УДК 336.7

Черевко Олександр Володимирович
доктор економічних наук, професор,
професор кафедри менеджменту
та економічної безпеки,
Черкаський національний університет
імені Богдана Хмельницького
Андрієнко Василь Миколайович
доктор економічних наук, професор,
професор кафедри менеджменту
та економічної безпеки,
Черкаський національний університет
імені Богдана Хмельницького
Напора Ірина Юріївна
аспірант кафедри менеджменту
та економічної безпеки,
Черкаський національний університет
імені Богдана Хмельницького

ДЖЕРЕЛА ВИНИКНЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКІВСЬКИХ УСТАНОВ

Досліджено сучасні підходи до трактування поняття «загроза». Розглянуто класифікацію загроз інформаційній безпеці в банківських установах. Наведено способи реалізації загроз інформаційні безпеці банку. Узагальнено ідентифікацію загроз інформаційній системі в банківських установах за джерелами утворення. Визначено вплив інформаційної безпеки на інші складові системи економічної безпеки та запропоновано заходи нейтралізації загроз інформаційній безпеці в банківських установах.

***Ключові слова**: загроза; банківська установа; безпека; інформаційна безпека; внутрішні загрози; зовнішні загрози*

Постановка проблеми. Забезпечення інформаційної безпеки банківської установи набуло особливого значення у зв'язку зі стрімким розвитком комп'ютеризації банківської діяльності та використанням новітніх інформаційний технологій. Для побудови ефективної системи захисту необхідно проаналізувати захищеність банку з точки зору можливих загроз інформаційній безпеці банківських установ. Отже, існує необхідність виявлення особливостей формування джерел виникнення загроз інформаційній безпеці банківських установ.

Аналіз останніх досліджень і публікацій. Питання щодо джерел виникнення загроз інформаційній безпеці банківських установ висвітлені у наукових працях вітчизняних та зарубіжних вчених. Окремим аспектам даного питання в своїх роботах приділяють увагу Кавун С. В., Мігус І. П., Обозна А., Олійник А. В., Ревенков В. П., Страхарчук А. Я. та інші. Проте, аналіз наукових праць показав відсутність єдиного підходу щодо визначення поняття «загроза», класифікації джерел виникнення загроз, що свідчить про актуальність даного дослідження.

Мета та завдання статті. Мета статті полягає у вивченні теоретичних підходів до ідентифікації встановлення джерел виникнення загроз інформаційній безпеці банківських установ. Основними завданнями, які повинні допомогти досягти поставленої мети є: дослідження підходів до трактування терміну «загроза», висвітлення підходів до класифікації загроз інформаційній системі в банківських установах та способів реалізації загроз інформаційні безпеці банку, узагальнення ідентифікації загроз інформаційній системі в банківських установах за джерелами

утворення, визначення впливу інформаційної безпеки на інші складові системи економічної безпеки банку, висвітлення заходів нейтралізації загроз інформаційній системі в банківських установах.

Викладення основного матеріалу дослідження. Комп'ютеризація діяльності банківських установ підвищила роль інформаційної безпеки в системі економічної безпеки. Для виявлення та усунення внутрішніх та зовнішніх загроз необхідно забезпечити системний підхід в організації системи інформаційної безпеки банківських установ. При розробці засобів захисту слід мати необхідну інформацію про характер можливих загроз.

Незважаючи на численні наукові праці з даного питання на сьогодні немає однозначного трактування терміну «загроза».

Барановський О. І. зазначає, що загроза є специфічною формою ризику. При цьому він вважає, що «…перехід ризику в загрозу починається тоді, коли з'являються негативні якісні зміни в економічних системах, що пов'язані зі значними фінансовими втратами, збитками, які спричиняють банкрутство…» [1, с. 261].

Так, на думку Мігус І. П. поняття «загроза» являє собою певну подію, що впливає на діяльність суб'єктів господарювання, тоді як «ризик» виступає результатом впливу загроз на господарську діяльність суб'єктів господарювання [2].

Як вважає Кавун С. В. загроза – це подія, яка потенційно може порушити одну з властивостей інформації, що захищається [3, с. 32].

Пестовська З. С. трактує загрозу як нереалізовану, але реально існуючу (з певною вірогідністю) можливість нанесення банку будь-якого збитку [4].

Згідно стандарту НБУ загроза це – потенційна причина небажаного інциденту, який може призвести до шкоди для системи або організації [5, с. 4].

