Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)
www. economy.nayka.com. ua | № 12, 2018 | 27.12.2018 р.

DOI: 10.32702/2307-2105-2018.12.103

УДК 336.77

Н. О. Дорошенко,
доцент кафедри фінансів та кредиту, кандидат економічних наук
Харківський національний університет імені В.Н. Каразіна, м. Харків
Ю. А. Буряк,
студентка, Харківський національний університет імені В. Н. Каразіна, м. Харків

РЕАЛЬНІ ГРОШІ У ВІРТУАЛЬНОМУ СВІТІ: ПОЛЬСЬКА ПРАКТИКА

N. O. Doroshenko
Associate Professor Finance and Credit Department, Candidate of Economic Sciences,
Kharkiv National University of V.N. Karazin, Kharkiv
Yu. A. Buriak
student, Kharkiv National University of V.N. Karazin, Kharkiv

REAL MONEY IN THE VIRTUAL WORLD: POLISH PRACTICE

У статті розглядаються сучасні тенденції банківської політики світу на прикладі використання електронного банкінгу в Польщі. З цією метою опрацьовано наступні ключові питання: аналіз еволюції становлення електронного банкінгу в Польщі, конкретизація сутності та основ їх характеристик електронного банкінгу; охарактеризування механізму забезпечення безпеки даних клієнтів на прикладі провідних банків Польщі, розкриття головної мети та особливостей застосування методів аутентифікації клієнтів та авторизації банківських транзакцій; формулювання переваг та слабких сторін, що виникають у процесі роботи з електронним банкінгом.
У дослідженні відзначено, що в сучасних умовах широкого вжитку здобули розрахунки електронними грошима. Такі розрахунки відбуваються відносно нескладно: мобільний додаток на смартфоні або банківський рахунок в Інтернет – це нововведення останніх років, що полегшує наше життя щодня. Для сучасного покоління електронний банкінг є вже чимось буденним.
Динамічний розвиток технологій наприкінці XX і початку XXI століття вплинув на розвиток фінансового сектору. Отже, що банківський сектор, один з небагатьох, постійно використовує можливості, що випливають із технологічного розвитку.

The article examines the current trends in the banking policy of the world by using the example of electronic banking in Poland. For this purpose, the following key issues were analyzed: the analysis of the evolution of electronic banking in Poland, the specification of the essence and the basis of their characteristics of electronic banking; characterizing the mechanism of customer data security by the example of the leading banks of Poland, disclosing the main goal and the peculiarities of using the methods of authentication of clients and authorization of banking transactions; the formulation of advantages and disadvantages that arise in the process of working with electronic banking.

The study noted that under current conditions of widespread use electronic money was calculated. Such calculations are relatively simple: a mobile application on a smartphone or an online bank account is a creature of the last years that makes life easier for our daily life. For today's generation, electronic banking is something routine.
The main and most important threat that awaits any user of Internet banking is the risk of fraudulent hacking and unauthorized access to the funds on the account.
The only significant danger that may lie in the hands of users of these systems is the risk of unlawful seizure of their money by cybercriminals, using the capabilities of Internet banking systems.
Therefore, banks are trying to use various systems and mechanisms designed, if not to guarantee, then at least, to increase the security of using online banking.
Using the example of Polish banks, the article examines how banks make every effort to ensure that the technical means of the Internet banking system protect users' money and financial information from intruders. To provide quality services to their customers, banks today need to provide the highest level of data protection.
The dynamic development of technologies in the late 20th and early 21th centuries influenced the development of the financial sector. It's safe to say that the banking sector, as one of the few, is constantly using the opportunities arising from technological development.

Ключові слова: *онлайн-розрахунки; електронний банкінг; мобільний банкінг; банківська діяльність; ринок фінансових послуг; банківські системи безпеки; кібербезпека; нові технології.*

Key words: *online calculations; electronic banking; mobile banking; banking; financial services market; banking security systems; cyber security; new technologies.*

Постановка проблеми. Технологічний прогрес, досягнення в сфері комп'ютерних, інформаційних та комунікаційних технологій, створення глобальної мережі Інтернет, можливості мобільного зв'язку сформували базу для впровадження і розповсюдження технології електронного банкінгу. Електронний банкінг як один із найбільш динамічних видів дистанційного банківського обслуговування, отримав широке поширення в Америці та Європі, поступово завойовує і український ринок. Впровадження електронного банкінгу дає змогу фінансовим інститутам збільшити обсяг клієнтів, укріпити конкурентну позицію, а також вийти на нові географічні ринки, але при цьому має і свої недоліки у сфері безпеки даних клієнтів, що свідчить про актуальність питань, які розглядаються в межах цієї публікації.

