Типові зауваження до Інформаційної довідки щодо умов та порядку діяльності оператора послуг платіжної інфраструктури, що подається до Національного банку України, в частині захисту інформації

Зауваження 1: Надання неповної інформації щодо програмного забезпечення, яке використовуватиметься оператором послуг платіжної інфраструктури (далі – Оператор) у процесі надання послуг платіжної інфраструктури.
Коментар: Таблиця 3 пункту 3 Інформаційної довідки повинна включати в себе все програмне забезпечення, що використовується для забезпечення інформаційної безпеки та кібербезпеки у процесі надання послуг, в тому числі антивірусне програмне забезпечення, систему керування базами даних, криптографічні бібліотеки, програмне забезпечення для роботи із засобами захисту інформації, програмне забезпечення програмно-технічних комплексів, центрів генерації та сертифікації ключів тощо.

Зауваження 2: Зміст пунктів 4, 5 та 6 Інформаційної довідки не відповідає додатку 10 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 (зі змінами).
Коментар: Типовою є ситуація, коли Оператор замість заповнення пунктів 4, 5 та 6 Інформаційної довідки вказує лише посилання на інші документи Оператора, в яких відповіді на вказані пункти є неповними та не конкретними. До Інформаційної довідки можуть бути долучені інші документи, але в Інформаційній довідці має бути чітке посилання на пункти, в яких міститься вичерпна інформація відповідно до вимог Положення № 43.

Зауваження 3: Відповідно до пункту 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 (зі змінами), визначено, що для криптографічного захисту інформації, вимога щодо захисту якої встановлена законом, повинні використовуватися засоби, які мають чинний експертний висновок Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок). Невиконання цієї вимоги є порушенням законодавства.
Коментар: Оператор послуг платіжної інфраструктури під час обміну інформаційними повідомленнями з іншими учасниками платіжних систем, користувачами, платіжною організацію, розрахунковим банком повинен відповідно до законів України здійснювати шифрування електронних документів на переказ під час їх передачі засобами телекомунікаційного зв'язку. Шифрування має здійснюватися за допомогою засобу, що має чинний експертний висновок Держспецзв'язку. Це може бути як шифрування даних за

допомогою програмних або програмно-апаратних засобів, так і шифрування каналу передачі даних за допомогою засобів захисту мережі з використанням захищеного протоколу (VPN, TLS). Експертний висновок повинен мати саметой засіб, який здійснює шифрування. При використанні декількох ступенів захисту (наприклад, шифрування даних на прикладному рівні (application level) та шифрування каналу передачі даних на рівні мережі (наприклад, засобом захисту мережі) експертний висновок повинен мати принаймні один засіб захисту інформації.

Зауваження 4: Правилами платіжної системи на оператора послуг платіжної інфраструктури покладається збереження архівів електронних документів, проте Оператор не надав опис порядку проведення перевірки цілісності, достовірності та авторства даних під час створення, копіювання та зберігання електронних архівів відповідно до вимог статті 19 Закону України "Про платіжні системи та переказ коштів в Україні".
Коментар: Оператор при наданні послуг, відмінних від оброблення інформації за операціями в міжнародних карткових платіжних системах, повинен в пункті 9 Інформаційної довідки вказати, яким чином перевіряється цілісність, достовірність та авторство електронних документів на носіях інформації, на яких ці електронні документи зберігаються (відповідно до статті 19 Закону України "Про платіжні системи та переказ коштів в Україні"). Криптографічні засоби захисту інформації, за допомогою яких виконується така перевірка, повиннімати чинний експертний висновок Держспецзв'язку. Також потрібно надати опис процедури перевірки цілісності, достовірності та авторства даних на носіях інформації при копіюванні електронних документів з цих носіїв. Крім того необхідно зазначити найменування носіїв інформації.

