УДК 336.71

Мельниченко О. В.

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ ПРИ РОБОТІ З ЕЛЕКТРОННИМИ ГРОШИМА

Стаття присвячена аудиту інформаційної безпеки банку при роботі з електронними грошима. Автором розглянуто основні вимоги та принципи проведення аудиту, 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. Крім того, у статті приділено увагу соціальній інженерії та акцентовано увагу на необхідності проведення аудиту підготовки фахівців банків, задіяних у роботі з електронними грошима, та користувачів (власників) електронних грошей.

Ключові слова: електронні гроші, аудит, інформаційна безпека, банки, атаки, соціальна інженерія

Бібл.: 24.

Мельниченко Олександр Віталійович – кандидат економічних наук, доцент, Університет банківської справи Національного банка України (вул. Андріївська, 1, Київ, 04070, Україна)

Email: amelnitschenko@yahoo.de

УДК 336.71

Мельниченко А. В.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДЕНЬГАМИ

Статья посвящена аудиту информационной безопасности банка при работе с электронными деньгами. Автором рассмотрены основные требования и принципы проведения аудита, определены главные направления проверки, в частности, организационно-технического и правового обеспечения банков для предупреждения нарушения целостности, доступности, конфиденциальности и наблюдаемости информационных систем, что обеспечивают функционирование систем электронных денег. Кроме того, в статье уделено внимание социальной инженерии и акцентировано внимание на необходимости проведения аудита подготовки специалистов банков, задействованных в работе с электронными деньгами, и пользователей (собственников) электронных денег.

Ключевые слова: электронные деньги, аудит, информационная безопасность, банки, атаки, социальная инженерия

Библ.: 24.

Мельниченко Александр Витальевич – кандидат экономических наук, доцент, Университет банковского дела Национального банка Украины (ул. Андреевская, 1, Киев, 04070, Украина)

Email: amelnitschenko@yahoo.de

UDC 336.71

Melnychenko O. V.

AUDIT OF BANK'S INFORMATION SECURITY WHEN WORKING WITH ELECTRONIC MONEY

The article is devoted to the audit of the bank's information security when working with electronic money. The author considers main requirements and principles of conducting audit, identifies main directions of the audit, in particular, organisational-technical and legal provision of banks for prevention of violation of integrity, accessibility, confidentiality and observance of information systems, which ensure functioning of the electronic money systems. Moreover, the article pays attention to social engineering and focuses on the necessity to conduct audit of training of bank specialists that deal with electronic money operations and users (owners) of electronic money.

Key words: electronic money, audit, information security, banks, attacks, social engineering

Bibl.: 24.

Melnychenko Oleksandr V. – Candidate of Sciences (Economics), Associate Professor, University of Banking of the National Bank of Ukraine (vul. Andriyivska, 1, Kyiv, 04070, Ukraine)

Email: amelnitschenko@yahoo.de

Вступ. У сучасних умовах ведення бізнесу найважливіше місце в усіх сферах економіки, безумовно, посідає інформація. 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.

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. При цьому фінансовій безпеці банку сучасні науковці надають такі характеристики [5, с. 150]:

- забезпечується рівноважний і стійкий фінансовий стан банку;
- вона сприяє ефективній діяльності банку;
- є можливість на ранніх стадіях визначати проблеми і уникати чи ліквідовувати їх;
- нейтралізуються кризи та запобігається банкрутство.

За даними Національного банку України, з особистих рахунків фізичних осіб за 2012 рік зникло 11,4 млн грн,

загальна кількість шахрайських операцій із платіжними картками виросла на 47 %, з 35 до 57 збільшилася кількість банків, з рахунків яких зникали кошти [11]. Найбільшу частку несанкціонованих списань займали рахунки фізичних осіб – користувачів систем дистанційного банківського обслуговування, що пов'язано з використанням комп'ютерної та іншої техніки, а також мережі Інтернет.

На науш думку, електронні гроші, – це, в першу чергу, 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.

