Типові зауваження до документів платіжної системи, платіжною організацією якої є резидент України

Зауваження: Відсутній або не чинний експертний висновок Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) для засобів криптографічного захисту інформації, вимога щодо захисту якої встановлена законом.

У відповідності до п. 38.2 Закону України "Про платіжні системи та переказ коштів в Україні" електронні документи на переказ, розрахункові документи під час їх передавання засобами телекомунікаційного зв'язку повинні бути зашифровані. Розділом IV 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, для криптографічного захисту інформації, вимога щодо захисту якої встановлена законом, повинні використовуватися засоби, що мають чинний експертний висновок Держспецзв'язку. Невиконання цієї вимоги є порушенням законодавства.

Коментар: В поданих правилах платіжних систем (далі – Правила) зустрічаються ситуації, коли електронні документи на переказ передаються засобами телекомунікаційного зв'язку без шифрування або для шифрування використовуються засоби, що не мають чинного експертного висновку Держспецзв'язку. Законодавством вимагається шифрування, яке може бути виконане декількома способами. Це може бути як шифрування за допомогою програмних або програмно-апаратних засобів, так і шифрування за допомогою засобів захисту мережі з використанням захищеного протоколу (VPN, TLS). Експертний висновок повинен мати саме той засіб, який здійснює шифрування. При використанні декількох ступенів захисту (наприклад, шифрування каналу мережевим маршрутизатором та криптографічною бібліотекою) експертний висновок повинен мати принаймні один засіб захисту інформації.

Зауваження: Платіжна організація платіжної системи планує оброблення та зберігання інформації про операції в хмарних сервісах поза межами території України (Amazon, Google або інші хмарні сервіси).

Оброблення та зберігання інформації про операції з переказу коштів на серверах за межами території України порушує вимоги пункту 5 розділу I Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України, затвердженого постановою Правління Національного банку України № 75 від 04.07.2018.

Коментар: У випадках, коли інформація, що зберігається, передається чи обробляється в платіжній системі може бути віднесена до інформації про банківські операції з переказу коштів (наприклад, коли переказ коштів здійснюється з використанням банківських рахунків), така інформація повинна зберігатися і оброблятися на серверах, що розміщені на території України. У випадках, коли платіжна організація планує зберігання такої інформації в

хмарах Amazon, Google або інших хмарних сервісах, варто зазначити, що в цих сервісах буде оброблятися і зберігатися інформація, яка жодним чином не стосується банківських операцій з переказу коштів.

Зауваження: Не виконується вимога щодо формування та зберігання архівів електронних документів, що створюються при проведенні переказу коштів та операцій з електронними грошима.

Вимога передбачає визначення порядку проведення перевірки цілісності, достовірності та авторства даних під час створення, копіювання та зберігання електронних архівів документів на переказ, відповідно до вимог статті 19 Закону України "Про платіжні системи та переказ коштів в Україні".

Коментар: Правила платіжної системи повинні містити опис, яким чином може бути перевірена цілісність, достовірність та авторство електронних документів на носіях, на яких ці електронні документи зберігаються. У випадку використання для цього криптографічних засобів захисту інформації ці засоби повинні мати чинний експертний висновок Держспецзв'язку. Окрім того, правилами повинно бути передбачено порядок перевірки цілісності, достовірності та авторства даних на носіях інформації при копіюванні електронних документів з цих носіїв інформації.

Зауваження: Не виконується вимога ст. 18 Закону України "Про платіжні системи та переказ коштів в Україні", відповідно до якої електронний підпис є обов'язковим реквізитом електронного документу на переказ, а учасник платіжної системи має передбачити під час приймання електронних документів на переказ процедуру перевірки електронного підпису та процедуру перевірки цілісності, достовірності та авторства електронного документу на переказ.

Коментар: Електронний документ на переказ повинен мати електронний підпис, а учасник платіжної системи при прийманні електронних документів на переказ має передбачити процедуру перевірки електронного підпису та процедуру перевірки цілісності, достовірності та авторства електронного документу на переказ. Оскільки вимога щодо наявності електронного підпису є вимогою закону, необхідно, щоб криптографічний засіб створення електронного підпису мав чинний експертний висновок Держспецзв'язку. В Правилах платіжної системи необхідно вказати засоби створення електронного підпису, надати інформацію де та ким цей електронний підпис створюється та де і ким він перевіряється. Під час створення електронного підпису на електронний документ необхідно передбачити процедуру перевірки цілісності, достовірності та авторства електронного документу на переказ.

