О.В. ПОПОВИЧ,
к.е.н., доцент, Національний авіаційний університет,
К.О. ВОЙНОВСЬКА,
студентка, Національний авіаційний університет

Особливості аудиту інформаційної безпеки банку при роботі з електронними грошима

Стаття присвячена контролю інформаційної безпеки в банку при роботі з електронними грошима, їх аудиту. Приділено увагу основним вимогам проведення аудиту інформаційної безпеки, визначено головні напрями перевірки, зокрема, організаційно–технічної та правової забезпеченості банків для запобігання порушення цілісності, доступності, конфіденційності та спостережності інформаційних систем, що забезпечують функціонування систем електронних грошей.

Ключові слова: *аудит, контроль, електронні гроші, інформаційна безпека, банки.*

О.В. ПОПОВИЧ,
к.э.н., доцент, Национальный авиационный университет,
К.О. ВОЙНОВСЬКАЯ,
студентка, Национальный авиационный университет

Особенности аудита информационной безопасности банка при работе с электронными деньгами

Статья посвящена контролю информационной безопасности в банке при работе с электронными деньгами, их аудита. Уделено внимание основным требованиям проведения аудита информационной безопасности, определены главные направления проверки, в частности организационно–технической и правовой обеспеченности банков для предотвращения нарушения целостности, доступности, конфиденциальности и наблюдаемости информационных систем, обеспечивающих функционирование систем электронных денег.

Ключевые слова: *аудит, контроль, электронные деньги, информационная безопасность, банки.*

This article is devoted to information security controls at the bank when dealing with electronic money, their audit. Attention is paid to the basic requirements of auditing information security, identifies the key areas of audit, including organizational, technical and legal sufficiency of banks to prevent violation of the integrity, availability, confidentiality and observability of information systems for the operation of electronic money.

Keywords: *audit, control, electronic money, information security, banks.*

Постановка проблеми. Під час роботи з грошовими коштами інформаційна безпека відіграє вирішальну роль у добробуті суспільства й фінансовій безпеці окремих економічних суб'єктів та держави в цілому. Діяльність банківських установ пов'язана з обігом грошових коштів, тому на особливу увагу завжди заслуговує питання їх використання та роботи з ними відповідно до чинного законодавства України. Тому особливу увагу слід приділяти її безпеці – захищеності інформації та інфраструктурі, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації та вказаній інфраструктурі.

Ураховуючи також технології організації їх обігу, що використовуються учасниками систем електронних грошей, питання здійснення належного аудиту інформаційної безпеки банків при роботі з даним платіжним засобом набуває особливої актуальності.

Аналіз досліджень та публікацій з проблеми. Питанням обліку і аудиту в Україні присвячено праці вітчизняних учених М.Т. Білухи, Ф.Ф. Бутинця, А.М. Герасимовича, Г.М. Давидова, Н.І. Дорош, Є.В. Мниха, О.А. Петрик, М.С. Пушкаря, В.С. Рудницького та інших. Серед науковців, що приділяють увагу питанням аудиту в банках, варто виділити О.В. Васюренка, Л.М. Кіндратську, О.І. Кірєєва, Г.П. Табачук, Б.Ф. Усача. Питанням інформаційної безпеки присвячені публікації А.Ю. Берко, А.М. Зими, В.В. Карасюка, О.А. Мясіщева, О.С. Олексюка, І.В. Рішняк, М.А. Судейко, І.О. Трубіна тощо.

Однак питанням аудиту інформаційної безпеки, захищеності банків під час роботи з електронними грошима присвячена недостатня увага науковців.

Метою статті є вивчення підходів до організації інформаційної безпеки в банках, обґрунтування методології аудиту електронних грошей у банках України як складової системи контролінгу та надання пропозицій щодо проведення аудиту інформаційної безпеки під час роботи банків з електронними грошима.

Виклад основного матеріалу. У сучасних умовах ведення бізнесу важливе місце в усіх сферах економіки займає інформаційна безпека. Особливо велике значення вона має при роботі з грошима, оскільки від їх захищеності залежить добробут суспільства та економічна безпека держави. Так, на сьогодні актуальним стало питання визначення підходів та принципів аудиту з електронними грошима, які набувають все більшої популярності й з часом можуть замінити паперові.