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

Аналіз останніх досліджень і публікацій. Питанням фінансової та економічної безпеки суб'єктів господарювання та держави присвячені праці вітчизняних (Барановського О. І., Єпіфанова А. О.) та зарубіжних науковців. Питанням інформаційної безпеки присвячені публікації Берко А. Ю., Зими А. М., Карасюка В. В., Мясіщева О. А., Олексюка О. С., Рішняк І. В., Судейко М. А., Трубіна І. О. тощо.

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

Метою цієї статті є вивчення сучасних підходів до організації інформаційної безпеки в банках та надання пропозицій щодо проведення аудиту інформаційної безпеки під час роботи банків з електронними грошима.

Виклад основного матеріалу

Інформаційна безпека

Велику увагу інформаційній безпеці під час роботи суб'єктів господарювання з електронними грошима приділяє у своїх працях Трубін І. О. Його роботи щодо функціонування систем електронних грошей присвячені, в основному, питанням правового регулювання обігу й 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 [22, с. 9], автор, на нашу думку, помилково ототожнює їх із безготівковими коштами. Підтвердженням цього є дані Національного банку України про те, що за 9 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 [19]. При цьому за допомогою системи електронних платежів Національного банку України не здійснювались перекази електронних грошей, а загальний обсяг операцій із ними склав 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» [21, с. 5]. Якщо Трубін І. О. мав на увазі розміщення банками коштів, що є забезпеченням емітованих електронних грошей, то це також було зроблено помилково, про що детально йдеться в роботі автора цієї статті [8].

Однак, ми підтримуємо Трубіна І. О. в тому, що електронні гроші – це, в першу чергу, 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 [22, с. 4].

У роботі зазначеного автора [23] детально досліджено вивченість у літературі питань інформаційної безпеки в процесі функціонування систем електронних грошей. Так, науковцем узагальнено думки інших науковців і виокремлюються наступні 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 [23, с. 4, 6].

У роботі Олексюка О. С. мова йде також про те, що сьогодні гроші перетворюються на інформаційний ресурс [13, с. 218] і тому електронні гроші вразливі, зокрема, для шахраїв, забезпечених настільки сучасними засобами, наскільки сучасними є і їх об'єкти [13, с. 222].

Під загрозою загалом розуміється можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого, те, що може заподіяти зло чи неприємність [3, с. 387]. Це потенційна можливість порушення інформаційної безпеки, настання небажаного інциденту, який може завдати шкоди системі чи організації [20].

Спроба реалізації загрози називається атакою, а особа, котра здійснює таку спробу, – зловмисником (порушником). Під атакою мається на увазі рішуча дія, спрямована на досягнення якої-небудь мети [3, с. 44]. Це навмисні дії, спрямовані на порушення характеристик інформації.

Інформаційній безпеці сьогодні приділяється увага як науковців, так і держави. Так, серед основних напрямів державної політики з питань національної безпеки України в інформаційній сфері відповідно до Закону України «Про основи національної безпеки України» [17] є:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов

для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

- активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

При цьому, під інформаційним суверенітетом держави на законодавчому рівні розуміється здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [16].

Забезпечення інформаційної безпеки передбачає збереження властивостей інформації та запобігання несанкціонованим діям в інформаційній системі шляхом вжиття організаційно-технічних заходів для запобігання заподіянню шкоди інтересам власників інформації чи інформаційної системи.

За словами Крюкова О. І. [6, с. 3], інформаційна безпека – це суспільні правовідносини щодо організації створення, підтримки, охорони та захисту необхідних для суспільства безпечних умов життєдіяльності, які також пов'язані з організацією технологій створення, розповсюдження, зберігання та використання інформації для забезпечення функціонування і розвитку інформаційних ресурсів.

У роботі зазначеного автора велика увага приділяється саме інформаційній безпеці держави, яка, ми вважаємо, тісно пов'язана з її фінансовою безпекою в сучасних умовах використання інформаційних систем і технологій у здійсненні розрахунків та переказів коштів у середині держави та за її межі.

