УДК 658.5

Л.В. Куделя, аспірант
Луганський національний аграрний університет

АВТОМАТИЗОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ – ІНСТРУМЕНТ ГАРАНТУВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Постановка проблеми. Одна із важливих проблем підприємств на сьогодні полягає в тому, що воно існує в забрудненому, дуже фрагментарному, неточному, спотвореному інформаційному середовищі, в якому важко приймати рішення. Сучасні інформаційні технології дають змогу підприємствам реалізувати власні інтереси та пришвидшити процеси обміну та співпраці. Нині одним із показників і передумов успішного ведення бізнесу є використання сучасних автоматизованих систем облікової інформації. Їхнє застосування надає нові можливості для розвитку й оптимізації підприємництва, підвищує продуктивність праці, дає змогу ефективно використовувати ресурси, підвищувати якість управління бізнесом. Проведення обліку в умовах автоматизованих облікових систем залежить від рівня автоматизації бухгалтерського обліку, наявності методик здійснення автоматизованого обліку, ступеня доступності облікових даних, складності оброблення інформації. Автоматизовані системи сприяють розвитку безпеки інформаційної системи та виробництва потрібної для організації інформації, яка є необхідною для ефективного управління всіма її ресурсами, створення інформаційного та технічного середовища для управління її діяльністю. Автоматизована інформаційна система, як система управління, тісно пов'язується, як з системами збереження так і з іншими− з системами,що забезпечують обмін інформацією в процесі управління. Вона охоплює сукупність засобів та методів, що дозволяють користувачу збирати, зберігати, передавати і обробляти відібрану інформацію.

Аналіз останніх досліджень та публікацій. Окремі аспекти в області інформаційної безпеки аналізували такі дослідники, як: М. Гамбала, В. Мартинович, О.А. Сороківська, В.Л. Левко [2, 3, 5, 6]. Дотепер серед учених, що досліджують проблеми інформаційної безпеки, не вироблено загального підходу до визначення основного понятійного апарата щодо зазначеної проблематики. Аналіз наукових підходів щодо визначення інформаційної безпеки дозволив поділити існуючі поняття інформаційної безпеки на кілька груп:

1) інформаційна безпека – це безпосередньо стан захищеності інтересів особистості, суспільства та держави в інформаційній сфері;

2) інформаційна безпека, як стан соціально-політичного середовища, при якому забезпечується захист особистості, суспільства, держави;

3) інформаційна безпека як право, гарантія одержання достовірної інформації [4, с. 67]. Одним із найпоширеніших підходів полягає в тому, що інформаційна безпека (яка є складовою частиною національної безпеки) розглядається в контексті проблем національної безпеки. Так, наприклад, український дослідник М. Галамба справедливо вважає, що «інформаційна складова» не може існувати поза цілями загальної національної безпеки так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки [5, с. 89]. Інформаційні зв'язки в системі національної безпеки такі складні та багаторівневі, як і її структура. Проте таке дослідження ускладнюється тим, що потребує компетентності дослідника як у бухгалтерському обліку, так і в сучасних автоматизованих системах і технологіях та проблемах економічної безпеки. Саме тому проблеми автоматизованих систем бухгалтерського обліку досліджують небагато науковців і практиків. Так, у роботі [6, с. 78] поняття "економічної безпеки на підприємстві" розглядають, як сукупність умов та чинників, які забезпечують незалежність цього підприємства, його стабільність і стійкість, здатність до постійного оновлення та самовдосконалення.

Постановка завдання – дати узагальнення характеристики інформаційної безпеки підприємства та висвітлення комплексу заходів, за допомогою яких можна розглядати автоматизовані облікові системи, як інструмент забезпечення економічної безпеки на підприємстві.

Виклад основного матеріалу. Зі зростанням науково-технічного прогресу суспільства зростає і важливість питання інформаційної безпеки громадянина, суспільства та держави. Інформація є чинником,який може призвести до значних технологічних аварій,конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему,роботу наукових центрів. Тому чим вищий рівень інтелектуалізації та інформатизації суспільства,тим потрібнішою стає надійна інформаційна безпека,оскільки реалізація інтересів,людини все більше здійснюється за допомогою інформатизації. Під інформаційною безпекою підприємства пропонуємо розуміти суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності. Інформаційна безпека має три основні складові: конфіденційність, цілісність та доступність. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність

означає захист точності і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час. Інформаційна безпека в сучасних умовах здобуває все більшу актуальність і значимість, є одним із пріоритетних напрямків забезпечення національної безпеки України, а також міжнародної безпеки, що вимагає теоретичного осмислення основних положень інформаційної безпеки для вдосконалення правової бази та політичної практики. Тому чим вища активність громадян, організацій або держав у кіберпросторі, тим гостріше перед суспільством постають проблеми забезпечення своєї інформаційної безпеки. І сьогодні є всі підстави думати, що національна безпека країн залежатиме від забезпечення інформаційної безпеки.

