БУХГАЛТЕРСЬКИЙ ОБЛІК, АНАЛІЗ І АУДИТ

УДК 657.422.8

М. М. Ігнатенко

ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ОРГАНІЗАЦІЙ В УМОВАХ АВТОМАТИЗАЦІЇ ОБЛІКУ ТА ФІНАНСОВОЇ ЗВІТНОСТІ

***Анотація**. У статті визначено переваги впровадження автоматизації, програмного забезпечення й комп'ютеризації облікових процесів вітчизняних підприємств та організацій. Надано змістовну характеристику гідностей та властивостей найбільш вживаних програм. Одночасно виявлено ризики й загрози інформаційній безпеці, їх джерела та прояви. Обґрунтовано комплекс заходів збереження та зміцнення інформаційної безпеки. Розроблено алгоритм їх впровадження. Надано пропозиції щодо здійснення подальших досліджень.*

***Ключові слова**: підприємства, організації, інформаційна безпека, комп'ютерні мережі, автоматизація, бухгалтерський облік, фінансова звітність, програмні продукти.*

***Summary**. The article outlines the advantages of introducing automation, software and computerization of accounting processes of domestic enterprises and organizations. An informative description of the merits and properties of the most used programs is provided. At the same time, risks and threats to information security, their sources and manifestations are revealed. The complex of measures for preservation and strengthening of information security is substantiated. The algorithm of their implementation is developed. Submitted suggestions for further research.*

***Key words**: enterprises, organizations, information security, computer networks, automation, accounting, financial reporting, software products.*

Постановка проблеми. У формуванні сучасних мереж бухгалтерського обліку та фінансової звітності на підприємствах і в організаціях всіх видів діяльності та господарювання провідне місце займає автоматизація. Використання відповідних програмних продуктів забезпечує можливість здійснення моніторингу і контролю за відповідністю й точністю облікових даних і процесів. При цьому комп'ютерні мережі забезпечують надійність інформаційних зв'язків як всередині бухгалтерії, так і між бухгалтерією та іншими структурними підрозділами підприємства. Проте питання інформаційної безпеки також мають бути у полі зору працівників та власників. Зважаючи на це, перспективною є така організація роботи бухгалтерії при застосуванні комп'ютерів, що складається з двох основних відділів: відділу інформаційної системи та відділу контролю.

Аналіз останніх досліджень і публікацій. Проблеми формування інформаційної безпеки, автоматизації бухгалтерського обліку та фінансової звітності підприємств знаходяться в полі зору багатьох дослідників. Зокрема, йдеться про роботи О. С. Можаєва, І. А. Рябініна, Г. М. Черкесова та ін. Проте питання захисту інформації в умовах автоматизації обліку та облікових процесів, впровадження нових програмних продуктів, з одного боку та зростання ризиків і загроз збереження їх цілісності через можливі кібератаки — з іншого, потребують подальших досліджень.

Метою статті є встановлення тенденцій удосконалення здійснення бухгалтерського обліку та фінансової звітності на засадах автоматизації та обґрунтування вирішення проблем комп'ютеризації облікових процесів, забезпечення інформаційної безпеки підприємств і організацій.

Виклад основного матеріалу дослідження. Впровадження автоматизації та комп'ютеризації бухгалтерського обліку й фінансової звітності на підприємствах і в організаціях національного господарства України всіляко сприяє удосконаленню їх діяльності та управління розвитком. Це значно зменшує адміністративні витрати, підвищує ефективність роботи підрозділів бухгалтерії, контролінгу, фінансово-аналітичної служби. Так, найбільш відома та впроваджувана програма «1-С: Підприємство» значно спрощує реєстрацію

Бібліографія ДСТУ:

Ігнатенко М. М. Формування інформаційної безпеки підприємств і організацій в умовах автоматизації обліку та фінансової звітності / М. М. Ігнатенко // Вісник Бердянського університету менеджменту і бізнесу. — 2017. — № 4 (40). — С. 84–88.

