Рекомендації Національного банку України щодо складання правил платіжної системи, платіжною організацією якої є резидент

Відповідно до статті 9 Закону України "Про платіжні системи та переказ коштів в Україні" (далі – Закон про платіжні системи) Національний банк України (далі – Національний банк) веде Реєстр платіжних систем, систем розрахунків, учасників цих систем та операторів послуг платіжної інфраструктури (далі – Реєстр). Платіжні організації платіжних систем (далі – платіжна організація) мають право здійснювати діяльність в Україні виключно після їх реєстрації шляхом унесення відомостей про них до Реєстру.

Унесення відомостей до Реєстру щодо внутрішньодержавної платіжної системи та міжнародної платіжної системи, платіжною організацією якої є резидент, здійснюється Національним банком після узгодження правил цієї платіжної системи.

Порядок узгодження Національним банком правил платіжної системи, платіжною організацією якої є резидент (далі – Правила), установлений Положенням про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затвердженим постановою Правління Національного банку України від 04 лютого 2014 року № 43 (далі – Положення № 43).

I. Рекомендації щодо оформлення та подання Правил до Національного банку

Правила мають бути викладені українською мовою, затверджені керівним органом платіжної організації, підписані керівником та прошиті. Рекомендується, щоб Правила мали наскрізну порядкову нумерацію пунктів, пронумеровані глави/розділи (за необхідності), а також сторінки.

Одночасно з документами на паперових носіях до Національного банку обов'язково подаються копії цих документів в електронному вигляді, створені у вигляді файлів, які містять відскановані з паперових носіїв зображення документів.

Сканування з паперових носіїв зображення документів здійснюється з урахуванням таких вимог:

формат готового файла – pdf;

документи, що містять більше однієї сторінки, скануються в один файл;

роздільна здатність сканування не нижче ніж 300 dpi.

Електронні копії документів подаються до Національного банку на одному або кількох компакт-дисках формату CD-R або DVD-R. Перед поданням до Національного банку компакт-диск (компакт-диски) необхідно перевірити на наявність вірусів із використанням спеціалізованого антивірусного програмного забезпечення. Під час подання електронних копій документів до Національного банку слід ураховувати, що компакт-диск

(компакт-диски), який(і) містить(ять) віруси, не можуть бути прийняті Національним банком.

ІІ. Загальні рекомендації до Правил

У Правилах має бути зазначено найменування платіжної системи, вид платіжної системи (система переказу коштів, карткова платіжна система, система розрахунків за валютні цінності та фінансові інструменти) із зазначенням її ознаки (внутрішньодержавна/міжнародна).

Правила не повинні містити положень, які протирічать законодавству України, зокрема Закону про платіжні системи, нормативно-правовим актам Національного банку, прийнятим на виконання цього Закону.

Правила повинні у повній мірі розкрити всі положення, передбачені пунктом 4 розділу ІІ Положення № 43. Якщо в Правилах є посилання на інші внутрішні документи, то ці документи необхідно подати до Національного банку разом із Правилами.

У Правилах необхідно використовувати терміни та визначення відповідно до термінів і визначень, наведених у законодавстві України, зокрема Законі про платіжні системи та нормативно-правових актах Національного банку.

Правила повинні містити актуальну інформацію щодо функціонування платіжної системи. Не рекомендується надавати в Правилах опис послуг, які в платіжній системі не надаватимуться.

ІІІ. Рекомендації до положень, які повинні містити Правила (пункт 4 розділу ІІ Положення № 43)

1. Організаційна структура платіжної системи.

Рекомендується визначити права, обов’язки та відповідальність кожного зі структурних елементів платіжної системи.

Структурними елементами платіжної системи є:

1) платіжна організація[1]. Необхідно навести інформацію про юридичну особу, яка виконує функції платіжної організації, її найменування, код за ЄДРПОУ, організаційно-правову форму, керівні органи платіжної організації, їх повноваження.

Якщо платіжна організація виконуватиме функції учасника платіжної системи, то в Правилах має бути зазначено, що на неї поширюватимуться положення Правил, які стосуються діяльності учасника платіжної системи. Також необхідно врахувати, що платіжна організація може здійснювати переказ коштів у платіжній системі в разі наявності:

[1] Платіжна організація – це юридична особа, що визначає правила роботи платіжної системи, а також виконує інші функції щодо забезпечення діяльності платіжної системи та несе відповідальність згідно із Законом про платіжні системи та договором (п.1.28 статті 1 Закону про платіжні системи).

