УДК 004.01:65.012.48

КОНТРОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

© 2015 **ЯНЧЕВ А. В.**

УДК 004.01:65.012.48

Янчев А. В. Контроль інформаційної безпеки в системах електронного документообігу

Досліджено місце інформаційного ризику в контексті функції захисту інформації; проаналізовано динаміку зростання інформаційних загроз сучасності в системах електронного документообігу; розроблено концептуальну модель інформаційного захисту систем електронного документообігу; запропоновано науково обґрунтовану класифікацію інформаційних загроз, яка дозволяє чітко визначити потенційні види загроз, коло об'єктів захисту та комплекс заходів, що сприятиме досягненню стійкого стану інформаційної безпеки.

Ключові слова: *електронний документообіг, інформаційний захист, загроза, інформаційна безпека.*
Рис.: *3.* ***Табл.:*** *3.* ***Бібл.:*** *9.*

Янчев Андрій Володимирович *– кандидат економічних наук, доцент, обліково-фінансовий факультет, Харківський державний університет харчування та торгівлі (вул. Клочківська, 333, Харків, 61051, Україна)*
E-mail: *yanchev.andrei@rambler.ru*

УДК 004.01:65.012.48

Янчев А. В. Контроль информационной безопасности в системах электронного документооборота

Исследована роль информационного риска в контексте функции защиты информации; проанализирована динамика роста информационных угроз в системах электронного документооборота; разработана концептуальная модель информационной защиты систем электронного документооборота; предложена научно обоснованная классификация информационных угроз, которая позволяет четко определить потенциальные виды угроз, круг объектов защиты и комплекс мероприятий, которые способствуют достижению устойчивого состояния информационной безопасности.

Ключевые слова: *электронный документооборот, информационная защита, угроза, информационная безопасность.*
Рис.: *3.* ***Табл.:*** *3.* ***Библ.:*** *9.*

Янчев Андрей Владимирович *– кандидат экономических наук, доцент, учетно-финансовый факультет, Харьковский государственный университет питания и торговли (ул. Клочковская, 333, Харьков, 61051, Украина)*
E-mail: *yanchev.andrei@rambler.ru*

UDC 004.01:65.012.48

Yanchev A. V. Control of Information Security in Electronic Documents Management Systems

The role of information risk in the context of function of the information protection has been explored; the growth dynamics of threats to the information security in the systems of electronic document management has been analyzed; a conceptual model of protecting the information in electronic documents management systems has been developed; a scientifically grounded classification of information security threats, which provides with clearly identified potential threats, the circle of objects for protection and the range of activities that contribute to the attainment of steady state of information security, has been proposed.

Key words: *electronic document management, information protection, threats, information security.*
Pic.: *3.* ***Tabl.:*** *3.* ***Bibl.:*** *9.*

Yanchev Andrey V. *– Candidate of Sciences (Economics), Associate Professor, Faculty of Accounting and Finance, Kharkiv State University of Food Technology and Trade (vul. Klochkivska, 333, Kharkiv, 61051, Ukraine)*
E-mail: *yanchev.andrei@rambler.ru*

Рівень інтегрованості України до світових інформаційних процесів щороку зростає. Проникнення інформаційних технологій у всі сфери життя українського суспільства досягає загальносвітових показників, створюючи інформаційне суспільство. Невизначеність і породжений нею ризик є невід'ємною частиною практично всіх прийнятих рішень в управлінні діяльністю підприємств [1, с. 57]. Діяльності будь-якого підприємства притаманне розмаїття ризиків – економічних, екологічних, соціально-політичних, правових. Проте революція у сфері комунікацій та інформації зумовила актуалізацію відносно нового виду ризиків – інформаційного. Функції захисту інформації мають виконуватися в рамках функцій її збору та обробки. Відповідно інформаційний захист є істотною складовою інформаційної системи бухгалтерського обліку та становить одну з головних функцій сучасної системи управління [2, с. 35].

Сьогодні Україна все частіше стикається з усе більш масштабними проявами комп'ютерної злочинності, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем [3]. Високий рівень загроз у кібернетичному просторі підтверджується дослідженнями відомого німецького оператора зв'язку Deutsche Telecom, за даними якого Україна опинилася на четвертій позиції у світі серед країн – джерел кібернетичних атак. Тільки протягом лютого 2013 р. з території України їх було здійснено 566 тисяч.