Аналіз останніх публікацій. Дослідження, що присвячені розкриттю сутності, особливостей застосування та поширення електронних розрахунків і мобільного банкінгу та їх впливу на економіку, активно відображено в публікаціях зарубіжних спеціалістів. Серед них Бєрнацький К. [1], Кшиштошек М. [2] та Залеська М., [5]. До вітчизняних експертів у сфері віртуальних грошей та онлайн-банкінгу належать Єсіна О. Г., [6], Михайлюк, Г. О. [7], Олещук М. Г.,[8], Сербина О. Г., [9] та інші. Вищезгадані вчені зробили великий внесок в опис ключових понять про віртуальні розрахунки та мобільний банкінг, спрямовані переважно на сучасні тенденції та роль ІТ- технологій у банківському секторі.

Формулювання цілей статті. Метою статті є дослідження сучасного стану систем захисту даних клієнтів банків Польщі, а також визначення основних напрямів розвитку сфери електронних розрахунків, а саме механізмів забезпечення кібербезпеки в банківському секторі, для банківського сектору України.

Виклад основного матеріалу. Реальність сьогодні така, що клієнт може керувати заощадженнями на поточній основі, за допомогою комп'ютеру або смартфону. Клієнт банку має постійний доступ до портфелю, але це визначається в більш широкому сенсі, ніж просто місце для зберігання готівки. Отримання інформації про залишок коштів на рахунку, перегляд історії транзакцій, здійснення переказу, збільшення позики або створення депозиту – це не проблема для користувачів онлайн-банкінгу.

Використання електронного банкінгу приносить багато переваг, але, незважаючи на це, побоювання та сумніви споживачів стають все більш поширеними. І це недарма – адже реальні гроші зберігаються у віртуальному світі. А банківським клієнтам хочеться бути впевненими в надійності забезпечення заощаджень.

Розглядаючи це питання, варто визначитися з сутністю терміну «електронний банкінг». В літературі є багато пояснень цього терміну, проте всі вони характеризуються спільним знаменником, що полягає у використанні сучасних технологій у банківських операціях.

З точки зору клієнта, електронний банкінг – це технічна процедура для здійснення банківських операцій, що позбавляє відвідування відділу банку. З точки зору банку – це форма обслуговування, яка полягає у наданні клієнтам доступу до своїх рахунків за допомогою комп'ютера або іншого електронного пристрою.

М. Залеська має подібну думку, і визначає електронний банкінг як «процес заміни традиційної моделі обслуговування споживачів у відділенні банку шляхом дистанційних форм надання банківських послуг»[5].

Електронний банкінг - це дуже широке поняття, яке складається з багатьох форм та варіацій, які потребують особливої уваги: домашній банківський сервіс, домашній банкінг, Інтернет-банкінг, мобільний банкінг, банківська розсилка за допомогою електронної пошти, платіжні та банківські картки.

Отже, електронний банкінг характеризується наступними положеннями:

1) самообслуговування – клієнт використовує спеціально розроблений інтерфейс, здатний безпосередньо зв'язатися з банківською системою;

2) різноманітність інструментів, що може використовувати клієнт;

3) мобільність і доступність, незалежно від місця знаходження клієнта та банку.

Початок електронного банкінгу в Польщі вважається кінець 90-х років, коли в 1990 році банк «Pekao S.A.» встановив перші банкомати. Три роки потому, платіжні картки були прийняті для використання Президентом Національного банку Польщі. Однак прорив відбувся в 2000 році, коли було запущено перший віртуальний банк у Польщі - mBank.

Він запропонував лише віртуальний контакт з клієнтом за допомогою інтегрованих каналів розподілу, тобто: Інтернет і мобільний телефон. mBank став першим на польському ринку, хто ініціював подальший розвиток електронного банкінгу. Все це призвело до того, що в 2018 році, за даними звіту польського банківського бізнесу, підготовленого редакцією Bankier.pl та PRNews.pl[4], у польських банках зареєстровано понад 46 мільйонів клієнтів, з яких 33 мільйони мають угоди щодо доступу до електронного банкінгу в Інтернеті. Варто також відзначити, що опитаними банками зареєстровано 9 мільйонів клієнтів мобільного банкінгу, що на 2 мільйони більше порівняно з 2017 роком. На рисунку 1 показано кількість користувачів мобільного банкінгу з чотирьох найбільш діючих банків у цій сфері в Польщі.

