Література

1. Ukrainian Retail Association. URL: https://rau.ua/uk/ecommerceuk/itogi-goda/

2. Воробйова О. Нормативно-правове забезпечення електронної торгівлі: міжнародний досвід. *Ефективність державного управління:* збірник наукових праць. 2015. С. 269.

3. Про захист прав споживачів: Закон України від 12.05.1991 № 1023-XII. *Відомості Верховної Ради УРСР.* 1991. № 30. Ст. 379.

4. Про електронну комерцію: Закон України від 03.09.2015 №675-VIII. *Відомості Верховної Ради України.* 2015. № 45. Ст. 410.

5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481.

С. В. Глібко,
к.ю.н., доцент, директор НДІ правового забезпечення інноваційного розвитку НАПрН України
ORCID: 0000-0003-3398-9276

ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЗДІЙСНЕННЯ РОЗРАХУНКОВИХ ОПЕРАЦІЙ БАНКАМИ

Активний розвиток інформаційних технологій у сфері банківської діяльності спричинює виникнення нових ризиків як для самих банківських установ, так і для їхніх клієнтів під час здійснення різних видів розрахункових операцій. З одного боку питання правового регулювання забезпечення інтересів клієнтів банків при проведенні розрахунків, як правило, пов'язується з відображенням у правовій формі маркетингових заходів банківських установ, використанням розробок програмних продуктів інших суб'єктів, які обов'язкові для застосування у зв'язку з участю банків у платіжних системах. У цих реаліях інтереси клієнтів є похідними, оскільки останні вимушені користуватися запропонованими послугами банків, і, знаходячись в нерівному економічному становищі, клієнти власними силами

[1] або участю в переговорному процесі при укладанні правочинів з банками не спроможні змінити або посилити свою захищеність певними технічними або програмними засобами. Варто зазначити, що на забезпечення безпеки здійснення платіжних операцій спрямовані функції уповноважених державних органів, насамперед Національного банку України (далі – НБУ).

На сучасному етапі розвитку банківських послуг в Україні так і у світі, в цілому, привертає така їх сфера як Інтернет-банкінг, система електронних платежів, а також здійснення інших видів діяльності банками із залученням електронних інформаційних засобів. Серед найближчих до цієї сфери відноситься функція НБУ щодо визначення напрямів розвитку сучасних електронних банківських технологій, створення та забезпечення безперервного, надійного та ефективного функціонування, розвитку створених НБУ платіжних та облікових систем, контроль за створенням платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації (п. 7 ч. 1 ст. 7 Закону України «Про НБУ»).

До недавнього часу при проведенні переказу коштів фізичними особами основні пріоритети та переваги, які відмічаються в сучасній банківській діяльності, значна кількість не мали чіткої правової форми або не відповідали правовим інститутам, або приводили до порушень інтересів клієнтів банків.

Останнім часом законодавство України поступово змінюється у бік регулювання інформаційної та кібербезпеки банківської діяльності в тому числі під час здійснення розрахункових операцій.

Так, Положенням про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженим Постановою Правління Національного банку України від 26.11.2015 № 829 (далі – Положення № 829) було врегульовано підстави та порядок отримання засобів захисту інформації Національного банку, які використовуються в системі електронних платежів Національного банку та інформаційних задачах (далі – ЗЗІ). Сторонами цих правовідносин є, з одного боку, організація як банківська або інша установа, яка є безпосереднім учасником системи електронних платежів Національного банку (далі – СЕП)

та/або інформаційних задач і використовує засоби захисту інформації Національного банку, а з іншого боку – НБУ. Відповідно до п. 19 цього Положення умовами для отримання ЗЗІ є:

1) приєднання організації-замовника до Єдиного договору для отримання таких видів послуг Національного банку: розрахунково-інформаційного обслуговування в системі електронних платежів Національного банку (для учасників СЕП); системою електронної пошти Національного банку (далі – система ЕП); із надання в користування засобів захисту інформації Національного банку, крім випадків, якщо організацією-замовником є державні установи, перелічені у п. 19 цього Положення.

