УДК 004

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБЛІКОВИХ ДАНИХ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Савченко Роман Олександрович
к.е.н, доцент, головний бухгалтер
Савченко Наталія Миколаївна
к.е.н, доцент
Поліський національний університет
м. Житомир, Україна

Аннотация. Підвищення ролі інформаційних ресурсів, що акумулює облікова система субєктів господарювання, зумовлює необхідність акцентування уваги адміністративного персоналу та власників підприємства на забезпеченні необхідного рівня дотримання їх інформаційної безпеки. Від рівня захисту облікової інформації залежить ступінь економічної безпеки підприємства, а отже, і ефективність його розвитку.

Ключові слова: інформаційні технології, суб'єкт господарювання, інформаційна безпека, конфіденційність, захист, облік

Застосування в господарській діяльності суб'єктів господарювання інформаційно-інноваційних технологій зумовлює необхідність використання механізмів захисту даних. Інформаційні системи, що використовуються при веденні бухгалтерського обліку, дають змогу забезпечити працездатність інфраструктури підприємства, здійснюють оптимізацію розміру фінансових та трудових витрат. Так як бази даних суб'єктів господарювання можуть містити значні обсяги конфіденційної інформації, актуальним стає питання забезпечення бажаного ступеня захищеності інформаційних систем.

З позиції інформаційних технологій захисту інформації, інформаційна безпека – це система заходів, що дає змогу виявляти: вразливі місця інформаційно-комунікаційної системи підприємства; небезпеки, які

загрожують їй, і методи нейтралізації виявлених загроз. Під загрозою треба розуміти подію, яка може викликати порушення функціонування інформаційної системи, включаючи спотворення, знищення або несанкціоноване використання бази даних підприємства [2].

Ефективне та злагоджене функціонування інформаційного середовища потребує розробки та впровадження низки організаційно-правових заходів, зокрема заходів щодо своєчасної організації функціонування системи інформаційної безпеки. Однією із складових інформаційної безпеки є інформаційна безпека підприємництва, в рамках якої має здійснюватися дієвий захист джерел інформації про комерційну діяльність підприємств усіх форм власності, інформаційно-аналітичних систем збору та обробки фінансової, податкової інформації [1].

Загрози інформаційній безпеці суб'єктів господарювання можуть виникати внаслідок:

- навмисних чи ненавмисних дій співробітників підприємства, його власників чи зовнішніх суб'єктів (наприклад, контрагентів, органів державної влади, співробітників банківських установ тощо);
- впливу об'єктивних та суб'єктивних чинників (наприклад, розвиток інноваційних технологій, надзвичайні події тощо).

В зв'язку з цим, головною метою інформаційної безпеки облікової системи є забезпечення стабільного та ефективного функціонування суб'єкта господарювання на поточний та майбутні періоди. При цьому будь-який механізм захисту інформаційного масиву суб'єкту господарювання має гарантувати дотримання наступних вимог (рис.1):

