Рекомендації для підготовки документів платіжної системи, платіжною організацією якої є резидент, що подаються до Національного банку України, в частині захисту інформації

1. Загальні положення

Ці Рекомендації розроблено з метою надання допомоги платіжним організаціям платіжних систем у підготовці, в частині системи захисту інформації, правил платіжної системи, платіжною організацією якої є резидент (далі – Правила), порядок узгодження яких встановлений Положенням про порядок реєстрації платіжних систем, учасників платіжних систем та операторів послуг платіжної інфраструктури (затверджено постановою Правління Національного банку України від 04.02.2014 року № 43 (далі – Положення № 43).

Відповідно до вимог розділу II Положення № 43 Правила повинні містити опис системи 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.

Якщо правила платіжної системи містять відомості щодо захисту інформації, які містять банківську таємницю, то такі відомості мають бути викладені в окремому документі, оформленому відповідно до нормативно-правових актів Національного банку України.

Положення Рекомендацій не поширюються на платіжні системи, платіжною організацією яких є Національний банк.

Терміни та поняття, які вживаються в Рекомендаціях, застосовуються в значеннях, визначених законами України та нормативно-правовими актами Національного банку України.

2. Схема та опис руху інформаційних повідомлень

Правила платіжної системи повинні містити схему руху інформаційних повідомлень (далі – Схема обміну), яка може бути суміщена з іншими схемами, наприклад, зі схемою руху коштів. Оскільки не всі інформаційні повідомлення містять інформацію про платежі, у розділі, що описує систему захисту платіжної системи, рекомендовано надати спеціалізовану схему (схеми) руху інформаційних повідомлень, що включає в себе тільки ті компоненти системи, які приймають участь в обміні та обробленні такої інформації. Проте ця рекомендація не є обов'язковою і при описі системи захисту можна посилатись на Схему обміну.

Схема обміну повинна містити всі компоненти платіжної системи, які функціонують в системі. Такими компонентами можуть бути: учасники платіжної системи (далі – учасники), платники та отримувачі коштів, оператори послуг платіжної інфраструктури, розрахунковий банк, надавачі електронних довірчих послуг, програмно-технічні комплекси генерації і сертифікації ключів, інші платіжні системи тощо. Якщо учасник має в своєму складі декілька компонентів платіжної системи (наприклад, робоче місце касира та віддалений сервер, з яким він зв'язується по мережі), вони повинні бути відображені на схемі окремо.

На Схемі обміну рекомендовано показати взаємодію між клієнтами та учасниками або компонентами платіжної системи, якщо така взаємодія можлива декількома принципово різними способами (наприклад, через Інтернет-сайт та за допомогою програмно-технічного комплексу самообслуговування).

Якщо учасник має свою внутрішню інфраструктуру (сервери різного призначення, сховище архівів, інші компоненти), особливо коли ці компоненти знаходяться в різних приміщеннях, не об'єднаних одним контуром захисту, рекомендовано показати їх на загальній Схемі обміну або на окремій деталізованій схемі учасника.

Рекомендовано всі компоненти схеми, між якими передається інформація про платіж, дані платників та отримувачів, а також криптографічні ключі, з'єднувати за допомогою пронумерованих стрілок.

У випадку, якщо платіжна система обмінюється платіжною чи ключовою інформацією з іншими платіжними системами, ці платіжні системи також повинні бути показані на Схемі обміну разом з ланками обміну інформацією.

Правила повинні містити опис технічного та криптографічного захисту для кожної ланки Схеми обміну з посиланням на номер ланки.

3. Надання копій дозвільних документів на використання засобів захисту

На всі засоби технічного та криптографічного захисту інформації, які використовуються в платіжній системі при виконанні переказу, необхідно надати копії чинних експертних висновків уповноваженого органу, наприклад, Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок).

Вказані експертні висновки мають бути чинними на момент подання Правил для узгодження Національним банком України. Для засобів технічного захисту інформації допускається чинність на момент придбання засобу.