У міру ж інтенсифікації технічного прогресу й посилення «електронного співробітництва» держав ця залежність буде постійно зростати. Особливе місце приділяється інформаційним ресурсам в умовах ринкової економіки. У конкурентній боротьбі значно поширені різноманітні дії, спрямовані на одержання конфіденційної інформації різними способами. Встановлено, що сьогодні у світі 47 % охоронюваних відомостей добувається за допомогою технічних засобів промислового шпигунства. У цих умовах захист інформації від неправомірного оволодіння нею набуває всезростаючого значення. Тобто в економічній сфері зростає вразливість економічних структур від невірогідності, запізнювання й незаконного використання економічної інформації.

Проблеми формування інформаційного суспільства в Україні пояснюються швидким поширенням новітніх інформаційних технологій та глобалізацією світових інформаційних ринків. Головною інформаційною загрозою національній безпеці України слід вважати загрозу інформаційного впливу іншої сторони на свідомість та під свідомість особистості, інформаційні ресурси та інформаційну сферу машино ¬ технічних систем, нав'язування особистості, суспільству, державі бажаної системи цінностей, рішень у важливих сферах суспільної та державної діяльності. Власне все це є загрозою для України в життєво важливих сферах суспільної та державної діяльності, що реалізується на інформаційному рівні. Комплекс проблем,обумовлених можливістю втягнення України в інформаційну війну, вимагає розробки методологічних основ інформаційної безпеки, як фундаменту для формування і реалізації політики забезпечення національних інтересів на інформаційному рівні і створення національної системи інформаційної безпеки України. Під методологічними основами інформаційної безпеки слід розуміти єдність концептуальних, теоретичних і технологічних основ

забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, військової та екологічної, духовної тощо), а також сфер формування, циркулювання, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційне – аналітичне забезпечення органів державного управління в усіх різновидах діяльності тощо). Сутність та зміст інформаційної безпеки проявляється по особовому на кожному із рівнів державного управління зокрема на: стратегічному – Кабінет Міністрів України;тактичному – центральні виконавчі влади;оперативному – місцеві виконавчі влади (місцеві виконавчі адміністрації). Комісія з питань національної безпеки визначила такі потенційні загрози в інформаційній сфері: відсутність у міжнародного співробітництва об'єктивного уявлення про Україну; інформаційна експансія з боку інших країн;відтік інформації,що містить державну таємницю, а також конфіденційної інформації, що є власністю держави та підприємств; незбалансованість державної політики та відсутність необхідної інфраструктури в інформаційній сфері. Інформаційна безпека на підприємствах комплексне поняття, що містить в собі достатньо різнопланові аспекти. Воно включає в себе засоби фізичної перешкоди доступу зловмисників до захищеної інформації, керування доступом за допомогою регулювання ресурсів інформаційних систем та технологій, криптографічне закриття інформації, використання антивірусних програм, файерволів та інших засобів протидії шкідливим атакам. Крім того, до засобів захисту інформації відносять такі суто психологічні варіанти впливу на працівників, що мають доступ до секретних даних, такі як спонукання або примус. Автоматизована інформаційна система − взаємопов'язана сукупність даних, обладнання, програмних засобів, персоналу та стандартних процедур,які призначені для збору, обробки, розподілу та зберігання і представлення інформації згідно з вимогами, які випливають з цілей та місії сільськогосподарського підприємства. Автоматизовані облікові системи виступають потужним інструментом для гарантування економічної безпеки на підприємстві, бо без використання сучасних комп'ютерів і програм сама підприємницька діяльність стає неможливою. Управління загрозами здійснюється через запровадження заходів безпеки та планів на випадок непередбачених подій. Заходи безпеки передбачають попередження та розпізнання загроз. Для захисту інформації в автоматизованих облікових системах створюють комп’ютерну систему безпеки. Проблема полягає саме в тому, щоб визначити, яким чином автоматизовані облікові системи виступають інструментом для гарантування економічної безпеки на підприємстві і яку