для платіжної організації-банку – банківської ліцензії;

для платіжної організації – небанківської установи – статусу небанківської фінансової установи та ліцензії Національного банку на переказ коштів у національній валюті без відкриття рахунків;

2) розрахунковий банк[2]. Необхідно визначити вимоги платіжної організації платіжної системи до розрахункового банку та, якщо функції розрахункового банку виконуватиме платіжна організація-банк, то зазначити це в Правилах;

3) оператор послуг платіжної інфраструктури[3]. Необхідно чітко зазначити власні та/або сторонні процесингові, клірингові центри тощо використовуватимуться в платіжній системі.

Якщо в платіжній системі планується користуватися послугами стороннього оператора послуг платіжної інфраструктури, і цей оператор уже визначений, то пропонуємо зазначити його повне найменування, торговельну марку (у разі наявності). Необхідно врахувати, що відповідно до статті 9 Закону про платіжні системи оператори послуг платіжної інфраструктури мають право здійснювати діяльність в Україні виключно після їх реєстрації шляхом унесення відомостей про них до Реєстру;

4) учасники платіжної системи. Потрібно зазначити, хто може бути учасником платіжної системи. Необхідно врахувати вимоги статті 10 Закону про платіжні системи, відповідно до якої учасниками платіжної системи мають право бути банк, що має банківську ліцензію Національного банку, а також небанківська фінансова установа, яка має ліцензію Національного банку на переказ коштів у національній валюті без відкриття рахунків.

У разі здійснення переказу коштів в іноземній валюті в Правилах необхідно передбачити наявність в учасника міжнародної платіжної системи генеральної ліцензії Національного банку на здійснення валютних операцій.

Під час складання Правил необхідно врахувати, що законодавством України в частині приймання готівки для подальшого її переказу право залучати комерційних агентів надано виключно банкам (стаття 47 Закону України “Про банки і банківську діяльність”, постанова Правління Національного банку України від 12 лютого 2013 року № 42 “Про врегулювання питань щодо приймання готівки для подальшого її переказу”).

---

[2] Розрахунковий банк – уповноважений платіжною організацією відповідної платіжної системи банк, що відкриває рахунки учасникам платіжної системи та бере участь у проведенні взаєморозрахунків між ними (п.1.34 статті 1 Закону про платіжні системи).

[3] Оператор послуг платіжної інфраструктури – клірингова установа, процесингова установа та інші особи, уповноважені надавати окремі види послуг в платіжній системі або здійснювати операційні, інформаційні та інші технологічні функції щодо переказу коштів (п.1.20[1] статті 1 Закону про платіжні системи).

Також необхідно врахувати вимоги статті 295 Господарського кодексу України та статей 24, 32 Закону про платіжні системи.

2. Умови участі в платіжній системі, а також порядок вступу та виходу із цієї системи.

У Правилах має бути описаний порядок вступу/виходу до/з платіжної системи та загальні критерії, яким має відповідати учасник. Критеріями участі у платіжній системі можуть бути передбачені вимоги до учасників платіжної системи в частині їх фінансового стану, технологічних можливостей та інші вимоги, що можуть впливати на безперервне функціонування платіжної системи.

Необхідно врахувати, що нерезиденти для участі в міжнародній платіжній системі, платіжною організацією якої є резидент, повинні мати документ (ліцензію, дозвіл тощо), виданий відповідно до законодавства країни, у якій зареєстрований учасник, на підставі якого учасник має право здійснювати діяльність у сфері міжнародних переказів коштів.

Порядок вступу/виходу до/з платіжної системи, зокрема може включати:

порядок дій, які необхідно здійснити для вступу/виходу до/з платіжної системи;

перелік документів, які необхідно подати платіжній організації платіжної системи для вступу/виходу до/з платіжної системи.

Порядок виходу із платіжної системи має включати:

опис порядку виходу учасника із платіжної системи за власною ініціативою, а також за ініціативою платіжної організації через порушення учасником правил платіжної системи або якщо учасник більше не відповідає встановленим критеріям участі з наведенням виключного переліку підстав для прийняття такого рішення;

порядок завершення операцій та здійснення заключних взаєморозрахунків у разі неможливості виконання учасником своїх функцій у платіжній системі (зокрема для небанківських фінансових установ – зупинення/скасування ліцензії Національного банку на переказ коштів у національній валюті без відкриття рахунку).