Якщо експертний висновок містить вимоги до експлуатації сертифікованого засобу, необхідно надати копії сторінок експертного висновку, в яких ці вимоги прописані. В Правилах в описі відповідної ланки має бути вказано, що ці вимоги до експлуатації мають виконуватися.

Якщо платіжна система використовує дані держателів платіжних карток, в Правилах необхідно вказати відповідність платіжної системи вимогам міжнародного стандарту безпеки даних індустрії платіжних карток PCI DSS та надати копії чинних документів, що підтверджують відповідність (сертифікату та свідоцтва "Attestation of Compliance").

4. Опис засобів захисту мережі

В якості технічного захисту мережі можуть використовуватись міжмережеві екрани та файєрволи. В Правилах повинні бути вказані найменування засобів захисту мережі, які використовуються, та надано копії експертних висновків на ці засоби. Також необхідно зазначити яким чином для таких засобів захисту мережі забезпечується виконання вимог до умов експлуатації, наведених у відповідному розділі експертного висновку. У випадку наявності особливих вимог, що не співпадають з вимогами до експлуатації, потрібно надати їх опис.

Якщо на деякій ланці Схеми обміну зі сторони певної компоненти здійснюється фільтрація по IP-адресам чи портам, це повинно бути зазначено в Правилах. Якщо захищене з'єднання забезпечується шляхом створення VPN-каналу або HTTPS-з'єднання, це також необхідно описати. Для VPN-каналу необхідно зазначити технологію його створення (наприклад, IPSec), протокол (наприклад, ESP), алгоритми шифрування, механізм автентифікації та його алгоритм. Якщо використовується HTTPS-з'єднання, має бути також наведено параметри шифрування (наприклад: алгоритм хешування SHA2, ключ шифрування RSA з довжиною 2048 біт, видавець сертифікату компанія N).

Якщо в платіжній системі передбачається адміністративний доступ до мережевого обладнання за допомогою мережевого з'єднання, рекомендовано зазначити це в Правилах та надати опис захисту такого з'єднання.

5. Опис криптографічних алгоритмів, протоколів та ключів

У Правилах в описі механізму шифрування інформації під час обміну між компонентами платіжної системи має бути зазначено алгоритми шифрування, довжину ключів та паролів. Якщо дані, що передаються, підписані за допомогою електронного підпису (кваліфікований електронний підпис, удосконалений електронний підпис, MAC тощо), це також повинно бути зазначено.

Особисті ключі, паролі та інша конфіденційна інформація повинна передаватися в захищеному від перегляду та модифікації вигляді, що унеможливить її несанкціоноване використання. В Правилах необхідно зазначити порядок такого захисту.

6. Опис процедури автентифікації

Оскільки будь-який обмін інформацією при використанні відкритих мереж повинен розпочинатися із взаємної автентифікації (якщо тільки одна сторона одержує інформацію, автентифікація може бути односторонньою), має бути описано цей процес. Рекомендовано вказати яка автентифікація (однофакторна чи двохфакторна) застосовується. Якщо для цього використовуються криптографічні методи, має 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, рекомендовано зазначити яким чином захищається передача паролю. У випадках, коли замість паролю передається його хеш-функція, рекомендовано вказати алгоритм хешування та довжину хеш-функції. Якщо пароль до логіну є динамічним (наприклад, при використанні двохфакторної автентифікації), також це зазначити.

7. Рекомендації щодо використання електронного підпису

Відповідно до Закону України “Про платіжні системи та переказ коштів в Україні” документ на переказ повинен мати електронний підпис. В Правилах необхідно зазначити вид електронного підпису, який використовується суб’єктом платіжного ринку для підпису електронного документа на переказ та під час створення архівів електронних документів на переказ. Потрібно описати на якому етапі, яким способом та за допомогою яких засобів створюється електронний підпис, де здійснюється перевірка цього підпису, яким чином відбувається перевірка цілісності, достовірності та авторства електронного документу на переказ. Необхідно вказати які криптографічні алгоритми та з якою довжиною ключів будуть використовуватись.