Пропонуємо під поняттям «загроза» розуміти потенційно можливу подію, яка може зашкодити діяльності банківської установи.

Інформаційною безпекою можна вважати захищеність інформаційних систем та ресурсів від зовнішніх та внутрішніх загроз, що ускладнюють ефективне використання інформації [6].

Під поняттям «інформаційна безпека банку» ми розуміємо стан захищеності всіх інформаційних активів банку від внутрішніх і зовнішніх загроз При цьому під інформаційними активами ми розуміємо будь-яку інформацію, що має цінність для банківської установи, систему її обробки або місце зберігання [7, с. 78].

Отже, загроза інформаційній безпеці це сукупність факторів та дій, які створюють загрозу та можуть призвести до порушення інформаційної безпеки банківської установи.

Щодо ознак походження загроз, то прийнято розрізняти їх за умисним походженням (викрадання, перехоплення, розголошення,копіювання інформації, несанкціонований доступ тощо) та природним походженням (помилки при обробці інформації, нещасні випадки, стихійні лиха).

Розрізняють об'єктивні та суб'єктивні причини виникнення загроз. Об'єктивними є причини випадкові за характером та непов'язані безпосередньо з діяльністю людини. Суб'єктивні причини пов'язані з діяльністю людини і поділяються на навмисні (наприклад: промислове шпигунство) та ненавмисні (наприклад: недостатня підготовка співробітника) [8].

Основними способами реалізації загроз вважають:

- несанкціонований доступ до інформації,
- протиправний збір інформації (перехоплення, підслуховування),
- маніпулювання інформацією,
- випадкове або навмисне порушенням працездатності технічних засобів прийому, передачі, зберігання і обробки інформації,
- підкуп осіб, які працюють у банку,

– комп’ютерні віруси та шкідливі програми,
– кібератаки,
– стихійні лиха та техногенні катастрофи [9, 10].

Питання класифікації загроз інформаційній безпеці знайшло відображення у роботах ряду сучасних дослідників.

Так, Страхарчук А. Я., Страхарчук В. П. виокремлюють загрози інформаційній безпеці згідно таких ознак: за цілями реалізації; за принципом впливу на систему; за причинами появи помилок у системі захисту; за об'єктом атаки; за засобами атаки, які використовують [11].

Черевко О. В. класифікує загрози інформаційній безпеці за характером порушення, тяжкістю порушення, передбаченням наслідків, мотивацією, місцем виникнення, закінченістю, об’єктом впливу, причиною виникнення, каналом проникнення, видом реалізації загрози, походженням, розміром збитку [12].

Користін О. Є. виділяє такі групи загроз інформаційній безпеці, як програмні, технічні (у тому числі радіоелектронні), фізичні, інформаційні [6].

Серед способів класифікації найбільш узагальненою, на думку Кавуна С. В., є класифікація за наслідками можливого впливу на інформацію, а саме: загрози порушення конфіденційності, загрози порушення цілісності, загрози порушення доступності [3, с. 33].

Важливим завданням для стабільного та ефективного функціонування основних складових економічної безпеки є виявлення джерел загроз (рис. 1).

Не можна не погодитися з Яременко С. М., що оптимальним підходом до визначення структури комплексної системи економічної безпеки є ресурсний підхід. Оскільки основними ресурсами, які забезпечують діяльність банку є фінансові, матеріальні, інформаційні та кадрові, то структура системи економічної безпеки складається з безпеки матеріальних ресурсів, безпеки фінансових ресурсів, кадрової безпеки та інформаційної. Дії системи економічної безпеки мають бути спрямовані на захисти вищезазначених ресурсів при їх формуванні та використанні [15].

