УДК 657

***Муравський В.В.*,**
викладач кафедри економічної кібернетики та інформатики
Тернопільський національний економічний університет

ІНФОРМАЦІЙНІ ПРАВОПОРУШЕННЯ В КОМП'ЮТЕРНИХ СИСТЕМАХ БУХГАЛТЕРСЬКОГО ОБЛІКУ

Постановка проблеми. Бухгалтерський облік є джерелом інформаційних ресурсів для оцінки, аналізу і прогнозування економічних процесів на підприємстві. В Україні, яка стала на шлях побудови правової держави з ринковою економкою та вступила в міждержавні економічні інституції, появилася потреба в переході від забезпечення окремих ділянок обліку, аналізу, контролю та прогнозування до комплексного, інтегрованого процесу вирішення цих питань. Значно зросли обсяги інформації, яку необхідно збирати, передавати, перетворювати, розповсюджувати та використовувати для прийняття управлінських рішень. З'явилася потреба у створенні інтегрованих інтелектуальних інформаційних систем для розрахунково-діагностичних цілей, підтримки прийняття та виконання дій по управлінню підприємством.

Прискоренню науково-технічного і соціально-економічного прогресу сприяє застосування нових автоматизованих інформаційних систем, обчислювальних мереж і комплексів, інформаційно-комп'ютерних технологій, розвиток засобів телекомунікації, мобільного зв'язку, які дозволили автоматизувати виробництво, спростили вибір альтернатив та прийняття ефективних управлінських рішень.

Чільне місце серед комп'ютерних інформаційних систем займають інформаційні автоматизовані системи бухгалтерського обліку, які крім реєстрації господарських операцій забезпечують переробку різних вхідних даних в надійну оперативну інформацію, необхідну для управління господарськими процесами на основі новітніх програмно-апаратних засобів з аналізом, оцінкою потреби їх впровадження в конкретні сфери діяльності суб'єктів ринку і практику менеджменту, маркетингу, управління персоналом, фінансами, інвестиціями, закупками, запасами, збереженням, збутом і реалізацією товарів та послуг.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження проблем інформаційної безпеки в автоматизованих системах бухгалтерського обліку та забезпечення достовірності інформації здійснили такі вітчизняні та зарубіжні науковці, як Ю.М. Арсеньєв, Ф.Ф. Бутинець, О.С. Височан, В.М. Гужва [4], Т.Ю. Давидова, В.В. Євдокимов, Н.В. Єрьоміна, В.П. Завгородній, А.Г. Загородній, С.В. Івахненков, Ю.А. Кузьмінський, О.С. Краєва, Т.А. Писаревська, В.Ф. Ситник [6], Г.А. Титоренко, С.І. Шелобаєв, В.Д. Шквір [7], Дж. Боднар [8] та інші.

Проте, із загостренням конкуренції на рину товарів і послуг, із впровадженням нових інформаційних технологій та автоматизованих систем обробки інформації значного поширення набув промисловий шпіонаж та появилися нові методи несанкціонованого отримання конфіденційної інформації, спостерігається комп'ютерне шахрайство, втручання до процесів обробки інформації з метою фальсифікації даних та програм, комп'ютерний саботаж. Питання забезпечення безпеки при обробці інформації залишається відкритим і потребує постійного дослідження та уваги науковців.

Постановка завдання. Метою дослідження є класифікація та узагальнення проблем інформаційної безпеки в комп'ютерних системах бухгалтерського обліку, пошук дієвих засобів запобігання правопорушень при роботі з економічною інформацією та надання пропозицій щодо усунення наслідків таких правопорушень.

Виклад основного матеріалу дослідження. Для забезпечення інформаційної безпеки необхідно постійно підтримувати наступні властивості інформації [2]:

- доступність – забезпечити безперешкодний доступ суб'єктів до потрібних даних і готовність відповідних служб надати інформацію за вимогою;
- цілісність – властивість її достовірності, яка складається з адекватності (повноти і точності) та неспотвореності;
- конфіденційність – суб'єктивно визначена властивість, яка вказує на введення обмежень для суб'єктів, що мають доступ до інформації та забезпечують збереження її від осіб, які не мають доступу, з метою захисту прав інших суб'єктів інформаційних відносин;
- безпечність – захист інформації від витоку, модифікації або втрати. Витік – це ознайомлення сторонньої особи зі змістом секретної чи конфіденційної інформації. Модифікація – несанкціонована зміна інформації, коректна по формі і змісту, але інша по смислу. Втрата інформації – її фізичне знищення.