2) забезпечення відповідності приміщень, у яких будуть оброблятися електронні банківські документи, використовуються та зберігаються ЗЗІ, вимогам, визначеним Правилами;

3) призначення посадових осіб, відповідальних за зберігання та використання ЗЗІ;

4) наявність лист-доручення (довіреність) про отримання конкретних ЗЗІ особі, відповідальній за отримання ЗЗІ для організації.

Забезпечення інформаційної безпеки здійснюється, зокрема, за допомогою: 1) технологічних засобів контролю, вбудованих в програмно-технічні комплекси СЕП, які не можуть бути відключені. У разі виявлення нестандартної ситуації, яка може свідчити про підозру щодо несанкціонованого доступу до СЕП від імені певного учасника СЕП, автоматично припиняється приймання початкових електронних розрахункових документів та повідомлень від цього учасника; 2) застосування декількох методів шифрування інформації які, серед іншого, забезпечують сувору автентифікацію відправника та отримувача електронного банківського документа, цілісність кожного документа в результаті неможливості його підроблення або несанкціонованого модифікування в шифрованому вигляді.

Внутрішній контроль за функціонуванням такої системи безпеки розрахунків здійснюється за допомогою обов'язкового інформування організацією Департаменту безпеки НБУ про порушення, виявлені ЗЗІ та порушення діяльності власне ЗЗІ та управління ними. В цьому аспекті привертає увагу ст. 13 Закон України «Про довірчі

електронні послуги», відповідно до ч. 2 якої встановлюється максимальний ліміт на інформування контролюючих органів про порушення безпеки персональних даних клієнтів у 24 години. Також у Положенні № 829 встановлено надавання письмових або усних відомостей на вимогу Департаменту безпеки про стан ЗЗІ та їх використання, стан захисту інформації в системах, на які поширюються вимоги Національного банку щодо інформаційної безпеки, технологію оброблення електронних банківських документів в організації та систему захисту інформації під час їх оброблення.

Зовнішній контроль за функціонування ЗЗІ здійснюється за допомогою таких процедур як проведення планових та позапланових перевірок стану інформаційної безпеки в організаціях Департаментом безпеки НБУ, відповідно до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України, затвердженого ПП НБУ № 829.

Ще одним нормативно-правовим актом, що регулює безпеку розрахунків є Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене ПП НБУ від 28 вересня 2017 року № 95 (далі – Положення № 95) і введене в дію у 2018 році, в основу якого було покладено міжнародні стандарти з інформаційної безпеки такі як ISO / IEC 27001, ISO / IEC 27002 та PCI DSS [2]. Метою цього акту є забезпечення ефективного захисту від кібератак на банківські установи. Відповідно до цього Положення на банківську установу покладається обов'язок повного забезпеченні кібербезпеки, що тягне за собою широке залучення ІТ спеціалістів. Так, зокрема, кожен банк зобов'язаний утворити власну систему управління інформаційною безпекою (далі – СУІБ). Для цього формується колективний керівний орган з питань впровадження та функціонування СУІБ (далі - керівний орган СУІБ) або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити відповідне положення. До складу керівного органу СУІБ обов'язково входять голова правління банку та/або його заступника, що відповідає за інформаційну безпеку банку, керівники підрозділів банку – власники критичних бізнес-процесів

банку та керівник підрозділу банку з управління ризиками. Крім того Банк зобов'язаний створити підрозділ з інформаційної безпеки не менше як із двох працівників зі складу штатних працівників банку, а також призначити відповідальну особу за інформаційну безпеку банку (Chief information security officer, CISO), яка має повноваження, достатні для прийняття управлінських рішень (посада не нижче заступника голови правління банку), та забезпечує: 1) стратегічне керівництво з питань інформаційної безпеки банку; 2) визначення напрямів розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку банку; 3) відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів; 4) контроль за впровадженням заходів безпеки інформації в банку.