References (APA):

Ignatenko, M. M. (2017). *Formuvannia informatsiinoi bezpeky pidpryiemstv i orhanizatsii v umovakh avtomatyzatsii obliku ta finansovoi zvitnosti* [Formation of information security of enterprises and organizations in the conditions of authorization of accounting and financial statements]. *Visnyk Berdianskoho universytetu menedzhmentu i biznesu*, 4 (40), 84–88 (in Ukr.).

та ведення господарських операцій підприємствами, які займаються виробничою діяльністю.

Програма «Бест-Звіт» призначена для автоматизації процесів підготовки, подання, прийняття, контролю, збереження, обробки та аналізу документів підприємствами, що звітують керівним державним органам, або державним установам контролю. Її функціональні можливості, як і попередньої програми, справляють велике враження у контексті удосконалення складання фінансової звітності [1, с. 195]. Зокрема, програма охоплює бази основних документів, що постійно поповнюються; дозволяє вести реєстр та комплект форм звітності як за типовими зразками, так і орієнтованими на підприємства різних видів діяльності із можливістю створювати й коригувати власні комплекти форм звітності; забезпечує перевірку коректності заповнення звітних документів, формування пакетів електронної звітності для передання у автоматизоване робоче місце збору і обробки.

Також програма має можливості обробки й аналізу інформації, яку містять звітні документи за допомогою вбудованого генератора звітів і засобами Windows (Word, Excel). Наявний модуль «Бухгалтерський календар» із функціями планувальника автоматично співставляється з комплектом форм звітності та сплати податків. Підключення групи первинної документації означає, що бланки платіжного доручення, податкової накладної, посвідчення про відрядження тощо завжди наготові. Сервісні функції автоматизованої системи забезпечують: наявність засобів адміністрування системи і розподілу доступу; авторизацію доступу за ім'ям та паролем користувача; наявність засобів управління резервними копіями баз даних; можливість прийняття пакетів звітності у електронному виді — файлів; можливість автоматичної вставки значень реквізитів з підпорядкованих форм до головних у процесі введення інформації.

Крім цього, автоматично відбувається перевірка пакетів звітності, реєстрація її форм при введенні або прийнятті пакетів у електронному виді. Отже, програма «Бест-Звіт» має дуже високі операційні характеристики. У неї висока швидкість в роботі, введення інформації в первинний документ проводиться на робочій станції. Вона має високу технологічну надійність, стійкість до відмов і збоїв; якщо такі випадки трапляються, то руйнування баз даних не відбувається [2, с. 60]. Простота установки й експлуатації виключає необхідність наявності в штаті фахівця-адміністратора бази даних. Таким чином, автоматизована система формування звітної обліково-фінансової документації виключає можливість допущених помилок, береже робочий час.

Однак за наявності таких безсумнівних переваг перед підприємствами та організаціями виникають нові проблеми, насамперед, інформаційної безпеки. Це питання захисту інформації від несанкціонованого втручання, юридичної доказовості електронних первинних документів. Також можливими є ризики втрати або псування інформації під час вимкнення електроенергії, небезпека проникнення комп'ютерних вірусів, зламу облікової інформації, кібератак тощо.

У сучасних умовах господарювання проблеми інформаційної безпеки підприємств і організацій за наявності автоматизованого бухгалтерського обліку й обліково-фінансової звітності розглядаються теоретиками та практиками кількох галузей знань: юристами, представниками служби безпеки, фахівцями інформаційних мереж, бухгалтерами, менеджерами. Надійний захист інформації в розроблюваних і функціонуючих системах обробки даних може бути ефективним, якщо він буде надійним на всіх об'єктах і в усіх елементах системи, які можуть бути піддані загрозам.