У міжнародному стандарті з інформаційної безпеки, який затверджений Національним банком України як державний стандарт [20], йдеться про інформаційну безпеку як про захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику і отримання максимальних рентабельності інвестицій та бізнес-можливостей. Вона досягається шляхом упровадження певного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури, а також програмні та апаратні функції.

Зазначеним стандартом визначено, крім іншого, джерела формування вимог безпеки, які доцільно ідентифікувати, у 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.

На законодавчому рівня під інформаційною безпекою сьогодні розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [18].

Окремі науковці [14; 15] вважають таке визначення неповним, оскільки воно не враховує поділу інформаційної безпеки на типи та інформаційний розвиток. Тому пропонують визначення даної категорії як стану захищеності особи, суспільства, держави й інформаційно-технічної інфраструктури, при якому досягається інформаційний розвиток і сторонні (внутрішні й зовнішні) інформаційні впливи не завдають їм суттєвої шкоди та дозволяють нормально їм функціонувати.

Загалом сьогодні під інформаційною безпекою розуміється захищеність інформації та систем, що її підтримують, від впливів випадкового чи навмисного, штучного чи природного характеру [4; 10; 14; 15].

Таке визначення вони вважають більш оптимальним, оскільки воно об'єднує пасивну (стан захищеності) та активну (стан інформаційного розвитку) складові. Крім того, воно більш лаконічне і передбачає поділ інформаційної безпеки на різновиди.

До напрямів інтересів банків при їх роботі з електронними грошима (як і традиційно під час роботи з інформацією, забезпечуючи її безпеку) слід, на нашу думку, віднести:

1. Доступність, під якою розуміється можливість за прийнятний час, у зручний для користувача, наділеного необхідними повноваженнями, спосіб одержати необхідну інформаційну послугу [4; 9; 10, с. 108].

Під час роботи з електронними грошима їх користувачі (власники) фактично повністю залежні від доступності інформації в системі електронних грошей. Так, не отримавши інформації про достатність залишку коштів у електронному гаманці покупця, продавець не надасть відповідної послуги за запитом клієнта. Таким чином, буде повністю порушена соціальна стабільність та підірвано авторитет електронних грошей даної системи.

2. Цілісність – захищеність інформації від руйнування і несанкціонованої зміни [4; 9; 10, с. 108].

Учасниками систем електронних грошей велика увага приділяється також даній характеристиці. Повне чи часткове знищення, викривлення, модифікація, нав'язування хибної інформації може зумовити перетік коштів між рахунками та викрадення коштів клієнтів, наприклад, при зміні інформації про рахунок клієнта, на який відбувається виведення електронних грошей.

3. Конфіденційність – це захист від несанкціонованого доступу до інформації, ознайомлення з нею [4; 9; 10, с. 108]. Конфіденційність – найбільш опрацьований аспект інформаційної безпеки, яка однак у системах електронних грошей найменш важлива. Банки беруть на себе відповідальність за дотримання конфіденційності інформації, що належить, зокрема, до банківської таємниці, а порушення щодо її розголошення суворо караються відповідно до чинного законодавства.

Як відомо, питання ідентифікації клієнтів, а, відтак, збереження та захист конфіденційної інформації, що становить банківську таємницю, у системах електронних грошей та банках як їх основних учасниках взагалі не актуальне, оскільки при розрахунках електронними грошима ідентифікується електронний гаманець, а не його власник [7; 8].

4. Спостережність – властивість, що дозволяє фіксувати діяльність користувачів і процесів та однозначно установлювати їхню причетність до певних подій із метою запобігання порушення політики безпеки та можливості притягнення їх до відповідальності [9].

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[1] коштує зловмисникам за різними даними приблизно 100 тис. грн [1].

Аудит інформаційної безпеки

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, зокрема, 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. Відповідно, доцільно, на нашу думку, також здійснити оцінку витрат на участь у навчальних заходах, зокрема, з питань функціонування систем електронних грошей та організації їх обігу, захисту тощо.