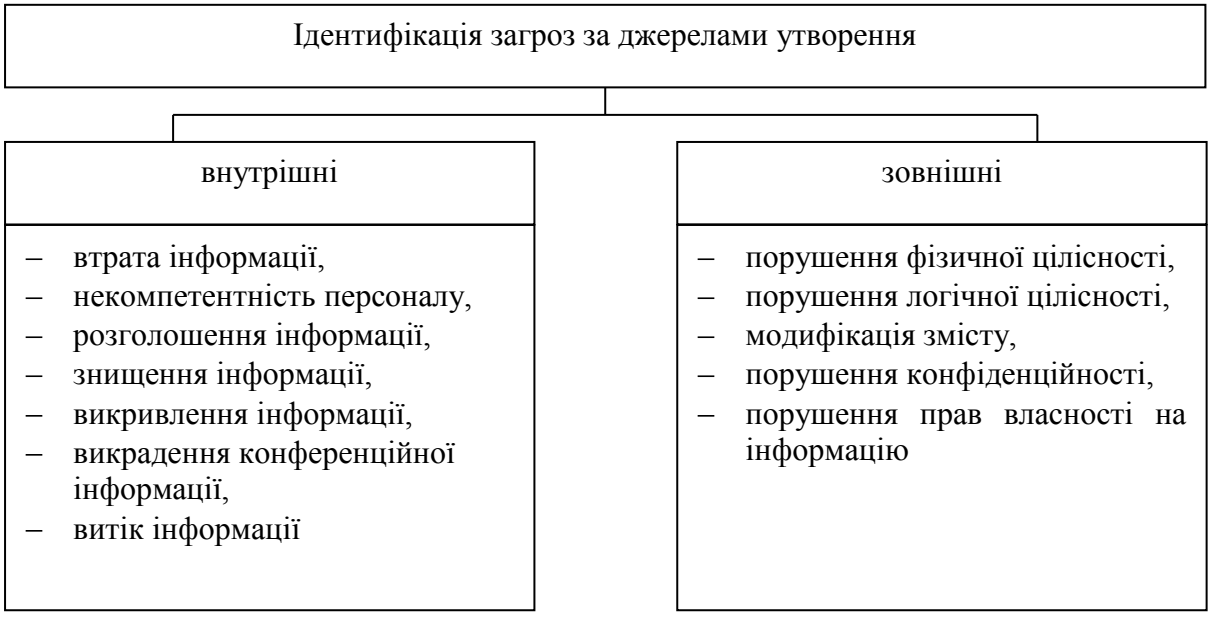

Рис. 1. Ідентифікації загроз інформаційної безпеки банківських установ [3, 8,13,14].

Розглянемо як саме впливає інформаційна безпека банківської установи на інші складові її економічної безпеки (табл. 1).

Таблиця 1

Вплив інформаційної безпеки на інші складові системи економічної безпеки банківської установи [15, 16, 17, 18].

Складові системи економічної безпеки банківської установи	Внутрішні джерела загроз	Зовнішні джерела загроз
Фінансова безпека	– фальшування витрат; – зловживання реальними активами банку чи клієнта; – перевищення повноважень управлінським персоналом; – підробка документів або внесення до них недостовірних даних; – втрата інформації щодо фінансової діяльності банківської установи	– втрата фінансової стійкості банківської установи; – шахрайства з рахунками клієнтів банку; – підроблених платіжних документів і пластикових карток; – крадіжки фінансових коштів
Кадрова безпека	– втрата інформації щодо персональних даних співробітників та керівного складу; – заподіяння майнової шкоди шляхом обману або зловживання довірою персоналу банківської установи; – загроза фізичній і професійній безпеці співробітників та керівного складу	– порушення прав власності на інформацію; – загроза персоналу банку, реалізація якої здатна погіршити стан кадрового напрямку діяльності; – втрата цінного фахівця; – шантаж співробітників та керівного складу
Майнова безпека	– провокування до здійснення або безпосереднього здійснення свідомо збиткових фінансових операцій; – загрози з боку конкурентів, які прагнуть до посилення власних позицій	– погіршення конкурентних позицій банківської установи; – погіршення іміджу банківської установи; – погіршення відносин з клієнтами банківської установи; – дискредитації суперника в очах партнерів і держави

В банківській установі зберігається і обробляється значний обсяг інформації і вона повинна бути захищена відповідними засобами як від внутрішніх, так і від зовнішніх загроз.

Для захисту від внутрішніх загроз необхідний комплексний підхід, тобто чітка структура відповідальних за інформаційну безпеку, контроль за користувачами, методи ідентифікації для доступу до інформації, контроль документообігу. При реалізації завдань широкого застосовуються DLP-системи. Вони забезпечують моніторинг поточного стану захисту і оповіщення про витоки інформації [19].

Щодо захисту від зовнішніх загроз необхідна грамотна політика безпеки, застосування HIPS (технологія, заснована на перехопленні звернень до ядра операційної системи і блокуванні виконання потенційно небезпечних дій) та інших програмних засобів захисту інформації. Цього захисту буде достатньо від усіх типів шкідливого програмного забезпечення [20].