Необхідно звернути увагу, що Положення № 95 містить термін «критичні бізнес-процеси банку» як бізнес-процеси діяльності банку, визначені банком критичними щодо інформаційної безпеки за результатом їх оцінювання банком за такими критеріями: конфіденційність, цілісність, доступність. Таким чином можна зробити висновок, що фактично НБУ передає повноваження визначення з метою подальшого посиленого контролю потенційно-небезпечних процесів банків самим банкам, з урахуванням специфіки їхньої діяльності.

Положенням № 95 на банк покладаються обов'язки щодо контролю за користувачами. Так, зокрема, банк зобов'язаний запровадити такі заходи контролю доступу до інформаційних систем банку: 1) перевірку наявності у користувача дозволу керівництва та власника інформаційної системи на такий доступ; 2) заборону одноосібного ініціювання заявки, підтвердження та надання доступу; 3) перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень; 4) періодичну перевірку відповідності наданих прав доступу користувачеві тим, що діють на момент перевірки. Банк зобов'язаний використовувати механізми багатофакторної автентифікації під час надання доступу для виконання функцій адміністрування або супроводження САБ. Банк зобов'язаний забезпечити блокування облікових записів користувачів в інформаційних системах банку в таких випадках: 1) п'яти невдалих спроб автенти-

фікації поспіль (автоматичне блокування); 2) відсутності реєстрації користувача в інформаційних системах банку протягом 90 календарних днів; 3) звільнення користувача.

Також, привертають увагу норми Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України, затвердженого ПП НБУ від 4 липня 2018 року № 75 (далі – Положення № 75). Відповідно до цього Положення банк зобов'язаний визначити критичними щодо інформаційної безпеки бізнес-процеси діяльності банку, у яких здійснюються формування, оброблення, передавання та зберігання електронних банківських документів. Однією з вимог інформаційного забезпечення операційної діяльності є вимога щодо передавання електронних банківських документів, втрата або несанкціоноване ознайомлення з якими може завдати збитків банку, його структурним підрозділам або клієнту банку, відповідними каналами зв'язку електронною поштою або в режимі реального часу лише зашифрованими та з обов'язковим наданням підтвердження про їх отримання. Встановлено обов'язкову реєстрацію всіх подій доступу, усіх операцій та інших дій, їх фіксацію в автоматизованій системі в захищеному від модифікації електронному журналі із здійсненням постійного контролю за його цілісністю.

Крім того, цим актом було закріплено так зване правило «двох рук», сутністю якого є те, що операція не може бути ініційована та виконана одним користувачем системи. Виняток може бути зроблений для операцій, що здійснюються автоматично системами автоматизації банківської діяльності.

У Положенні № 75 визначено обов'язок банку надавати достатню інформаційну підтримку для прийняття користувачами правильного рішення про те, яке з джерел інформації слід уважати сумнівним, а яке – достовірним.

Привертають увагу також деякі положення Закону України «Про електронні довірчі послуги», які стосуються банківської сфери. Відповідно до ст. 9 цього Закону Національний банк України створює засвідчувальний центр для забезпечення внесення кваліфікованих надавачів електронних довірчих послуг у банківській системі Укра-

їни та кваліфікованих надавачів електронних довірчих послуг при здійсненні переказу коштів (учасників платіжних систем) до Довірчого списку відповідно до вимог цього Закону. До повноважень Національного банку України у сферах електронних довірчих послуг та електронної ідентифікації належить:

– встановлення вимог, яким повинні відповідати кваліфіковані надавачі електронних довірчих послуг, внесені до Довірчого списку за поданням засвідчувального центру, у тому числі вимог до їхніх програмно-технічних комплексів;

– встановлення порядку надання та використання електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів;

– встановлення порядку надання послуги постачання передачі сигналів точного часу засвідчувальним центром кваліфікованим надавачам електронних довірчих послуг, внесеним до Довірчого списку за поданням засвідчувального центру, та визначення джерела синхронізації часу;

– державне регулювання з питань електронної ідентифікації у банківській системі України;

– здійснення інших повноважень у сферах електронних довірчих послуг та електронної ідентифікації у банківській системі України, визначених законом.