Зазначимо, що електронні гроші (e–money) – одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі. Тобто це означення грошей чи фінансових зобов'язань, обмін та взаєморозрахунки з яких проводяться за допомогою інформаційних технологій [1].

Під інформаційною безпекою сьогодні розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам

інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує.

Інформаційна безпека – процес, який забезпечує збереження властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно–технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи [2].

Згідно із Законом України «Про аудиторську діяльність» [11] аудитом є перевірка даних бухгалтерського обліку і показників фінансової звітності суб'єкта господарювання з метою висловлення незалежної думки аудитора про її достовірність в усіх суттєвих аспектах та відповідність вимогам законів України, нормативно–правовим актам та внутрішнім нормативним документам суб'єкта, що перевіряється.

Відповідно до Положення про організацію внутрішнього аудиту в комерційних банках України [12] аудит банку – це визначення стану банку на основі перевірки правильності складання та підтвердження достовірності фінансової звітності, відповідність обліку та дій банку вимогам чинного законодавства тощо та підготовка висновків для надання інформації керівництву, акціонерам (учасникам) банку та іншим користувачам. А аудиторська перевірка – система засобів перевірки документів інформаційної системи, облікових записів, статистичних матеріалів, а також контроль за достовірністю виконання необхідних процедур. Отже, аудит є складовою частиною системи контролю в банку.

Отже, система контролінгу банківських установ включає в себе облік, контроль та аудит. І при роботі банків з електронними грошима набуває особливого значення, оскільки даний платіжний засіб, ми вважаємо, має великий потенціал і може набути в майбутньому широкого застосування. Тому питання фінансового контролю як складової системи контролінгу банку, який зорієнтований на майбутнє через контрольні заходи історичної інформації, набуває неабиякого значення.

Зазначимо, що об'єктом аудиту електронних грошей в банку є організаційно–правовий механізм їх обігу, а предметом – сукупність об'єктів аудиторського контролю:

– система емісії електронних грошей;

– система обліку операцій з електронними грошима;

– нормативно–правове забезпечення роботи банку з електронними грошима;

– інформаційна система та система інформаційної безпеки тощо.

Значення аудиту електронних грошей в банках та його роль обумовлюється підвищенням цінності інформації, згенерованої в процесі обліку операцій, оскільки аудитор критично оцінює її, зменшує інформаційний ризик та сприяє посиленню контролю над нею в інтересах суспільства – користувачів даного платіжного засобу. Така діяльність аудиторів визначена у міжнародних Концептуальних основах завдань з надання впевненості [15] як завдання з надання впевненості, коли фахівець–практик надає висновок, призначений підвищити ступінь довіри щодо результату оцінки або визначення предмета перевірки за належними критеріями.

Головними функціями аудиту електронних грошей в банківських установах є:

1. Контроль за виконанням вимог чинного законодавства щодо емісії та організації обігу електронних грошей. Нормативно–правові акти, що регулюють питання функціонування систем електронних грошей, їх обіг, використання, облік операцій з ними тощо, визначають механізм та обмеження щодо роботи з даним платіжним інструментом. А порушення вимог, встановлених органами державної влади щодо електронних грошей, може призвести до накладання санкцій на банки.

2. Забезпечення ліквідності банку. Її суть полягає у недопущенні перенесення коштів з рахунків, на яких розміщено забезпечення електронних грошей, на інші рахунки чи використання їх для фінансування активних операцій або з іншою метою, що суперечить їх призначенню, для отримання доходів. Необхідність виокремлення даної функції полягає у ризику втрати ліквідності банку чи банківської системи в цілому, а також ризику зростання інфляції за рахунок віртуальної емісії грошей та збільшенні грошової маси в країні.

Особливість зазначених функцій полягає у тому, що нехтування принципами роботи з електронними грошима ставить під загрозу економічну та фінансову безпеку банку, банківську систему та суспільно–економічний лад держави.