роль вони відіграють. Автоматизована облікова система – це система, в якій інформаційний процес бухгалтерського обліку автоматизований завдяки застосуванню спеціальних методів оброблення даних, які застосовують комплекс розрахункових, комунікаційних і інших технічних засобів, щоб отримати і передати інформацію, необхідну фахівцям-бухгалтерам для виконання функцій управлінського і фінансового обліку. На тих підприємствах, на яких організація управління та обліку перебуває у незадовільному стані, створення й використання автоматизованої системи бухгалтерського обліку здатне не лише прискорити процес обробки інформації, а й істотно впорядкувати та удосконалити його. Така можливість зумовлена тим, що автоматизований спосіб обробки облікової інформації вимагає формального та чіткого опису облікових процедур у вигляді алгоритмів, що впорядковує виконання обов'язків обліковими працівниками. Ведення обліку в умовах автоматизованих облікових систем залежить від таких факторів: рівня автоматизації бухгалтерського обліку та контролю, наявності методик проведення автоматизованого обліку, ступеня доступності облікових даних, складності обробки інформації. При цьому велике значення мають власні характеристики системи обробки даних, оскільки вони впливають на ступінь розробленості бухгалтерської системи. Використання АОС у системі економічної безпеки на підприємстві забезпечується шляхом:1) дотримання суб'єктами правових відносин норм, вимог і правил організаційного та технічного характеру щодо захисту опрацьованої інформації; 2) використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку та АОС загалом, засобів захисту інформації, які відповідають встановленим вимогам щодо її захисту (мають відповідний сертифікат); 3) перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку та АС загалом встановленим вимогам щодо захисту інформації (сертифікація засобів обчислювальної техніки, засобів зв'язку і АС); 4) здійснення контролю щодо захисту інформації. Результатами порушення прав захисту інформації в автоматизованих облікових системах можуть бути: витік інформації, втрата інформації, підроблення інформації, порушення роботи АОС. Автоматизованою системою безпеки на підприємстві має управляти головний фахівець з безпеки, який повинен звітувати безпосередньо керівнику про кожну фазу життєвого циклу автоматизованих облікових систем. У разі ефективного застосування АОС нівелювання ризиків, які пов'язані з безпекою підприємства, можна передбачати чотири етапи:

1. Ідентифікацію засобів захисту на визначеній ділянці автоматизованої системи.

2. Оцінку надійності засобів захисту на цій ділянці.

3. Оцінку ймовірності, що акт порушення безпеки буде успішний, з огляду на набір засобів захисту на цій ділянці автоматизованої системи і їхньої надійності.

4. Оцінку втрат, що понесе підприємство, якщо акт порушення безпеки обмине засоби захисту в цьому місці автоматизованої системи.

Аналіз чотирьох етапів ризиків, пов'язаних з безпекою підприємства під час використання автоматизованих облікових систем, дає змогу визначити їх слабкі місця. Ризик, пов'язаний з безпекою, – це очікувана величина витрат за визначений період з огляду на надійність засобів захисту. Слабкі місця виникають тому, що немає жодного засобу, щоб запобігти акту порушення безпеки, або є імовірність, що засіб гарантування безпеки на визначеній ділянці автоматизованої системи не спрацює проти специфічного інциденту, що відбудеться. Щодо організаційної структури автоматизованих облікових систем, то керівництво може застосувати такі дії: розподіл обов'язків, нагляд, вимушені відпустки та зміна роботи (посади), подвійний контроль, "судовий облік" (опис діяльності осіб, зацікавлених у попередженні та розпізнаванні шахрайства і злочину співробітників). Розподіл обов'язків передбачає розподіл функцій дозволу та запису операцій, розподіл функцій дозволу та зберігання активів, розподіл функцій запису операцій та зберігання активів. При цьому застосовують такі контрольні процедури, як перевірка виконання операцій відповідно до розподілених обов'язків, перевірка застосування затверджених бланків документів і записів, перевірка здійсненого доступу до активів відповідно до санкцій керівництва, незалежні перевірки стану активів у підзвітності матеріально відповідальних осіб і результатів їх діяльності, перевірка процесу опрацювання інформації відповідно до дозволів, її точності, повноти окремих операцій. На тих підприємствах, де організація управління та обліку перебуває у незадовільному стані, створення й використання автоматизованої системи бухгалтерського обліку здатні не лише прискорити процес оброблення інформації, а й істотно впорядкувати та покращити його. Така можливість зумовлена тим, що автоматизований спосіб оброблення облікової інформації потребує формального та чіткого опису облікових процедур у вигляді алгоритмів, що впорядковує виконання обов'язків обліковими працівниками. Ведення обліку в умовах автоматизованих облікових системах залежить від таких чинників: рівня автоматизації бухгалтерського обліку та контролю, наявності методик здійснення автоматизованого обліку, ступеня доступності облікових даних, складності опрацювання інформації. При цьому велике значення мають

власні характеристики системи оброблення даних, тому що вони впливають на ступінь розроблення бухгалтерської системи. Існує два основних підходи до аналізу вразливих місць і загроз автоматизованих облікових систем на підприємстві – кількісний та якісний. Кількісний підхід до оцінки ризику — кожен рівень ризику потенційних збитків обчислюється як результат добутку вартості окремого збитку та вірогідності його виникнення. При застосуванні кількісного підходу може бути складно оцінити кожен випадок збитку та вірогідність його виникнення, а також передбачити майбутні події. Якісний підхід до оцінки ризику показує вразливі місця та загрози системи,суб'єктивно розставляючи їх у порядку значущості для сукупної доступності компанії ризику потенційних збитків. Незалежно від методів, які застосовуються, будь-який аналіз має містити оцінку ризиків, які впливають на припинення виробництва, втрату програмного забезпечення, втрату даних, апаратного забезпечення, виробничих потужностей, послуг і працівників.