У зв'язку з цим для створення засобів захисту важливо визначити природу загроз, форми і шляхи їх можливого прояву і здійснення, перелік об'єктів та елементів, які, з одного боку, можуть бути піддані (побічно або безпосередньо) погрозам з метою порушення захищеності інформації, а з іншого — можуть бути досить чітко локалізовані для організації ефективного захисту інформації. При проведенні дослідних робіт в цьому напрямі необхідно розмежувати два класи ризиків: перший — для автономних персональних комп'ютерів (ПК) і автономних комп'ютерних мереж; другий — для систем, що мають вихід у великі мережі, включаючи Інтернет.

У спеціальній літературі під об'єктом інформаційної безпеки розуміється такий структурний компонент автоматизації обліку та звітності, в якому перебуває або може перебувати інформація, що підлягає захисту, а під елементом захисту — сукупність даних, яка може містити відомості, що підлягають захисту [3, с. 127]. Практика показує, що інформація в процесі введення, зберігання, обробки, виведення і передачі піддається різним випадковим впливам, у результаті яких на апаратному рівні відбуваються фізичні зміни в сигнальних формах її представлення. Якщо в якомусь чи в якихось розрядах цифрового коду, що несе інформацію, відбулося інвертування двійкового знаку (з 1 на 0 або навпаки) і воно не виявлено спеціальними апаратними засобами функціонального контролю, то при подальшій обробці інформації або буде отриманий невірний результат, або повідомлення попрямує за помилковою адресою, або відбудуться інші небажані події (руйнування, модифікація, витік інформації та ін.)

На програмному рівні у результаті випадкових впливів може відбутися зміна алгоритму обробки інформації на непередбачений і, як наслідок

цього, припинення або модифікація облікового процесу, в результаті якого знову ж можливі руйнування або витік інформації (при переплутуванні, наприклад, адресата). Причинами випадкових впливів при функціонуванні комп'ютерних систем можуть бути: відмови і збої апаратури у разі її неякісного виконання і фізичного старіння; перешкоди в каналах і на лініях зв'язку від впливу зовнішнього середовища; аварійні ситуації (пожежа, повінь, вихід з ладу електроживлення та ін.); помилки і прорахунки розробників і виробників ПК; алгоритмічні і програмні помилки, помилки людини при роботі з ПК.

Зловмисні чи навмисні загрози — результат активного впливу людини на об'єкти і процеси з найрізноманітніших причин (матеріальний інтерес, бажання нашкодити, розвага із самоствердженням своїх здібностей та ін.) У якості об'єктів забезпечення інформаційної безпеки в системах обробки облікових даних у таких випадках можна виокремити такі: термінали користувачів (персональні комп'ютери, робочі станції мережі); термінал адміністратора мережі або груповий абонентський вузол; вузол зв'язку; засоби відображення інформації; засоби документування інформації; комп'ютерний зал і сховище носіїв інформації; зовнішні канали зв'язку та мережеве обладнання; накопичувачі та носії інформації.

Відповідно до наведеного вище визначення, в якості елементів захисту виступають блоки (порції, масиви, потоки та ін.) інформації в об'єктах захисту. Це дані і програми в основній пам'яті комп'ютера; дані і програми на зовнішньому носії або гнучкому і жорсткому дисках; дані, відображувані на екрані монітора; дані, що виводяться на принтер при автономному та мережевому використанні ПК; пакети даних, що передаються каналами зв'язку; дані, що розмножуються (тиражовані) за допомогою копіювально-розмножувального устаткування; паролі й пріоритети зареєстрованим користувачам; службові інструкції щодо роботи з комплексами завдань; архіви даних і програмне забезпечення та ін.

Необхідно зазначити, що доступ до об'єктів та елементів захисту інформації теоретично і практично можливий для двох категорій осіб: законних користувачів і порушників [4, с. 62]. За відсутності на робочому місці законного користувача або через його недбале ставлення до своїх посадових обов'язків, через недостатній захист інформації кваліфікований порушник може здійснити шляхом введення відповідних запитів (команд) несанкціонований доступ до інформації. При досить вільному доступі в приміщення, де встановлені засоби, можна візуально спостерігати інформацію на засобах відображення і документування, а також викрасти носії з інформацією або зняти з них копію. При безконтрольному завантаженні в комп'ютер програми порушник може модифікувати облікові та звітні дані й алгоритми, ввести шкідливу програму типу «троянський кінь», за допомогою якої згодом він може реалізовувати потрібні для себе функції.