Підрозділом реагування на комп'ютерні надзвичайні події України CERT-UA, який функціонує у складі Державної служби спеціального зв'язку та захисту інформації України, протягом 2012 р. зафіксовано та вжито заходи з реагування на 31 комп'ютерний інцидент, які стосувалися захищеності інформаційних ресурсів державних органів. Найбільш розповсюдженими різновидами атак були такі: несанкціонований доступ до автоматизованих систем (17 випадків) та DDoS атаки (6 випадків) на державні інформаційні ресурси. Крім того, на 150 веб-сайтах українського сегмента мережі Інтернет для протидії несанкціонованому втручанню спецслужбами України було вжито заходів з блокування/видалення фішингового контенту. При цьому маємо враховувати, що за перше півріччя 2013 р. кількість таких інцидентів уже становила 33, що однозначно свідчить про зростання відповідних загроз.

Тривожною є і порівняльна статистика. Якщо за весь 2012 р. було зафіксовано лише п'ять випадків експлуатації технічних вразливостей систем, то лише за першу половину 2013 р. кількість таких випадків становила 13. Інший небезпечний показник: якщо протягом

усього 2012 р. був зафіксований лише один випадок цільового враження державних інформаційних ресурсів, то за першу половину 2013 р. таких випадків зафіксовано шість. Усе це свідчить не просто про кількісне зростання спроб стороннього впливу на державні інформаційні ресурси, а про збільшення кількості цілком свідомих атак на певні системи. Ці атаки все частіше проводяться не просто методами, схожими на дрібне хуліганство, а з цільовим використанням вразливостей систем.

Про ситуацію загострення в Україні кібербезпечної проблематики свідчать і звітні показники Служби безпеки України. Слідчими органами СБУ протягом другого півріччя 2012 р. і першого півріччя 2013 р. порушено 114 кримінальних проваджень у справах використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку, із них у другому півріччі 2012 р. – 45, у першому півріччі 2013 р. – 59 за ст. 361, 361-1, 361-2, 362, 363 розділу XVI Кримінального кодексу України.

Ще більш показовими є дані МВС України відносно зростання рівня кіберзлочинності. Стрімко зростає кількість шахрайств, які здійснюються за допомогою високих інформаційних технологій: лише за шість місяців 2013 р. їх було виявлено 986, у той час як за весь 2012 р. їх виявлено 1663. Щодо зростання кількості виявлених злочинів, пов'язаних із незаконними діями з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення: за весь 2012 р. виявлено 21 випадок, у той час як стільки ж виявлено лише за півроку 2013 р.

Мета статті полягає в розробці теоретичних засад і прикладних рішень з побудови надійної системи інформаційного захисту як складової системи контролю економічної безпеки суб'єктів господарювання та елементу інформаційної політики держави, що набуває актуальності внаслідок експоненціального зростання кількості злочинів у інформаційній сфері, швидкого розповсюдження систем електронного документообігу, появи глобальних баз даних (у тому числі персональної інформації та інформації, що є комерційною таємницею).

Зміст інформаційного захисту полягає в забезпеченні всього комплексу організаційно-технічних, організаційно-режимних заходів кадрової роботи, що спрямовано на збереження таємниці та належного контролю працівників обліку [4, с. 267]. Погоджуючись із думкою автора, вважаємо, що до кадрової компоненти системи інформаційного захисту слід віднести не лише облікових працівників, а й весь персонал підприємства, задіяний у створенні документів, їх внесенні до бази даних, обробці, підготовці узагальнених звітів, передачі та використанні документів. Така система, на наш погляд, має складатися з низки компонентів, комплексна взаємодія яких забезпечує досягнення стану захищеності суб'єкта господарювання від загрози матеріальних втрат (*рис. 1*).