При цьому спеціального нормативно-правового акту НБУ на виконання положень цього Закону поки прийнято не було.

Внесення в реєстр на сайті НБУ операторів послуг платіжної інфраструктури відповідає принципу внесення в реєстр усіх фінансових установ а підкреслить виконання функцій держави при реалізації грошово-кредитної політики, але таці структури не є фінансовими установами, а тільки суб'єктами інфраструктури. Також, додатково, необхідно визначитися з переліком операторів послуг платіжної інфраструктури, які повинні бути враховані в переліку суб'єктів первинного фінансового моніторингу згідно зі ст. 5 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

Необхідно звернути увагу на зміст Проекту ПП НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків» [3]. Планується поширення цього положення на платіжні організації платіжних систем та систем розрахунків, створених резидентами України; учасників-резидентів платіжних систем та систем розрахунків, створених як резидентами, так і нерезидентами України; операторів послуг платіжної інфраструктури; а також платіжні організації міжнародних платіжних систем, створених нерезидентами, у частині їх діяльності на території України.

Серед ключових положень цього акту щодо безпеки здійснення розрахункових операцій банків можливо виділити наступні:

1. Суб'єкт платіжного ринку зобов'язаний використовувати засоби захисту мережі (апаратні та/або програмні), які мають чинний на момент початку експлуатації системи захисту мережі сертифікат відповідності або позитивний експертний висновок ДССЗЗІ, у випадках їх застосування для захисту мережевого з'єднання між компонентами суб'єкта платіжного ринку або передавання між компонентами незашифрованої інформації без електронного підпису.

2. Суб'єкт платіжного ринку зобов'язаний налаштувати засоби захисту мережі таким чином, щоб критичні дані під час передавання даних були захищені від несанкціонованого перегляду та модифікації.

3. Проект передбачає визначення та перелік критичних даних, які по суті, замінять закріплений в Положенні № 95 термін «критичні бізнес-процеси банку». Так, критичні дані – це дані, несанкціоноване використання яких призводить до порушення безпеки інформації в системі або порушення прав користувачів системи. До них належать: електронні документи на переказ; незашифровані та незахищені від модифікації дані, зчитані з електронного платіжного засобу; логіни та паролі.

4. Суб'єкт платіжного ринку для виконання операцій з переказу коштів через захищене Інтернет-з'єднання, з метою підтвердження достовірності сервера повинен використовувати сертифікати відкритого ключа, видані центрами сертифікації, які забезпечують перевір-

ку достовірності домену та організації (гарантійна сума сертифіката не може бути меншою 10 000 дол. США).

Доцільно також дослідити зміст проекту Закону України «Про внесення змін до деяких законодавчих актів України щодо регулювання переказу коштів» № 7270 [4] (далі - Проект № 7270) від 09.11.2017. Зокрема, цим Проектом передбачено криміналізацію діяння за незаконні дії з підробки платіжних інструментів та інших засобів доступу до банківських рахунків, електронних грошей, і засобів доступу до них, платіжних пристроїв, засобів ідентифікації (верифікації) особи власника банківського рахунку та/або користувача електронних платіжних засобів, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених платіжних інструментів, платіжних пристроїв або їх використання чи збут, а також незаконне заволодіння платіжними інструментами або засобами ідентифікації (верифікації) особи власника банківського рахунку, користувача електронних платіжних засобів, засобами доступу до банківських рахунків, засобами доступу до електронних грошей. У примітці до редакції ст. 200 Кримінального кодексу України встановлено, що під засобами ідентифікації (верифікації) особи власника банківського рахунку, користувача електронних платіжних засобів слід розуміти електронний підпис, в тому числі електронний цифровий підпис, персональний ідентифікаційний номер та додаткові засоби ідентифікації (верифікації). Також планується введення у дію ст. 2001 «Незаконні дії з електронними грошима», диспозиція якої передбачає випуск електронних грошей без узгодження правил використання електронних грошей з Національним банком України та/або здійснення операцій з ними (розповсюдження, надання засобів поповнення, приймання електронних грошей в обмін на готівкові та/або безготівкові кошти) без узгодження правил використання електронних грошей з Національним банком України.