Серед напрямів аудиту електронних грошей особливу увагу слід приділити:

1. Перевірці системи електронних грошей як сукупності відносин між емітентом, оператором, агентами, торговцями та користувачами щодо здійснення випуску, обігу та погашення електронних грошей [3].

2. Проведенню аудиту в банках – емітентах електронних грошей.

3. Контролю за роботою агентів банків – осіб, які на підставі договору, укладеного з емітентом, забезпечують розповсюдження електронних грошей (агенти з розповсюдження), надають засоби поповнення електронними грошима електронних пристроїв (агенти з поповнення), здійснюють обмінні операції з електронними грошима (агент з обмінних операцій) та приймання електронних грошей в обмін на готівкові чи безготівкові кошти (агенти з розрахунків).

4. Перевірка суб'єктів господарювання, які здійснюють операції з електронними грошима.

Слід при цьому зазначити, що контроль за роботою системи електронних грошей є фактично оверсайтом – наглядом, який має право здійснювати в Україні виключно Національний банк України [14, 15].

Аудит й інформаційна безпека електронних грошей є взаємозалежними.

У роботі О.С. Олексюка мова йде про те, що сьогодні гроші перетворюються на інформаційний ресурс [9], і тому електронні гроші вразливі, зокрема, для шахраїв, забезпечених настільки сучасними засобами, наскільки сучасними є і їх об'єкти [8]. Під загрозою загалом розуміється можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого, те, що може заподіяти зло чи неприємність [4]. Це потенційна можливість порушення інформаційної безпеки, настання небажаного інциденту, який може завдати шкоди системі чи організації [6].

Спроба реалізації загрози називається атакою, а особа, котра здійснює таку спробу, – зловмисником (порушником). Під атакою мається на увазі рішуча дія, спрямована на до–

сягнення якої–небудь мети [3]. Це навмисні дії, спрямовані на порушення характеристик інформації.

До категорій спектру інтересів банків при їх роботі з електронними грошима слід, на нашу думку, віднести: забезпечення доступності, цілісності, конфіденційності та спостережності інформаційних ресурсів та інфраструктури, що її підтримує.

Доступність – це можливість за прийнятний час одержати інформаційну послугу: використовуючи визначені системи і технології власнику (користувачу) електронних грошей отримати доступ до свого електронного гаманця, до даних щодо наявності та залишку на ньому коштів для оплати необхідних йому благ.

Під цілісністю мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Конфіденційність – це захист від несанкціонованого доступу до інформації.

Спостережність – властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних ресурсів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

З метою забезпечення більшої безпеки розрахунків електронними грошима Національний банк України свого часу розробив проект змін до Положення про електронні гроші в Україні, який, однак, до сьогодні не прийнятий. Зазначеним документом передбачається встановити в Україні ліміти на зняття з електронного гаманця готівки – 500 грн. на день та 4000 грн. на місяць, ліміт за операціями протягом місяця – 25000 грн., а максимальна сума однієї операції – 8000 грн. Такі обмеження вже запроваджені однією із систем електронних грошей в Україні. Вони дозволяють мінімізувати ймовірність атаки з боку зловмисників через незначні суми коштів, якими можна заволодіти, отримавши доступ до необхідної інформаційної системи, наприклад, електронного гаманця власника (користувача електронних грошей). Це пояснюється низькою ефективністю у співвідношенні затрат порушників на створення засобів завдання атаки та розміру отриманих вигод. Так, одна DDoS–атака (атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial–of–service attack) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними для користувачів, для яких комп'ютерна система була призначена) кошту [8].

Аудиторам, що проводять перевірку інформаційної системи банку, який є учасником системи електронних грошей, слід звертати увагу на дієздатність:

а) технічних засобів, до яких, зокрема, належать:

– обмеження довжини, складності та часу життя паролів;

– використання систем мережевих екранів і системи запобігання вторгнень на мережевому рівні;

– використання систем антивірусного захисту;

– використання для доступу до основних бізнес–систем термінальних серверів;

б) організаційних заходів:

– заборона на передачу своїх облікових даних в інформаційних системах;

– правила використання ресурсів мережі Інтернет і корпоративної пошти;

– правила використання засобів обробки та передачі електронної інформації;

– порядок обробки персональних даних.