Відповідно до вимог 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, необхідно вказувати найменування криптографічних алгоритмів та довжини ключів, що при цьому використовуються. У випадках використання кваліфікованого електронного

підпису достовірність та авторство перевіряються за допомогою властивостей цього підпису. При використанні удосконаленого електронного підпису для підтвердження авторства необхідно використовувати додаткові механізми його підтвердження, наприклад, підписання акту про визнання ключів.

Зауваження: Порядок експлуатації засобу захисту інформації суттєво відрізняється від вимог до порядку експлуатації цього засобу, вказаних в чинному експертному висновку до нього.
Коментар: У випадку, якщо засіб захисту інформації використовується як єдиний засіб, що шифрує інформацію на певній ланці обміну інформаційними потоками, цей засіб повинен мати чинний експертний висновок Держспецзв'язку (для технічних засобів захисту інформації цей висновок може бути чинним на момент побудови системи захисту). Такий експертний висновок може містити вимоги до умов їх експлуатації. У випадку, якщо правилами платіжної системи не передбачено виконання цих вимог, або вказано вимоги, що їм суперечать, відповідну ланку обміну інформаційними потоками неможна вважати захищеною.

Зауваження: Здійснюється посилання на нормативно-правові акти, що втратили чинність, або використовуються терміни, що містяться в скасованих нормативно-правових актах.
Коментар: Платіжні організації платіжних систем інколи роблять в своїх Правилах посилання на нормативно-правові акти Національного банку або Закони України. З метою зменшення частоти перегляду Правил рекомендується не використовувати такі посилання або робити загальні посилання, наприклад: "у відповідності до чинного законодавства України". Особливо частою помилкою є використання понять "ЕЦП", "ЦСК" та інших термінів Закону України "Про електронний цифровий підпис", оскільки 7 листопада 2018 року цей закон втратив з чинність. Натомість використання електронних підписів на даний час регулюється законом України "Про електронні довірчі послуги".

Зауваження: Пакет документів не повний.
Коментар: Платіжні організації при подачі правил платіжних систем роблять в документах посилання на експертні висновки або сертифікати, однак в поданих комплектах документів ці документи відсутні.

Зауваження: Відсутній опис захисту інформації на деяких ланках схеми обміну інформаційними потоками.
Коментар: В Правилах під час опису системи захисту платіжна організація платіжної системи повинна відповідно до вимог Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури надати опис захисту інформації на кожній ланці обміну інформаційними потоками. Інформаційні потоки, що описуються, повинні забезпечувати виконання всіх послуг, які планує надавати платіжна

система та враховувати різні типи технічних засобів, що можуть використовуватися (ПТКС, термінал, інтернет-сайт, пункт надання послуг) включаючи найменування алгоритмів, довжину ключів.

Типовою помилкою є опис інформаційних зв'язків лише між процесинговим центром та іншими компонентами платіжної системи, з якими він взаємодіє. Правила платіжної системи повинні включати опис всіх ланок, в тому числі і ланок обміну інформацією між користувачами і учасниками платіжних систем. З поданого опису повинно бути зрозуміло, яким чином здійснюється шифрування та захист від несанкціонованої модифікації інформації на кожній ланці обміну інформаційними потоками. У випадках, коли для встановлення захищеного з'єднання використовується автентифікація або інший протокол, вони мають бути описані.

Зауваження: Не вказано ланки обміну інформаційними повідомленнями, де використовуються технології, протоколи або засоби.
Коментар: Окремі правила платіжних систем містять окрім схеми інформаційних потоків лише загальний перелік засобів захисту інформації та протоколів обміну ключами чи іншою інформацією. В той же час не вказано де саме використовуються зазначені засоби і протоколи та які ланки обміну інформаційними повідомленнями вони захищають.

Зауваження: В наданій схемі обміну інформаційними повідомленнями не зазначені окремі послуги, які платіжна система планує надавати відповідно до своїх Правил.
Коментар: В деяких випадках перелік послуг, які планує надавати платіжна система передбачає наявність компонент (наприклад, ПТКС, каси, інтернет-сайти, пункти учасника), які не згадуються при описі захисту інформації. Також подібні зауваження до поданих пакетів документів виникають, коли в різних розділах використовується різна термінологія. Наприклад, в одному розділі особа що здійснює переказ називається користувачем, а в іншому розділі ця особа називається платником, а користувачем називається працівник учасника, що одержує доступ до програмно-апаратного комплексу.