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. У таких документах слід з'ясувати наявність рекомендацій, зокрема, щодо:

- обмеження довжини, складності та часу життя паролів, які забезпечують доступ до електронних гаманців чи інших елементів інформаційної системи;
- доцільності в тому, щоб пароль був відомий лише одному користувачеві. У разі інциденту винен буде власник облікового запису, тому що відсутні докази, що це зробив не він, про що буде зафіксовано в протоколах дій співробітників, які є підтвердженням будь-яких дій в інформаційних системах. Тому, власник облікового запису чи електронного гаманця зацікавлений, щоб його пароль був відомий тільки йому;
- заборони використання функцій автоматичного запам'ятовування паролів, якщо така можливість надається інформаційною системою;
- рекомендації, що паролі для доступу до інформаційних систем не слід використовувати в інших середовищах;
- уникнення підглядання іншими особами під час введення паролів;
- зміни пароля у разі встановлення або підозри на компрометацію пароля або його передачі іншим особам.

Так, пароль доступу не повинен: бути пустим або простим, наприклад, «12345»; збігатися з ім'ям користувача, номером мобільного телефону тощо; бути словниковим словом; угадуватися на основі інформації про користувача. При цьому, пароль повинен містити не менше 8 символів та комбінацію з цифр, літер у верхньому та нижньому регістрі, а також спеціальних символів (~! @ # $% ^ & * () {} "| \ /.,;: < > ').

Разом з тим, доцільно проводити перевірку правових аспектів, які полягають у формуванні правил поведінки персоналу, формування методик виявлення та розкриття правопорушень за допомогою інформаційних систем і технологій [23, с. 4, 6].

Отже, проводячи аудит інформаційної безпеки банку, який є учасником систем електронних грошей, необхідно

[1] 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 [22]

звертати увагу не лише на традиційні організаційні й технічні заходи, а й на психологічну підготовленість працівників до методів соціальної інженерії. Такий підхід до проведення сучасного аудиту в банку дозволятиме забезпечити інформаційну безпеку на належному рівні в умовах стрімкого розвитку технологій та ґрунтовного підходу до категорії «інформаційна система», яка є значно ширшою, ніж, наприклад, комп'ютерна, фінансова чи економічна безпека та і вимагає особливої підготовки аудиторів і залучення експертів до проведення перевірок.

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.

Протистояння методам соціальної інженерії

Слід також пам'ятати, що зловмисники не обходяться лише технічною озброєністю, коли намагаються добути цінну інформацію. Часто ними використовуються психологічні навички, щоб увести користувача в оману і отримати необхідну інформацію. Наука, що вивчає можливість отримання інформації внаслідок людської неуважності, використання простих паролів та не застосованих необхідних заходів безпеки – це соціальна інженерія [2]. Вона є також способом переконання користувачів повідомити важливу інформацію.

Методів соціальної інженерії існує достатньо багато, зокрема:

1. Претекстінг.

Претекстінг – першочергові заходи зловмисника, спрямовані на здобуття необхідної інформації для здійснення атак за допомогою соціотехнік. По-перше, зловмисник буде намагатися роздобути якомога більше інформації про свою жертву, використовуючи соціальні мережі, пошукові системи та засоби вербального спілкування. По-друге, буде збирати ту ж саму інформацію про довірену особу, яку жертва буде знати опосередковано, але при цьому проявляти достатній рівень довіри.

2. Мережеві атаки. Маскування під внутрішнього користувача.

3. Мережеві атаки. Суперечливий метод.

Зловмисники іноді можуть скористатися методом від супротивного, щоб змусити користувача зробити те, що необхідно зловмисникові. При цьому зловмисник пропонує користувачеві спочатку варіант дій, який є абсолютно неприйнятним для користувача, а потім пропонує більш м'який варіант, який користувач інтуїтивно порівняє з попереднім варіантом і вирішить, що другий варіант є найбільш прийнятним. Хоча насправді зловмисник створює лише уявну ілюзію вибору у користувача, насправді зловмисник точно знає, що захоче вибрати користувач. Слід зазначити, що в даному методі зловмисник не маскується під внутрішнього користувача.