Зауваження 5: Не виконується вимога статті 18 Закону України "Про платіжні системи та переказ коштів в Україні", відповідно до якої електронний підпис є обов'язковим реквізитом електронного документа на переказ. Оператор повинен передбачити під час приймання електронних документів на переказ процедуру перевірки електронного підпису та процедуру перевірки цілісності, достовірності та авторства електронного документа на переказ.
Коментар: Оскільки наявність електронного підпису на електронному документі на переказ є вимогою закону, необхідно, щоб криптографічний засіб електронного підпису мав чинний експертний висновок Держспецзв'язку. Оператор повинен зазначити в пунктах 3 та 5 Інформаційної довідки конкретні засоби створення електронного підпису та його перевірки, які він використовує під час здійснення своєї діяльності. Також в пункті 8 Інформаційної довідки необхідно навести найменування криптографічних алгоритмів та довжини ключів, які використовуються як при створенні, так і при перевірці електронного підпису.

У випадку використання удосконаленого електронного підпису на електронних документах на переказ, необхідно передбачити використання

додаткових механізмів для встановлення авторства електронного документа, наприклад, підписання сторонами взаємодії акту про визнання ключів електронного підпису. Якщо використовується кваліфікований електронний підпис, то такі додаткові механізми вказувати необов'язково.

Зауваження 6: В Інформаційній довідці наведені посилання на нормативно-правові акти Національного банку та закони України, що втратили чинність, або використовуються терміни, що містяться в скасованих нормативно-правових актах.
Коментар: Рекомендується не використовувати посилання на нормативно-правові акти Національного банку та закони України або робити загальні посилання, наприклад, "відповідно до чинного законодавства України".

Помилкою є використання понять "ЕЦП", "ЦСК" та інших термінів із Закону України "Про електронний цифровий підпис", оскільки 07.11.2018 цей Закон втратив чинність. Натомість використання електронних підписів на даний час регулюється Законом України "Про електронні довірчі послуги".

Зауваження 7: Пакет документів не повний.
Коментар: Оператор в наданій Інформаційній довідці зазначає про використання криптографічних або технічних засобів захисту інформації та вказує, що ці засоби мають чинний експертний висновок Держспецзв'язку, однак в документах такі експертні висновки відсутні. Оператор також повинен відслідковувати термін дії експертних висновків на засоби криптографічного захисту інформації. У випадку, якщо термін дії вже закінчився, а Держспецзв'язку не видала нового позитивного експертного висновку, Оператору необхідно подбати про заміну такого криптографічного засобу захисту на інший.

Зауваження 8: Відсутні чинний сертифікат PCI DSS та/або свідоцтво про відповідність ("Attestation of Compliance") в тих випадках, коли вони вимагаються.
Коментар: У випадках, якщо Оператор планує надавати послуги обробки операцій в міжнародних карткових платіжних системах, він повинен надати копії чинного сертифікату PCI DSS та "Attestation of Compliance". Якщо Оператор не планує надавати жодних інших послуг, то пункти 8 та 9 Інформаційної довідки ним не заповнюються.

Зауваження 9: В Інформаційній довідці (пункт 8) відсутній опис захисту інформації на деяких ланках схеми руху інформаційними повідомленнями.
Коментар: Оператор для узгодження умов та порядку своєї діяльності повинен надати в пункті 8 Інформаційної довідки опис технології захисту інформації та порядок автентифікації під час інформаційної взаємодії з платіжною організацією, учасниками платіжної системи, платіжними пристроями, користувачами, банком-емітентом електронних грошей, комерційними

агентами, розрахунковим банком тощо, з якими Оператор здійснює обмін інформацією відповідно до схем, наведених в пункті 4 Інформаційної довідки. Такий опис має включати: найменування алгоритмів і довжину ключів, паролів, технологію використання засобів захисту інформації, інформацію про розробника засобів, систему керування ключами.

Не потрібно надавати опис системи захисту інформації на ланках, в яких Оператор не задіяний.

Зауваження 10: Оператор не надав опис системи захисту інформації під час надання окремих видів послуг, зазначених ним в таблиці 2 Інформаційної довідки.
Коментар: Деякі Оператори надають широкий спектр послуг. Серед послуг можуть бути як надання операційних або технологічних функцій під час переказу коштів в платіжних системах, так і послуги з обліку використання електронних грошей. Зазначаючи в таблиці 2 надання операційних, інформаційних та інших технологічних функцій, що забезпечують використання електронних грошей, Оператори часто не надають належної уваги опису системи захисту інформації під час здійснення таких операцій. В цьому випадку, Оператор повинен надати в пункті 8 Інформаційної довідки опис технології обміну інформацією під час здійснення операцій з електронними грошима та описати інформаційну взаємодію з агентами, користувачами, банком-емітентом, уключаючи інформацію про засоби захисту інформації, криптографічні алгоритми, довжину ключів тощо.