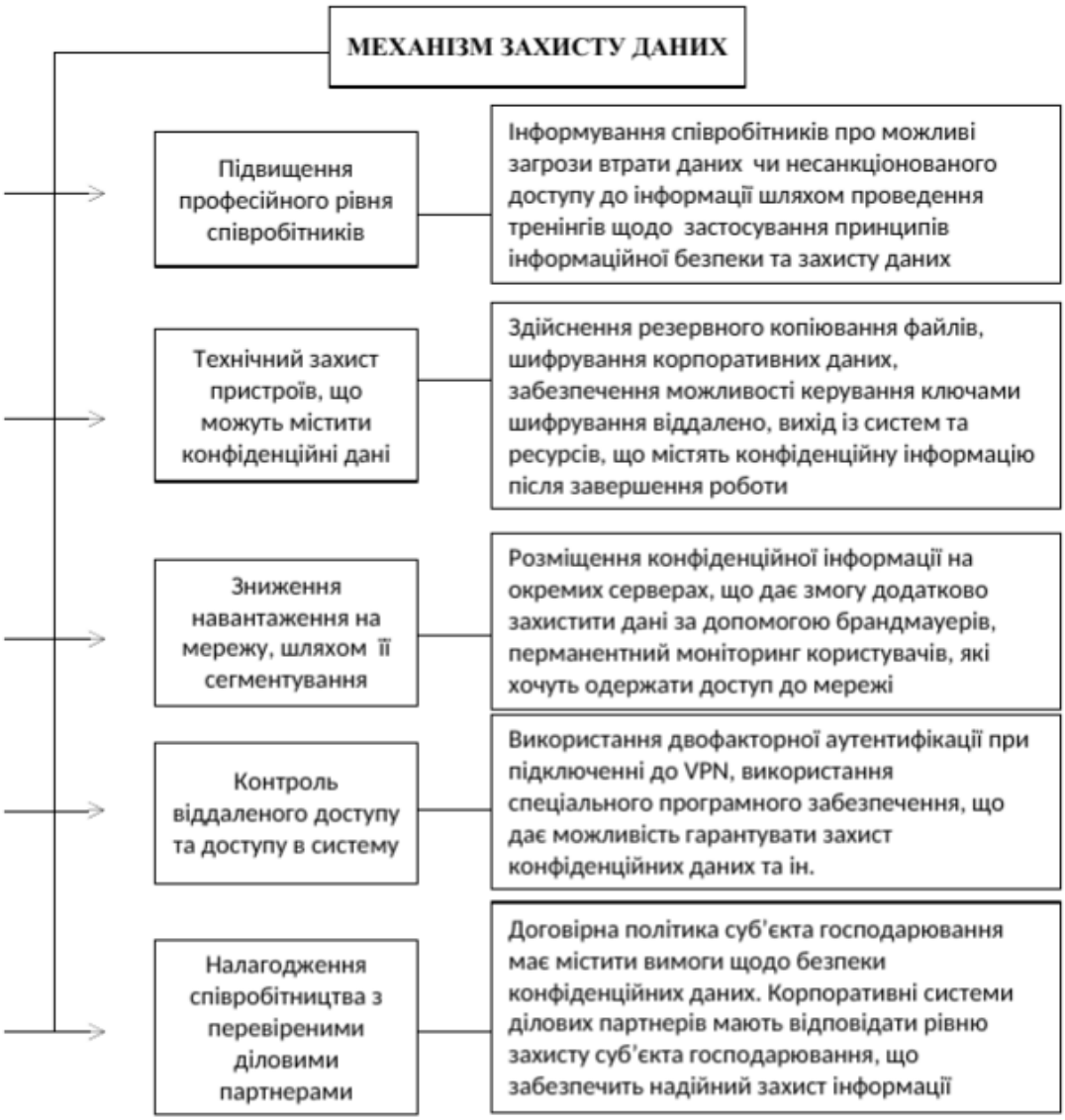

Рис. 1 Механізм захисту даних в межах інформаційної безпеки облікової системи суб’єкта господарювання

Дотримання правил захисту даних дасть змогу мінімізувати ризики ведення господарської діяльності та забезпечить уникнення збоїв при здійсненні бізнес-процесів. І хоча інформаційна безпека є індивідуальною справою конкретного підприємства, що має враховувати його організаційну побудову та специфіку діяльності, великий вплив на неї мають зовнішні чинники. Так, потрібно пам’ятати, що будь-який механізм захисту даних не буде ефективно працювати, якщо він не буде базуватися на положеннях нормативно-правових актів. Адже саме держава має бути заінтересована в інформаційній безпеці діяльності суб’єктів підприємництва. Огляд положень

чинних нормативно-правових актів в сфері інформаційної безпеки суб'єктів господарювання дає змогу стверджувати, що більшість з них несуть декларативний характер, вони не враховують специфіку інформатизації окремих господарюючих одиниць. При прийнятті підприємством рішення про вибір підходу щодо формування системи менеджменту інформаційної безпеки доцільно враховувати рекомендації ISO / IEC 27003 «Information technology – Security techniques – Information security management system implementation guidance». Положення даного міжнародного стандарту ґрунтуються на методології процесного підходу, включаючи специфікацію всіх формальних атрибутів можливих процесів системи менеджменту інформаційної безпеки [4]. Власники та адміністративний персонал суб'єкта господарювання мають бути наділені повноваженнями із визначення рівня ризику в сфері забезпечення необхідного ступеня інформаційної безпеки. Адже саме вони несуть відповідальність за вкладення фінансових, матеріальних та трудових ресурсів в систему інформаційної безпеки суб'єкта господарювання та підтримання належного рівня ефективності її функціонування. За для досягнення максимального ступеня захисту облікової системи доцільним є використання лише ліцензійного професійного програмного забезпечення. Адже постачальники ліцензійного програмного забезпечення не лише здійснюють сервісну та технічну підтримку, але й гарантують стабільність роботи ПК, коректність роботи програмного забезпечення, дають можливість відстежувати витік інформації, запобігають несанкціоновану віддаленому доступу до даних, що можуть носити конфіденційний характер та ін. Потрібно також використовувати антивірусне програмне забезпечення, налаштувати щоденне копіювання облікових даних, генерувати надійні паролі. Слід зазначити, що не існує універсального механізму, використання якого б дало змогу гарантувати захист інформаційних ресурсів суб'єктів господарювання. Ключовим принципом у запобіганні вторгнення є активність. Це означає постійне тестування систем безпеки перед тим, як зловмисник зробить це. Для запобігання втручанню та несанкціонованому доступу до організаційних даних

і мереж можна вжити багато заходів, але жодна мережа не є повністю безпечною [3]. Постійний розвиток інноваційних технологій, винахідливість зловмисників та швидкість їх дій зумовлюють необхідність інтеграційного використання набору методів та способів захисту інформаційного масиву. При цьому сподіватись лише на захист з боку технологій буде не зовсім правильно. Адже є людський фактор, який не можна ігнорувати. Постійне інформування співробітників суб'єкта господарювання, що мають доступ до облікових даних або ж формують їх сприятиме підвищенню рівня захисту облікової інформації. Таким чином, розвиток інформаційних технологій сприяє зниженню трудомісткості облікових робіт, розширює інформаційні можливості суб'єктів господарювання, з одночасним підвищенням ступеню ризику витоку даних. В зв'язку з цим доцільним є використання перманентних заходів захисту облікових даних, які будуть давати змогу запобігати виникненню випадковим загрозам та навмисним діям, відновлення пошкоджень та усунення проблем.

СПИСОК ЛІТЕРАТУРИ

1. Абакумов В.М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони. *Форум права*. 2012. № 4. С. 10 – 16

2. Городянська Л.В., Цюкало Л.В. Інформаційна безпека суб'єктів малого підприємництва в умовах цифровізації. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. № (70). С. 105–114.

3. Чех Н.О., Конопліна О.О., Шахвердян Д.С. Забезпечення інформаційної безпеки бухгалтерського обліку підприємств. *Управління та адміністрування*. 2019, том 2, випуск 148. С. 111 - 117

4. ISO/IEC 27003 : 2010 Information technology — Security techniques — Information security management system implementation guidance. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-1:v1:en