Зауваження: Не вказано, які саме електронні платіжні засоби можуть використовуватися для ініціювання платежу.
Коментар: Законом України "Про платіжні системи та переказ коштів в Україні" визначено, що електронний платіжний засіб – це платіжний інструмент, який надає його держателю можливість за допомогою платіжного пристрою отримати інформацію про належні держателю кошти та ініціювати їх переказ. Проте, розробники правил платіжних систем помилково вважають, що терміни "Електронний платіжний засіб" і "Платіжна картка міжнародної платіжної системи VISA чи MasterCard" є тотожними. Насправді, платіжні системи платіжних організацій-резидентів можуть для своїх платіжних систем розробляти і впроваджувати власні електронні платіжні засоби.

Також слід мати на увазі, що якщо в деяких випадках задіяні платіжні картки міжнародних платіжних систем, їх використання не є предметом розгляду в правилах, оскільки їх використання регламентується правилами відповідних платіжних систем. Також слід звернути увагу, що сертифікація за PCI DSS є сертифікацією відповідності саме для міжнародних платіжних систем і жодним чином не закриває питання щодо захисту інформації у платіжних системах-резидентів.

Зауваження: Не вказано вимоги до паролів, процедури їх створення чи заміни, не описано технології їх передачі;
Коментар: У випадку використання для автентифікації паролів необхідно вказати вимоги до цих паролів та надати опис процедури їх передачі та заміни.

Зауваження: Відсутнє розшифрування скорочень.
Коментар: Дуже часто в правилах Платіжних систем зустрічаються скорочення ПЦ, РПЦ, КЦ, ПУ, ПТК, ЕДП, тощо, про зміст яких можна лише здогадуватися та скорочення яких не надано. Рекомендується подібні скорочення розшифровувати в словнику термінів або під час першого їх використання.

Зауваження: Не правильно вказано інформацію щодо криптографічних алгоритмів або протоколів.
Коментар: В описах захисту інформації часто зустрічаються помилки пов'язані з поняттями захисту інформації та криптографії. Наприклад, геш функцію SHA-1 визначено як алгоритм автентифікації, sha256RSA названо симетричним алгоритмом блочного шифрування; вказано довжину ключів криптографічного алгоритму, яка не передбачена стандартами для цього алгоритму. Також інколи правилами платіжних систем декларуються технічні операції, які не можуть бути виконані за допомогою вказаних засобів, наприклад, неможливо зберігати удосконалений електронний підпис в мікропроцесорних картках "CryptoCard-337".

Зауваження: Наявні протиріччя або несумісність інформації в різних розділах поданих документів.
Коментар: В наданих пакетах документів зустрічаються випадки, коли інформаційна довідка містить одні вимоги до захисту певних ланок, а Правила містять зовсім інші. 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 вказано, 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 інформаційних повідомлень. Найчастіше така ситуація трапляється при поданні змін до Правил, коли зміни вносяться лише в деякі розділи Правил.

Зауваження: Надана схема обміну інформаційними повідомленнями дозволяє здійснити відомі атаки.
Коментар: Інколи за результатом розгляду Правил платіжної системи з'ясовується, що за поданої схеми обміну інформаційними повідомленнями та її системи захисту можливо здійснити відомі види атак. Найпростішою з таких атак є атака "людина посередині", коли зловмисник може перехопити інформаційний потік між різними компонентами системи та модифікувати його, залишившись при цьому непоміченим. Така атака можлива, коли платник здійснює платіж через інтернет-сайт учасника, а код підтвердження одержує від процесингового центру системи.

Зауваження: Документи оформлено неналежним чином.
Коментар: Часто буває ситуація, коли подані пакети документів не можуть бути проаналізовані на відповідність законодавству з технічних причин. Зокрема:

– подано сканований документ, але якість сканування не дозволяє проаналізувати окремі схеми, оскільки написи на ній нерозбірливі;

– при друкуванні схем, що на екрані виглядають якісно, друкуються з відображенням тільки окремих частин, розриваються на шматки, друкуються в неправильному кодуванні тощо;

– в сканкопіях документів пропущено окремі сторінки або відскановано лише частину сторінки;

– наявні посилання на неіснуючі пункти або сторінки;

– помилково замість актуальних подано застарілі версії документів.