Також рекомендуємо передбачити в Правилах положення про відповідальність учасників, користувачів платіжної системи, що беруть участь у проведенні операцій з переказу коштів з урахуванням вимог, установлених розділом VII Закону про платіжні системи.

У випадку залучення учасником платіжної системи комерційних агентів для здійснення переказу коштів у Правилах необхідно:

врахувати, що здійснювати валютні операції можуть комерційні агенти, які мають на це право відповідно до валютного законодавства України;

передбачити відповідальність учасника платіжної системи, що залучає комерційного агента, за операції, які здійснюються цим комерційним агентом.

3. Система управління в платіжній системі ризиками ліквідності, кредитним, правовим, операційним, системним і порядок урегулювання неплатоспроможності й інших випадків нездатності виконання учасниками платіжної системи своїх зобов'язань, у тому числі порядок створення та використання страхового фонду (за його наявності).

Під системою управління ризиками в платіжній системі необхідно розуміти комплекс заходів, направлений на забезпечення безперервної діяльності платіжної системи. Рекомендується визначити перелік ризиків, притаманних платіжній системі, та систему управління ними за кожним ризиком окремо.

Рекомендуємо в Правилах в описі порядку створення/використання страхового фонду зазначити інформацію щодо установи, у якій зберігаються кошти страхового фонду (розрахунковий банк або інша установа).

4. Види послуг з переказу коштів, які надаватимуться в платіжній системі, із зазначенням ініціаторів та отримувачів переказу коштів (юридичні та/або фізичні особи), видів валют переказу тощо.

Необхідно визначити фактичний перелік послуг, які надаватимуться в платіжній системі із зазначенням ініціаторів та отримувачів переказу коштів, видів валют переказу коштів, форми ініціювання переказу за кожним видом послуг.

Для правил міжнародних платіжних систем рекомендується зазначити, що транскордонний переказ коштів здійснюється за неторговельними поточними операціями та непов'язаний з підприємницькою та інвестиційною діяльністю.

У разі здійснення переказу коштів з/на поточні рахунки, відкриті у банках України, Правила мають містити норму щодо дотримання банками – учасниками системи режимів використання рахунків клієнтів, визначених нормативно-правовими актами Національного банку.

5. Порядок ініціювання та здійснення переказу і взаєморозрахунків за цим переказом у платіжній системі, уключаючи:

1) опис платіжних інструментів, за допомогою яких здійснюються ініціювання та виплата суми переказу коштів у платіжній системі [для систем переказу коштів – з наведенням зразків документів на переказ та видачу готівки (за наявності)].

Потрібно навести опис платіжних інструментів, які використовуються для ініціювання переказу коштів. Відповідно до статті 1 Закону про платіжні системи до платіжних інструментів належать:

документ на переказ – "електронний або паперовий документ, що використовується суб'єктами переказу, їх клієнтами, кліринговими, еквайринговими установами або іншими установами – учасниками платіжної системи для передавання доручень на переказ коштів. До документів на переказ

належать розрахункові документи, документи на переказ готівки, міжбанківські розрахункові документи, клірингові вимоги";

електронний платіжний засіб – платіжний інструмент, який надає його держателю можливість за допомогою платіжного пристрою отримати інформацію про належні держателю кошти та ініціювати їх переказ. Різновидами електронних платіжних засобів є платіжна картка та мобільний платіжний інструмент.

У Правилах необхідно чітко зазначити, який документ видається клієнту на підтвердження операцій ініціювання та виплати суми переказу.

У разі здійснення в платіжній системі операцій з ініціювання та виплати готівкою у Правилах необхідно:

навести зразки документів на переказ і видачу готівки. У цьому разі необхідно врахувати вимоги розділу IV Інструкції про ведення касових операцій банками в Україні, затвердженої постановою Правління Національного банку України від 01 червня 2011 року № 174 (далі – Інструкція № 174), щодо оформлення операцій з приймання та видачі готівки та додатка 5 Положення про форму та зміст розрахункових документів, затвердженого наказом Міністерства фінансів України від 21 січня 2016 року № 13, у частині застосування фіскального касового чека за приймання та переказ готівкових коштів через програмно-технічні комплекси самообслуговування;

відобразити обов'язки учасників платіжної системи, банків та їх комерційних агентів, визначені в пунктах 24.4, 24.5, 24.7 статті 24 Закону про платіжні системи.

