Типові зауваження до документів міжнародної платіжної системи, платіжною організацією якої є нерезидент, в частині захисту інформації

Зауваження 1: Відповідно до підпункту 3 пункту 1 розділу IV Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затвердженого постановою Правління Національного банку України від 04.02.2014 № 43, платіжна організація міжнародної платіжної системи – нерезидента в пакеті документів повинна надати копії документів, що визначають технологію здійснення переказу коштів учасниками платіжної системи, уключаючи технологію обміну інформацією у міжнародній платіжній системі та опис системи захисту, яка використовуватиметься міжнародною платіжною системою на території України. Проте в наданому пакеті документів копії таких документів відсутні.

Коментар: Типовою ситуацією під час розгляду пакетів документів міжнародної платіжної системи, платіжною організацією якої є нерезидент, є подання лише загальних правил платіжної системи без належного опису системи захисту. В таких випадках платіжній організації необхідно подати додатково Інформаційну довідку щодо захисту інформації учасниками-резидентами цієї платіжної системи та слід врахувати, що учасники-резиденти мають виконувати вимоги українського законодавства щодо захисту інформації.

Відповідно до пункту 9.2.1 статті 9 Закону України «Про платіжні системи та переказ коштів в Україні» правила платіжної системи мають установлювати систему захисту інформації. Тому платіжній організації міжнародної платіжної системи необхідно надати повний опис системи захисту інформації, а саме: опис для кожної ланки схеми інформаційних потоків та для всіх видів послуг з переказу коштів, які платіжна система планує надавати в Україні, зазначивши криптографічні алгоритми захисту, довжину ключів, програмні та апаратні засоби криптографічного захисту, технологію їх використання, систему керування ключами, вказати розробників засобів.

Порядок захисту та використання засобів захисту інформації учасниками міжнародних платіжних систем визначається правилами цих систем, а за відсутності в правилах відповідних положень – законами України та нормативно-правовими актами Національного банку України (відповідно до пункту 38.3 статті 38 Закону України «Про платіжні системи та переказ коштів в Україні»). Отже, за відсутності в правилах вищезазначених положень, відповідно до вимог розділу IV Наказу № 141 (Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141) платіжній організації необхідно надати копії чинних дозвільних документів на криптографічні засоби захисту інформації (копії експертних висновків та/або сертифікатів відповідності уповноваженого органу), що використовуються учасниками платіжної системи на території України.

Зауваження 2: Відповідно до статті 18 Закону України "Про платіжні системи та переказ коштів в Україні" електронний підпис є обов'язковим реквізитом електронного документа на переказ. Тому потрібно зазначити, на яких ланках і за допомогою яких механізмів, криптографічних засобів та алгоритмів створюється/перевіряється електронний підпис учасниками платіжної системи.

Коментар: Оскільки учасники-резиденти міжнародної платіжної системи – нерезидента знаходяться в українській юрисдикції, вони мають виконувати норми українського законодавства. Однією з таких норм є вимога, що електронний підпис є обов'язковим реквізитом електронного документа на переказ, а учасник-резидент платіжної системи має передбачити під час приймання електронних документів на переказ процедуру перевірки

електронного підпису та процедуру перевірки цілісності, достовірності та авторства електронного документа на переказ. У випадках, коли створення електронного підпису не передбачено правилами платіжної системи, платіжна організація повинна вказати яким чином учасники платіжної системи виконуватимуть цю норму. Виконання цієї норми можливо шляхом створення електронного підпису відповідальною особою учасника-резидента для електронних документів під час їх отримання від платіжної системи.

Зауваження 3: Згідно з вимогами Закону України "Про електронні довірчі послуги" необхідно вказати, на якій підставі визнаються чинними в Україні сертифікати ключів, що використовуються для захисту обміну інформацією між учасниками міжнародної платіжної системи та процесинговим центром платіжної системи.
Коментар: Відповідно до вимог розділу VI Закону України "Про електронні довірчі послуги" електронні довірчі послуги, що надаються відповідно до вимог нормативно-правових актів, що регулюють правові відносини у сфері електронних довірчих послуг в іноземних державах, визнаються в Україні електронними довірчими послугами того самого виду в разі відповідності хоча б одній з таких умов:

– центральний засвідчувальний орган чи засвідчувальний центр в Україні підтверджують відповідність кваліфікованого надавача електронних довірчих послуг іноземної держави вимогам українського законодавства;

– кваліфікований надавач електронних довірчих послуг внесений до Довірчого списку держави, з якою Україна уклала відповідний двосторонній або багатосторонній міжнародний договір.

Також іноземні сертифікати відкритих ключів можуть бути визнані шляхом укладанням договору між сторонами про взаємне визнання цих сертифікатів.