4. Метод «дорожнє яблуко».

Цей метод атаки являє собою адаптацію зловмисного програмного забезпечення і полягає у використанні фізичних носіїв інформації. Зловмисник може підкинути інфікований CD або флеш в місці, де носій може бути легко знайдений. Носій підробляється під офіційний і супроводжується підписом, призначеним викликати цікавість. Слід зазначити, що у випадку з USB-flash зловмисне програмне забезпечення може бути вшито у носій на апаратному рівні, тобто бути записаним у мікросхеми. Будь-яка антивірусна перевірка не виявить його на такому носії. Такий пристрій або інший сучасний пристрій може бути і офіційно вручений жертві із найкращими побажаннями.

5. Методи конкурентної розвідки.

Розповсюджений метод, при якому співробітнику банку пропонується нібито корисна інформація, отримана нелегальним способом. Після копіювання інформації, яка є свого роду приманкою, на флеш-носій із комп'ютера користувача записуються необхідні дані. Копіювання і запис проходять одночасно, а процес запису на флеш-пам'ять припиняється одночасно із завершенням копіювання, щоб не виникало підозри.

6. Пошук інформації в смітті.

Конфіденційна інформація, що міститься на паперових носіях або на електронних носіях інформації, які вийшли з ладу, при попаданні до рук зловмисника може бути відтворена за допомогою технічних засобів.

Зважаючи на викладене, аудиторам слід приділяти увагу готовності працівників банків протистояти методам соціальної інженерії. Вона може бути досягнута як завдяки підвищенню кваліфікації працівників на спеціалізованих курсів, так і через проведення навчальних заходів всередині компанії.

Висновки.

За даними Української міжбанківської асоціації членів платіжних систем ЕМА, протягом січня – вересня 2013 року було здійснено 257 спроб списання коштів із рахунків клієнтів банків на загальну суму 108,7 млн грн, у 2012 році їх налічувалось 179 на суму 150,1 млн грн, а у 2011 році – 6 спроб на суму 14,9 млн грн [1]. Більшість шахрайський операцій були реалізовані через низький рівень обізнаності клієнтів банків з питань інформаційної безпеки. Тому питання аудиту інформаційної безпеки та проведення її аудиту сьогодні набуває значної актуальності, особливо це стосується роботи банків з електронними грошима, оскільки цьому питанню у сучасній науковій літературі приділяється недостатньо уваги.

У цій статті нами було розглянуто основні вимоги та принципи проведення аудиту інформаційної безпеки банків під час роботи з електронними грошима, визначено головні напрями проведення перевірки, зокрема, організаційно-технічної та правової забезпеченості банків для запобігання порушення цілісності, доступності, конфіденційності та спостережності інформаційних систем, що забезпечують функціонування систем електронних грошей. Крім того, нами виділено ще один важливий аспект захищеності банків, якому слід приділяти особливу увагу аудиторам, – забезпечення підготовленості працівників банків та користувачів (власників) електронних грошей для уникнення атак шахраїв за допомогою методів соціальної інженерії.