Також слід пам'ятати, що зловмисники розуміють, що одними лише технічними методами не обійтися, якщо необхідно добути цінну інформацію. Тому часто вони використовують і психологічні навички, щоб ввести користувача в оману. Тобто тут йде мова про соціальну інженерію – науку, що вивчає можливість отримання інформації внаслідок людської неуважності, використання простих паролів та не застосованих необхідних заходів безпеки [7].

Велику увагу інформаційній безпеці під час роботи суб'єктів господарювання з електронними грошима приділяє у своїх працях І.О. Трубін. Його роботи щодо функціонування систем електронних грошей присвячені в основному питанням правового регулювання обігу і використання цього платіжного засобу, а також інформаційно–технічній захищеності систем електронних грошей. Однак питання економічної суті положень його тверджень мають дискусійний характер. Так, зазначаючи, що електронні гроші є основним елементом системи електронних платежів [6], автор, на нашу думку, помилково ототожнює їх із безготівковими коштами. Підтвердженням цього є дані Національного банку України про те, що за дев'ять місяців 2013 року учасниками системи електронних платежів Національного банку України здійснено початкових платежів і надіслано електронних розрахункових повідомлень на суму 9 019 594 млн. грн. Дана система забезпечує здійснення розрахунків у межах України між банками і виконання міжбанківських переказів є обов'язковим для банків України [11]. При цьому за допомогою системи електронних платежів Національного банку України не здійснювались перекази електронних грошей, а загальний обсяг операцій із ними становив усього (у порівнянні з переказом безготівкових коштів) 511 тис. грн. [12].

Крім того, автор відносить до переваг запровадження розрахунків електронними грошима в бізнесі те, що банки, зокрема, отримують можливість «здійснювати певні операції із «залишками» коштів». При цьому не зрозуміло, що мається на увазі під «певними операціями» [7]. Можна підтримати І.О. Трубіна в тому, що електронні гроші – це насамперед інформація, дані про суму емісії та емітента, про їх забезпеченість іншими формами грошей, про їхню купівельну спроможність, а також про електронний гаманець, на якому вони зберігаються тощо, які він вбачає як інформацію про кількісне вираження вартості грошового еквівалента [4].

У роботі зазначеного автора [2] детально досліджено вивченість у літературі питань інформаційної безпеки у процесі функціонування систем електронних грошей. Так, науковцем узагальнено думки інших науковців і виокремлюються такі заходи забезпечення інформаційної безпеки організацій:

– організаційні – підготовка персоналу, структура служби охорони, наявність та якість аналітичних служб;

– технічні (програмні) – спрямовані на обмеження програмно–апаратного доступу до інформаційної системи;

– правові – полягають у формуванні правил поведінки персоналу, формування методик виявлення та розкриття

правопорушень за допомогою інформаційних систем і технологій [6].

Джерела формування вимог безпеки, які доцільно ідентифікувати, в тому числі й банкам – учасникам систем електронних грошей:

1. Результат оцінки ризиків для банків, який ураховує загальну бізнес–стратегію та цілі. При цьому визначаються загрози ресурсам системи управління інформаційною безпекою, оцінюються її вразливості та ймовірності подій, і визначається величина потенційного впливу.

2. Правові вимоги, що базуються на законодавстві, нормативно–правових актах та вимогах контрактів.

3. Власний вибір принципів, цілей та бізнес–вимог щодо оброблення інформації, розроблений банком для внутрішнього використання.

Проводячи аудит інформаційної безпеки банку при роботі з електронними грошима, здійснюючи перевірку організаційно–технічної та правової готовності установи до роботи із даним платіжним засобом, аудиторам слід приділяти увагу підготовці персоналу банку, відповідального за інформаційну безпеку, організації доступів до елементів інформаційної системи, обмеженням програмно–апаратного доступу до інформаційної системи тощо. Так, одним із напрямів підвищення безпеки банку є постійне та систематичне підвищення кваліфікації зазначеної категорії працівників, зокрема, участі у конференціях, симпозіумах, виставках відповідної тематики.