У разі здійснення в платіжній системі операцій переказу коштів з використанням електронних платіжних засобів у Правилах необхідно:

навести зразок квитанції, що підтверджує виконання операцій із використанням електронних платіжних засобів. Необхідно врахувати вимоги розділу IV Інструкції № 174 та Положення про порядок емісії електронних платіжних засобів і здійснення операцій з їх використанням, затвердженого постановою Правління Національного банку України від 05 листопада 2014 року № 705, щодо оформлення відповідної квитанції;

передбачити порядок повернення коштів ініціатору переказу, у тому числі альтернативний спосіб їх повернення, у разі неможливості повернути кошти в той спосіб, у який було здійснено переказ.

У разі здійснення в платіжній системі операцій переказу коштів з використанням розрахункових документів у Правилах необхідно:

урахувати, що розрахунковий документ на переказ коштів має містити обов'язкові реквізити, які визначені Інструкцією про безготівкові розрахунки в Україні в національній валюті, затвердженою постановою Правління Національного банку України від 21 січня 2004 року № 22;

передбачити порядок відкликання розрахункових документів з урахуванням вимог, установлених статтею 23 Закону про платіжні системи;

2) опис руху інформаційних повідомлень і руху коштів із часу ініціювання переказу до завершення взаєморозрахунків за цим переказом у платіжній системі (уключаючи схематичне зображення).

Необхідно навести зображення схеми руху інформаційних повідомлень та руху коштів із часу ініціювання переказу до його завершення в платіжній системі, а також навести опис кожної ланки цієї схеми. Рекомендується рух коштів та інформаційних повідомлень відображати різними позначками. Кожне умовне позначення руху коштів/інформаційних потоків на схемі пронумерувати. В описі до схеми навести посилання на номери потоків;

3) перелік реквізитів документів на переказ, що дають змогу однозначно ідентифікувати платіжну систему, ініціатора переказу коштів та його отримувача.

Реквізити документів на переказ, за допомогою яких здійснюється ініціювання та виплата переказу повинні чітко ідентифікувати платіжну систему, ініціатора переказу та його отримувача;

4) опис регламенту проведення взаєморозрахунків.

У Правилах рекомендується описати порядок відкриття рахунків у розрахунковому банку учасникам платіжної системи та проведення взаєморозрахунків між ними, а також часові періоди, протягом яких проводяться взаєморозрахунки в платіжній системі.

Порядок ініціювання та здійснення переказу і взаєморозрахунків за цим переказом у міжнародній платіжній системі додатково має містити опис механізму забезпечення виконання вимог валютного законодавства України, зокрема в частині:

здійснення переказів та порядку їх виплати, уключаючи інформацію щодо порядку встановлення курсу валют під час виплат переказів;

розрахунків (клірингу) з учасниками платіжної системи-нерезидентами, які здійснюватимуться в іноземній валюті;

сплати комісійної винагороди як користувачами, так й учасниками платіжних систем. Необхідно врахувати, що на території України комісійна винагорода сплачується виключно в гривнях.

У правилах міжнародних платіжних систем під час опису видів послуг з переказу коштів, порядок ініціювання та здійснення переказу рекомендується розмежовувати на транскордонні та внутрішньодержавні перекази.

6. Порядок застосування дати валютування (у разі її використання).

Датою валютування є зазначена платником у розрахунковому документі або в документі на переказ готівки дата, починаючи з якої кошти, переказані платником отримувачу, переходять у власність отримувача. До настання дати валютування сума переказу обліковується в обслуговуючому(ій) отримувача банку або в установі – учасниці платіжної системи. У разі використання в

платіжній системі дати валютування Правила необхідно доповнити порядком її застосування.

Якщо дата валютування в платіжній системі не використовуватиметься, то про це має бути зазначено у Правилах.

7. Строки проведення переказу коштів.

Строки проведення переказу визначені статтею 8 Закону про платіжні системи. Строки проведення переказу за допомогою платіжних інструментів, крім установлених пунктами 8.1 – 8.4 цієї статті Закону, визначаються правилами платіжної системи та договорами, що укладаються між учасниками та користувачами платіжної системи. Строк виконання міжбанківського переказу, що здійснюється на підставі клірингових вимог, не може перевищувати строк, установлений пунктом 8.4 цієї статті.

Учасники платіжної системи мають забезпечити пересилання паперових документів на переказ у межах України в строк до семи робочих днів, а в межах однієї області – до трьох робочих днів.

Правила повинні містити чіткі строки проведення переказу коштів у платіжній системі.