ЛІТЕРАТУРА

1. В Украине растет финансовая киберпреступность [Електронний ресурс]. – Режим доступу: http://www.capital.ua/publication/10487-v-ukraine-rastet-finansovaya-kiberprestupnost-chtoby-zaschitit-dannye-tolko-v-etom-godu-banki-potratili-3-mln-grn
2. Бурячок В. Л., Корченко О. Г., Бурячок Л. В. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем // Захист інформації. – 2012. – № 4. – С. 5 – 12.
3. Бусел В. Т. Великий тлумачний словник сучасної української мови / Уклад і голов. ред. В. Т. Бусел. – К.: Ірпінь; ВТФ «Перун», 2007. – 1736 с.
4. Галицкий А. В., Рябко С. Д., Шаньган В. Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.
5. Єпіфанов А. О. Фінансова безпека підприємств і банківських установ [Текст] : монографія / за заг. редакцією д-ра екон. наук, проф. А. О. Єпіфанова [А. О. Єпіфанов, О. Л. Пластун, В. С. Домбровський та ін.]. – Суми: ДВНЗ «УАБС НБУ», 2009. – 295.
6. Крюков О. І. Інформаційна безпека держави в умовах глобалізації // Державне будівництво. – 2007. – № 2 [Електронний ресурс]. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2007-2/doc/1/10.pdf
7. Мельниченко О. Аналіз стану використання сучасних платіжних засобів у контексті виведення готівкових коштів з поза банківського обігу в Україні // Вісник Національного банку України. – 2013. – № 1. – С. 26 – 32.
8. Мельниченко О. В. Теоретичні засади електронних грошей // Бізнес Інформ. – 2013. – №8. – С. 284 – 290.
9. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України, затверджені 01.03.2011 р. [Електронний ресурс]. – Режим доступу : http: www.bank.gov.ua/doccatalog/document?id=72235
10. Мясіщев О. А. Напрямки вирішення проблем захисту інформації в мережах / О. А. Мясіщев, А. В. Джулій // Вісник Хмельницького національного Університету. Серія : «Технічні науки». – 2009. – № 4. – С. 107 – 112.
11. На крючке у хакеров [Електронний ресурс]. – Режим доступу: http: www.depo.ua/ru/delovaja-stolica/2013_ds/fevral_ds2013/8-614/99411.htm
12. Обсяг електронних грошей в Україні виріс на 42% [Електронний ресурс]. – Режим доступу : http://www.epravda.com.ua/news/2013/05/29/377302/
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. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи // Юридичний журнал. – 2009. – № 5 [Електронний ресурс]. – Режим доступу : http://www.justinian.com.ua/article.php?id=3222
16. Про Національну програму інформатизації. Закон України [Електронний ресурс]. – Режим доступу: http:// www. zakon1.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

REFERENCES

Buriachok, V. L., Korchenko, O. H., and Buriachok, L. V. "Sotsialna inzheneriia iak metod rozvidky informatsiino-telekomunikatsiinykh system" [Social engineering as a method of intelligence information and telecommunication systems]. Zakhyst informatsii, no. 4 (2012): 5-12.

Busel, V. T. Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy. [Great Dictionary of the modern Ukrainian language]. K.; Irpin: Perun, 2007.

"DoS-ataka" [DoS-attack]. http://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0

Galitskiy, A. V., Riabko, S. D., and Shangan, V. F. Zashchita informatsii v seti – analiz tekhnologiy i sintez resheniy [Protection of information in networks - analysis and synthesis technology solutions]. Moscow: DMK Press, 2004.

Kriukov, O. I. "Informatsiina bezpeka derzhavy v umovakh hlobalizatsii" [Information security in the context of globalization]. http://www.kbuapa.kharkov.ua/e-book/db/2007-2/doc/1/10.pdf

[Legal Act of Ukraine] (2011). http:www.bank.gov.ua/doccatalog/document?id=72235

[Legal Act of Ukraine]. http://zakon1.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80

[Legal Act of Ukraine]. http:zakon4.rada.gov.ua/laws/show/964-15

[Legal Act of Ukraine]. http:zakon.rada.gov.ua/go/537-16

[Legal Act of Ukraine] (2010).

Melnychenko, O. "Analiz stanu vykorystannia suchasnykh platizhnykh zasobiv u konteksti vyvedennia hotivkovykh koshtiv z poza bankivskoho obihu v Ukraini" [Analysis of the use of modern means of payment in the context of the withdrawal of cash from circulation outside banks in Ukraine]. Visnyk Natsionalnoho banku Ukrainy, no. 1 (2013): 26-32.

Melnychenko, O. V. "Teoretychni zasady elektronnykh hroshei" [The theoretical basis of electronic money]. Biznes Inform, no. 8 (2013): 284-290.