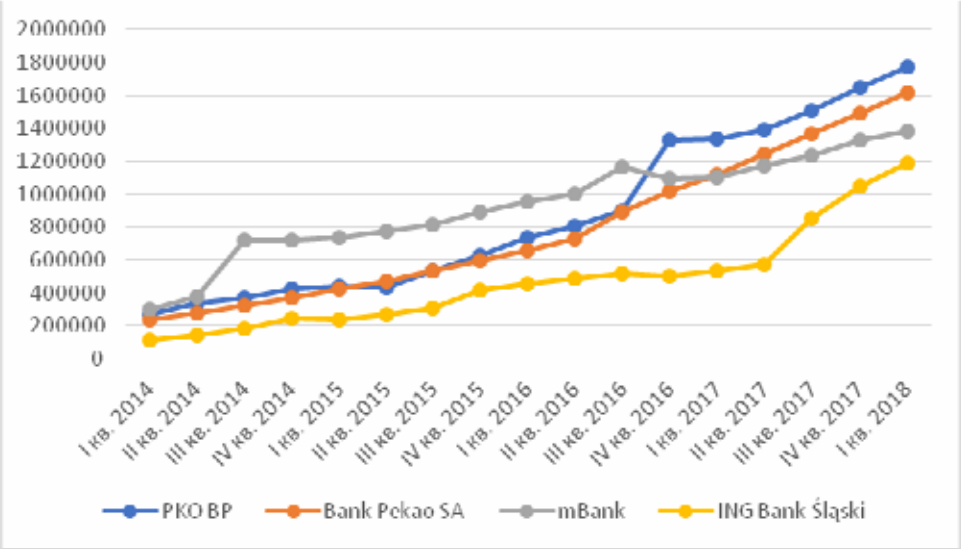

Рис. 1. Кількість користувачів мобільного банкінгу провідних банків Польщі за період I квартал 2014 – I квартал 2018 [4]

Наприкінці 2013 року мобільний банкінг налічував близько 1 мільйона людей. Наприкінці першого кварталу 2018 року вже 8 мільйонів. На польському ринку лідирує PKO BP - майже 1,8 мільйонів клієнтів, що використовують мобільний банкінг. На другому місці – банк Pekao, що має 1,6 мільйона клієнтів. Третім є mBank – кількість активних клієнтів онлайн-банкінгу в цьому банку наблизилася до 1,4 млн. осіб. Активним клієнтом (користувачем) онлайн-банкінгу визнають особу, яка входить до мобільного додатку щомісяця зі смартфона або планшета.

Однією з найважливіших проблем електронного банкінгу є системи безпеки. З року в рік спостерігається збільшення обсягів операцій в Інтернет, а отже - і кількість випадків, що загрожує безпеці клієнтів також зростає. Редактори порталів Bankier.pl та PRNews.pl в 2018 році провели опитування, в яких вони запитували читачів про свої очікування щодо безпечності банків. Кожен десятий респондент відповідав, що сподівається на підвищення безпеки даних в банках. Проведене дослідження свідчить, що в даний час кібербезпека для клієнтів банку важливіша, ніж бонуси або спеціальні пропозиції в банках.

В 2014 році - коли з'явилася велика кількість комп'ютерних шахрайств, банки почали приділяти особливу увагу політиці захисту даних. Вони спиралися на цілеспрямовані напади на користувачів

фінансових установ та викрадення готівкових коштів за допомогою анонімних рахунків. В даний час найбільш поширеними загрозами є: атаки на APT (Advanced Persistent Threat), шкідливі програми - так зване зловмисне (вірусне) програмне забезпечення, сканування - копіювання вмісту магнітної смуги карти та фішингу - сповільнення паролів або атаки на пристрої клієнта. Яскравим прикладом є вірус, який останнім часом нападав на клієнтів банку та заміняв екран входу в мобільних додатках.

Наприкінці 2017 року два польські банки - mBank та PKO Bank Polski опублікували повідомлення про існуючу загрозу. Наведені приклади є лише незначною частиною того, що стоять перед IT-персоналом найбільших банків світу.