Загрози інформаційної безпеки мають тактичний характер і чинять прямий вплив на руйнування чи ослаблення фінансово-майнового стану [5, с. 179]. Отже, підприємствам необхідно чітко визначити потенційні види загроз, коло об'єктів захисту та комплекс заходів, що сприятимуть досягненню стійкого стану інформаційної безпеки. Вирішенню зазначеного комплексу завдань сприятиме науково обґрунтована класифікація інформаційних загроз.

У літературних джерелах низка авторів приділяли увагу як питанням класифікації загроз економічній безпеки взагалі [5, с. 180], так і виділенню груп загроз і правопорушень у сфері застосування інформаційних технологій зокрема [2, с. 138 – 139; 6, с. 80; 7, с. 118; 8, с. 193 – 200]. Спільним для більшості класифікацій є виділення в ролі класифікаційної ознаки виду загроз (втручання, шахрайство, перехоплення, кіберзлочинність, компрометація, розголошення інформації, відмова в ін-

Рис. 1. Концептуальна модель інформаційного захисту систем електронного документообігу

формації та ін.); вірогідність виникнення (висока, середня, низька); санкціонованість доступу; види шкідливих програм (вірус, троянський кінь, черв та ін.). Наведені точки зору орієнтовано більшою мірою на технологічні аспекти цілісності інформаційних систем і процесів передачі даних (технічні, програмні). На основі аналізу основних загроз систем електронного документообігу загрози економічної та інформаційної безпеки необхідно класифікувати для найбільш повної й адекватної ідентифікації: за ступенем усвідомлення (*табл. 1*); за джерелом загрози, за природою виникнення, за ймовірністю реалізації, за відношенням до виду людської діяльності, за об'єктом посягання, за наслідками, за можливостями прогнозування (*рис. 2*).

Одна з основних цілей моделювання в галузі інформаційної безпеки (*ІБ*) – побудова моделі, яка враховувала б найбільшу кількість чинників впливу і дозволяла б розраховувати ймовірність виникнення вразливості та реалізації загрози, обчислювати час реалізації загрози і можливі збитки, визначати ефективність упровадження засобів захисту та ступінь захищеності системи [9, с. 142]. Запропонована класифікація загроз безпеці електронного документообігу може бути

Таблиця 1

Види загроз безпеки інформації та їх характеристика

Ненавмисні загрози	**Навмисні загрози**	
	Пасивні	**Активні**
Помилки у вхідній інформації	Використання ресурсів за призначенням	Крадіжка обладнання
		Саботаж
		Порушення апаратної або програмної інфраструктури
Порушення інфраструктури (коротке замикання, стихійне лихо, перепади струму)	Несанкціонований перегляд інформації (підслуховування, шпигунство)	Навмисний злом системи безпеки (підбір пароля)
		Порушення роботи web-сайта
		Шкідливі програми (вірусні програми)
Характеристика		
Джерела: некваліфіковані дії чи неуважність користувачів або адміністрації, вихід із ладу апаратних засобів, помилки в програмному забезпеченні, стихійні катаклізми, бруд, пил тощо	Мають на меті завдання збитку користувачам інформаційної системи	
	Спрямовані на несанкціоноване використання інформаційних ресурсів системи, не порушуючи при цьому її функціонування	Спрямовані на цілеспрямований вплив на апаратні, програмні та інформаційні ресурси
	Джерелом пасивних загроз можуть бути як внутрішні користувачі системи, які можуть мати ненавмисний характер, так і зовнішні користувачі, метою яких є навмисні порушення	Джерелами активних загроз можуть бути зовнішні користувачі, несумлінні працівники, комп'ютерні віруси

