УДК 340.13

Т.О. Чернадчук
кандидат юридичних наук, доцент
Сумський національний аграрний університет

ПРАВОВІ ЗАСАДИ ОРГАНІЗАЦІЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ: ОКРЕМІ ПИТАННЯ

У статті проаналізовано стан правового забезпечення організації платіжної системи в Україні, визначено основні питання захисту інформації при проведені переказу, запропоновано спеціальні принципи, на яких має будуватися система захисту інформації.

Ключові слова: *платіжна система, внутрішньодержавна платіжна система, міжнародна платіжна система, внутрішньобанківська платіжна система, платіжна організація, офісайт, реконсиляція, інформація, інформаційна безпека, принцип забезпечення цілісності інформації, принцип забезпечення конфіденційності інформації, принцип забезпечення доступу до інформації, принцип відповідальності.*

I. Вступ

У сучасних умовах особливої актуальності набувають питання організації грошових розрахунків, що зумовлено значною роллю грошового обігу в забезпеченні розвитку економіки держави. Провідна роль у процесі здійснення суб'єктами переказу коштів і розрахунків відводиться платіжним системам та системам розрахунків, оскільки саме надійні й ефективні платіжні системи забезпечують розрахунки за зобов'язаннями та є запорукою стабільного функціонування фінансової системи й економіки країни загалом. Через платіжні системи проходять значні грошові потоки, тому порушення в роботі цих систем, невиконання одним чи кількома членами, учасниками платіжної системи своїх зобов'язань можуть призвести до системного ризику, негативно вплинути на стабільність фінансової системи країни, підірвати довіру суспільства до грошей. Таким чином, на сьогодні значне місце відведено дослідженню правових засад організації платіжних систем.

Відповідно до законодавства, платіжна система – це платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. Вказана в законі сукупність елементів не відповідає ознаці достатності складових, що забезпечують цілісність системи, оскільки без таких осіб, заходів, явищ та інструментів, як банкомати, документи (в тому числі електронні) на переказ грошей, електронні засоби телекомунікації та програмне забезпечення програмно-технічних комплексів, за допомогою яких здійснюється переказ грошей, заходи безпеки функціонування платіжної системи, клірингові установи, спеціальний платіжний засіб тощо, сучасна платіжна система позбавлена матеріального змісту, а відтак, не може нормально функціонувати. Включення вищеперелічених елементів до складу платіжної системи необхідно визнати обов'язковим, оскільки без урахування їх специфіки неможливі як організаційне моделювання структури будь-якої платіжної системи, так і дійове правове регулювання грошового обігу через прогалини в організації грошової системи [1, с. 353]. На сьогодні актуальним питанням правового забезпечення організації платіжної системи не приділяється достатньої уваги.

II. Постановка завдання

Мета статті – на основі аналізу чинного законодавства з'ясувати стан правового забезпечення організації платіжної системи в Україні; визначити основні питання захисту інформації при проведенні переказу; запропонувати спеціальні принципи, на яких має будуватися система захисту інформації.

III. Результати

За загальним правилом, відповідно до ст. 9 Закону України "Про платіжні системи та переказ грошей в Україні" [2], переказ в Україні може здійснюватися за допомогою внутрішньодержавних платіжних систем, в яких платіжна організація є резидентом, що здійснює свою діяльність і забезпечує проведення переказу коштів виключно в межах України та міжнародних платіжних систем, в якій платіжна організація може бути як резидентом, так і нерезидентом і яка здійснює свою діяльність на території двох і більше країн та забезпечує проведення переказу коштів у межах цієї платіжної системи, у тому числі з однієї країни в іншу.

В Україні функціонують платіжні системи, які створені:

– Національним банком – Система електронних платежів (далі – СЕП), яка забезпечує здійснення розрахунків у межах України між банками як за дорученнями клієнтів банків, так і за зобов'язан-

нями банків та інших учасників системи. У СЕП виконуються міжбанківські перекази у файловому режимі та в режимі реального часу. Здійснення банком початкових платежів у файловому режимі є обов'язковим, а в режимі реального часу – за його вибором. Разом з тим учасник системи, який працює в СЕП у файловому режимі, забезпечує приймання платежів у режимі реального часу. У файловому режимі обмін міжбанківськими електронними розрахунковими документами здійснюється шляхом приймання-передавання документів, сформованих у файл; Національна система масових електронних платежів – внутрішньодержавна банківська багатоемітентна платіжна система масових платежів, в якій розрахунки за товари та послуги, одержання готівки й інші операції здійснюються з використанням спеціальних платіжних засобів за технологією, що розроблена Національним банком України;

– державними банками та державними установами – платіжні системи державних банків, Державного казначейства України та Українського державного підприємства поштового зв'язку "Укрпошта";
– установами приватного сектору – внутрішньодержавні та міжнародні платіжні системи банків і небанківських установ.