Для забезпечення безпеки інформації є необхідним комплексний захист всіх компонентів інформаційних технологій та автоматизованої системи обробки (технічних та апаратних засобів,

програмних засобів, даних, персоналу підприємства). З цією метою будується система захисту – комплекс спеціальних засобів законодавчого і адміністративного характеру, організаційних заходів, фізичних та програмно-апаратних засобів захисту, а також спеціального персоналу, який забезпечує безпеку інформації, інформаційних технологій та автоматизованої системи в цілому.

Для створення ефективної системи захисту необхідно визначити, що таке загроза безпеці інформації, які є шляхи для несанкціонованого доступу до даних, якими каналами можливий витік інформації.

Загроза безпеці інформації – це дія або подія, які можуть знищити, спотворити або привести до несанкціонованого використання інформаційних ресурсів [1].

Загрози поділяють на *випадкові* та *навмисні*. *Випадкові* можуть виникати при неправильних діях персоналу, помилках в програмному забезпеченні, виході з ладу технічних засобів. *Навмисні*, на відміну від випадкових, спрямовані на нанесення збитків підприємству чи організації та поділяються на *активні* і *пасивні*.

Пасивні загрози не впливають на функціонування інформаційної системи і метою мають несанкціоноване отримання інформації.

Активні загрози спрямовані на порушення нормального функціонування системи шляхом навмисного впливу на технічні засоби та програмне забезпечення, діями по знищенню, спотворенню чи модифікації інформації.

До основних загроз безпеці інформації відносять:

- втрата конфіденційності інформації;
- несанкціоноване використання інформації;
- компрометація інформації;
- помилкове використання інформаційних ресурсів;
- відмова від інформації.

Розкриття конфіденційності інформації та несанкціоноване її використання здійснюється шляхом непередбаченого доступу сторонніх осіб до баз даних і наносить власнику цих даних значний збиток.

Компрометація інформації відбувається через несанкціоновані зміни зловмисниками даних у базах, через що власник інформації або змушений відмовитися від неї, або здійснити додаткові процедури по її відновленню і піддається загрозі в прийнятті неправильних рішень.

Помилкове використання інформаційних ресурсів може бути причиною наявних помилок в програмному забезпеченні і спонукає користувача до неправильних дій та здійснення недостовірних висновків.

Основними шляхами порушення інформаційної безпеки є:

- застосування підслуховуючи пристроїв;
- перехват електронних випромінювань;
- викрадення носіїв інформації та відходів документів;
- читання залишкової інформації в пам'яті системи після здійснення санкціонованих запитів;
- копіювання носіїв інформації через подолання системи захисту;
- маскування під зареєстрованого користувача;
- використання програмних пасток;
- використання недоліків операційної системи та програмних засобів;
- незаконне підключення до технічних засобів та каналів передавання інформації;
- зламування системи захисту інформації;
- впровадження та використання комп'ютерних вірусів.

Для створення ефективної системи захисту інформації необхідно:

- виявити можливі шляхи витоку інформації і несанкціонованого доступу до даних;
- виявити джерела і види загроз безпеці інформації;
- створити математичну модель потенційного порушника;
- вибрати відповідні методи, механізми і засоби захисту;
- створити замкнену комплексну систему захисту на етапі проектування інформаційної системи.

На стадії передпроектного обстеження необхідно:

- визначити, яка інформація є конфіденційною, оцінити рівень її конфіденційності та обсяг;
- вивчити можливості використання готових сертифікованих систем захисту, що пропонуються на ринку;
- визначити, які технічні засоби необхідно встановити, які режими обробки інформації (діалоговий, режим реального часу тощо);
- встановити, який персонал підприємства буде задіяний для роботи з інформацією, характер його взаємодії між собою та службою безпеки;
- забезпечити режим секретності на стадії розробки.

При експлуатації інформаційної системи бухгалтерського обліку необхідно передбачити ряд методів захисту інформації (рис. 1).