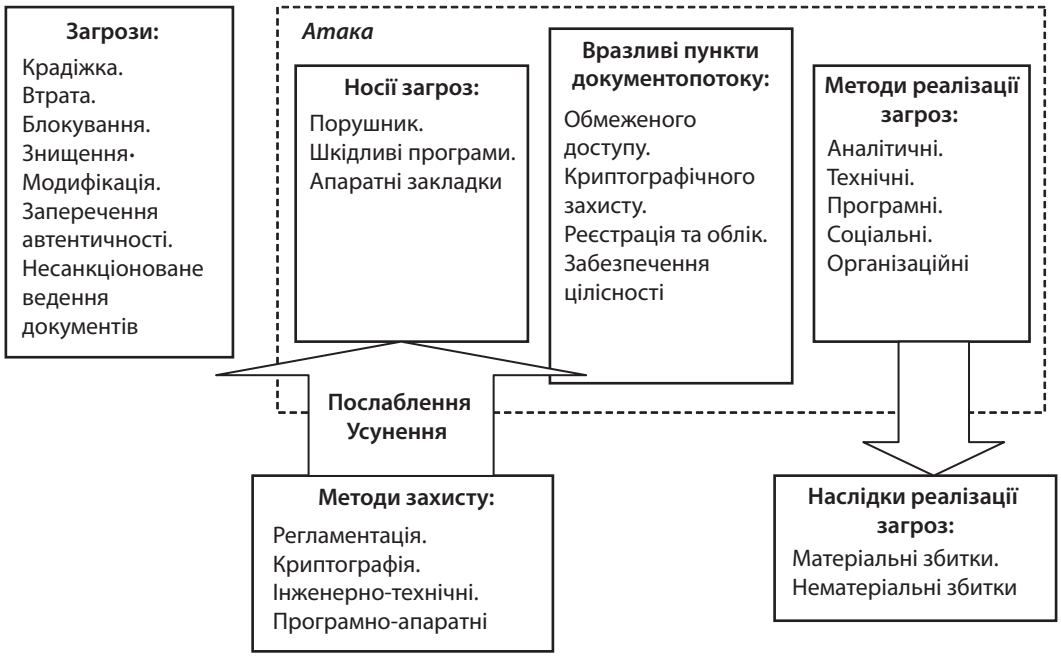

Рис. 2. Класифікація загроз у системі електронного документообігу

основою для вироблення методики оцінки актуальності тієї чи іншої загрози з метою вибору методів і засобів для їх запобігання або нейтралізації. У разі виявлення актуальних загроз експертно-аналітичним методом визначаються об'єкти захисту, схильні до дії тієї чи іншої загрози, характерні джерела цих загроз і вразливості, що сприяють реалізації загроз.

На підставі аналізу складається матриця взаємозв'язку джерел загроз і вразливостей, із якої визначаються можливі наслідки реалізації загроз (атаки) і обчислюється коефіцієнт значущості (ступеня небезпеки) цих атак як добуток коефіцієнтів небезпеки відповідних загроз і джерел загроз, визначених раніше. При цьому під актуальною слід вважати загрозу, яка може бути реалізована в системі електронного документообігу і становить небезпеку для електронного архіву. Для складання переліку актуальних загроз застосовується оцінка можливості реалізації загрози шляхом розрахунку рівня вихідної захищеності системи та частоти (імовірності) реалізації можливої загрози. Коефіцієнт вихідної захищеності системи електронного документообігу – узагальнений показник, який залежить від технічних та експлуатаційних характеристик системи (*табл. 2*), яка була розроблена для оцінки захищеності систем персональних даних. Для даного дослідження пристосовано вербальний розрахунковий інструментарій захищеності, який є актуальним для локальних систем електронного документообігу.

Вихідний ступінь захищеності визначається таким чином.

1. Система електронного документообігу має високий рівень вихідної захищеності, якщо не менше 70% характеристик відповідають рівню «високий» (підсумовуються позитивні рішення за першим стовпцем, відповідним високому рівню захищеності), а решта – середнього рівня захищеності (позитивні рішення за двома стовпцями).

2. Система електронного документообігу має середній рівень вихідної захищеності, якщо не виконуються умови по пункту 1 і не менше 70% характеристик відповідають рівню не нижче «середній» (береться відношення суми позитивних рішень за двома стовпцями, відповідними середньому рівню захищеності, до загальної кількості рішень), а решта – низькому рівню захищеності.

3. Система електронного документообігу має низький ступінь вихідної захищеності, якщо не виконуються умови пунктів 1 і 2.

