УДК 004.9:336.7

МАЙДАНЮК Надія Володимирівна,
викладач кафедри комп'ютерної математики
та інформаційної безпеки,
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»,
м. Київ, Україна

ПЕРСПЕКТИВНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

У статті розглянуто питання перспективних технологій підтримки інформаційної безпеки в банківському секторі.

Обґрунтовано доцільність застосування в банках симетричного та асиметричного методів шифрування даних для захисту банківської інформації.

Розглянуто питання ефективності захисту банківських інформаційних систем за допомогою криптографічних алгоритмів. Показано, що ефективність захисту банківської інформації значною мірою залежить від безпечного розподілу ключів між користувачами банківської інформаційної системи.

Розглянуто ситуації вибору методу розподілу ключів та показано, що вибір того чи іншого методу залежить від структури системи і технології оброблення даних.

Оригінальність статті полягає в теоретичному обґрунтуванні комплексного підходу до створення криптографічних методів захисту банківських даних із використанням електронного цифрового підпису в середовищі «хмарних обчислень», що є тим більш актуальним, що в Україні вже існують проекти переходу на хмарні технології IT-інфраструктур банківської системи, зокрема IT-інфраструктури Національного банку України.

Показано, що розвиток теоретико-методологічних підходів щодо забезпечення інформаційної безпеки в банківській сфері дозволить банкам та їх клієнтам не тільки зменшити період «незахищеності» (від днів або годин до секунд), а ще й отримати набагато кращий захист банківської інформації й убезпечити фінансові системи як окремих країн, так і глобального економічного простору. У зв'язку з цим автор наголошує на необхідності продовжувати дослідження в цьому напрямі й розробляти нові прогресивні технології захисту інформації, які будуть ефективними в банківському секторі.

Ключові слова: *банк, банківська інформація, захист інформації, інформаційна безпека, інформаційні технології, криптографія, хмарні технології.*

Постановка проблеми. В останні роки питання інформаційної безпеки стають все більш актуальними в банківській сфері, тим більш, що розвиток нових технологій дистанційного віддаленого банкінгу виводить необхідність забезпечення високого рівня захисту інформації на одну з передових задач банківського сектору.

Інформаційні технології традиційно розглядаються банками як одна з основних конкурентних переваг. Зниження матеріальних витрат банків за рахунок IT в останній рік придбало особливу актуальність. Незважаючи на фінансові труднощі, бюджети, що виділяються на автоматизацію управління ефективністю банків, не знижуються. Разом з тим підвищуються вимоги щодо забезпечення захисту банківської інформації та загального рівня інформаційної безпеки банків. Про це свідчить інтерес банків до засобів інформаційної безпеки – це структурований ринок зі своїми правилами і гравцями, тенденціями та етапами розвитку.

Аналіз останніх досліджень і публікацій показав, що, незважаючи на те, що загальні положення законодавчого регулювання інформаційного простору закріплені в Законі України «Про інформацію» [1], банки у своїй практичній діяльності мають

певні проблеми щодо організації інформаційної безпеки на належному рівні, що призводить до відчутних втрат. Про це свідчать праці провідних вчених у галузі інформаційної безпеки та банківської діяльності, зокрема Бурячка В. Л., Аулова І. Ф., Горбенка І. Д., Гнатюка С., Степаненко О. П. і багатьох інших [2-5]. Зокрема, в роботі [2] розглядається задача захисту кібернетичного простору держави, де циркулює велика кількість критичної інформації, у цій роботі визначено характерні ознаки кібербезпеки держави, а також проведено аналіз проблем кібернетичної безпеки України. В роботі [3] наводиться класифікація та огляд основних технологій хмарних обчислень, а також аналіз сучасного стану застосування та досліджень в галузі безпеки хмарних технологій. У [4] автором було досліджено поточний стан і перспективи глобального розвитку хмарних технологій та сервісів. Проте питання забезпечення інформаційної безпеки в банківській сфері на сьогодні висвітлені в наукових джерелах недостатньо, що зумовлює вибір теми даного дослідження.

Метою та завданнями дослідження є дослідження питань інформаційної безпеки в банківському секторі, визначення перспективних інформаційних технологій підтримки банківської діяльності та виокремлення засобів криптографічних алгоритмів захисту інформації.

Наукова новизна одержаних результатів полягає в теоретичному обґрунтуванні комплексного підходу до створення криптографічних методів захисту банківських даних з використанням електронного цифрового підпису в «хмарних обчислень».