Особливо небезпечна ситуація, коли порушником є користувач комп'ютерної системи, що має згідно зі своїми функціональними обов'язками законний доступ до однієї частини інформації, але звертається до іншої за межами своїх повноважень. Несанкціонований доступ до інформації може відбуватися під час технічного обслуговування (профілактики або ремонту) комп'ютерів за рахунок прочитання інформації на машинних та інших носіях, незважаючи на її видалення (стирання) користувачем звичайними методами. Інший спосіб — прочитання інформації з носія під час його транспортування без охорони всередині об'єкта або регіону.

Сучасні засоби обчислювальної техніки базуються на широкому застосуванні інтегральних схем. При роботі таких схем відбуваються високочастотні зміни рівнів напруги і струмів, а це, у свою чергу, призводить до виникнення в ланцюгах живлення, у ефірі, в близько розташованій апаратурі тощо різних електромагнітних полів і наведень, які за допомогою спеціальних засобів можна трансформувати в оброблювану інформацію [5, с. 127]. Причому, зі зменшенням відстані між приймачем порушника та апаратними засобами імовірність такого роду знімання і розшифровки інформації збільшується.

Несанкціоноване ознайомлення з інформацією розділяється на пасивне і активне. У першому випадку не відбувається порушення інформаційних ресурсів. Порушник лише отримує можливість розкривати зміст повідомлень, використовуючи це надалі у своїх корисливих цілях. У другому випадку порушник може вибірково змінити, знищити, переупорядкувати й перенаправити повідомлення, затримати і створити підроблені повідомлення та ін. Для забезпечення безпеки інформації в особистих комп'ютерах і, особливо, в офісних системах та комп'ютерних мережах проводяться різні заходи, що об'єднуються поняттям «інформаційна безпека». Інформаційна безпека — це сукупність організаційних (адміністративних) і технологічних заходів, програмно-технічних засобів, правових та морально-етичних норм, спрямованих на протидію загрозам порушників з метою зведення до мінімуму можливого збитку користувачам і власникам автоматичних систем обліку і звітності.

На практиці при формуванні інформаційної безпеки підприємств і організацій склалися два підходи: фрагментарний та комплексний. У першому випадку заходи щодо захисту спрямовуються на протидію цілком певним загрозам при су-

воро визначених умовах, наприклад, обов'язкова перевірка носіїв антивірусними програмами, застосування криптографічних систем шифрування і т. д. При комплексному підході різні заходи протидії загрозам об'єднуються, формуючи так звану архітектуру безпеки систем [6, с. 108]. Дослідження практики функціонування систем обробки даних і комп'ютерних мереж показали, що існує досить багато можливих напрямів витоку інформації та шляхів несанкціонованого доступу до неї в системах і мережах. Це перехоплення електронних випромінювань; примусове електромагнітне опромінення (підсвічування) ліній зв'язку; дистанційне фотографування; перехоплення акустичних хвильових випромінювань.

Також йдеться про розкрадання носіїв інформації і виробничих відходів систем обробки даних, зчитування інформації з масивів інших користувачів, копіювання носіїв інформації і файлів з подоланням заходів захисту. Може бути використана модифікація програмного забезпечення шляхом виключення або додавання нових функцій, здійснене використання недоліків операційних систем і прикладних програмних засобів, незаконне підключення до апаратури та ліній зв'язку, в тому числі в якості активного ретранслятора; зловмисний вивід з ладу механізмів захисту. Фіксуються випадки маскування під зареєстрованого користувача і присвоєння собі його повноважень, введення нових користувачів, впровадження комп'ютерних вірусів. Крім того, система захисту не повинна допускати, щоб зловмисник міг зняти із себе відповідальність за формування помилкової або руйнування облікової інформації.