Тому, щоб зберегти поточні темпи розвитку, необхідно постійно вдосконалювати політику безпеки. Це стосується як розширенні внутрішніх банківських систем, так і вдосконалення методів аутентифікації та авторизації, а також обізнаності кінцевих споживачів.

На цьому етапі виникає питання - хто стоїть на стражі заощаджень? Існує безліч заходів, які мінімізують хакерські атаки, наприклад: використання брандмауерів, антивірусів або уникнення входу в банкінг із пристроїв, підключених до загальнодоступних мереж Wi-Fi. На жаль, клієнти банків часто нехтують елементарними принципами безпечного використання електронного банкінгу. Одночасно вони створюють можливості для зловживання хакерами. Тоді навіть найкраща система безпеки може виявитися ненадійною. Клієнти повинні пам'ятати, що раціональна поведінка захищає від загроз, що чекають в Інтернеті.

Інструменти авторизації та аутентифікації для транзакцій, здійснених на рівні онлайн-банкінгу, є широко поширеними методами, що використовуються практично в усіх банківських установах. Сучасні польські банки використовують дворівневий рівень безпеки.

Перший використовується при вході в обліковий запис, інший - для підтвердження транзакції. До них відносяться: паролі, скетч-карти, текстові повідомлення, жетони та електронні підписи. Найпоширенішою з них є дозвіл за допомогою SMS-коду, отриманого замовником. Це простий, дуже зручний і відносно безпечний спосіб. SMS-повідомлення з одноразовим паролем, який використовується для підтвердження транзакції, надсилається на вказаний клієнтом номер. Клієнт приймає транзакцію, копіюючи комбінацію номерів. Але цей інструмент не забезпечує 100% надійності. За останні кілька років спостерігаються численні атаки на мобільні пристрої. Вони полягали в тому, щоб взяти повідомлення з кодом авторизації, а потім відправити їх злочинцям, які таким чином мали б змогу відраховувати кошти з рахунків клієнтів. Ці атаки показали, що метод, який протягом багатьох років вважався безпечним має дефекти і недоліки. Інший метод, який користується популярністю одноразовий скетч-код. Хоча цей інструмент може здатися трохи застарілим, але він має важливу заслугу – він усуває чутливість до атак, пов'язану з відсутністю взаємозалежності між кодом і підтвердженою операцією. Однак ці методи характеризуються багатьма труднощами, тобто необхідністю замовляти наступні картки з кодами після вичерпання пулу.

Через незручності для їх використання для клієнтів більшість банків перейшли на пропозиції для окремих споживачів. Сьогодні все частіше банки самі встановлюють мобільні додатки на смартфонах або планшетах їх клієнтів. У цій версії вони являють собою підтвердження транзакції, а також додаткову безпеку під час входу в систему. Методи автентифікації також повинні містити паролі, надані під час входу в систему. Серед них, статичний пароль, який є рядком символів, встановлений клієнтом, і їх розширення - маскуються паролі, що полягають у введенні випадковим чином вибраних системою символів. Електронні підписи, що дозволяють входити в систему та приймати замовлення в електронній формі, стають все більш поширеними.

Біометричні системи – це наступна група динамічно розроблених методів контролю доступу до електронного банкінгу. Це автоматичні методи перевірки та ідентифікації клієнтів, що є найбільш надійними з точки зору безпеки, оскільки вони належать тільки одній особі. Біометричні системи досліджують фізичні особливості клієнтів, такі як відбитки пальців, системи кровоносних судин, діафрагми та поведінкові ознаки, пов'язані з поведінкою особи, наприклад, рукописний підпис (табл. 1).

Таблиця 1.

Порівняння типів біометричних вимірювань, що використовуються в банківській сфері в Польщі [2]

Метод вимірювання	Біометричний метод	Безпека вимірювань	Точність вимірювання	Вартість реалізації
Кровоносні судини пальців	Світло інфрачервоного діапазону	Висока	Висока	Низька
Голосовий профіль	Аналіз голосу	Висока	Висока	Низька
Рукописний підпис	Графологічний аналіз	Низька	Середня	Середня
Рух кровоносних судин	Світло інфрачервоного діапазону	Висока	Висока	Низька
Відбиток пальців	Відбиток пальців	Середня	Середня	Низька
Сканування сітківки ока	Сканування сітківки ока	Висока	Висока	Висока

Всі ці інструменти, як окремо, так і в різних комбінаціях, використовуються банками Польщі. У деяких з них потрібен лише пароль для онлайн-банкінгу. В деяких випадках використовуються інноваційні рішення, в яких, за межами паролю, є ще жест**.** Деякі додатки також використовують мобільні токени, які встановлюються як окремі 4-значні спеціальні паролі для програми. Додатковим захистом є також автентифікація пристрою, з якого ми входимо.