Виклад основного матеріалу дослідження. Згідно з [6] інформаційна безпека – це стан захищеності систем оброблення та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.

На цей час розбудова систем інформаційної безпеки для банківської сфери розглядається переважно на рівні інформаційних систем окремих банків. Через адміністративні та фінансові перепони не ставиться питання про поєднання наявних інформаційних ресурсів банків з органами державної влади, підприємствами, страховими компаніями та іншими організаціями, діяльність яких безпосередньо пов’язана з діяльністю банків. Разом з тим сучасні інформаційні технології надають можливість із невеликими витратами спростити доступ фахівців банківської сфери до наявних баз даних, інформаційних та освітніх порталів, не втрачаючи жодного з напрацювань останніх років. З огляду на це, метою є висвітлення підходів інформаційної безпеки, які дають змогу максимально ефективно та з мінімальними витратами розбудовувати сервіс-орієнтовану інфраструктуру банківської системи із відповідним рівнем інформаційної безпеки надання сервісних послуг банкам, ІТ-фахівцям банківської сфери та ін.

Ідея створення єдиної системи онлайн-підтримки для фахівців банківської сфери могла б бути реалізована на базі інформаційних ресурсів Національного банку України шляхом створенням потужного центру обробки даних (ЦОД) на базі технології «хмарних» обчислень.

Технології хмарних обчислень «Cloud Computing» можуть виявитися корисними в таких трьох ключових сферах (рис.1).

1. Новаторство в бізнесі. Технології «хмарних обчислень» сприяють інноваціям, оскільки дозволяють організаціям швидко й економічно ефективно досліджувати потенціал нових можливостей оптимізації бізнесу на базі ІТ-технологій за рахунок їхнього гнучкого масштабування практично без обмежень.

Рис.1. Технології «хмарних обчислень»

2. Надання послуг. Технології «хмарних обчислень» забезпечують динамічну доступність IT-додатків та інфраструктури. Модель «хмарних обчислень» здатна вдосконалити діяльність організації в таких сферах, як сервісно-орієнтованої архітектури управління інформацією й послугами, що, у свою чергу, підтримує ініціативи компанії з надання послуг.

3. IT-оптимізація. Модель «хмарних обчислень» забезпечує високий ступінь масштабованості, оскільки дозволяє організації швидко розширити набір IT-сервісів або одержати до них доступ без необхідності капітальної модернізації свого базового центру оброблення даних.

Необхідно зазначити, що в основу «хмарних обчислень» були покладені такі технології:

- віртуалізація;
- кластерізація;
- балансування навантаження;
- розподілені розрахунки;
- автоматичне встановлення і налаштування додатків;
- захищенний віддалений доступ.

Західні корпорації активно впроваджують у свій бізнес інформаційні технології, розбудовуючи й оптимізуючи структуру управління. Для них поняття «підвищення ефективності» і «скорочення витрат» уже не просто слова, а результат [3].

На сьогодні світовими провідними організаціями, що займаються питаннями безпеки в хмарі, є CSA, ENISA і NIST. Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки в хмарі.

Більшість з проблем захисту інформації користувача в «хмарі» можна вирішити шляхом використання існуючих методів криптографічного захисту інформації, адміністративних заходів з боку як постачальника хмарних послуг, так і користувача, укладання договорів на надання послуг, які б враховували індивідуальні потреби клієнтів, прийняття міжнародних стандартів у галузі, введення контролю з боку держави та створення незалежних експертів у цій галузі [4]. Використання хмарних сервісів суттєво змінило підхід користувача до роботи з інформацією та програмами. Хмарні системи дозволяють мати доступ до інформації та серверів з будь-якого місця світу, звільнивши користувачів від необхідності мати стаціонарний комп’ютер та зробивши доступнішою

спільну роботу багатьох людей, які можуть знаходитися в різних місцях. І ця обставина, пов'язана з архітектурою «хмари», призводить до об'єктивних проблем забезпечення інформаційної безпеки.

Головна мета шифрування (кодування) інформації – її захист від несанкціонованого доступу. Системи криптографічного захисту (системи шифрування інформації) для банківських on-line-систем можна розділити і за різними ознаками:

- за принципами використання криптографічного захисту (вбудований в систему або додатковий механізм, який може бути відключений);
- за способом реалізації (апаратний, програмний, програмно-апаратний);
- за криптографічними алгоритмами, які використовуються (загальні, спеціальні);
- за цілями захисту (забезпечення конфіденційності інформації (шифрування) і захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачі);
- за методом розподілу криптографічних ключів (базових / сеансових ключів, відкритих ключів) тощо.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм – це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв'язаного (шифрованого) тексту [7].