Враховуючи важливість, масштабність і складність вирішення проблеми збереження та безпеки інформації, рекомендується розробляти архітектуру безпеки в декілька етапів: аналіз можливих загроз; розробка систем безпеки; реалізація систем; супровід систем. Необхідно зауважити, що на конкретному об'єкті і в конкретній системі обробки даних з усього різноманіття загроз і можливих ризиків слід, насамперед, вибрати найбільш ймовірні, а також ті, які можуть завдати найбільш суттєвий збиток. Алгоритм розробки систем інформаційної безпеки підприємств і організацій в умовах автоматизації бухгалтерського обліку й обліково-фінансової звітності передбачає використання різних заходів організаційно-адміністративного, технічного, програмного, технологічного, нормативно-правового, морально-етичного характеру та ін.

Організаційно-адміністративні засоби формування інформаційної безпеки зводяться до регламентації доступу до інформаційних і обчислювальних ресурсів, функціональних процесів і систем обробки даних, до регламентації діяльності персоналу та ін. Їх мета — найбільшою мірою ускладнити або виключити можливість реалізації загроз безпеці. Технічні засоби захисту покликані створити певне фізично замкнуте середовище навколо об'єкта й елементів захисту. У цьому випадку використовується установка засобів фізичної перешкоди для захисного контуру приміщень, де ведеться обробка інформації — кодові замки, охоронна сигналізація — звукова, світлова, візуальна без запису та із записом на відеоплівку.

Програмні засоби і методи захисту активніше і ширше за інших застосовуються в системах інформаційної безпеки в персональних комп'ютерах та комп'ютерних мережах, реалізуючи такі функції захисту, як: розмежування і контроль доступу до ресурсів; реєстрація та аналіз процесів, що протікають, подій, користувачів; запобігання можливих руйнівних впливів на ресурси; криптографічний захист інформації; ідентифікація і аутентифікація користувачів і процесів та ін.

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. Серед них найбільш поширеними є: створення архівних копій носіїв; ручне або автоматичне збереження оброблюваних файлів у зовнішній пам'яті комп'ютера; реєстрація користувачів комп'ютерних засобів у журналах; автоматична реєстрація доступу користувачів до тих або інших ресурсів; розробка спеціальних інструкцій щодо виконання всіх технологічних процедур та ін. [7, с. 264].

До нормативно-правових і морально-етичних заходів забезпечення інформаційної безпеки підприємств і організацій відносяться діючі в країні закони, нормативні акти, що регламентують правила поводження з інформацією та відповідальність за їх порушення. Це етичні норми ділової поведінки, корпоративної культури, розробка й дотримання яких сприяє збереженню та зміцненню інформаційної безпеки. Тільки спільне застосування всього арсеналу засобів забезпечення алгоритмів, програмної, технічної, технологічної та інших складових інформаційної безпеки дозволяє досягати високої якості й корисності автоматичних програм обліку і звітності, баз обліково-фінансових даних, потрібних для їх подальшого використання в системах управління й прийняття управлінських рішень.

Висновки. Впровадження автоматизованих систем і програм здійснення бухгалтерського обліку й формування обліково-фінансової звітності є вагомим чинником підвищення ефективності

функціонування вітчизняних підприємств і організацій. Воно сприяє значному скороченню їх витрат на обліково-аналітичні процеси. Проте через специфіку автоматизації й комп'ютеризації (під'єднання до більш глобальних мереж, використання типових програм та показників обліку тощо) збільшується відкритість інформаційних систем, зростають загрози комерційній таємниці та ризики конкурентоспроможної діяльності загалом. Це актуалізує значимість забезпечення та подальшого удосконалення інформаційної безпеки підприємств і організацій на перспективу.

Література

1. Євдокимов В. В. Особливості впровадження комп'ютерних систем бухгалтерського обліку на великих підприємствах [Електронний ресурс] / В. В. Євдокимов // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. — 2009. — № 1 (13). — С. 193–202. — Режим доступу : http://eztuir.ztu.edu.ua/1796/1/20.pdf.

