Рекомендації Національного банку України для подання Інформаційної довідки щодо умов та порядку діяльності оператора послуг платіжної інфраструктури, в частині захисту інформації

Інформаційна довідка щодо умов та порядку діяльності оператора послуг платіжної інфраструктури (далі – Інформаційна довідка) подається до Національного банку України для узгодження умов та порядку діяльності оператора послуг платіжної інфраструктури за зразком, наведеним у додатку 10 до Положення № 43[1] (зі змінами).

Під час заповнення Інформаційної довідки в частині захисту інформації пропонуємо врахувати такі рекомендації.

До пункту 1 Інформаційної довідки: щодо опису видів послуг, які планує надавати оператор послуг платіжної інфраструктури

Оператор послуг платіжної інфраструктури (далі – Оператор) може надавати широкий спектр операційних, інформаційних та інших технологічних функцій щодо переказу коштів, в тому числі й послуги, які стосуються захисту інформації щодо переказу коштів. Наприклад, це можуть бути послуги формування, перевірки та підтвердження чинності сертифіката удосконаленого електронного підпису засобами програмно-технічного комплексу Оператора. В такому випадку, в рядку 14 таблиці 2 Інформаційної довідки (“інші послуги”) необхідно поставити позначку “так” і надати перелік таких послуг.

До пункту 3 Інформаційної довідки: щодо програмного забезпечення, яке використовуватиметься оператором послуг платіжної інфраструктури у процесі надання послуг платіжної інфраструктури

У випадку використання Оператором спеціалізованого програмного забезпечення/комплексу для захисту інформації (криптографічні бібліотеки, програмне забезпечення для роботи із засобами захисту інформації, програмне забезпечення програмно-технічних комплексів, центрів генерації і сертифікації ключів, антивірусне програмне забезпечення тощо) рекомендується вказати таке програмне забезпечення в таблиці 3 Інформаційної довідки.

До пункту 4 Інформаційної довідки: щодо опису руху інформаційних повідомлень під час надання послуг платіжної інфраструктури та його схематичного зображення (окремо за кожним видом послуги оператора послуг платіжної інфраструктури) із зазначенням ролі та функції оператора послуг платіжної інфраструктури в процесі інформаційної взаємодії

У випадку надання Оператором послуг, які стосуються захисту інформації та про які вказано в пункті 1 Інформаційної довідки, в пункті 4 Інформаційної

[1] Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затверджене постановою Правління Національного банку України від 04.02.2014 №43

довідки надається короткий опис руху інформаційних повідомлень та його схематичне зображення під час надання таких послуг.

Рекомендуємо, щоб усі компоненти на схемі руху інформаційних повідомлень, між якими передається інформація про платежі/перекази, були з'єднані за допомогою пронумерованих стрілок. Так само на схемі пропонуємо зазначити маршрути розповсюдження криптографічних ключів або сертифікатів.

Якщо Оператор при проведенні транзакції обмінюється платіжною чи ключовою інформацією з декількома платіжними системами (під час здійснення переказу коштів за участю двох і більше платіжних систем) або із системою використання електронних грошей, то рекомендуємо, щоб такі суб'єкти інформаційної взаємодії були відображені на схемі разом з ланками обміну інформацією.

До пункту 5 Інформаційної довідки: щодо схеми комплексу програмно-апаратних засобів, які використовуватимуться оператором послуг платіжної інфраструктури для надання своїх послуг, із описом функціонального призначення та взаємозв'язку його компонентів

Компонентами такої схеми мають бути: програмно-технічні комплекси генерації, сертифікації ключів, технічні пристрої, операційні та технологічні засоби, сервери різного призначення (баз даних, авторизації, додатків, маршрутизації, зберігання архівів електронних документів тощо), засоби захисту мережі, інші компоненти.

Одними з основних засобів, що використовуються Оператором для захисту своїх інформаційних ресурсів, є апаратні, програмні або програмно-апаратні засоби захисту мережі. Під час опису функціонального призначення цих засобів необхідно вказати, для яких видів послуг ці засоби використовуються (з переліку, наведеного у таблиці 2 Інформаційної довідки). У випадках, коли засоби використовуються для захисту інформації, вимога щодо захисту якої встановлена законодавством України, має бути надано копії чинних експертних висновків уповноваженого органу на такі засоби[2].

До пункту 6 Інформаційної довідки: щодо інформації про інформаційно-комунікаційні технології, які будуть застосовуватися під час надання послуг платіжної інфраструктури

Під час надання інформації щодо інформаційно-комунікаційних технологій слід враховувати, що до таких технологій відносяться технології захисту інформації під час використання хмарних сервісів, сервісів мобільного та інтернет-банкінгу, технологій захисту інформації під час використання електронних платіжних засобів та термінального обладнання, модулів безпеки (HSM), засобів моніторингу, засобів виявлення шахрайських операцій, захищені мережеві протоколи (VPN, HTTPS, SFTP, TLS, TELNET, PPTP тощо).

