрема, усунення причин відповідної загрози (наприклад, відмова від використання встановленого програмного забезпечення, що істотно порушує вимоги інформаційної безпеки);
- обмеження ризику – впровадження спеціальних засобів контролю, що знижують імовірність реалізації інформаційної загрози та (або) її наслідки;
- передача ризику – створення умов для компенсації потенційних втрат шляхом передачі ризику третій особі, наприклад, використовуючи страхування або віддаючи окремі функції на аутсорсінг.

Представлені вище способи не є взаємовиключними та можуть застосовуватися комплексно.

Але запобігання інформаційним небезпекам не повинно зводитись до одного тільки зниження ризиків. Оскільки настання кризових ситуацій практично неможливо прогнозувати, необхідно створити цілу низку заходів, і перш за все, систем контролю для швидкого реагування та прийняття вірних управлінських рішень.

Так, для автоматизованої форми обліку дуже важливо мати надійний захист та щоденне резервне копіювання даних на безпечних носіях. Не повинна вважатися застарілою роздруківка найбільш важливих фінансових документів на папері, щоб робота бухгалтерської служби не припинялася, наприклад, із за перебоїв електроенергії.

Зауважимо, що не менш важливим фактором безпеки бухгалтерського обліку є використання лише ліцензованого програмного забезпечення, яке має службу технічної підтримки, оновлення уразливих компонентів тощо.

Також, проблема заслуговує більш уважного відношення від керівників підприємств, які все ще використовують застарілі моделі управління. Формування нового підходу потребує перегляду кадрових питань, нових форм контролю й обов'язкового урахування факторів, що характерні новій цифровій економіці.

Отже, у ході дослідження нами зроблено висновок, що на даному етапі інформаційні загрози є недооціненими та недостатньо вивченими у розрізі облікової діяльності підприємств. У той час як економічний потенціал усе більшою мірою визначається рівнем розвитку інформаційної структури, пропорційно зростає потенційна уразливість економіки від інформаційних впливів. Тому так важливо всебічно вивчити види інформаційних загроз і розробити заходи щодо їх уникнення. Це в першу чергу формування нового підходу до управління підприємством, захисту внутрішньої інформації від зовнішнього втручання, аналіз інформаційних ризиків при прийнятті управлінських рішень тощо.

Література:

1. Овсянніков В.В., Дехтяр С.В., Паламарчук С.А., Черниш Ю.О., Шемендюк О.В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки. Сучасні інформаційні технології у сфері безпеки та оборони. 2015. № 3(24). С. 187-193.

2. Ткачук Т. Формування системи інформаційної безпеки бізнесу. Бізнес і безпека. 2009. №4. С. 19-23.

3. Муравський В. Забезпечення інформаційної безпеки в автоматизованих системах бухгалтерського обліку. Економічний аналіз. 2013. Вип. 12. Ч. 4. С. 232-235.

4. Шишкова Н.Л. Засоби підвищення керованості безпекою облікової інформації. Економічний вісник. 2016. №3. С. 119-127.

5. Ілляшенко К.В. Інформаційний взаємозв'язок аналізу та бухгалтерської звітності. Вісник ХНТУСГ: економічні науки. 2012. №127. С. 118-123.