Рівень конкуренції в банківській сфері та рівень криміналізації не дозволяють допускати витік закритої інформації банківської установи. Реалізація повного переліку заходів системи захисту інформації дозволить отримати комплексний захист інформації від втручання [21, с. 397].

Виокремимо наступні заходи нейтралізації загроз інформаційній безпеці банківської установи:

- технічні (апаратно-програмні) заходи, що перешкоджають впровадженню програм перехоплення ключів та паролів, ненавмисному вчиненню порушення,
- організаційні заходи (регламентація дій, введення заборон, підбір і робота з кадрами, навчання персоналу, посилення відповідальності і контролю, організація зберігання і використання носіїв, сувора регламентація допуску),
- технологічні заходи (застосування спеціальних програм виявлення і знищення вірусів та контроль за помилками операторів введення даних),
- фізичний захист каналів зв'язку,
- резервування критичних ресурсів,
- автоматична реєстрація дій персоналу,
- застосування фізичних і технічних засобів розмежування доступу і перешкоджають несанкціонованої модифікації апаратно-програмної конфігурації АРМ,
- використання додаткових фізичних і технічних засобів захисту тощо [22, 23].

Виявлення та ідентифікація загроз є найбільш важливою задачею для забезпечення інформаційної безпеки банківської установи та економічної безпеки банку вцілому.

Оскільки спостерігається перевага внутрішніх загроз інформаційній безпеці банківських установ над зовнішніми, аналіз вищезазначених середовищ має проводитися комплексно та одночасно.

Проведення ідентифікації загроз у сфері інформаційної безпеки банківських установ необхідне для побудови дієвої системи інформаційної безпеки.

Висновки та перспективи подальших досліджень. За результатами проведеного аналізу ми можемо зробити наступні висновки:

- досліджено сучасний підхід до трактування поняття «загроза», що дало змогу запропонувати авторське визначення;
- висвітлено підходи багатьох авторів до класифікації загроз інформаційній системі в банківських установах;
- розглянуто вплив інформаційної безпеки на інші складові системи економічної безпеки банківських установ.

Дослідження джерел виникнення загроз інформаційній безпеці банківських установ дає основу для побудови ефективної системи інформаційної безпеки банківських установ.

Список використаних джерел

1. Барановський О. І. Фінансові кризи: передумови, наслідки і шляхи запобігання: монографія / О. І. Барановський. – К.: Київ. нац. торг.-екон. ун-т, 2009. – 754 с.
2. Мігус П. І. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання [Електронний ресурс] / П. І. Мігус., С. М Лаптєв // Ефективна економіка. – 2011. – № 12. – Режим доступу: http://www.economy.nayka.com.ua/index.php?operation=1&iid=821.].
3. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 352 с.
4. Пестовська З. С. Індикатори фінансової безпеки банківської діяльності: макро- та мікроекономічний рівень [Електронний ресурс] / З. С. Пестовська //Теоретико-методологічні засади прискорення процесів соціально-економічного розвитку регіону: колект. моногр. / [Ткаченко В. А. та ін. ; за заг. ред. П. І. Сокуренка]; Дніпропетр. ун-т ім. Альфреда Нобеля, Кременчуц. ін-т. - Кременчук : Щербатих О. В. [вид.], 2013. – Розділ 4.7. – С. 338-347. – Режим доступу: http://duep.edu/uk/naukovi-publikatsiji-v-ukrajini-