Незважаючи на велику кількість захистів різних рівнів для коштів клієнтів, сам банк є джерелом всіх процесів захисту. Ключовим завданням є розробка відповідної політики безпеки на технічному рівні, тобто інфраструктури та додатки. Проте один важливий операційний рівень інтегровано з процесами та людськими ресурсами.

Автори другого спеціального звіту «Безпека електронного банкінгу» [4], використовують класифікацію, яка, крім політики безпеки, також включає процес управління інцидентами, а також превентивними механізмами, як це показано на схемі (рис. 2).

Управління інцидентами - це сукупність процесів та заходів, що враховує події, пов'язані з передбачуваною загрозою доступності, конфіденційності та цілісності інформації або систем, що є програмним забезпеченням банку. Це стосується обох електронних банківських рівнів безпеки у банківських системах та пристроях, що використовуються клієнтом. SOC (Security Operations Center) - це система, що дозволяє виявити критичні місця в системі. Це інструмент, в якому потрібна взаємодія IT-департаментів, а також поліції чи прокуратури, з тим щоб можна було створити більш високий рівень безпеки, співпрацюючи один з одним. У свою чергу, SIEM (Security Information and Event Management) - це система, що збирає дані зі станцій, серверів і мережевого трафіку в режимі реального часу та забезпечує постійний аналіз цих даних. Варто також згадати системи боротьби з шахрайством, відстежують та обчислюють ступінь ризику, що виникає при кожній транзакції. Коли пороги, визначені організацією, перевищені, спрацьовує тривога або передача блокується.

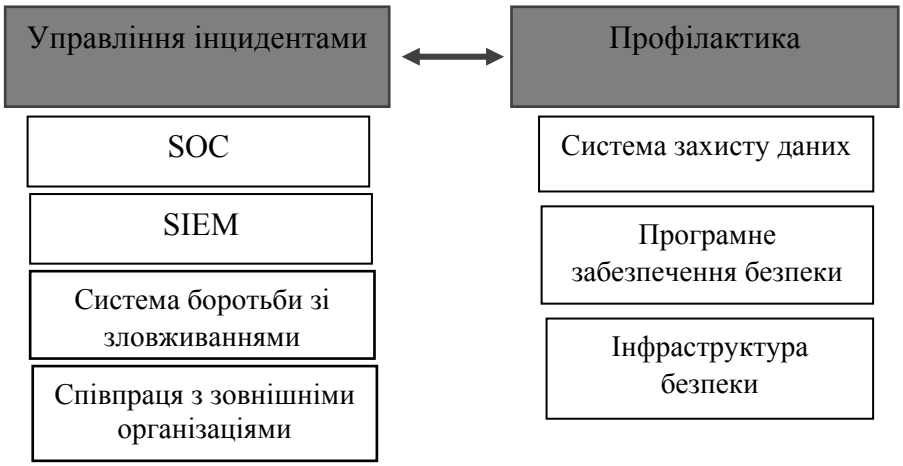

Рис. 2. Класифікація систем внутрішньої безпеки [5]

Система «запобігання», включає в себе методи попередження захисту банківських систем від загроз, виявлених на ранньому етапі, та тих, що виникають як нові. Ці механізми можна розділити на три групи: захист даних (захист системи), захист програмного забезпечення та безпека інфраструктури. Всі групи взаємопов'язані для виявлення реальної загрози, виявлення помилкової тривоги та вжиття відповідних заходів.

Висновок. Електронна система банківських послуг приносить користь як банкам, так і клієнтам. Завдяки модерністським рішенням клієнти мають змогу в будь-який час керувати своїми заощадженнями. Це особливо важливо в ті часи, коли кожна хвилина на вагу золота. Враховуючи, що постійна турбота про безпеку є однією з основних бар'єрів для розвитку електронного банкінгу, установи приділяють все більше уваги забезпеченню максимально можливого рівня безпеки, спираючись на успішний досвід. Інструменти, які використовують клієнти, повинні бути максимально відповідними їм, а також часто індивідуалізованими. Саме тому польські банки використовують різні методи - від найпростіших (паролів) до найсучасніших (біометричні методи).