Висновки та пропозиції. З вищезазначеного формулюється важлива думка, інформаційна безпека являє собою одне із найважливіших понять у науці і різних сферах підприємницької діяльності. Облік є важливою функцією управління і багато нових концепцій менеджменту побудовані саме навколо автоматизованих облікових систем, які відіграють значну роль на сучасних підприємствах. Вони безпосередньо обслуговують процеси планування і прийняття рішень, допомагають розробити номенклатуру і технологію виготовлення та реалізації товарів і послуг. Під час застосування автоматизованих облікових систем, підприємство може використовувати їх як інструмент для забезпечення економічної безпеки цього підприємства і за допомогою цих інструментів дає змогу: 1) досліджувати найважливіші чинники, які впливають на стан функціональних складників економічної безпеки; 2) вивчати основні процеси, що впливають на гарантування економічної безпеки підприємства; 3) розробляти заходи щодо забезпечення максимально високого рівня функціональних складників економічної безпеки підприємства. Незважаючи на те, що в Україні прийнято і чинна низка нормативних актів, проблему функціонування автоматизованих облікових систем, як інструментів економічної безпеки під час застосування комп'ютерних програм бухгалтерського обліку на підприємствах досі не вирішено. Безпека – сфера достатньо закрита, а пов'язані з нею проблеми – однієї з найскладніших у розвитку автоматизованих облікових систем. Оскільки на підприємствах переважна більшість процесів автоматизовані, то будь-який збій може призвести до великих збитків. Отже, із-за провадженням автоматизованих облікових систем на підприємстві,

бухгалтери та управлінці отримують численні переваги. Для того, що б це не було проблематично, на підприємстві потрібно створити ефективну автоматизовану облікову систему з найменшими витратами, добрати персонал для роботи з цією системою, вибрати оптимальну облікову систему для підприємства, вибрати структуру комп'ютерної бухгалтерії для того, щоб ефективно гарантувати економічну безпеку на підприємстві.

Бібліографічний список: 1. Барчан Г.Ю. Безпека і бізнес: правові та управлінські аспекти: монографія / Г.Ю. Барчан, О.Г. Барчан. – К.: Сталь, 2008. – 164 с. 2. Левко В.Л. Економічна безпека підприємства: навч. посібник [для вищ. навч. закладів] / В.Л. Левко, Н.В.Ващенко. – К.: Центр учб. літ-ри, 2008. – 240с. 3. Сороківська О.А. Інформаційна безпека підприємства:нові загрози та перспективи / О.А. Сороківська, В.Л. Левко// Вісн. Хмельницького нац. ун-ту. – 2010. – № 2. – Т.2. – С. 32-35. 4. Петрина О.Б. Передумови формування та зміст економічної безпеки підприємства // Наук. вісник НЛТУ України. – 2010. – Вип. 20.3. – С. 206-216. 5. Стратегічні напрямки соціально – економічного розвитку держави в умовах глобалізації: збірник тез міжнародної науково – практичної конференції (м. Хмельницьк, 18−20 квітня 2013 року). – Хмельницький: Хмельницький університет управління та права, 2013. – 514 с. 6. Федоркова І.Н.Сучасне інформаційне суспільство: критичний аналіз [текст] / І.Н. Федоркова. – Чернівці: Рута, 2008. – 140 с.

Куделя Л.В. Автоматизированные учетные системы – инструмент обеспечения экономической безопасности предприятия. Данная статья дает определение информационной безопасности и раскрывает сущность этого определения, показывает роль информационной безопасности в деятельности предприятия; раскрывает комплекс мероприятий, с помощью которых возможно рассматривать автоматизированные учетные системы, как инструмент обеспечения экономической безопасности на предприятии.

Kudelya L. Computer aided registration systems – instrument of providing of economic security of enterprise. This article is gives determination of informative safety and exposes essence of this determination, the role of informative safety shows in activity of enterprise, exposes the complex of measures with a help, which possible to examine automatic registration systems, as an instrument of avouching for economic security on an enterprise.