Платіжна система (крім внутрішньобанківської платіжної системи) діє відповідно до правил, установлених платіжною організацією відповідної платіжної системи. Внутрішньобанківська платіжна система, що являє собою програмно-технічний комплекс з власними засобами захисту інформації, який експлуатується комерційним банком або об'єднанням банків і здійснює розрахунки між установами цього банку (об'єднання), діє відповідно до внутрішніх документів банку. Українські банки широко використовують систему "клієнт – банк", пропонуючи платіжні послуги своїм клієнтам на базі сучасних технологій. Діяльність платіжної системи має відповідати вимогам законодавства України. Широко використовується система масових платежів за допомогою пластикових карток.

Безперечно, важливим чинником успішного функціонування платіжної системи є нормативно-правова база, орієнтована на створення сприятливих умов для її ефективної діяльності, забезпечення своєчасного завершення розрахунків між суб'єктами господарювання. Загальні засади функціонування платіжних систем в Україні, відносини у сфері переказу коштів регулюють Конституція України, Закони України "Про Національний банк України", "Про банки і банківську діяльність", "Про поштовий зв'язок", "Про платіжні системи та переказ коштів в Україні", інші акти законодавства України й нормативно-правові акти Національного банку України, а також Уніфіковані правила та звичаї для документарних акредитивів Міжнародної торгової палати, Уніфіковані правила з інкасо Міжнародної торгової палати, Уніфіковані правила стосовно договірних гарантій Міжнародної торгової палати та інші міжнародно-правові акти з питань переказу коштів.

Базовим законом, що визначає загальні засади функціонування платіжних систем в Україні та загальний порядок проведення переказу коштів у межах України, є Закон України "Про платіжні системи та переказ коштів в Україні". Законом визначено загальні засади функціонування платіжних систем і систем розрахунків в Україні, поняття та загальний порядок проведення переказу коштів у межах України, встановлено відповідальність суб'єктів переказу, а також визначено загальний порядок здійснення нагляду (оверсайта) за платіжними системами. Незважаючи на те, створена платіжна система державною чи приватною установою, найважливішим питанням є виявлення та ефективне управління ризиками в цій системі. Виходячи із цієї концепції, Національний банк, запроваджуючи нагляд (оверсайт) за платіжними системами, прагне захистити фінансову систему від впливу системного та інших ризиків, які властиві платіжним системам.

У процесі нагляду (оверсайта) Національний банк України здійснює діяльність з моніторингу, оцінювання платіжних систем і в разі необхідності ініціює зміни щодо їх діяльності з метою забезпечення безперервного, надійного та ефективного функціонування відповідних систем.

Правила платіжної системи мають установлювати організаційну структуру платіжної системи, умови участі, порядок вступу й виходу із системи, управління ризиками, порядок ініціювання та здійснення переказу й взаєморозрахунків за цим переказом у системі, порядок вирішення спорів учасників між собою та між учасниками й користувачами, систему захисту інформації, порядок проведення реконсиляції (процедури контролю, яка полягає в ідентифікації та перевірці виконання кожного переказу коштів за допомогою показників, визначених платіжною системою).

Правила платіжної системи, а також договори, що укладаються платіжною організацією платіжної системи з учасниками цієї системи, мають передбачати порядок врегулювання випадків нездатності виконання учасниками платіжної системи своїх зобов'язань.

Платіжна організація є базовим елементом платіжної системи, оскільки є організатором системи суспільних відносин зі здійснення переказу грошей у межах платіжної

системи, залучає до її роботи членів платіжної системи, які разом з нею утворюють апарат платіжної системи і є складовою національної системи органів, які сприяють організації та функціонуванню грошового обігу в Україні.

Враховуючи те, що електронні документи на переказ, розрахункові документи та документи за операціями із застосуванням електронних платіжних засобів можуть містити інформацію, що є банківською таємницею або є інформацією з обмеженим доступом, яка, у свою чергу, під час їх передавання засобами телекомунікаційного зв'язку потребує відповідного захисту від несанкціонованого доступу (доступу до інформації осіб, які не мають на це прав або повноважень); несанкціонованих змін інформації (внесення змін або часткового чи повного знищення інформації особами, які не мають на це права або повноважень); несанкціонованих операцій з компонентами платіжних систем (використання або внесення змін до компонентів платіжної системи протягом її функціонування особами, які не мають на це права або повноважень), актуального значення набувають питання захисту інформації при проведенні переказу. Система такого захисту повинна забезпечувати безперервний захист інформації щодо переказу коштів на всіх етапах її формування, обробки, передачі та зберігання.