Спеціальні криптоалгоритми мають таємний алгоритм шифрування, в той час як загальні криптоалгоритми є повністю відкритими і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту.

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їх висока криптостійкість доведена. Ці алгоритми оприлюднюють для обговорення, при цьому також визначають премію за успішну спробу його «злому». Криптостійкість загальних алгоритмів визначається ключем шифрування та генерується методом випадкових чисел і не може бути повторена протягом певного часу. Зазначимо, що криптостійкість таких алгоритмів буде тим вища, чим більшою буде довжина ключа.

Всі криптографічні алгоритми можна використовувати з різними цілями, зокрема:

- для шифрування інформації, тобто приховування змісту повідомлень і даних;
- для забезпечення захисту даних і повідомлень від модифікації.

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка називається електронним цифровим підписом. Формуючи електронний цифровий підпис, виконують такі операції:

- за допомогою одностороннього хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;
- отримане значення хеш-функції шифрується:
  а) таємним або відкритим,
  б) таємним і відкритим ключами відправника і одержувача повідомлення (для алгоритму RSA);
- використовуючи значення хеш-функції і секретного ключа за допомогою спеціального алгоритму, обчислюють значення цифрового підпису.

Для того, щоб перевірити цифровий підпис, потрібно:

- виходячи зі значення цифрового підпису та використовуючи відповідні ключі, обчислити значення хеш-функції;
- обчислити хеш-функцію з тексту повідомлення;
- порівняти ці значення. Якщо вони збігаються, то сполучення не є модифікованим і відправлено саме цим відправником.

Останнім часом використання електронного цифрового підпису значно поширюється, зокрема для регулювання доступу до конфіденційної банківської інформації та ресурсів системи, особливо для on-line-систем реального часу [8].

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

1. Метод базових/сеансових ключів. Такий метод описано в [9] і може бути застосовано для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Застосування такої схеми розподілу ключів потребує значного часу і значних витрат.

2. Метод відкритих ключів. Такий метод описано в [10] і може бути застосовано для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Крім того, використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі.

Вибір того чи іншого методу залежить від структури системи і технології оброблення даних. Жоден із цих методів не забезпечує «абсолютного» захисту інформації, але гарантує, що вартість «злому» у кілька разів перевищує вартість зашифрованої інформації, що особливо важливо для банківського сектору.

Щоб використовувати систему криптографії з відкритим ключем, потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів – через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат – це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності.

Електронний цифровий підпис (ЕЦП) (англ. digital signature) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Надійний засіб електронного цифрового підпису – це той засіб, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Одним із елементів обов’язкового реквізиту є електронний підпис, який використовується для ідентифікації автора та/або підписувала електронного документа іншими суб’єктами електронного документообігу.

Оригіналом електронного документа вважається електронний примірник з електронним цифровим підписом автора.

При підписанні електронного документу його початковий зміст не змінюється, а додається блок даних, так званий Електронний цифровий підпис. Отримання цього блоку можна розділити на два етапи:

1. На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest).

Цей відбиток має такі особливості:

– фіксовану довжину, незалежно від довжини повідомлення;
– унікальність відбитку для кожного повідомлення;
– неможливість відновлення повідомлення по його відбитку.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, що відобразиться при перевірці Електронного цифрового підпису.

2. На другому етапі відбиток документу шифрується за допомогою програмного забезпечення і особистого ключа автора.

Розшифрувати ЕЦП і одержати початковий відбиток, який відповідатиме документу, можна тільки використовуючи Сертифікат відкритого ключа автора.

Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем автора підтверджує авторство документу (рис.2).

Перевірка Електронного цифрового підпису одержаного документу проводиться декількома етапами:

1. На першому етапі адресат за допомогою програмного забезпечення Сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа.

2. За допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний, обчислюється його відбиток.