Зауваження 11: В описі системи захисту інформації в пункті 8 Інформаційної довідки відсутній опис технології використання засобів захисту інформації, які вказані в пунктах 3 та 5 Інформаційної довідки.
Коментар: Деякі Оператори вказують в пунктах 3 та 5 Інформаційної довідки засоби захисту інформації, проте з інформації, наведеної в пункті 8, неможливо визначити, де саме використовуються зазначені засоби та які ланки обміну інформаційними повідомленнями вони захищають.

Зауваження 12: В пункті 8 Інформаційної довідки не вказано вимоги до паролів, процедури їх створення та заміни, не описано технології їх передавання.
Коментар: У разі використання паролів для автентифікації необхідно вказати вимоги до цих паролів (мінімальна довжина, наявність великих та малих літер, спецсимволів тощо). Також потрібно вказати вимоги до процедури генерації паролів, їх зберігання, передавання і заміни.

Зауваження 13: Використовуються скорочення та абревіатури, що не є загальновживаними і не мають тлумачення в Інформаційній довідці або додаткових документах.
Коментар: Часто в Інформаційній довідці, наданій Оператором, зустрічаються скорочення ПЦ, РПЦ, КЦ, ПУ, ПТК, ЕДП тощо, про зміст яких можна лише

здогадуватися та тлумачення яких не надано. Рекомендується скорочення та абревіатури розшифровувати в словнику термінів або під час їх першого використання.

Зауваження 14: Неправильно наведено інформацію щодо криптографічних алгоритмів або протоколів.
Коментар: В пункті 8 Інформаційної довідки часто зустрічаються помилки, пов'язані з поняттями захисту інформації та криптографії. Наприклад, геш-функцію SHA-1 визначено як алгоритм автентифікації; алгоритми sha256 або RSA названо симетричним алгоритмом блокового шифрування; вказано довжину ключів криптографічного алгоритму, яка не передбачена стандартами для цього алгоритму. Інколи описуються технічні операції, які не можуть бути виконані за допомогою вказаних засобів, наприклад, неможливо зберігати удосконалений електронний підпис в мікропроцесорних картках.

З метою спрощення процедури погодження документів рекомендується не надавати блок-схеми та опис криптографічних алгоритмів, якщо вони описані у відповідних стандартах або Оператор не є їх розробником. Також не потрібно надавати лістинги коду програмного забезпечення, формати команд API, структуру бази даних.

Зауваження 15: Інформація, що розміщена в різних пунктах Інформаційної довідки, є суперечливою.
Коментар: В різних пунктах наданої Інформаційної довідки зустрічається суперечлива інформація. Наприклад, на схемі комплексу програмно-апаратних засобів, які використовуватимуться оператором послуг платіжної інфраструктури для надання своїх послуг (пункт 5 Інформаційної довідки) не зазначені компоненти або ланки обміну, які були описані в пункті 8. І навпаки, в пунктах 4, 5 можуть бути не зазначені компоненти або ланки обміну, які описані в інших пунктах Інформаційної довідки.

Помилкою є невідповідність схеми руху інформаційних повідомлень та схеми захисту інформації на кожній ланці обміну інформаційних повідомлень.

Зауваження 16: Інформаційна довідка оформлена неналежним чином.
Коментар: Часто буває ситуація, коли подані документи не можуть бути проаналізовані на відповідність законодавству з технічних причин. Зокрема:

– якість сканування поданих документів не дозволяє проаналізувати окремі схеми, оскільки написи на них нерозбірливі;

– схеми, які на екрані виглядають якісно, друкуються окремими частинами, в неправильному кодуванні тощо (це наслідок використання неправильного формату при збереженні документів);

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

– наявні посилання на пункти або сторінки, що відсутні в документах;

– помилково замість актуальних подано застарілі версії документів.