На нашу думку, основними напрямами діяльності банківських підрозділів щодо захисту інформації (інформаційної безпеки) є розробка основних напрямів використання технічних та програмних засобів і способів захисту електронної банківської інформації; аналіз та організація діяльності щодо виявлення можливих каналів втрати банківської інформації за допомогою технічних засобів захисту. Заходи щодо забезпечення інформаційної безпеки банку мають бути систематичними й здійснюватися в комплексі з іншими заходами. Важливе значення для забезпечення інформаційної безпеки банківської діяльності має законодавчий рівень такого забезпечення. При розробці системи забезпечення інформаційної безпеки банку особливу увагу потрібно приділяти оцінюванню відповідності управлінських рішень, технологій, підходів та конкретних програмно-апаратних засобів вимогам чинного законодавства.

Адміністративний рівень інформаційної безпеки реалізується у формі прийнятої політики безпеки, що містить основні принципи та правила, дотримання яких забезпечить цілісність і конфіденційність банківської інформації. Такі принципи та правила політики безпеки містяться в спеціальному документі й відповідних організаційно-розпорядчих документах, які стосуються всіх сфер банківської діяльності і є комплексом управлінських рішень та інструкцій щодо регламентації дій як у звичайному режимі банківської діяльності, так і в екстремальних випадках.

На програмно-технічному рівні застосовується система взаємопов'язаних заходів, які забезпечують ефективну та безпечну роботу серверів безпеки, а також сталу керованість інформаційної системи банку, можливість її розвитку з одночасною протидією новим загрозам при збереженні таких властивостей, як висока ефективність та простота й зручність використання. З метою виконання зазначених вимог здійснюється збір, узагальнення та аналіз інформації з питань перспективного програмно-технічного забезпечення інформаційної безпеки. За результатами такого аналізу з урахуванням вимог Національного банку України вносяться пропозиції щодо впровадження перспективних програмних та технічних засобів захисту в інформаційні системи.

Надійність та ефективність банківської діяльності забезпечується шляхом реалізації відповідних вимог до системи безпеки (безперервність, плановість, конкретність, активність, універсальність, комплексність), а важливою складовою банківської безпеки є інформаційна безпека.

Інформаційна банківська безпека та захист банківської інформації не є тотожними поняттями, оскільки інформаційна безпека охоплює не тільки поняття захисту, а й аутентифікацію, аудит інформаційних систем, виявлення несанкціонованого проникнення в інформаційну систему банку. Так, наприклад, при передаванні даних з використанням комп'ютерних мереж можуть виникнути проблеми, пов'язані з інформаційною безпекою, зокрема якщо банк має територіально відокремлені структурні підрозділи, розташовані на значній відстані один від одного, то при пересиланні інформації загальнодоступною мережею необхідно бути впевненим, що ніхто не зможе скористатися цією інформацією або змінити її. Можуть виникнути проблеми як для банку, так і для його клієнта при розрахунках в інтернет-крамниці, коли оплата відбувається в електронному вигляді. Покупець повинен мати гарантії, що він одержить оплачений товар, відповідно розрахувавшись, а номер його кредитної картки не стане нікому відомий. Тому працівники банківської установи повинні вміти визначати критичні інформаційні ресурси банку та рівень їх захищеності від різних атак, які можуть здійснювати зловмисники або конкуренти, що використовують різні вразливі місця захисту інформаційної системи.

Основними порушеннями інформаційної банківської безпеки, звертають увагу фахівці банківської справи, є втрата конфіденцій-

ності (розкриття інформаційних ресурсів), втрата цілісності (їх неавторизована модифікація), втрата доступності (неавторизована втрата доступу до цих ресурсів).

Отже, з метою запобігання порушенням інформаційної безпеки інформаційних банківських ресурсів потрібно виявляти та аналізувати вразливі місця інформаційної системи банку та ресурси, які потребують захисту, а також імовірні атаки, які можуть відбутися в конкретному оточенні. Після цього потрібно визначити інформаційні ризики для інформаційного ресурсу, обрати контрзаходи згідно з обраною політикою банківської безпеки й забезпечити їх реалізацію за допомогою механізмів і сервісів безпеки [3, с. 45–46].