i-za-kordonom/kafedra-mizhnarodnih-finansiv-obliku-ta-opodatkuvannja.
5. СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» (ISO/ IES 27002:2005, MOD). [Електронний ресурс]. – Режим доступу: http://kyianyn.files.wordpress.com/2010/12/nbu-27002.pdf.
6. Економічна безпека: навч. посіб. [Електронний ресурс] / О. Є. Користін, О. І. Барановський, Л. В. Герасименко та ін.; за ред. О. М. Джужі. – К.: Алерта; КНТ; Центр учбової літератури, 2010. – 368 с.– Режим доступу: http://westudents.com.ua/knigi/113-ekonomchna-bezpeka-koristn-o.html.
7. Напора І. Ю. Інформаційна безпека банківських установ як об'єкт наукових досліджень / І. Ю. Напора // Вісник черкаського університету. Серія: Економічні науки. – 2014. – №39 (332). - С. 77-80.
8. Ревенков П. В. Защита информации в банке: основные угрозы и борьба с ними [Електронний ресурс] / П.В. Ревенков – Режим доступу: http://www.uipdp.com/articles/2011-05/22.html.
9. Диба М. Інформаційні ризики в банківській діяльності / М. Диба, М. Зубок, С. Яременко // Вісник Національного банку України. – 2007. – № 9. – С. 28-36.
10. Савченко А. Інформаційна безпека банків: шляхи розв'язання проблеми [Електронний ресурс] / А. Савченко, І. Івченко // Вісник Національного банку України. – 2010. – № 5 (171) Травень. – Режим доступу: htt ://www.bank.gov.ua/doccatalog/document?id=60948.
11. Страхарчук А. Я. Інформаційні системи і технології в банках: навч. посіб. [Електронний ресурс] / А. Я. Страхарчук, В. П. Страхарчук ; НБУ, Ун-т банк. справи. – К. : УБС НБУ – Знання, 2010. – 515 с. – Режим доступу: http://libfree.com/102585050-bankivska_spravainformatsiyni_sistemi_i_tehnologiyi_v_bankah__straharchuk_aya.html.
12. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту [Електронний ресурс] / О. В. Черевко // Ефективна економіка. – 2014. – № 5. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3304.].
13. Кравченко А. М. Особливості захисту інформаційних систем у банківських установах / А. М. Кравченко, А. А. Орєхов, А. Г. Гаркунов // Сучасний захист інформації. – 2013. – №2. – С. 53-55.
14. Ярочкин В. И. Основы безопасности бизнеса и предпринимательства [Електронний ресурс] / В. И. Ярочкин, Я. В. Бузанова М: Академический Проект: Фонд «Мир», 2005. – 208 с. – Режим доступу: http://finances.social/biznesa-osnovyi/osnovyi-bezopasnosti-biznesa.html.
15. Яременко С. М. Комплексна система економічної безпеки банку та її структура / С. М. Яременко // Вісник КЕФ КНЕУ імені В. Гетьмана. – 2011. – №1. – С.213-221.
16. Гончарова К. Г. Кадрова безпека, як складова економічної безпеки банківської установи [Електронний ресурс] / К. Г. Гончарова // Ефективна економіка. – 2015. – № 11. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4602.
17. Кадрова безпека суб'єктів господарської діяльності: менеджмент інсайдерами / колективна монографія за заг. ред. проф. Мігус І. П. [Текст]. – Черкаси: вид-во «МАКЛАУТ», 2012. – 315 с.
18. Юрін Я. Фінансова і інвестиційна безпека банків та її вплив на загальноекономічну безпеку держави / Я. Юрін, А Сундук. // Вісник Національного банку України. – 2004. – № 7. – С.18-20.
19. Обозна А. Вплив інформаційних технологій на розвиток банківських електронних розрахунків / А. Обозна // Матеріали Міжнародної науково-технічної конференції. «Фундаментальні та прикладні проблеми сучасних технологій» –19-21 травня 2015 року – Т.: ТНТУ, 2015 – С. 262-263.
20. Войтович О. П. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів [Електронний ресурс] / О. П. Войтович, В. О. Вітюк, В. А. Каплун // Інформаційні технології та комп'ютерна інженерія. – 2013. – № 3. – С. 4-9. – Режим доступу: http://nbuv.gov.ua/UJRN/Itki_2013_3_3.
21. Єпіфанов А. О. Методологічні складові ефективного розвитку банківського сектору економіки України [Текст]: монографія / А. О. Єпіфанов. – Суми: Університетська книга, 2007. – 417 с.
22. Олійник А. В.. Інформаційні системи і технології у фінансових установах [Текст]: навч. посібник / А. В. Олійник, В. М. Шацька. – Л. : Новий Світ-2000, 2006. – 436 с. / Режим доступу: http://buklib.net/books/28625/
23. Грибунин В. Г. Комплексная система защиты информации на предприятии учеб. пособие для стул. высш. учеб. заведений / В. Г. Грибунин, В. В.Чудовский. – М. Издательский центр «Академия», 2009. – 416 с. / Режим доступу: http://www.studfiles.ru/preview/4309896/