Проводячи аналіз організаційних заходів, спрямованих на захист інформації, аудиторам доцільно приділити увагу наявності та якості документів, що регламентують емісію, обіг та погашення електронних грошей. Крім того, банкам–емітентам слід розробити ґрунтовні та докладні інструкції для користувачів щодо роботи з електронними грошима.

За даними Національного банку України, з особистих рахунків фізичних осіб в нашій державі за 2013 рік зникло 11,4 млн. грн., а загальна кількість шахрайських операцій із платіжними картами виросла на 47% і з 35 до 57 збільшилася кількість банків, з рахунків яких зникали кошти. Найбільшу частку несанкціонованих списань займали рахунки фізичних осіб. Найбільша частка зловмисних операцій з коштами клієнтів банку припадає на системи дистанційного банківського обслуговування, що пов'язане з використанням комп'ютерної та іншої техніки, а також мережі Інтернет [8].

Висновки

Основні вимоги проведення аудиту інформаційної безпеки банків під час роботи з електронними грошима, визначено головні напрями проведення перевірки, розглянуто особливості аудиту інформаційної безпеки електронних грошей та функції й напрями аудиту електронних грошей.

Аудит інформаційної безпеки банку під час роботи з електронними грошима – це не інструмент перевірки чи контролю, а засіб надання впевненості користувачам у тому, що система є надійною, безпечною та не створить фінансової та соціальної напруженості в суспільстві.

Список використаних джерел

1. Арнес А. Аудит / А. Арнес, Дж. Лоббек. – М.: Финансы и статистика, 1995. – 560 с.

2. Аудит: учебник для вузов / В.И. Подольский, Г.Б. Поляк, А.А. Савин и др.; под ред. проф. В.И. Подольского. – 2–е изд. – М.: ЮНИТИ–ДАНА, 2000. – 655 с.

3. Бардаш С.В. Економічний контроль в Україні: системний підхід: монографія / С.В. Бардаш. – К.: КНТЕУ, 2010. – 656 с.

4. Бондар В.П. Концепція розвитку аудиту в Україні: теорія, методологія, організація: монографія / В.П. Бондар. – Житомир: ЖДТУ, 2008. – 456 с.

5. Бутинець Т.А. Управлінський контроль та його елементи / Т.А. Бутинець // Вісник Житомирського державного технологічного університету, 2010. – №1 (51) [Електрон. ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/portal/ Natural/Vzhdtu/econ/2010_1/6.pdf

6. Крюков О.І. Інформаційна безпека держави в умовах глобалізації // Державне будівництво. – 2007. – №2 [Електрон. ресурс]. – Режим доступу: http://www.kbuapa.kharkov.ua/e–book/db/2007–2/doc/1/10.pdf

7. Трубін І.О. Електронні гроші: суть та особливості / І.О. Трубін, А.В. Бодюк // Формування ринкових відносин в Україні. – 2006. – №9. – С. 33–36.

8. Мельниченко О.В. Теоретичні засади електронних грошей // Бізнес Інформ. – 2013. – №8. – С. 284–290.

9. Петрик О.А. Аудит: методологія і організація: монографія / О.А. Петрик. – К.: КНЕУ, 2003. – 260 с.

11. Про аудиторську діяльність. Закон України від 22.04.93 №3125–XII [Електрон. ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3125–12

12. Положення про організацію внутрішнього аудиту в комерційних банках України, затверджене постановою Правління Національного банку України від 20.03.98 №114 [Електрон. ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/ v0548500–98

13. Олексюк О.С. Електронні гроші та їх розвиток / О.С. Олексюк, О.В. Мостіпака // Інноваційна економіка. – 2010. – №17. – С. 217–223.

14. Остроухов В. До проблеми забезпечення інформаційної безпеки України / В. Остроухов, В. Петрик // Політичний менеджмент. – 2008. – №4. – С. 135–141.

15. Міжнародні стандарти контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг / Пер. з англ. О.Л. Ольховікова, О.В. Селезньов, О.О. Зєніна, О.В. Гик, С.Г. Біндер. – Ч. 1. – К.: Міжнародна федерація бухгалтерів, Аудиторська палата України, 2010. – 846 с.