8. Порядок проведення моніторингу з метою ідентифікації помилкових/неналежних переказів, суб'єктів цих переказів (у разі надання послуг із застосуванням електронних платіжних засобів).

Відповідно до статті 40^1 Закону про платіжні системи вимога щодо здійснення моніторингу з метою ідентифікації помилкових та неналежних переказів, суб'єктів помилкових та неналежних переказів та вжиття заходів із запобігання або припинення зазначених переказів установлена для карткових платіжних систем, у яких послуги надаються з використанням електронних платіжних засобів. У цьому разі Правила повинні містити порядок здійснення та параметри такого моніторингу.

9. Вимога до учасників платіжної системи повідомляти один одного про помилкові/неналежні перекази, суб'єктів цих переказів

Правилами повинна бути передбачена вимога до учасників платіжної системи з метою належної ідентифікації суб'єктів помилкових та неналежних переказів та вжиття заходів щодо запобігання або припинення зазначених переказів повідомляти один одного про таких суб'єктів та перекази.

10. Порядок виконання вимог законодавства України у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, які поширюватимуться на учасника платіжної системи.

Правила мають містити положення про порядок виконання учасниками платіжної системи вимог законодавства України у сфері запобігання та протидії

легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

11. Система захисту інформації, що висвітлює:

схему обміну інформацією, яка використовується в платіжній системі;

технологію обміну інформацією в платіжній системі, уключаючи порядок обміну інформацією з віддаленими робочими місцями приймання/виплати переказів (уключаючи порядок доступу, формування/перевірки електронних підписів, шифрування тощо);

технологію обміну інформацією між платіжною системою і системою автоматизації банку для обліку переказів коштів (уключаючи порядок доступу, формування/перевірки електронних підписів, шифрування тощо);

систему захисту інформації на всіх етапах функціонування платіжної системи, уключаючи найменування алгоритмів і довжину ключів, паролів, технологію використання засобів захисту інформації, інформацію про розробника цих засобів, систему керування ключами;

1) рекомендації до схеми та опису руху інформаційних повідомлень.

Правила повинні включати схему руху інформаційних повідомлень, яка може бути суміщена з іншими схемами, наприклад, схемою руху коштів. Оскільки не всі інформаційні повідомлення містять інформацію про платежі, у розділі, що описує систему захисту платіжної системи, за потреби може бути надана спеціалізована схема (схеми) руху інформаційних повідомлень, що включає тільки ті компоненти системи, які беруть участь в обміні та обробленні такої інформації. Проте ця рекомендація не є обов’язковою і під час опису системи захисту може здійснюватися посилання на загальну схему.

Схема обміну інформацією повинна містити всі компоненти платіжної системи, які функціонують у системі. Такими компонентами можуть бути платники та одержувачі коштів, надавачі послуг, що працюють із клієнтами, процесинговий центр, розрахунковий банк, центр сертифікації ключів, інші учасники та компоненти. Якщо певний учасник має кілька компонентів системи (наприклад, робоче місце касира та віддалений сервер, з яким він зв’язується по мережі), то вони повинні бути відображені на схемі окремо.

Якщо клієнти можуть взаємодіяти з учасниками або компонентами платіжної системи кількома принципово різними способами (наприклад, через інтернет-сайт та за допомогою програмно-технічних комплексів самообслуговування), то це також повинно бути відображено на схемі.

Якщо учасник платіжної системи має певну внутрішню структуру (сервери різного призначення, сховище архівів тощо), особливо коли вони розташовані в різних приміщеннях, необ’єднаних одним контуром захисту, то вони також повинні бути відображені на загальній схемі або на окремій деталізованій схемі учасника системи.

Усі компоненти на схемі обміну інформаційними повідомленнями, між якими передаються інформація про платіж, дані платників та одержувачів, а також ключі, повинні бути поєднані за допомогою пронумерованих стрілок.

Якщо платіжна система обмінюється платіжною чи ключовою інформацією з іншими платіжними системами, то ці платіжні системи також повинні бути відображені на схемі разом із ланками обміну інформацією;

2) рекомендації до опису криптографічного захисту інформації на кожній ланці.

У Правилах повинно бути надано опис технічного та криптографічного захисту для кожної ланки з посиланням на номер ланки схеми руху інформаційних потоків;

3) рекомендації щодо надання копій дозвільних документів на використання засобів захисту.