Під час складання переліку актуальних загроз безпеці кожного ступеня вихідної захищеності ставиться у відповідність числовий коефіцієнт *Y*, а саме:

Таблиця 2

Показники ступеня захищеності

Технічні та експлуатаційні характеристики	Рівень		
	високий	середній	низький
1. За територіальною розгалуженістю:			
– розподілена СЕД, що охоплює декілька областей;	–	–	+
– розподілена СЕД у рамках одного населеного пункту;	–	–	+
– корпоративна СЕД, що охоплює декілька віддалених структурних підрозділів;	–	+	–
– кампусна СЕД, розгорнута в близько розташованих будівлях;	–	+	–
– локальна СЕД у рамках одного приміщення	+	–	–
2. За наявністю з'єднання з мережами загального користування:			
– багатоточкове з'єднання;	–	–	+
– одноточкове з'єднання;	–	+	–
– фізично відділене з'єднання	+	–	–
3. За процедурами обробки:			
– зчитування, пошук;	+	–	–
– уведення, видалення, систематизація;	–	+	–
– модифікація, передавання	–	–	+
4. За обмеженням доступу:			
– з відкритим доступом;	–	–	+
– фізичне обмеження;	–	–	+
– системне обмеження;	–	+	–
– електронні ключі	+	–	–
5. За інтеграцією з іншими системами ЕД:			
– інтегровані;	–	–	+
– одномодульні	+	–	–
6. За видом контролю:			
– система внутрішнього контролю;	–	–	+
– система адміністрування ЕД;	–	+	–
– IT–аудит	+	–	–

Примітки: СЕД – система електронного документообігу; ЕД – електронний документообіг.

0 – для високого ступеня вихідної захищеності;

5 – для середнього ступеня вихідної захищеності;

10 – для низького ступеня вихідної захищеності.

Під частотою (імовірністю) реалізації загрози мають на увазі показник, який визначається експертним шляхом і характеризує, наскільки ймовірною є реалізація конкретної загрози безпеці електронного документообігу. Уводяться чотири вербальні градації цього показника:

- *малоймовірно* – відсутні об'єктивні передумови для здійснення загрози (наприклад, загроза розкрадання носіїв інформації особами, які не мають легального доступу в приміщення, де останні зберігаються);
- *низька ймовірність* – об'єктивні передумови для реалізації загрози існують, але вжиті заходи істотно ускладнюють її реалізацію (наприклад, використано відповідні засоби захисту інформації);
- *середня ймовірність* – об'єктивні передумови для реалізації загрози існують, але вжиті заходи щодо забезпечення безпеки СЕД недостатні;
- *висока ймовірність* – об'єктивні передумови для реалізації загрози існують і заходів щодо забезпечення безпеки не вжито.

Під час складання переліку актуальних загроз безпеці СЕД кожній градації ймовірності виникнення загрози ставиться у відповідність числовий коефіцієнт *Y*, а саме: 0 – для малоймовірної; 2 – для низької ймовірності; 5 – для середньої ймовірності; 10 – для високої ймовірності загрози.

За значенням коефіцієнта реалізованості загрози *Y* формується вербальна (словесна) інтерпретація реалізованості загрози:

$0 < Y < 0{,}3$ – можливість реалізації загрози низька;

$0{,}3 < Y < 0{,}6$ – можливість реалізації загрози середня;

$0{,}6 < Y < 0{,}8$ – можливість реалізації загрози висока;

$Y > 0{,}8$ – можливість реалізації загрози дуже висока.

У ході оцінки небезпеки на основі опитування експертів (фахівців у галузі захисту інформації) визначається вербальний показник небезпеки для системи електронного документообігу (*табл. 3*). Цей показник має три значення: низька – реалізація загрози може призвести до незначних негативних наслідків для системи електронного документообігу; середня – реалізація загрози може призвести до негативних наслідків для системи електронного документообігу; висока – реалізація загрози може призвести до значних негативних наслідків для системи електронного документообігу.

Застосування цього підходу до оцінки вразливості дозволило вперше запропонувати алгоритм оцінки загроз інформаційній безпеці систем електронного документообігу (*рис. 3*).

ВИСНОВКИ

Використання запропонованого підходу дає можливість:

- установити пріоритети цілей безпеки для суб'єкта відносин;
- визначити перелік актуальних джерел загроз;
- визначити перелік актуальних вразливостей;
- оцінити взаємозв'язок вразливостей, джерел загроз, можливості їх здійснення;
- визначити перелік можливих атак на об'єкт;
- розробити сценарії можливих атак;
- описати можливі наслідки реалізації загроз;
- розробити комплекс захисних заходів і систему управління економічною та інформаційною безпекою підприємства.