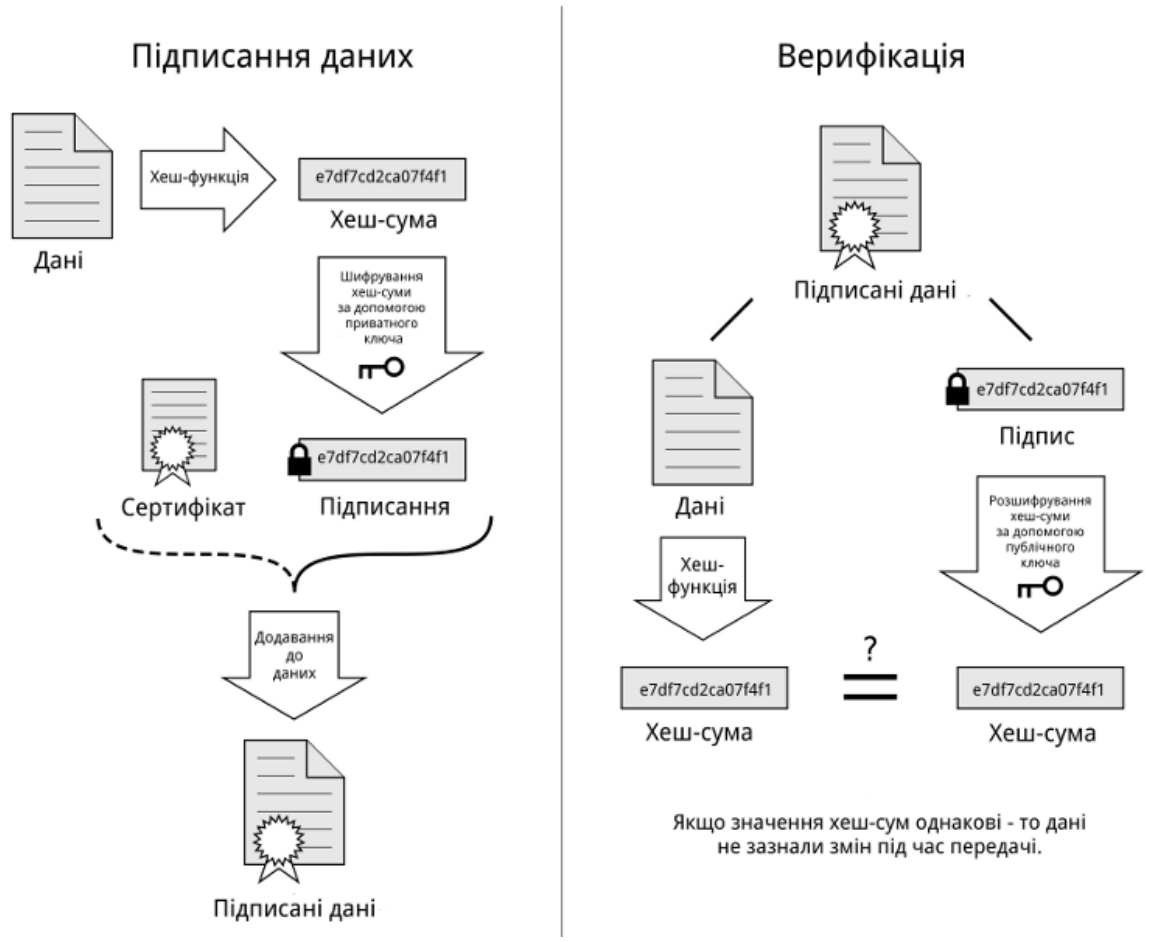

Рис.2. Ілюстрація цифрового підпису даних

3. При перевірці ЕЦП порівнюються відбитки початкового і одержаного документів. Результат перевірки – одна з відповідей: «вірний»/«невірний» [11].

В будь-якому випадку для створення належної інформаційної безпеки в банківській сфері ризики та загрози банківській діяльності повинні бути ретельно розглянуті та ідентифіковані.

Вразливості банківської діяльності можуть бути ідентифіковані в таких областях: банківська система в цілому, банк, процеси та процедури банківської діяльності, банківські інформаційні системи, інформаційно-комунікаційні технології підтримки банківської діяльності, персонал, конфігурація програмно-технічних комплексів, залежність від зовнішніх організацій тощо.

Система інформаційної безпеки повинна створити безпечне та надійне функціонування банківської системи та окремих її елементів. Тому впровадження та функціонування системи інформаційної безпеки є комплексним завданням, спрямованим на забезпечення безпеки інформаційних ресурсів, і стосується всіх банків, їхніх підрозділів і власників бізнес-процесів у банківській системі [5].

Висновки та перспективи подальших розвідок. Питання інформаційної безпеки в банківський сфері, що розглянуто в статті, є вкрай важливими сьогодні, оскільки стрімкий розвиток інформаційних технологій і зростання питомої ваги операцій віддаленого банківського обслуговування в загальному обсязі банківських операцій зумовлює підвищення вимог щодо рівня захисту банківської інформації.