На всі засоби технічного та криптографічного захисту інформації, які використовуються в платіжній системі під час виконання переказу, надаються копії чинних експертних висновків уповноваженого органу (наприклад, Державної служби спеціального зв'язку та захисту інформації України).

Зазначені експертні висновки мають бути чинними на момент подання Правил, для засобів технічного захисту допускається чинність на момент придбання засобу. В останньому випадку необхідно надати копії документів, що підтверджують дату придбання.

Якщо експертний висновок містить додаткові вимоги до експлуатації сертифікованого засобу, то копія сторінок експертного висновку, у якому ці вимоги зазначені, також має бути надана. В описі відповідної ланки має бути зазначено, що ці вимоги до експлуатації мають виконуватися.

Якщо платіжна система використовує дані держателів платіжних карток, то слід зазначити у вимогах про відповідність міжнародному стандарту безпеки даних індустрії платіжних карток PCI DSS та надати копії підтвердних документів (сертифіката та "Attestation of Compliance");

4) рекомендації до опису засобів для захисту мережі.

Як технічний захист мережі можуть бути використані різні міжмережеві екрани та файєрволи. Для них повинні бути зазначені зразки засобів захисту мережі та надано копії експертних висновків.

Також необхідно зазначити, яким чином для таких засобів забезпечується виконання вимог до умов експлуатації, наведених у відповідному розділі експертного висновку. У разі наявності особливих вимог, що не збігаються з вимогами до експлуатації, потрібно додати їх опис.

Якщо на деякій ланці з боку будь-якої компоненти здійснюється фільтрація за IP-адресами чи портами, то це повинно бути зазначено. Якщо захищене з'єднання може бути забезпечене шляхом створення VPN-каналу або HTTPS-з'єднання, то це також має бути зазначено. Для VPN-каналу необхідно зазначити технологію його створення (наприклад, IPSec), протокол (наприклад,

ESP), алгоритми шифрування, механізм автентифікації та його алгоритм. У разі HTTPS-з'єднання має бути також зазначено параметри шифрування (наприклад, алгоритм хешування SHA1, ключ шифрування RSA з довжиною 2048 біт, видавець сертифіката компанія N).

Якщо платіжна система передбачає доступ до мережевого обладнання за допомогою мережевого з'єднання, то необхідно це зазначити та подати опис захисту цієї мережі;

5) рекомендації до опису криптографічних алгоритмів, протоколів, довжин паролів та ключів.

Під час опису механізму шифрування інформації під час обміну між компонентами платіжної системи має бути зазначено алгоритм шифрування та довжину ключа. Якщо дані, що передаються, підписані за допомогою електронного підпису (MAC, електронний цифровий підпис тощо), це також повинно бути зазначено.

Закриті ключі, паролі та інша подібна інформація повинна передаватися в захищеному від перегляду та модифікації вигляді, що унеможливить її несанкціоноване використання;

6) рекомендації до опису процедури автентифікації.

Оскільки будь-який обмін інформацією під час використання відкритих мереж повинен розпочинатися із взаємної автентифікації (у випадках, коли тільки одна сторона одержує інформацію, автентифікація може бути односторонньою), має бути описано цей процес. Якщо для цього використовуються криптографічні методи, то має бути зазначено, за допомогою яких криптографічних засобів це здійснюється, за допомогою яких алгоритмів та з якою довжиною ключів. Якщо використовується автентифікація за допомогою логіна та пароля, то необхідно зазначити, яким чином захищається передавання пароля до даного логіна. Якщо замість пароля передається його хеш-функція, то необхідно зазначити алгоритм хешування та його довжину. Якщо пароль до логіна є динамічним (наприклад, під час використання двофакторної автентифікації), то необхідно це зазначити;

7) рекомендації в частині використання електронного підпису.

Відповідно до Закону про платіжні системи документ на переказ повинен мати електронний підпис. У зв'язку з цим у Правилах необхідно чітко зазначити, на якому етапі, яким способом та за допомогою яких засобів він накладається, де здійснюється перевірка цього підпису, яким чином відбувається перевірка цілісності, достовірності та авторства електронного документа на переказ. Також зазначити, які криптографічні алгоритми та з якою довжиною ключів використовуватимуться.

Також необхідно зазначити, яким чином буде здійснюватися ідентифікація отримувача документа на переказ;

8) рекомендації до опису системи управління ключовою інформацією.