Результати оцінки та аналізу загроз можуть бути використані в ході вибору адекватних оптимальних методів запобігання загроз, а також під час аудиту реального стану інформаційної безпеки об'єкта. ■

ЛІТЕРАТУРА

1. Вигівська І. М. Бухгалтерський облік заходів управління ризиками діяльності підприємств / І. М. Вигівська // Вісник Житомирського державного технологічного університету. Економічні науки. – Житомир : ЖДТУ, 2010. – № 3 (53), Ч. 1. – С. 57 – 61.

2. Крутова А. С. Облік в системі електронної комерції : монографія / А. С. Крутова – Харків : ХДУХТ, 2010. – 396 с.

3. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік [Електронний ресурс]. – Режим доступу : http://dknii.gov.ua/?q=node/1469

4. Івахненков С. В. Інформаційні технології в організації бухгалтерського обліку: Історія, теорія, перспективи : наукове видання / С. В. Івахненков. – Житомир : АСА, 2001. – 416 с.

5. Гнилицька Л. В. Обліково-аналітичне забезпечення економічної безпеки підприємства : монографія / Л. В. Гнилицька. – К. : КНЕУ, 2012. – 305 с.

6. Кавун С. В. Інформаційна безпека : навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків : Вид. ХНЕУ, 2008. – 352 с.

7. Laudon, Kenneth C. E-commerce: business, technology, society / Kenneth C. Laudon, Carol Guercio Traver. – USA : Addison-Wesley, 2002 – 762 p.

Таблиця 3

Матриця оцінки показника небезпеки загрози

Вербальна реалізація загрози	Показник небезпеки загрози (вербальний)		
	Низька	Середня	Висока
Низька	неактуальна	неактуальна	актуальна
Середня	неактуальна	актуальна	актуальна
Висока	актуальна	актуальна	актуальна
Надвисока	актуальна	актуальна	актуальна