Актуальність розглянутих питань в статті також обумовлено і тим фактом, що в Україні вже існують проекти переходу на хмарні технології ІТ-інфраструктур банківської системи, зокрема ІТ-інфраструктури Національного банку України.

Тому розвиток теоретико-методологічних підходів щодо забезпечення інформаційної безпеки в банківській сфері дозволить банкам та їх клієнтам не тільки зменшити період «незахищеності» (від днів або годин до секунд), а ще й отримати набагато кращий захист банківської інформації й убезпечити фінансові системи як окремих країн, так і глобального економічного простору. Саме тому потрібно продовжувати дослідження в цьому напрямі й розробляти нові прогресивні технології захисту інформації, які будуть ефективними в банківському секторі.

Список використаних джерел

1. Про інформацію : закон України [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2657-12.
2. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства /В.Л. Бурячок // Сучасна спец. техніка. – 2011. – № 3. – С. 104–114.
3. Аулов І.Ф., Горбенко І.Д. Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі / І.Ф. Аулов, І.Д. Горбенко // Прикладная радиоэлектроника. – 2013. – Т. 12. – № 2. – С. 194-201.
4. Гнатюк С. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики: аналітична записка [Електронний ресурс] /С. Гнатюк. – Режим доступу: //www.niss.gov.ua/articles /1191.
5. Степаненко О.П. Формування системи інформаційної безпеки в банківському секторі України /О.П. Степаненко// Моделювання та інформаційні системи в економіці. – 2015. – № 91. – С. 17-35.
6. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41650.
7. Kessler G. C. An Overview of Cryptography [Electronic resource]. – Access mode: http://www.garykessler.net/library/crypto.html.
8. Офіційний інформаційний ресурс Акредитованого центру сертифікації ключів Інформаційно-довідкового департаменту ДФС [Електронний ресурс]. – Режим доступу: http://acskidd.gov.ua.
9. ISO 8532:1995 Preview. Securities – Format for transmission of certificate numbers [Electronic resource]. – Access mode: https://www.iso.org/standard/23243.html.
10. ISO 11166-1:1994. Banking – Key management by means of asymmetric algorithms - Part 1: Principles, procedures and formats [Electronic resource]. – Access mode: https://www.iso.org/standard/19176.html.
11. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерний системах и сетях [под ред. д.т.н. профессора В.Ф.Шаньгин]. – М.: Радио и связь, 2001. – 376 с.

References

1. Law of Ukraine On Information [Electronic resource]. – Access mode: http://zakon3.rada.gov.ua/laws/show/2657-12.
2. Burachok V.L. (2011) Cyber security – a major factor of sustainable development of the modern information society. *Suchasna spetstekhnika, 3,* 104-114.
3. Aulov I.F., Gorbenko I.D. (2013) Cloud computing and analysis of information security in the cloud Prikladnaya radioelektronika, 2/12, 194-201.
4. Gnatyuk C. Prospects cloud computing market in Ukraine: benefits and risks analytical note [Electronic resource]. – Access mode: www.niss.gov.ua/articles / 1191.
5. Stepanenko O.P. (2015) Formation of information security in the banking sector of Ukraine. *Modelyuvannya ta informatsiyni systemy v ekonomitsi, 91,* 17-35.
6. Sun Heat 1.1-003-99 terminology in the field of information security in computer systems from unauthorized access [Electronic resource]. – Access mode : http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41650.
7. Kessler G. C. An Overview of Cryptography [Electronic resource]. – Access mode: http://www.garykessler.net/library/crypto.html.
8. Official Resource Certification Authority the Information Department DFS [electronic resource]. – Access mode: http://acskidd.gov.ua.
9. ISO 8532:1995 Preview. Securities – Format for transmission of certificate numbers [Electronic resource]. – Access mode: https://www.iso.org/standard/23243.html.
10. ISO 11166-1:1994. Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats [Electronic resource]. – Access mode: https://www.iso.org/standard/19176.html.
11. Romanets Yu.V., Tymofeev P.A., Shanhyn V.F (2001). Protection of information in computer systems and networks*. M .: Radio and Communications,* 376 p.