У найближчому майбутньому очікується швидкий розвиток систем захисту клієнтів. Тим часом процеси та системи, такі як раніше згадані SIEM, будуть розвиватися в рамках внутрішніх рішень банківських установ. SOC банківські установи, які мають на меті залучити найбільшу групу клієнтів, повинні пам'ятати, що користувачі не приймають складні та важкодоступні методи, тому вони намагатимуться максимально спростити свої інструменти, не втрачаючи у ефективності.

Отже, вітчизняній банківській системі потрібно розвиватись, спираючись на досвід польських банків. Це стосується організації Інтернет-банкінгу, розширення спектру послуг, їх якості, а особливо надійності.

Головною умовою успішного розвитку Інтернет-банкінгу в Україні є насамперед інформування потенційних клієнтів про можливості цього виду обслуговування, його переваги та можливості для самих клієнтів. Також основним завданням для банківської системи є розробка найнадійніших систем захисту інформації, впровадження та постійна модернізація сучасного технічного та технологічного забезпечення.

В подальших дослідженнях на цю тематику варто зробити порівняльний аналіз систем безпеки найкрупніших банків України та Польщі, що надасть змогу оцінити розбіжності в системі захисту та факторах, що впливають на електронний банкінг.

Література.

1. Biernacki K., E-Banking Innovations in Poland, «Perspectives of innovations, economics and business», vol. 13, no. 2 2013.
2. Krzysztószek M., Bankowość elektroniczna w teori i praktyce, Materiały edukacyjne dla środowiska szkolnego, Wydanie l, 2017, https://www.knf.gov.pl, 07.02.2018,
3. Raport Polska bankowosć w liczbach-III kwartał 2018, https//prnews.pl, 08.08.2018.
4. Raport PRNews.pl: Rynek bankowości mobilnej – I kw. 2017.
5. Zaleska M., Bankowość, Wydawnictwo C.H.Beck, Warszawa 2013
6. Єсіна О. Г., Сучасний ринок дистанційних банківських послуг в Україні. / О. Г. Єсіна // Соціально-економічні аспекти розвитку економіки та управління: збір наукових статей. – 2015. – №. 2. – С. 46-49.
7. Михайлюк, Г. О. Розвиток Інтернет-банкінгу як нетрадиційної банківської операції [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/1_KAND_2010/Pravo/9_5726 4.doc.htm.
8. Олещук М. Г. Впровадження інноваційних ІТ-технологій як напрямок підвищення конкурентоспроможності банків на ринку банківських послуг України// Науковий вісник ДДМА. – 2010. – № 1(6Е). – С. 351-358.
9. Сербина О. Г., Пономар В. В. Тенденції розвитку мобільного банкінгу в Україні //Молодий вчений. – 2014. – №. 3 (06). – С. 53-55.

References.

1. Biernacki K. (2013), *E-Banking Innovations in Poland,* Perspectives of innovations, economics and business, vol. 13, no. 2.
2. Krzysztoszek M. (2017), “Banking in Theory and Practice”, Educational Materials For The School Environment, [Online], vol. 1, available at: https://www.knf.gov.pl, (Accessed 24 November 2018).
3. Report on Polish banking in numbers - III quarter 2018, available at: https//prnews.pl, (Accessed 28 November 2018).
4. “Mobile banking market - the first quarter. 2018”, Raport PRNews, available at: https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-i-kw-2017-360755., (Accessed 14 November 2018).
5. Zaleska M., (2013), “Banking”, C.H.Beck Publishing House, Warszawa, vol. 1, pp. 10–12.
6. Yesina O. H. and Esyna O. H. (2015), “The modern market of remote banking services in Ukraine”, Socio-economic aspects of development economics and management: collection of scientific articles, vol. 2., pp. 46-49.
7. Mykhajliuk, H. O., (2014), “Development of Internet banking as an unconventional banking operation”, available at: http://www.rusnauka.com/1_KAND_2010/Pravo/9_5726 4.doc.htm, (Accessed 4 November 2018).
8. Oleschuk M. H., (2010), “Implementation of innovative IT technologies as a direction of increasing the competitiveness of banks in the Ukrainian banking market”, Naukovyj visnyk DDMA, vol. 1 (6E), pp. 351-358.
9. Serbyna O. H. And Ponomar V. V., (2014), “Trends in Mobile Banking Development in Ukraine”, Molodyj vchenyj, vol. 3 (06), pp. 53-55.

Стаття надійшла до редакції 18.12.2018 р.