2. Безродна Т. М. Обліково-аналітичне забезпечення управління підприємством: визначення сутності поняття / Т. М. Безродна // Вісник Східноукраїнського національного університету ім. В. Даля. — 2008. — № 10, ч. 2. — С. 58–62.

3. Житна І. П. Сучасні технології удосконалення системи автоматизації обліку та управління виробництвом / І. П. Житна, О. А. Садовніков // Управління розвитком. — 2010. — № 3. — С. 126–128.

4. Гнилицька Л. В. Обліково-аналітична інформація як визначальний чинник забезпечення економічної безпеки суб'єктів господарювання / Л. В. Гнилицька // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2011. — № 3 (157). — С. 57–65.

5. Клименко О. В. Інформаційні системи і технології в обліку : [навч. посіб.] / О. В. Клименко. — К. : Центр учбової літератури, 2008. — 320 с.

6. Домашенко С. В. Інформаційні технології в управлінні підприємством: електронний документообіг / С. В. Домашенко // Збірник наукових праць Таврійського державного агротехнологічного університету. Економічні науки. — 2013. — № 2 (3). — С. 103–112.

7. Озеран А. В. Теорія та методологія формування фінансової звітності підприємств : [монографія] / А. В. Озеран ; ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана». — К. : КНЕУ, 2015. — 471 с.

References

1. Yevdokymov, V. V. (2009). *Osoblyvosti vprovadzhennya kompyuternykh system bukhhalterskoho obliku na velykykh pidpryyemstvakh* [Features of introduction of computer accounting systems at large enterprises]. *Problemy teoriyi ta metodolohiyi bukhhalterskoho obliku, kontrolyu i analizu*, 1 (13), 193–202. Retrieved from http://eztuir.ztu.edu.ua/1796/1/20.pdf (in Ukr.).

2. Bezrodna, T. M. (2008). *Oblikovo-analitychne zabezpechennya upravlinnya pidpryyemstvom: vyznachennya sutnosti ponyattya* [Accounting and analytical support for enterprise management: the definition of the essence of the concept]. *Visnyk Skhidnoukrayinskoho natsionalnoho universytetu im.V. Dalya*, 10, 58–62 (in Ukr.).

3. Zhytna, I. P. & Sadovnikov, O. A. (2010). *Suchasni tekhnolohiyi udoskonalennya systemy avtomatyzatsiyi obliku ta upravlinnya vyrobnytstvom* [Modern technologies of improvement of the system of automation of accounting and production management]. *Upravlinnya rozvytkom*, 3, 126–128 (in Ukr.).

4. Hnylytska, L. V. (2011). *Oblikovo-analitychna informatsiya yak vyznachalnyy chynnyk zabezpechennya ekonomichnoyi bezpeky subyektiv hospodaryuvannya* [Accounting and analytical information as a determinant of economic security of economic entities]. *Visnyk Skhidnoukrayinskoho natsionalnoho universytetu imeni Volodymyra Dalya,* 3 (157), 57–65 (in Ukr.).

5. Klymenko, O. V. (2008). *Informatsiyni systemy i tekhnolohiyi v obliku* [Information systems and technologies in accounting]. Kyiv, Tsentr uchbovoyi literatury Publ. (in Ukr.).

6. Domashenko, S. V. (2013). *Informatsiyni tekhnolohiyi v upravlinni pidpryyemstvom: elektronnyy dokumentoobih* [Information technology in enterprise management: electronic document flow]. *Zbirnyk naukovykh prats Tavriyskoho derzhavnoho ahrotekhnolohichnoho universytetu*, 2 (3), 103–112 (in Ukr.).

7. Ozeran, A. V. (2015). *Teoriya ta metodolohiya formuvannya finansovoyi zvitnosti pidpryyemstv* [Theory and methodology of formation of financial reporting of enterprises]. Kyiv, KNEU Publ. (in Ukr.).