MAIDANIUK Nadiia Volodymyrivna,
Lecturer, Kyiv National Economic University
named after Vadym Hetman

ADVANCED TECHNOLOGIES SUPPORTING INFORMATION SECURITY IN BANKING AREA

Abstract. Introduction. *The article give a view of advanced technologies supporting information security in banking area, using cloud technologies in banking and providing the appropriate level of protection banking information in their application, here considered information security cryptographic algorithms.*

The expediency of applying to banks symmetric and asymmetric data encryption to protect banking information, because symmetric cryptographic algorithms can be divided into block and stream encryption, and using asymmetric cryptographic algorithms – generate additional information that is called electronic signature.

Purpose. *The study of information security issues in the banking sector, the definition of promising information technologies for supporting banking activities and the allocation of cryptographic information security algorithms.*

Methods. *The question of effective protection of banking information systems using cryptographic algorithms are considered. It is shown that the effectiveness of the protection banking information depends largely on the safe distribution of keys between users banking information system. Defined the key distribution methods, which should be applied in banking, including basic method / session keys and public key method are defined.*

Results. *We consider the situation of choosing the method of distribution of keys and shown that the choice of method depends upon the structure of the system and data processing technology. We remark that known methods of key distribution does not provide "absolute" protection of information, but ensured that the cost of "hacking" more in several times that the cost of encrypted information, which is especially important for the banking sector.*

Originality. *The originality of the article is a theoretical justification of an integrated approach to the creation of cryptographic methods to protect banking data using digital signatures among the "cloud computing", which is all the more important, that in Ukraine there are already projects transition to cloud IT infrastructures banking system, including IT infrastructure of the National bank of Ukraine.*

Conclusion. *It is concluded that the development of theoretical and methodological*

approaches to information security in the banking sector will allow banks and their customers not only reduce the period of "insecurity" (from days or hours to seconds) but also will get a much better protection of banking information and secure financial system both individual countries and the global economic space. Because of this, the author accent the importance of continue research in this area and developing new advanced technologies to protect information that will be effective in the banking sector.

Keywords: *bank, banking information, defense of information, information security, information technology, cryptography, cloud technology.*

Одержано редакцією: 28.04.2017
Прийнято до публікації: 10.05.2017

УДК 347.211

МАКАРЕВИЧ Ольга Вікторівна,
аспірант кафедри економіки і права,
Національний університет харчових технологій,
м. Київ, Україна

РОЛЬ ЗАХИСТУ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ПІДПРИЄМСТВ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Висвітлено загальне трактування поняття й структури економічної безпеки та інтелектуальної власності підприємства. Розглянуто сучасні стан та динаміку щодо захисту прав на об'єкти інтелектуальної власності відповідно до чинного законодавства України суб'єктами господарювання.

Ключові слова. *Інтелектуальна власність, економічна безпека.*

Постановка проблеми. Економічна безпека підприємства завжди займала провідну роль для успішного ведення господарської діяльності. В міру розвитку інтелектуальної економіки, НТП та безперервного посилення конкуренції за умов обмеженості ресурсів захист прав об'єктів інтелектуальної власності підприємства як напрям забезпечення стабільності і швидкої реакцій щодо ринкових змін стає визначальною компетенцією в усіх сферах діяльності суб'єктів господарювання.

Зважаючи, що захист прав інтелектуальної власності підприємств розглядається як функціональна складова економічної безпеки розгляд нормативно-правової бази щодо забезпечення захисту прав об'єктів інтелектуальної власності виявив деякі суперечливі питання з практичної точки зору для підприємницької діяльності в різних серах господарювання. Такий стан дещо обмежує використання та набуття компетенції підприємцями, що створює додаткові бар'єри для їх розвитку.

Аналіз останніх досліджень та публікацій. Дослідженнями поняття, складових, ролі економічної безпеки підприємства та інтелектуальної власні займаються багато провідних вітчизняних та зарубіжних вчених, серед яких слід виділити: В. Бєлокурова, Г. Жосана, С. Ільяшенка, І. Керницького, К. Коваленка, Г. Козаченка, Л. Корчевську, Т. Кузенка, Б. Кузіна, В. Левченка, Н. Лоханову, О. І. Барановський, І. О. Бланк, О. І. Захаров, П. Я. Пригунов, М. М. Єрмошенко, В. С. Сідак, М. І. Камлик, В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк, О. Ляшенка, С. Меламедоа, С. Михайлюка, В. Нагорного, М. Бєндікова, І. Бланка, Т. Васильціва, С. Владимирова, Л. Гончаренка, К. Горячеву, О. Груніна, С. Груніна,