Слід звернути увагу на опис процесу життєвого циклу криптографічних ключів, що використовуватимуться учасниками платіжної системи. Оскільки ключі під час свого життєвого циклу генеруються, вводяться в експлуатацію, пересилаються, зберігаються, архівуються, відновлюються та знищуються, для оцінки безпеки інформації необхідно описати кожен цей крок.

Так для опису процедури генерації ключів має бути зазначено, де саме він генерується та за допомогою яких засобів, надати експертні висновки на ці засоби (у яких має бути зазначено про перевірку генератора випадкових чисел). Оскільки ключі можуть пересилатися на токені, іншому захищеному засобі, зашифровані певним чином, опис повинен містити інформацію про спосіб пересилки ключів від місця генерації до користувачів ключа та метод захисту такої пересилки. У разі пересилання відкритого ключа на сертифікацію потрібно зазначати механізм, за допомогою якого центр сертифікації зможе пересвідчитися в авторстві власника ключа. Під час використання сертифікації відкритих ключів необхідно зазначити, за допомогою якого центру буде виконуватися така сертифікація, якщо центр сертифікації зареєстрований/акредитований, то надати відповідне свідоцтво про його реєстрацію/акредитацію.

Ураховуючи, що кожен ключ має певний термін життя, необхідно зазначити періодичність його заміни та надати інформацію про процес цієї заміни. Також потрібно зазначити, як зберігається та обліковується цей ключ під час строку свого використання;

9) рекомендації до опису вимог до приміщень обмеженого доступу.

Під час опису компонентів платіжної системи, необхідно описати загальні вимоги до приміщень (уключаючи вимоги щодо доступу, протоколювання цього доступу, наявність відеоспостереження тощо), у яких вони розміщуються, та/або надати посилання на стандарти, правила та інші документи, що містять такі вимоги, наприклад, Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04 липня 2007 року № 243.

Окрім фізичного доступу в Правилах необхідно описати вимоги щодо віддаленого доступу до серверів. Якщо сервери працюють (можуть працювати) у віртуальному середовищі, то слід зазначити про це, описавши вимоги до такої конфігурації;

10) рекомендації до опису вимог щодо розподілу прав доступу персоналу.

У Правилах необхідно окремо описати вимоги з розподілу обов’язків персоналу, який займається розробленням, тестуванням, налаштуванням та експлуатацією програмно-апаратних комплексів та програмного забезпечення. Також слід зазначити вимоги щодо доступу (локального та віддаленого) до баз даних, автоматизованого аудиту, протоколювання.

Якщо частина інформації не може бути за тих чи інших причин уключена до Правил, то її необхідно включити в додатково надану інформаційну довідку;

11) взаємодія з іншими платіжними системами.

Якщо платіжна система передбачає певний обмін з іншими платіжними системами, платіжною та ключовою системою, однак ще не працює з ними, то Правилами може бути передбачене формулювання загальних вимог до такої взаємодії, тобто повинні бути описані зовнішні інтерфейси. Допускається надавати в описі загальні вимоги, наприклад, для генерації та зберігання ключа має використовуватися технічний пристрій, що має чинний експертний висновок ДССЗЗІ;

12) якщо Правила містять відомості, що належать до інформації з обмеженим доступом, то такі відомості мають бути викладені в окремому документі з відповідним грифом обмеження доступу.

12. Порядок проведення реконсиляції.

У Правилах рекомендовано визначити порядок проведення реконсиляції, що є процедурою контролю, яка полягає в ідентифікації та перевірці виконання кожного переказу за допомогою щонайменше трьох показників.

13. Порядок здійснення платіжною організацією контролю за дотриманням учасниками платіжної системи вимог правил платіжної системи.

У Правилах необхідно визначити, яким чином платіжна організація здійснюватиме контроль за дотриманням учасниками платіжної системи вимог Правил. Рекомендується визначити періодичність та види контролю з боку платіжної організації, а також відповідальність учасників за недотримання Правил.

14. Порядок вирішення спорів учасників між собою і між учасниками та користувачами, пов’язаних із функціонуванням платіжної системи.

Правила повинні містити порядок вирішення спорів між користувачами та учасниками платіжної системи, учасниками між собою, між платіжною організацією та учасниками платіжної системи.

15. Порядок і строки зберігання паперових та електронних документів на переказ коштів, а також порядок створення архівів електронних документів відповідно до законодавства України, у тому числі нормативно-правових актів Національного банку.