Зауваження 4: Необхідно визначити порядок зберігання та захисту архівів електронних документів, що застосовуються при проведенні переказу на території України, відповідно до вимог статті 19 Закону України «Про платіжні системи та переказ коштів в Україні» та статей 12 і 13 Закону України «Про електронні документи та електронний документообіг».
Коментар: Учасники-резиденти повинні виконувати норми українського законодавства щодо збереження та захисту архівів електронних документів.

Пункт 19.2 статті 19 Закону України «Про платіжні системи та переказ коштів в Україні» визначає, що електронні документи повинні зберігатися на носіях інформації у формі, що дозволяє перевірити цілісність, достовірність та авторство електронних документів на цих носіях. Також при копіюванні електронного документа з носія інформації обов'язково має бути виконана перевірка цілісності, достовірності та авторства даних на цьому носії.

У зв'язку з цим необхідно вказати, яким чином учасники-резиденти міжнародної платіжної системи виконують вимоги пункту 19.2 цього Закону щодо захисту архівів електронних документів. Виконання цієї норми можливо шляхом створення/перевірки електронного підпису для електронних документів під час їх зберігання в архівах.

Зауваження 5: В правилах платіжної системи необхідно врахувати, що Національний банк України не здійснює сертифікацію програмного забезпечення та засобів захисту інформації.
Коментар: Українське законодавство не вимагає сертифікації програмного забезпечення платіжної системи, платіжною організацією якої є нерезидент, а Національний банк України не займається такою сертифікацією. Надання експертних висновків на засоби захисту інформації в Україні здійснює уповноважений орган – Державна служба спеціального зв'язку та захисту інформації в Україні.

Зауваження 6: В поданому пакеті документів містяться посилання на нормативно-правові акти, що втратили чинність, або використовуються терміни, що містяться в скасованих нормативно-правових актах.
Коментар: В документах необхідно здійснювати посилання тільки на чинні нормативно-правові акти або робити загальні посилання, наприклад: "відповідно до чинного законодавства України". Часто помилково використовуються терміни "ЕЦП", "ЦСК" та інші із Закону України "Про електронний цифровий підпис", який втратив чинність.

Зазначаємо, що 7 листопада 2018 року набрав чинності Закон України "Про електронні довірчі послуги". Цей Закон запроваджує поняття "кваліфікований електронний підпис" та "удосконалений електронний підпис", які замінили поняття "електронний цифровий підпис". Під час розроблення правил необхідно звертати увагу на чинність нормативно-правових актів та застосовувати терміни і поняття, визначені чинними нормативно-правовими актами.

Зауваження 7: Механізм розрахунку, заснований на багаторазовому ґешуванні за алгоритмом сімейства SHA-2, не є процедурою формування електронного підпису.
Коментар: В описах захисту інформації часто зустрічаються помилки, пов'язані з поняттями захисту інформації та криптографії. Найбільш поширеною є помилка, коли для створення електронного підпису використовують ґеш-функцію. Також зустрічаються випадки, коли асиметричний криптографічний алгоритм RSA названо симетричним криптографічним алгоритмом або згадується про відкритий ключ алгоритму AES (симетричний криптографічний алгоритм). Деякі помилки пов'язані з непрофесійним перекладом на українську мову, завдяки чому з'являться терміни на кшталт: "розділений симетричний ключ", "могутня власна ідентифікація", "криптографічна клавіша" тощо.

Зауваження 8: В поданих документах відсутнє розшифрування певних скорочень.
Коментар: Дуже часто в правилах платіжних систем зустрічаються різні скорочення, про зміст яких можна лише здогадуватися та скорочення яких не надано. Зазвичай, ці скорочення можуть бути загальновідомими в державах, резидентом якої є платіжна організація міжнародної платіжної системи, або міститися в нормативних документах цієї держави, але під час подачі таких правил рекомендується подібні скорочення розшифровувати в словнику термінів або під час першого їх використання.

Зауваження 9: Пакет документів неповний.
Коментар: Платіжні організації міжнародних платіжних систем при подачі правил платіжних систем роблять в документах посилання на копії експертних висновків або сертифікатів, однак в поданих комплектах документів ці документи відсутні.

Зауваження 10: Наявні протиріччя або несумісність інформації в різних розділах поданих документів.
Коментар: При подачі документів до Національного банку зустрічаються такі випадки, коли Інформаційна довідка містить одні вимоги до захисту певних ланок, а правила містять зовсім інші вимоги. Наприклад, в Інформаційній довідці вказується, що обмін інформацією між оператором послуг платіжної інфраструктури захищається за допомогою криптографічного алгоритму на базі еліптичних кривих, а в правилах зазначено, що на цій ланці використовується виключно алгоритм RSA. Зустрічаються також несумісності інформації, наданої в різних розділах правил. Помилкою є невідповідність або несумісність схеми обміну інформаційних потоків та схеми захисту інформації на кожній ланці обміну

інформаційними повідомленнями. Найчастіше така ситуація трапляється при поданні змін до правил, коли зміни вносяться лише в деякі розділи.