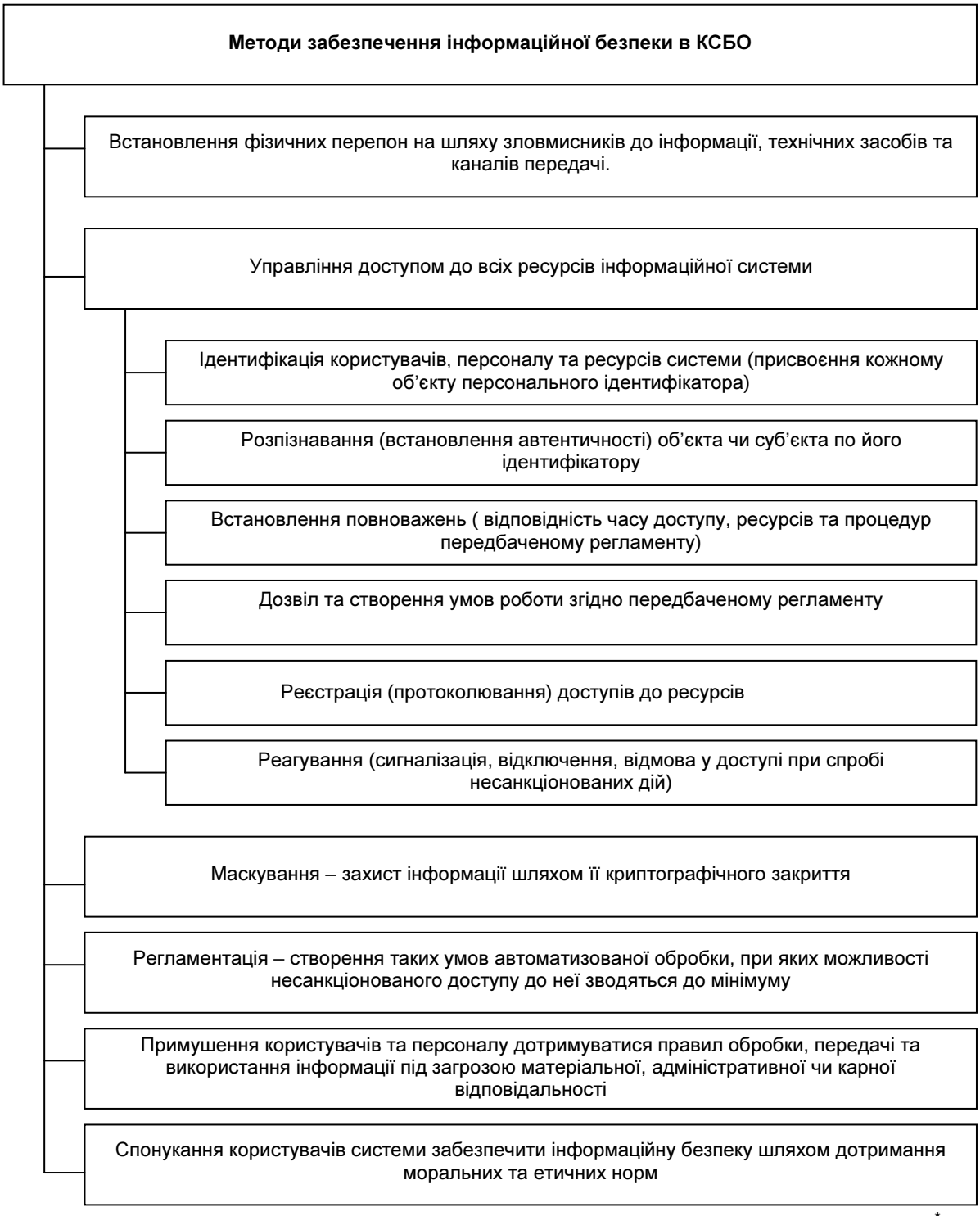

Рис. 1. Класифікація методів забезпечення інформаційної безпеки в КСБО*

** - Розроблено автором на основі [1; 2]*

Захист інформації базується на принципах системності, комплексності, неперервності, гнучкості, простоти захисних методів та способів. Створити абсолютно нездоланну систему захисту інформації в принципі неможливо, тому необхідно забезпечити прийнятний рівень безпеки, виходячи з можливих втрат від порушення конфіденційності інформації та фінансових витрат на впровадження системи захисту [3; 5].