8. Створення архівів електронних документів

Під час формування, використання та зберігання архівів електронних документів на переказ, які створюються в платіжній системі (далі – електронні архіви), повинна забезпечуватись їх цілісність, достовірність та авторство. Для цього під час формування архівів для них створюється електронний підпис.

Рекомендуємо зазначити, які засоби електронного підпису (вони повинні бути сертифіковані), криптографічні алгоритми та з якою довжиною ключів використовуються для перевірки цілісності, достовірності та авторства даних під час формування, використання та зберігання електронних архівів.

9. Опис системи управління ключовою інформацією

Оскільки криптографічні ключі, що використовуються для захисту інформації в платіжній системі, під час свого життєвого циклу генеруються, вводяться в експлуатацію, пересилаються, зберігаються, архівуються, відновлюються та знищуються, для оцінки безпеки інформації в Правилах необхідно описати кожен із вказаних етапів.

Для опису процедури генерації ключів потрібно вказати де та за допомогою яких засобів генеруються ключі, надати чинні експертні висновки на ці засоби. В експертних висновках має бути вказано про перевірку генератора випадкових чисел. Оскільки ключі можуть пересилатися на токені чи іншому захищеному засобі, зашифровані певним чином, рекомендуємо надати інформацію про спосіб пересилання ключів від місця генерації до користувачів ключів та метод захисту під час пересилання.

Якщо використовується процедура формування сертифікатів відкритих ключів, рекомендуємо вказати за допомогою якого програмно-технічного комплексу або надавача електронних довірчих послуг буде виконуватись така сертифікація. У випадку пересилання відкритого ключа на сертифікацію, рекомендуємо описати механізм, за допомогою якого програмно-технічний комплекс або надавач електронних довірчих послуг зможе пересвідчитись в авторстві власника ключа.

Враховуючи, що криптографічний ключ має певний термін життя, рекомендуємо вказати періодичність заміни ключа та надати інформацію щодо процедури цієї заміни, описати порядок зберігання та обліку ключа протягом терміну його використання.

10. Рекомендації до приміщень обмеженого доступу

В описі компонентів платіжної системи рекомендовано навести загальні вимоги до приміщень, в яких компоненти знаходяться (уключаючи вимоги щодо доступу, протоколювання доступу, наявність відеоспостереження, системи охоронної сигналізації тощо), 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.

У Правилах рекомендовано вказати вимоги захисту як до фізичного доступу, так і до віддаленого доступу до серверів. Також рекомендовано надати вимоги до конфігурації серверів, що працюють (можуть працювати) у віртуальному середовищі.

11. Вимоги щодо розподілу прав доступу персоналу

У Правилах рекомендовано окремо описати вимоги щодо розподілу обов'язків працівників, які займаються розробленням, тестуванням, налаштуванням та експлуатацією програмно-апаратних комплексів та програмного забезпечення. Також слід зазначити вимоги щодо прав доступу працівників (локального та віддаленого) до баз даних, автоматизованого аудиту, протоколювання.

12. Взаємодія з іншими платіжними системами

Якщо платіжна система передбачає обмін з іншими платіжними системами платіжною та ключовою інформацією, однак ще не працює з ними, Правилами може бути передбачене формулювання загальних вимог до такої взаємодії, тобто повинні бути прописані зовнішні інтерфейси. Допускається в описі надавати загальні вимоги, наприклад, "для генерації та зберігання криптографічних ключів має використовуватись технічний пристрій, що має чинний експертний висновок Держспецзв'язку".

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

I. Закони України:

- "Про платіжні системи та переказ коштів в Україні";
- "Про захист інформації в інформаційно-телекомунікаційних системах";
- "Про електронні довірчі послуги";
- "Про електронні документи та електронний документообіг".

II. 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 організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України, затверджене постановою Правління Національного банку України від 04.07.2018 № 75;
- 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;
- Положення про застосування електронного підпису та електронної печатки в банківській системі України, затверджене постановою Правління Національного банку України від 14.08.2017 №78 (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).