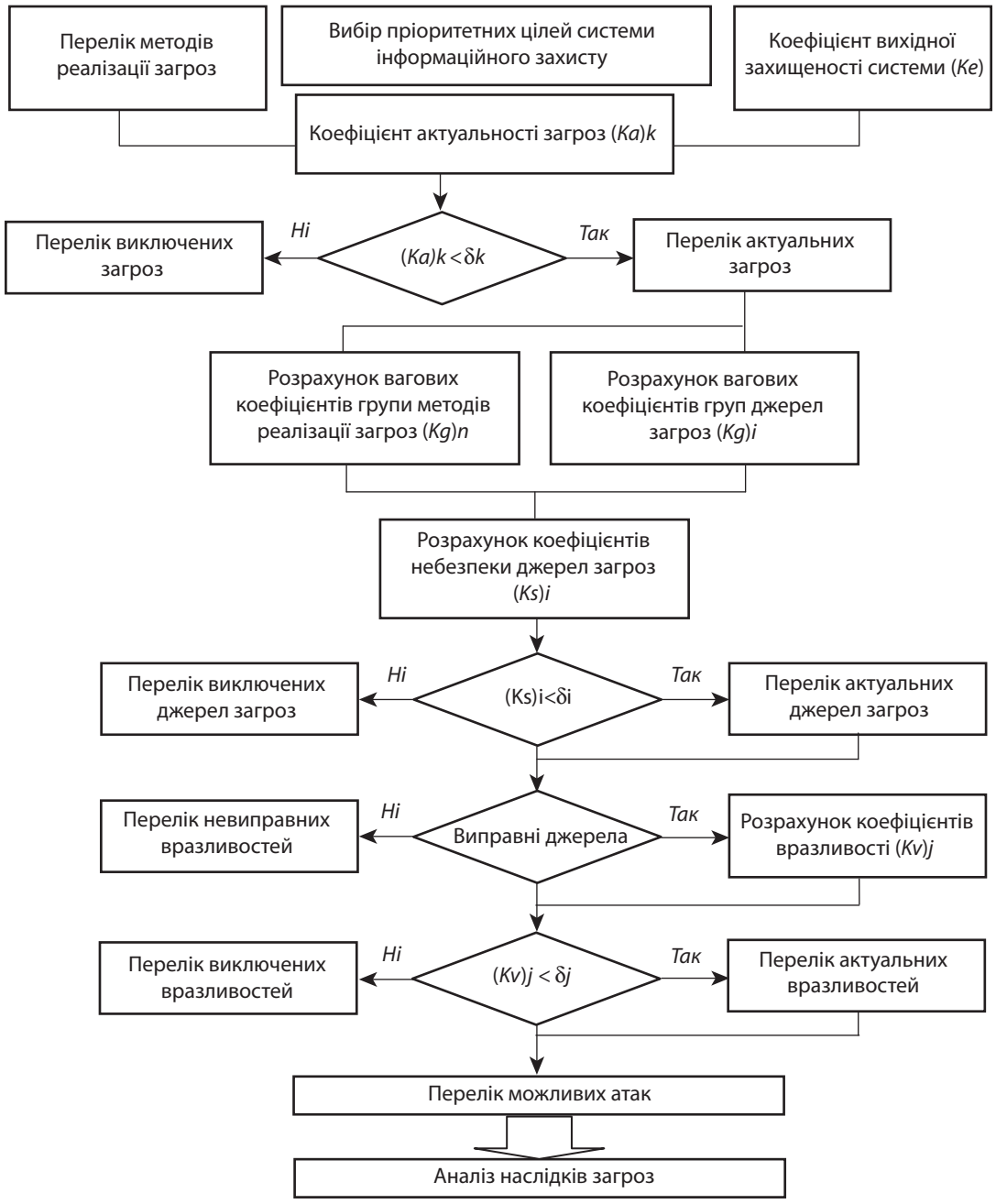

Рис. 3. Алгоритм оцінки загроз інформаційній безпеці систем електронного документообігу

8. Информационные технологии управления : научное издание / Под ред. проф. Г. А. Титоренко. – 2-е изд., доп. – М. : ЮНИТИ ДАНА, 2003. – 439 с.

9. Родін Є. С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки / Є. С. Родін // Математичні машини і системи. – 2012. – № 4. – С. 142 – 148.

REFERENCES

"Dopovid pro stan informatyzatsii ta rozvytok informatsiinoho suspilstva v Ukraini za 2013 rik" [Report on informatization and information society development in Ukraine in 2013]. http://dknii.gov.ua/?q=node/1469

Hnylytska, L. V. *Oblikovo-analytychne zabezpechennia ekonomichnoi bezpeky pidpryiemstva* [Accounting and analytical support to economic security]. Kyiv: KNEU, 2012.

Ivakhnenkov, S. V. *Informatsiini tekhnolohii v orhanizatsii bukhhalterskoho obliku: Istoriia, teoriia, perspektyvy* [Information technologies in accounting: History, Theory, Prospects]. Zhytomyr: ASA, 2001.

Informatsionnye tekhnologii upravleniia [Information technology management]. Moscow: YuNITI DANA, 2003.

Krutova, A. S. *Oblik v systemi elektronnoi komertsii* [The account in the system e-commerce]. Kharkiv: KhDUKhT, 2010.

Kavun, S. V., Nosov, V. V., and Manzhai, O. V. *Informatsiina bezpeka* [Information security]. Kharkiv: KhNEU, 2008.

Laudon, K. C., and Traver, C. G. *E-commerce: business, technology, societu.* USA: AddisonWesley, 2002.

Rodin, Ye. S. "Protsesni pidkhody do modeliuvannia u sferi upravlinnia ryzykamy informatsiinoi bezpeky" [Process modeling approaches in the management of information security risks]. *Matematychni mashyny i systemy*, no. 4 (2012): 142-148.

Vyhivska, I. M. "Bukhhalterskyi oblik zakhodiv upravlinnia ryzykamy diialnosti pidpryiemstv" [Accounting measures of risk management activity]. *Visnyk Zhytomyrskoho derzhavnoho tekhnolohichnoho universytetu. Ekonomichni nauky,* vol. 1, no. 3 (53) (2010): 57-61.