Методи забезпечення інформаційної безпеки реалізуються за рахунок застосування технічних, програмних, організаційних, законодавчих та морально-етичних засобів (рис. 2).

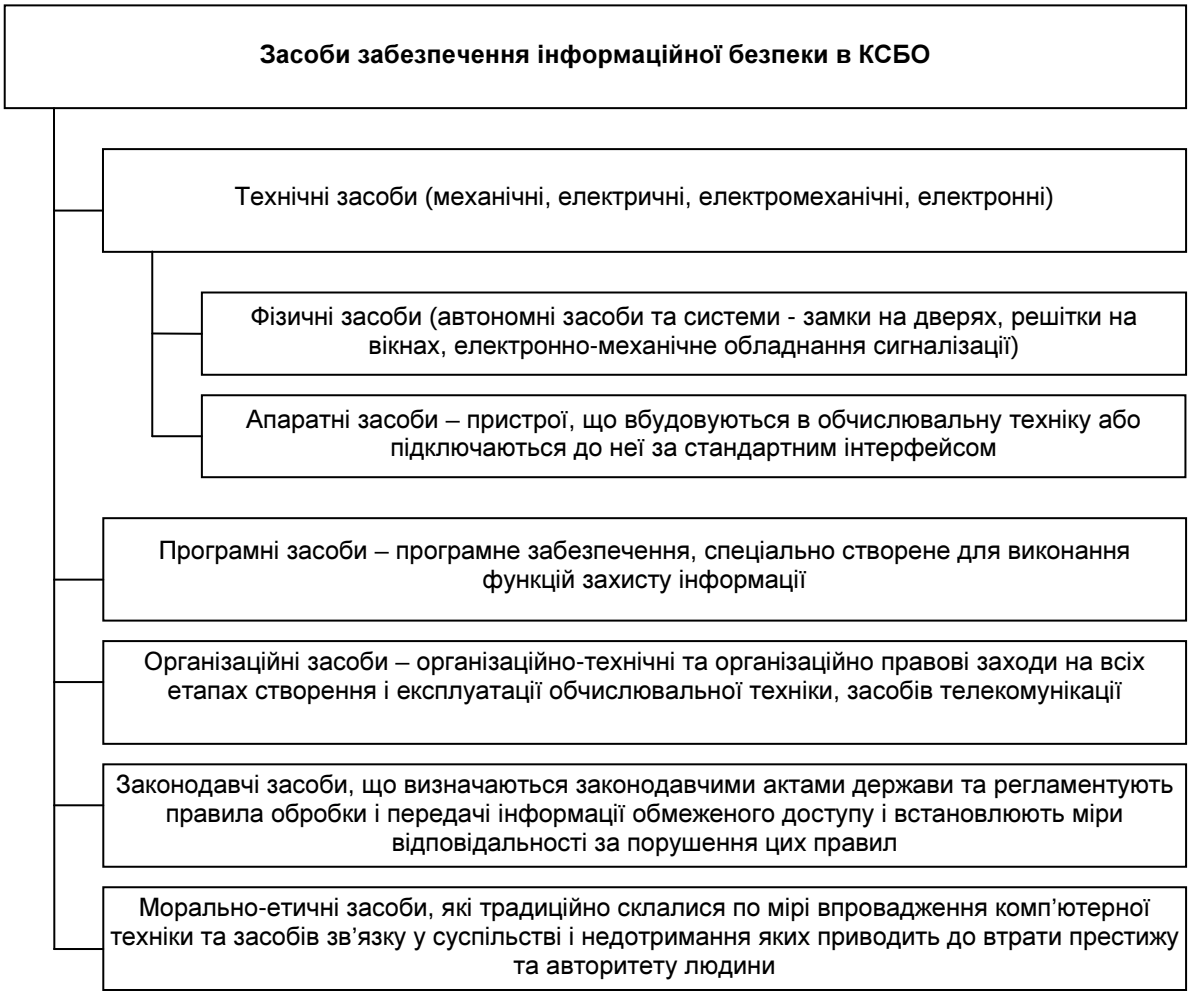

Рис. 2. Класифікація засобів забезпечення інформаційної безпеки в КСБО*

**Джерело:- Розроблено автором на основі [1; 2]*

Створивши на підприємстві належну систему захисту інформації, необхідно провести оцінку цієї системи з аналізом її характеристик і вимог шляхом сертифікації в процесі впровадження. Процес удосконалення системи захисту є неперервним в часі і здійснюється одночасно з функціонуванням комп'ютерної системи бухгалтерського обліку.