IV. Висновки

На нашу думку, політика інформаційної безпеки платіжних систем має визначати взаємопов'язану сукупність механізмів і сервісів безпеки, адекватну ресурсам, що захищаються, й оточенню, в якому їх використовують.

У свою чергу, система захисту інформації має будуватися на таких спеціальних принципах: забезпечення цілісності інформації (інформація не може бути модифікована неавторизованим користувачем і (або) процесом); принцип забезпечення конфіденційності інформації (інформація не може бути отримана неавторизованим користувачем і (або) процесом); забезпечення доступу до інформації (постійний та безперешкодний доступу до компонентів платіжної системи особам, які мають на це право або повноваження); заперечення відмови ініціатора від передання інформації (неможливість відмови ініціатора від факту передавання та отримувачем від факту прийняття документа на переказ, документа за операціями із застосуванням засобів ідентифікації, документа на відкликання); відповідальності (суб'єкти переказу несуть відповідальність за неналежне використання та зберігання засобів захисту інформації, що використовуються при здійсненні переказів).

Список використаної літератури

1. Алісов Є.О. Проблеми правового регулювання грошового обігу в Україні : дис. … д-ра. юрид. наук : 12.00.07 / Є.О. Алісов. – Х., 2006. – С. 445.
2. Про платіжні системи та переказ коштів в Україні : Закон України від 05.04.2001 р. № 2346-III [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/.
3. Чернадчук Т. Забезпечення інформаційної банківської безпеки як один із напрямів банківської діяльності / Т. Чернадчук // Юридична Україна. – 2013. – № 3. – С. 44–47.

Стаття надійшла до редакції 25.02.2014.

Чернадчук Т.А. Правовые принципы организации и информационной безопасности платежных систем: отдельные вопросы

В статье проанализировано состояние правового обеспечения организации платежной системы в Украине, определены основные вопросы защиты информации при проведении переводов, предложены специальные принципы, на которых должна строиться система защиты информации.

Ключевые слова: *платежная система, внутригосударственная платежная система, международная платежная система, внутрибанковская платежная система, платежная организация, оверсайт, реконсиляция, информация, информационная безопасность, принцип обеспечения целостности информации, принцип обеспечения конфиденциальности информации, принцип обеспечения доступа к информации, принцип ответственности.*

Chernadchuk T. Legal principles of information security and payment systems: particular items

In this article is analyzed the situation of the legal support of the Ukrainian payment system by the author. Attention is put on the question specified in the law a set of elements does not match attribute sufficient components to ensure the integrity because the absence of such person, measures, phenomenon and instruments like ATM (including electronic) for remittance, electronic telecommunications and software -software complexes, whereby the transfer of money, precautions functioning of the payment system, clearing agencies, special means of payment, etc., the current payment system is devoid of substantive content, and therefore can not function properly, including under the abovementioned elements in the payment system must recognize mandatory, because without them the specifics are not possible as the organizational structure modeling of any payment system and Characters legal regulation of money circulation through gaps in the monetary system. It is noted that the payment organization is a basic element of the payment system because it is an organizer of the social relation system in remittance in the measures of payment system, include in work all members of payment system which are together make payment system apparatus and is part of a national system of which contribute to the organization and functioning of money circulation in Ukraine. Other side making oversize by the National Bank of Ukraine plays the important role in efficient functioning of payment system in the country. It is underlined that the rules of payment system have to install the organizational structure of the payment system, conditions of participation, the order of entry and exit from the sys-

tem, risk Management, procedure for initiating and implementing the transfer and mutual transfer in this system, the procedure for settling disputes between members themselves and between members and users, information security system, procedure for reconciliation. Regulations of payment system, and also contracts which are made by the payment organization of payment system participants in the system have to order to predict the settlement of the cases failure to perform payment system participants of their obligations. It is determined some problematic points as for information protection during making transfer. Herewith the system of such protection must ensure continuous protection of information as for transfer money on all stages of its formation, processing, transmission and storage, the information security policy of payment systems should define coherent set of mechanisms and services, security, adequate resources to be protected, and the environment in which they are used. In turn, the information security system is based on the following specific principles: the principle of the integrity of information, the principle of ensure the confidentiality of information, the principle of access to information, the principle of denial initiator of the information transfer, the principle of responsibility.

Key words: *payment system, domestic payment system, international payment system, interbank payment system, payment organization, oversize, reconciliation, information, information security, the principle of the integrity of information, the principle of ensure the confidentiality of information, the principle of access to information, the principle of responsibility.*