[2] відповідно до вимог 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)

До пункту 8 Інформаційної довідки: щодо опису системи захисту інформації, яка використовуватиметься під час надання послуг платіжної інфраструктури, уключаючи найменування алгоритмів і довжину ключів, паролів, технологію використання засобів захисту інформації, інформацію про розробника засобів, систему керування ключами (заповнюється, якщо немає сертифіката PCI DSS або в разі надання оператором послуг платіжної інфраструктури інших видів послуг, ніж оброблення інформації за операціями в міжнародних карткових платіжних системах)

Система захисту інформації повинна бути описана для всіх видів послуг, що перераховані в пункті 1 Інформаційної довідки (таблиця 2), та для всіх типів інформаційної взаємодії Оператора з іншими суб'єктами, що відображені в пункті 4 Інформаційної довідки.

Система захисту інформації складається із внутрішніх документів Оператора, заходів з охорони приміщень, а також технологічних та програмно-апаратних засобів криптографічного захисту інформації, яка обробляється в платіжних системах. До внутрішніх документів Оператора належать документи, що містять вимоги по розподілу обов'язків персоналу, який займається розробленням, тестуванням, налаштуванням та експлуатацією програмно-апаратних комплексів та програмного забезпечення, а також вимоги щодо доступу (локального та віддаленого) до баз даних, автоматизованого аудиту, протоколювання.

Оператор може додати до пакету документів необхідні внутрішні документи або надати в пункті 8 Інформаційної довідки короткий опис вищезазначених вимог.

У випадку, якщо Оператор здійснює операційні функції, що забезпечують використання електронних грошей, необхідно надати опис вимог щодо розмежування прав доступу до інформаційних ресурсів під час використання електронних грошей[3].

Опис вимог безпеки до приміщень, в яких розміщено комплекс програмно-апаратних засобів Оператора, має включати вимоги щодо доступу до цих приміщень, протоколювання цього доступу, наявність відеоспостереження тощо. Замість опису можна надати посилання на стандарти, правила та інші документи, що містять такі вимоги, наприклад, на Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04.07.2007 № 243.

Також рекомендуємо описати вимоги щодо віддаленого доступу до серверів. Якщо сервери працюють (можуть працювати) у віртуальному та/або "хмарному" середовищі, слід вказати про це, зазначивши вимоги до такої конфігурації серверів.

Оскільки будь-який обмін інформацією при використанні відкритих мереж повинен розпочинатися із процедури автентифікації, пропонуємо надати опис цієї процедури. Якщо для цього використовуються криптографічні методи, має

[3] відповідно до вимог Положення про електронні гроші в Україні, затвердженого постановою Правління Національного банку України від 04.11.2010 № 481 (зі змінами)

бути вказано за допомогою яких криптографічних засобів це здійснюється, за допомогою яких алгоритмів та з якою довжиною ключів. Якщо використовується автентифікація за допомогою логіну та паролю, необхідно зазначити, яким чином захищається передача паролю до даного логіну. У випадках, коли передається замість паролю його ґешфункція, необхідно вказати алгоритм ґешування та його довжину. Якщо пароль до логіну є динамічним (наприклад, при використанні двофакторної автентифікації), рекомендуємо це зазначити.

Якщо під час обміну інформацією Оператора з іншими суб'єктами інформаційної взаємодії (відповідно до пункту 4 Інформаційної довідки) застосовується шифрування даних, необхідно зазначити засоби захисту інформації, алгоритми шифрування та довжини криптографічних ключів, а також рекомендуємо вказати де саме здійснюється шифрування та розшифрування інформації. Технологія захисту інформації щодо особистих ключів асиметричних криптографічних алгоритмів та паролів під час їх передачі має також бути описана.

У випадках, якщо під час інформаційної взаємодії Оператора використовується електронний підпис, про це необхідно також вказати. Особливу увагу слід звернути на випадки створення електронного підпису для електронних документів, що передбачено Законом України "Про платіжні системи та переказ коштів в Україні". В таких випадках необхідно в описі чітко зазначити, на якому етапі, яким способом та за допомогою яких засобів накладається електронний підпис, де здійснюється перевірка цього підпису, яким чином відбувається перевірка цілісності, достовірності та авторства електронного документу.

Для технологій захисту інформації, описаних в пункті 6 Інформаційної довідки, в пункті 8 Інформаційної довідки необхідно навести технологію їх використання. Для засобів захисту мережі рекомендується вказати, чи здійснюється фільтрація по IP-адресам або портам та які встановлено вимоги до використання і адміністрування цих засобів. У випадках наявності особливих вимог до мережевого обладнання, які необхідні для забезпечення надійного функціонування інфраструктури Оператора та які відрізняються від вимог виробника до експлуатації або доповнюють їх, потрібно додати опис цих додаткових вимог. Якщо Оператором передбачається доступ адміністратора (або іншого користувача) до мережевого обладнання для його налаштування та інших робіт за допомогою мережевого з'єднання, необхідно це вказати та надати опис захисту такої мережі.