Висновки з даного дослідження. Правильне розуміння проблем захисту інформації в інформаційних системах бухгалтерського обліку, їх належне виокремлення та класифікація дає можливість адекватно забезпечити інформаційну безпеку, знайти дієві методи запобігання зловживанням та спробам несанкціонованого доступу до інформації.

Бібліографічний список

1. Автоматизированные информационные технологии в экономике: учебник / под. ред. проф. Г.А. Титоренко. – М. : Компьютер, ЮНИТИ, 1999. – 400 с.

2. Арсеньєв Ю.Н. Информационные системы и технологии. Экономика. Управление. Бизнес [Текст] : учеб. пособие. / Ю.Н. Арсеньев, С.И. Шелобаев, Т.Ю. Давыдова. – М. : ЮНИТИ-ДАНА, 2006. – 447 с.

3. Інформаційні системи бухгалтерського обліку. [Текст]: / Ф.Ф. Бутинець, С.В. Івахненков, Т.В.Давидюк, Т.В. Шахрайчук ; за ред. проф. Ф.Ф. Бутинця. – 2-гє вид., доп. і перероб. – Житомир: ПП. „Рута", 2002. – 543 с.

4. Гужва В.М. Інформаційні системи і технології на підприємствах [Текст] : навч. посіб. / В.М. Гужва. – К. : КНЕУ, 2001. – 400 с.

5. Івахненков С.В. Інформаційні технології в організації бухгалтерського обліку та аудиту [Текст] : навч. посіб. / С.В. Івахненков. – К.: Знання-Прес, 2003. – 349 с.

6. Основи інформаційних систем [Текст]: / В.Ф. Ситник, Т.А. Писаревська, Н.В. Єрьоміна, О.С. Краєва. – К. : КНЕУ, 1997. – 252 с.

7. Шквір В.Д. Інформаційні системи і технології в обліку [Текст] : навч. посіб. / В.Д. Шквір, А.Г. Загородній, О.С. Височан. – 3-тє вид., перероб. і доп. – К. : Знання, 2007. – 439 с.

8. Bodnar George H. Accounting Information Systems [Text] : / George H. Bodnar, William S. Hopwood. – 7-th ed. – Upper Saddle River, Prentice-Hall, Inc., 1988. – 686 p.

Анотація

У статті обґрунтовано необхідність досліджень в галузі інформаційної безпеки, класифіковано та узагальнено проблеми захисту інформації в комп'ютерних системах бухгалтерського обліку, здійснено пошук дієвих засобів запобігання правопорушень при роботі з економічною інформацією та надано пропозиції щодо вибору методів та засобів комплексного захисту всіх компонентів інформаційних технологій та автоматизованої системи обробки облікової інформації (технічних та апаратних засобів, програмних засобів, персоналу підприємства).

Ключові слова: *інформаційна безпека, пасивні загрози, активні загрози, управління доступом, ідентифікація користувачів, методи, засоби захисту.*

Аннотация

В статье обоснована необходимость исследований в области информационной безопасности, классифицированы и обобщены проблемы защиты информации в компьютерных системах бухгалтерского учета, осуществлен поиск действенных средств предотвращения правонарушений при работе с экономической информацией и даны предложения по выбору методов и средств комплексной защиты всех компонентов информационных технологий и автоматизированной системы обработки учетной информации (технических и аппаратных средств, программных средств, персонала предприятия).

Ключевые слова: *информационная безопасность, пассивные, активные угрозы, управление доступом, идентификация пользователя, методы защиты.*

Annotation

The article substantiates the need for research in the field of information security, classified and summarized the problem of information security in computer systems accounting searched effective means of preventing crime when dealing with economic information and provided suggestions for the choice of methods and means of integrated protection of all components of information technology and automated process of accounting information (technical, hardware, software, personnel).

Key words*: informative safety, passive and active threats, access control, user identification, methods of informative safety providing.*