References

1. Baranovskyi, O. I. (2009). *Financial crisis: background, consequences and ways of prevention*. Kyiv: Kyiv national trade and economic university.
2. Mihus, P. I. & Laptiev, S. M. (2011). The need for the distinction between "threat" and "risk" in the diagnosis of the economic security of business entities. *Efektyvna ekonomika, 12*. Retrieved from http://www.economy.nayka.com.ua/index.php?operation=1&iid=821.
3. Kavun, S. V., Nosov, V. V. & Manzhai, O. V. (2008) *Informational security*. Kharkov: KhNUE.
4. Pestovska, Z. S. (2013). Indicators of Financial Security Banking: macro and micro level. In P. I. Sokurenka (Eds.), *Theoretical and methodological principles acceleration of socio-economic development* (pp. 338-347) Kremenchug: Shcherbatykh O. V. Retrieved from http://duep.edu/uk/naukovi-publikatsiji-v-ukrajini-i-za-kordonom/kafedra-mizhnarodnih-finansiv-obliku-ta-opodatkuvannja.
5. SOU NBU 65.1 N 2.0 ISMS: 2010 "Information technology. Methods of protection. Code of Practice for

Information Security Management» (ISO / IES 27002: 2005, MOD). Retrieved from http://kyianyn.files.wordpress.com/2010/12/nbu-27002.pdf.
6. Korystin, O. Je. Baranovsjkyj & O. I. Gherasymenko, L. V. (2010). *Economic security*. Kyiv: Alerta. Retrieved from http://westudents.com.ua/knigi/113-ekonomchna-bezpeka-koristn-o.html.
7. Napora, I. Ju. (2014). Information security of banks as the object of research. *Visnyk cherkasjkogho universytetu. Serija: Ekonomichni nauky, 39 (332)*, 77-80.
8. Revenkov, P. V. (2011). *Protection of information in the bank: the main threats and control*. Retrieved from http://www.uipdp.com/articles/2011-05/22.html.
9. Dyba, M., Zubok, M. & Jaremenko, S. (2007). Information risks in banking. *Visnyk Nacionaljnogho banku Ukrajiny, 9*, 28-36.
10. Savchenko, A. & Ivchenko, I. (2010, may). Information security of banks: solutions to problems. *Visnyk Nacionaljnogho banku Ukrajiny, 5 (171).* Retrieved from http://www.bank.gov.ua/doccatalog/document?id=60948.
11. Strakharchuk, A. Ja. & Strakharchuk, V. P. (2010). *Information systems and technology in banks*. Kyiv: UBS NBU-Znannja. Retrieved from http://libfree.com/102585050-bankivska_spravainformatsiyni_sistemi_i_tehnologiyi_v_bankah__straharchuk_aya.html.
12. Cherevko, O. V. (2014). The theoretical basis of the concept of information security and classification of information security threats. *Efektyvna ekonomika, 5.* Retrieved from http://www.economy.nayka.com.ua/?op=1&z=3304.
13. Kravchenko, A. M., Oriekhov, A. A. & Harkunov A. G. (2013). Features of protection of information systems in banks. *Suchasnyj zakhyst informaciji, 2*, 53-55.
14. Jarochkin, V. I. & Buzanova, Ja. V. (2005). *Business and Enterprise Security Essentials*. Moscow: Akademicheskij Proekt: Fond «Mir». Retrieved from http://finances.social/biznesa-osnovyi/osnovyi-bezopasnosti-biznesa.html.
15. Jaremenko, S. M. (2011). The complex system of economic security of the bank and its structure. *Visnyk KEF KNEU imeni V. Ghetjmana, 1*, 213-221.
16. Ghoncharova, K. Gh. (2015). Personnel security, economic security as part of a banking institution. *Efektyvna ekonomika, 11*. Retrieved from http://www.economy.nayka.com.ua/?op=1&z=4602.
17. Mihus, I. P. (Eds.). (2012). Personnel security business entities: management of insiders (edition). Cherkassy: MAKLAUT.
18. Yurin, Ya. & Sunduk, A. (2004). Financial and investment bank safety and its impact on overall economic security of the state. *Visnyk Nacional'noho banku Ukrajiny, 4*, 18-20.
19. Obozna, A. (2015, may) The impact of information technology on the development of banking electronic payments. *Materials of the International scientific conference. "Fundamental and applied problems of modern technology* (pp. 262-263). Ternopil: TNTU.
20. Voitovych, O. P., Vitiuk, V. O. & Kaplun, V. A. (2013). The questions of the signs of malicious software without a source. *Informacijni tehnologii' ta komp'juterna inzhenerija, 3*, 4-9. Retrieved from http://nbuv.gov.ua/UJRN/Itki_2013_3_3.
21. Jepifanov, A. O. (2007). *Methodological components of effective development of the banking sector of Ukraine*. Sumy: Universytetsjka knygha.
22. Oliinyk, A. V. & Shatska, V. M. (2006). *Information systems and technologies in financial institutions*. Lviv: Novyi Svit-2000, 2006. Retrieved from http://buklib.net/books/28625.
23. Hrybunyn, V. H. & Chudovskyi, V. V. (2009). *A comprehensive system of protection of information in the enterprise*. Moscow: Akademija. Retrieved from http://www.studfiles.ru/preview/4309896.