Під час визначення у Правилах порядку і строків зберігання паперових та електронних документів на переказ коштів, а також порядку створення архівів електронних документів необхідно врахувати вимоги:

статті 19 Закону про платіжні системи;

статей 12 і 13 Закону України “Про електронні документи та електронний документообіг”;

пункту 15 частини другої статті 6 Закону України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення”;

постанови Правління Національного банку України від 08 грудня 2004 року № 601, якою затверджено Перелік документів, що утворюються в діяльності Національного банку України та банків України, із зазначенням строків зберігання.

Необхідно розкрити, яким чином здійснюється перевірка цілісності, достовірності та авторства даних під час створення, копіювання та зберігання електронних архівів, а також зазначити технологію, найменування криптографічних засобів, алгоритмів та довжину ключів, які для цього використовуються.

16. Перелік законодавчих актів України, які необхідно використовувати під час розроблення правил платіжної системи, платіжною організацією якої є резидент, наведено в додатку до цих рекомендацій.

Додаток
до Рекомендацій Національного банку України щодо складання правил платіжної системи, платіжною організацією якої є резидент
(пункт 16 розділу III)

Перелік законодавчих актів України,
які необхідно використовувати під час розроблення правил платіжної системи, платіжною організацією якої є резидент

I. Законодавчі акти України:

Закон України "Про платіжні системи та переказ коштів в Україні";

Закон України "Про банки і банківську діяльність";

Закон України "Про інформацію";

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах";

Закон України "Про електронні документи та електронний документообіг";

Закон України "Про електронний цифровий підпис";

Закон України "Про захист персональних даних";

Закон України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення";

Закон України "Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг";

Декрет Кабінету Міністрів України від 19 лютого 1993 року № 15-93 "Про систему валютного регулювання і валютного контролю".

II. Нормативно-правові акти:

Інструкція про порядок відкриття, використання і закриття рахунків у національній та іноземних валютах, затверджена постановою Правління Національного банку України від 12 листопада 2003 року № 492;

Інструкція про безготівкові розрахунки в Україні в національній валюті, затверджена постановою Правління Національного банку України від 21 січня 2004 року № 22;

Інструкція про ведення касових операцій банками в Україні, затверджена постановою Правління Національного банку України від 01 червня 2011 року № 174;

Положення про порядок надання небанківським фінансовим установам, національному оператору поштового зв'язку генеральних ліцензій на здійснення валютних операцій, затверджене постановою Правління Національного банку України від 09 серпня 2002 року № 297;

Положення про організацію операційної діяльності в банках України, затверджене постановою Правління Національного банку України від 18 червня 2003 року № 254;

Перелік документів, що утворюються в діяльності Національного банку України та банків України, із зазначенням строків зберігання, затверджений постановою Правління Національного банку України від 08 грудня 2004 року № 601;

Положення про ведення касових операцій у національній валюті в Україні, затверджене постановою Правління Національного банку України від 15 грудня 2004 року № 637;

Положення про порядок формування, зберігання та знищення електронних архівів у Національному банку України і банках України, затверджене постановою Правління Національного банку України від 12 вересня 2006 року № 357;

Правила технічного захисту приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04 липня 2007 року № 243;

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141;

Правила здійснення за межі України та в Україні переказів фізичних осіб за поточними валютними неторговельними операціями та їх виплати в Україні, затверджені постановою Правління Національного банку України від 29 грудня 2007 року № 496;

Постанова Правління Національного банку України від 12 лютого 2013 року № 42 "Про врегулювання питань щодо приймання готівки для подальшого її переказу";

Положення про порядок видачі небанківським фінансовим установам ліцензії на переказ коштів у національній валюті без відкриття рахунків, затверджене постановою Правління Національного банку України від 26 лютого 2013 року № 57;

Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затверджене постановою Правління Національного банку України від 04 лютого 2014 року № 43;

Положення про порядок емісії електронних платіжних засобів і здійснення операцій з їх використанням, затверджене постановою Правління Національного банку України від 05 листопада 2014 року № 705;

Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні, затверджене постановою Правління Національного банку України від 28 листопада 2014 року № 755;

Положення про здійснення банками фінансового моніторингу, затверджене постановою Правління Національного банку України від 26 червня 2015 року № 417;

Положення про здійснення небанківськими фінансовими установами фінансового моніторингу в частині надання ними фінансової послуги щодо переказу коштів, затверджене постановою Правління Національного банку України від 15 вересня 2016 року № 388;

Положення про форму та зміст розрахункових документів, затверджене наказом Міністерства фінансів України від 21 січня 2016 року № 13.