Для VPN-каналу необхідно зазначити технологію його створення (наприклад, IPSec), протокол (наприклад, ESP), алгоритми шифрування, механізм автентифікації та його алгоритм. У випадку HTTPS-з'єднання має бути вказано параметри шифрування (наприклад: алгоритм ґешування SHA-2, ключ шифрування RSA з довжиною 2048 біт, видавець сертифікату компанія N).

В описі системи керування ключами рекомендується надати опис життєвого циклу криптографічних ключів. 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 вказано, де саме він генерується та за допомогою яких засобів. 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 випадку пересилки відкритого ключа на сертифікацію потрібно вказати механізм, за допомогою якого центр сертифікації зможе пересвідчитись в авторстві власника ключа. При використанні процедури сертифікації відкритих ключів необхідно вказати, за допомогою якого програмно-технічного комплексу або надавача електронних довірчих послуг буде виконуватись така сертифікація.

Враховуючи, що кожен ключ має певний термін життя, рекомендуємо вказати періодичність його заміни та надати інформацію про процес цієї заміни. Також потрібно вказати як зберігається та обліковується даний ключ під час терміну свого використання.

До пункту 9 Інформаційної довідки: щодо строків, порядку зберігання та захисту інформації щодо переказу коштів, який має передбачати зберігання даних про кожну операцію з переказу коштів з можливістю відновити дані про дату здійснення операції, ініціатора та отримувача переказу, місце ініціювання та виплати переказу, суму та валюту переказу коштів (заповнюється, якщо немає сертифіката PCI DSS або в разі надання оператором послуг платіжної інфраструктури інших видів послуг, ніж оброблення інформації за операціями в міжнародних карткових платіжних системах).

У цьому пункті Інформаційної довідки пропонуємо надати опис захисту інформації під час створення, зберігання та копіювання архівів електронних даних. Якщо Оператор здійснює формування та зберігання архівів електронних документів, що утворюються під час здійснення операцій при наданні послуг платіжної інфраструктури, необхідно вказати яким чином здійснюється перевірка 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”, статей 12 і 13 Закону України “Про електронні документи та електронний документообіг”.

Додаткові рекомендації

Оператор має право до Інформаційної довідки додавати інші документи, на які зроблено посилання в Інформаційній довідці, та які дозволяють розкрити окремі аспекти забезпечення захисту інформації під час надання послуг Оператором. При цьому такі документи не повинні містити інформацію, яка протирічить тому, що наведено в інших наданих документах або в Інформаційній довідці.

Такими документами можуть бути інструкції, положення, політики безпеки, чинні експертні висновки Держспецзв’язку на засоби захисту інформації, сертифікати відповідності тощо.

На всі засоби технічного та криптографічного захисту інформації, які використовуються під час здійснення операцій при наданні послуг платіжної інфраструктури, подаються копії чинних експертних висновків уповноваженого органу (наприклад, Державної служби спеціального зв'язку та захисту інформації України або авторитетних міжнародних організацій, що виконували аудит чи сертифікацію таких засобів).

Якщо експертний висновок містить вимоги до експлуатації сертифікованого засобу, то також має бути надано копії сторінок експертного висновку, де ці вимоги наведені.

У випадках, якщо Оператор зберігає та обробляє чи потенційно може обробляти дані держателів платіжних карток, слід зазначити про вимоги щодо відповідності міжнародному стандарту безпеки даних індустрії платіжних карток PCI DSS відповідного рівня цього Оператора та надати копії чинних підтверджуючих документів (сертифікату та "Attestation of Compliance").

Документи мають складатися українською мовою. Документи, складені іноземною мовою, мають супроводжуватися нотаріально засвідченим перекладом українською мовою.

Перелік законодавчих актів України, які рекомендовано використовувати з метою подання Інформаційної довідки щодо умов та порядку діяльності оператора послуг платіжної інфраструктури, в частині захисту інформації

Закони України

- Про інформацію
- Про захист інформації в інформаційно-телекомунікаційних системах
- Про електронні документи та електронний документообіг
- Про електронні довірчі послуги
- Про захист персональних даних
- Про Національний банк України
- Про платіжні системи та переказ коштів в Україні

Нормативно-правові акти

- Положення про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури, затверджене постановою Правління Національного банку України від 04.02.2014 № 43 (зі змінами)
- Положення про порядок емісії електронних платіжних засобів і здійснення операцій з їх використанням, затверджене постановою Правління Національного банку України 05.11.2014 № 705 (зі змінами)
- Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 (зі змінами)
- Положення про порядок формування, зберігання та знищення відокремлених електронних даних, отриманих за результатами роботи інформаційних систем у Національному банку України і банках України, затверджене постановою Правління Національного банку України від 14.09.2018 № 99
- Правила технічного захисту приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04.07.2007 № 243
- Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні, затверджене постановою Правління Національного банку України від 28.11.2014 № 755 (зі змінами)
- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 20.07.2007 № 141 (зі змінами)