CHEREVKO Oleksandr Volodymyrovych,
Doctor of economic Sciences, Professor,
Professor of the Department of Management
and economic security,
Bohdan Khmelnytsky National University of Cherkasy
ANDRIYENKO Vasil Mykolajovych,
Doctor of Economics, Professor, Professor of the Department
of Management and economic security,
Bohdan Khmelnytsky National University of Cherkasy
NAPORA Iryna Yuriyvna,
a graduate student of the Department of Management
and economic security,
Bohdan Khmelnytsky National University of Cherkasy

SOURCES OF INFORMATION SECURITY THREATS FOR BANKING INSTITUTIONS

Introduction. *The relevance of the study is due according to the increasing role of information security of banks for the banking sector of Ukraine. The vulnerability of the banking institution increases because of its dependence of information resources and networks. The use of information technology is a*

significant threat that requires constant monitoring and detailed analysis to minimize financial losses. It is obligatory to constantly improve the system of information safety due to the changing nature of internal and external factors. ***Purpose.*** *The purpose of this article is to review, synthesis and study of theoretical approaches to identify the sources of threats for banks information security.* ***Methods.*** *Monographic, theoretical generalization, systematization, analysis.****Results.*** *It is found out that the problem of research the sources of threats to information security of banking institutions is urgent for investigation. The modern approaches to the interpretation of the term «threat» are analyzed. It is considered the classification of information security threats in banking institutions. The ways to implement information security threats and to identify the threats to information system in banking institutions by sources of formation are offered. The influence of information security to other components of the system of economic security of banking institutions is grounded. The measures for neutralizing threats to information systems in banking institutions are offered.* ***Originality.*** *A definition of the term "threat" is offered. The influence of information security on the other components of the system of economic security of banking institutions is examined.* ***Conclusion.*** *The results of the analysis we made draw us to the following conclusions: it was studied the modern approach to the interpretation of the term "threat" that made it possible to offer the author's definition; it were described approaches of many authors for classification of threats to information systems in banking institutions; it was considered the influence of information security to other components of the system of economic security of banking institutions.The research of sources of threats to information security of banking institutions provides the basis for an effective information security system of banking institutions formation.*

Keywords: *threat; banking institution; security; informational security; internal threats; external threats.*

Одержано редакцією: 02.02.2016
Прийнято до публікації: 05.02.2016

УДК 330.46; 519.86

ДАНИЛЬЧУК Ганна Борисівна,
кандидат економічних наук, старший викладач кафедри економічної кібернетики,
Черкаський національний університет
імені Богдана Хмельницького
СОЛОВЙОВА Вікторія Володимирівна,
кандидат економічних наук, доцент, доцент кафедри фінансів і кредиту, Черкаський навчально-науковий інститут ДВНЗ «Університет банківської справи»

ВИКОРИСТАННЯ ЕНТРОПІЇ ПЕРЕСТАНОВОК ДЛЯ ПЕРЕДПРОГНОЗНОГО АНАЛІЗУ КРИЗОВИХ ЯВИЩ НА ФОНДОВОМУ РИНКУ

Застосування методів econофізики є сучасним інструментом при вивченні складних економічних систем. Стаття присвячена дослідженню кризових та передкризових станів таких систем із використанням ентропії перестановок. Проаналізовано поведінку ентропії перестановок на прикладі індексу Dow Jones Industrial Average (DJIA) фондового ринку США. Проілюстровано характерні особливості в поведінці запропонованого ентропійного показника у періоди криз. Зроблено висновки щодо можливості використання ентропії перестановок в якості індикатора-передвісника кризових явищ. Особливу увагу приділено вибору оптимальних параметрів розрахунку ентропії перестановок з метою визначення впливу на одержувані результати.

Ключові слова: *фондовий ринок, ентропія перестановок, патерн, криза, індикатор-передвісник, часові ряди*