Крім того планується внесення дій щодо незаконних дій з використанням електронних засобів до Кодексу про адміністративні правопорушення України.

Також цим законом планується введення терміну у визначення «платіжний моніторинг» як обов'язкової діяльності постачальника

послуг з переказу щодо контролю за операціями, які здійснюються із застосуванням електронних платіжних засобів та електронних грошей з метою виявлення та запобігання помилковим та неналежним переказам. Також встановлено порядок здійснення такого моніторингу.

Важливим положенням Проекту № 7270 є регулювання відповідальності банка та клієнта при втраті електронного платіжного засобу Законом України «Про платіжну систему та переказ коштів». Так, планується введення пункту 14.16, за яким «якщо банком-емітентом, платіжною установою – емітентом було дотримано вимог цього Закону та нормативно-правових актів НБУ до належної безпеки електронних платіжних засобів та платежів із їх використанням, і користувач негайно (протягом однієї години з моменту отримання повідомлення банку, платіжної установи про здійснену операцію, відповідно до контактної інформації, наданої користувачем), повідомив банк, платіжну установу про виявлення факту втрати електронного платіжного засобу, відповідальність користувача за кожну операцію (неналежний переказ), яка відбулася до моменту повідомлення банка, платіжної установи не може перевищувати 100 неоподатковуваних мінімумів доходів громадян». Також планується закріпити обов'язок емітента електронних грошей забезпечувати їх еквівалентною готівковою сумою без права розпорядження нею.

Таким чином, можна зробити висновок, що правовим засобом вирішення вищеокреслених проблем може бути реформування національного законодавства. Так, зокрема:

– встановлення заборони на відкриття рахунків без належної ідентифікації клієнта буде правовим засобом забезпечення виникнення та реалізації сталих цивільних та господарських відносин і передумовою введення механізму захисту доступу до інформації щодо рахунку та здійснення переказу коштів.

– правова регламентація використання електронних цифрових підписів, розширить можливості суб'єктів здійснення моніторингу та нагляду (контролю) щодо ідентифікації клієнта банку та аналізу розподілу ризиків на підставі договору при реалізації певних загроз, що призвели до втрати коштів.

Крім того, вважаємо за необхідне нормативне закріплення вимог щодо введення обов'язкової сертифікації НБУ програмно-технічних засобів платіжних організацій та операторів послуг платіжної як учасників, які надають послуги, пов'язані з переказом коштів.

Література

1. Глібко С. В. Правове регулювання безпеки проведення розрахунків. *Правова інформатика,* № 2(42). Київ, 2014. С. 165.

2. Постанова НБУ № 95 Як попередити банкопад 2.0? URL: https://www.my-itspecialist.com/uk/nbu_95/.

3. Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків: Проект ПП НБУ. URL: https://bank.gov.ua/control/uk/publish/article?art_id=78326032.

4. Про внесення змін до деяких законодавчих актів України щодо регулювання переказу коштів: Проект Закону України № 7270 від 09.11.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6284.

А. І. Денисов,
к.ю.н., доцент кафедри правового забезпечення господарської діяльності факультету №6 Харківського національного університету внутрішніх справ

ПРОТИДІЯ РЕЙДЕРСТВУ: ВИКОРИСТАННЯ ІНОЗЕМНОГО ДОСВІДУ З ПРОТИДІЇ АГРЕСИВНОМУ ПОГЛИНАННЮ

У останній час в нашій державі все більш актуальною стає проблематика протидії рейдерському захопленню підприємств. У інших країнах досить ефективно себе показали окремі правові механізми протидії рейдерству, що пов'язані з державним контролем та моніторингом у сфері агресивного поглинання підприємств.

Однією з найбільш ефективних форм рейдерського захоплення є безсумнівно агресивне злиття, коли завдяки наявності підробної чи навіть справжньої печатки та введення в оману нотаріуса (а інколи –