Miasishchev, O. A., and Dzhulii, A. V. "Napriamky vyrishennia problem zakhystu informatsii v merezhakh" [Towards solving the problems of information security in networks]. Visnyk Khmelnytskoho natsionalnoho Universytetu. Tekhnichni nauky, no. 4 (2009): 107-112.

"Na kriuchke u khakerov" [Hooked on hackers]. http:www.depo.ua/ru/delovaja-stolica/2013_ds/fevral_ds2013/8-614/99411.htm

Ostroukhov, V., and Petryk, V. "Do problemy zabezpechennia informatsiinoi bezpeky Ukrainy" [On the problem of information security of Ukraine]. Politychnyi menedzhment, no. 4 (2008): 135-141.

"Obsiah elektronnykh hroshei v Ukraini vyris na 42%" [The amount of electronic money in Ukraine increased by 42%]. http:www.epravda.com.ua/news/2013/05/29/377302/

Oleksiuk, O. S., and Mostipaka, O. V. "Elektronni hroshi ta ikh rozvytok" [Electronic money and its development]. Innovatsiina ekonomika, no. 17 (2010): 217-223.

Petryk, V. "Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby" [The essence of information security, society and the individual]. http:www.justinian.com.ua/article.php?id=3222

"Systema elektronnykh platezhiv Natsionalnoho banku Ukrainy za stanom na 1 zhovtnia 2013 roku" [EFT National Bank of Ukraine as of October 1, 2013]. http:www.bank.gov.ua/control/uk/publish/article?art_id=53861&cat_id=78675

17. Про основи національної безпеки України. Закон України [Електронний ресурс]. – Режим доступу: http://www. zakon4. rada.gov.ua/laws/show/964-15

18. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки. Закон України [Електронний ресурс]. – Режим доступу: http://www. zakon.rada.gov.ua/go/537-16

19. Система електронних платежів Національного банку України за станом на 1 жовтня 2013 року [Електронний ресурс]. – Режим доступу: http://www.bank.gov.ua/control/uk/publish/article?art_id=53861&cat_id=78675.

20. Стандарт Національного банку України СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD), затверджений постановою Правління Національного банку України від 28.10.2010 р. № 474.

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

22. Трубін І. О. Правові засади функціонування системи електронних платежів у сфері електронної комерції : автореф. дис. … кандидата юр. наук : 12.00.07 / Трубін Ігор Олексійович. К., 2012. – 20 с.

23. Трубін І. О. Теоретичні аспекти гарантування інформаційної безпеки в процесі функціонування систем електронних грошей [Електронний ресурс] / І. О. Трубін // Право та управління / Електронне наукове видання. – 2011. – № 3.

24. DoS-атака [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%-D0%BA%D0%B0

Trubin, I. O., and Bodiuk, A. V. "Elektronni hroshi: sut ta osoblyvosti" [Electronic money : the nature and characteristics]. Formuvannia rynkovykh vidnosyn v Ukraini, no. 9 (2006): 33-36.

Trubin, I. O. "Pravovi zasady funktsionuvannia systemy elektronnykh platezhiv u sferi elektronnoi komertsii" [Legal basis of the functioning of the electronic payment system in e -commerce]. avtoref. dys. … kandydata iur. nauk : 12.00. 07, 2012.

Trubin, I. O. "Teoretychni aspekty harantuvannia informatsiinoi bezpeky v protsesi funktsionuvannia system elektronnykh hroshei" [Theoretical aspects of ensuring information security in the operation of electronic money]. Pravo ta upravlinnia. Elektronne naukove vydannia, no. 3 (2011).

"V Ukraine rastet finansovaia kiberprestupnost" [In Ukraine, the growing financial cybercrime]. http://www.capital.ua/publication/10487-v-ukraine-rastet-finansovaya-kiberprestupnost-chtoby-zaschitit-dannye-tolko-v-etom-godu-banki-potratili-3-mln-grn

Yepifanov, A. O., Plastun, O. L., and Dombrovskyi, V. S. Finansova bezpeka pidpryiemstv i bankivskykh ustanov [Financial security companies and banking institutions]. Sumy: UABS NBU, 2009.