Рекомендації для підготовки документів, що подаються до Національного банку України з метою узгодження правил використання електронних грошей, в частині захисту інформації

1. Загальні положення

Ці Рекомендації розроблено з метою надання допомоги банкам-емітентам у підготовці документів, що подаються до Національного банку України з метою узгодження правил використання електронних грошей (далі – Правила), в частині захисту інформації. Порядок узгодження Правил встановлений вимогами Положення про електронні гроші в Україні, затвердженого постановою Правління Національного банку України від 04.11.2010 № 481 (далі – Положення про ЕГ).

Для проведення оцінки відповідності Правил законодавству України в частині захисту інформації опис системи захисту повинен включати все необхідне для проведення аналізу відповідно до законодавства та нормативно-правових актів Національного банку України (далі – Національний банк). Якщо частина інформації не може бути за тих чи інших причин внесена до Правил, її необхідно включити в "Інформаційну довідку про принципи технічної реалізації здійснення розрахунків із використанням електронних грошей" (далі – Інформаційна довідка).

1. Відповідно до підпункту 2 пункту 2 розділу 6 Положення про ЕГ банк-емітент повинен надати в Правилах інформацію про:

порядок здійснення операцій між емітентом, оператором, агентами, користувачами та торговцями, який має містити загальну схему всіх інформаційних потоків;

систему безпеки і захисту інформації та розмежування прав доступу до інформаційних ресурсів під час використання електронних грошей.

2. Відповідно до пункту 5.3 Положення про ЕГ банк-емітент повинен надати інформацію про:

запроваджені організаційні, процедурні заходи та використання технічних засобів з метою виявлення, а також запобігання, перешкоджання та протидії шахрайству;

систему захисту інформації, що застосовується банком-емітентом для забезпечення безперервного захисту інформації під час випуску, використання та погашення електронних грошей на всіх етапах їх формування, оброблення, передавання і зберігання.

Зазначаємо, що опис системи захисту потрібно надати для всіх інформаційних потоків, які визначені Правилами.

3. Відповідно до пункту 5.2 Положення про ЕГ банк-емітент або оператор зобов'язаний забезпечити фіксування всіх трансакцій електронних грошей за допомогою технічних засобів, а також зберігання відповідної інформації у формі, яка дає змогу перевірити її цілісність. Інформацію про це банк-емітент має надати для проведення оцінки відповідності Правил законодавству.

Якщо в Правилах або Інформаційній довідці є 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.

Терміни та поняття, які використовуються в Рекомендаціях, застосовуються в значеннях, наведених у законах України та нормативно-правових актах Національного банку.

2. Зберігання та облік електронних грошей

В наданих документах (Правилах та/або Інформаційній довідці) повинно бути чітко зазначено:

електронний пристрій, на якому зберігаються електронні гроші кожного користувача. Таким пристроєм може бути: чип платіжної картки/наперед оплаченої картки багатоцільового використання або іншого носія, комп'ютер користувача, сервер системи розрахунків електронними грошима (емітента та/або оператора);

де і яким чином ведеться облік операцій з електронними грошима емітента, користувачів, торговців та агентів;

засіб/метод доступу до електронних грошей (облікових записів/електронних гаманців), який надається користувачам: вебінтерфейс, встановлення спеціального програмного забезпечення, наперед оплачена картка тощо;

опис системи захисту електронних грошей (облікових записів/електронних гаманців) кожного користувача від несанкціонованого перегляду та модифікації.

3. Схема та опис руху інформаційних потоків

Документи повинні містити опис і загальну схему руху інформаційних потоків (повідомлень) (далі – Схема), яка може бути суміщена з іншими схемами, наприклад, руху грошових потоків. Оскільки не всі інформаційні повідомлення містять інформацію про операції з електронними грошима, то в описі системи безпеки і захисту інформації може бути надана спеціалізована схема руху інформаційних потоків, яка містить тільки ті компоненти інфраструктури системи розрахунків електронними грошима, які беруть участь в обміні та обробленні такої інформації.

Такими компонентами, в першу чергу, повинні бути суб'єкти, що здійснюють операції з електронними грошима (далі – Суб'єкти): банк-емітент, оператор, агенти, торговці та користувачі.

Також на Схемі зазначають технічні пристрої, операційні та технологічні засоби, сервери різного призначення (вебсервер, баз даних, авторизації, додатків, маршрутизації тощо), систему створення та зберігання архівів електронних документів, засоби захисту мережі, програмно-технічні комплекси генерації і сертифікації ключів та інші компоненти, які входять до складу внутрішньої

інфраструктури Суб’єктів, та використовуються при обміні інформацією під час операцій з електронними грошима.

Різні компоненти, які використовуються в процесі здійснення користувачем операцій з електронними грошима (наприклад, робоче місце касира, програмно-технічні комплекси самообслуговування, Інтернет-сайт, віддалений сервер), повинні бути відображені на Схемі окремо.

У випадку, якщо програмно-апаратні комплекси та сервери знаходяться в різних приміщеннях, не об’єднаних одним контуром захисту, вони також повинні бути відображені на загальній або спеціалізованій схемі.

4. Система захисту інформації

Для зручності рекомендується всі компоненти Схеми, між якими передається інформація про операції з електронними грошима, з’єднати за допомогою пронумерованих стрілок. При описі захисту інформації на кожній ланці можна посилатися на ці номери. Слід описати криптографічні та технічні засоби захисту, а також технологію захисту інформації для кожної ланки Схеми.

Такий захист інформації має складатися із захисту мережі за допомогою захищених мережевих протоколів та захисту даних, що передаються в мережі.

4.1. Засоби захисту мережі

В якості технічного захисту мережі, що забезпечує безпеку під час взаємодії Суб’єктів між собою, можуть використовуватись міжмережеві екрани та файєрволи. В документах необхідно вказати повне найменування засобів захисту мережі, зазначити ланки, на яких вони використовуються, та надати копії чинних експертних висновків уповноваженого органу на ці засоби, наприклад, Державної служби спеціального зв’язку та захисту інформації України (далі – Держспецзв’язок). Також необхідно зазначити, яким чином для таких засобів захисту мережі забезпечується виконання вимог до умов експлуатації, наведених у відповідному розділі експертного висновку.

Якщо на деякій ланці Схеми зі сторони певної компоненти здійснюється фільтрація по IP-адресам чи портам, це повинно бути зазначено в документах. Якщо захищене з’єднання забезпечується шляхом створення VPN-каналу або HTTPS-з’єднання, це також має бути вказано. 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 гешування SHA-2, ключ шифрування RSA з довжиною 2048 біт, видавець сертифікату компанія N).

Якщо передбачається адміністративний доступ до мережевого обладнання за допомогою мережевого з’єднання для налаштування та інших робіт, рекомендовано це вказати та надати опис захисту такого з’єднання.

4.2. Опис криптографічних протоколів, алгоритмів та ключів

В документах має бути зазначено, на яких етапах здійснюється шифрування і розшифрування інформації щодо операцій з електронними грошима та якими засобами, а також алгоритми шифрування, довжини ключів та паролів. Якщо дані, що передаються, підписані за допомогою електронного підпису (кваліфікований або удосконалений електронний підпис, MAC тощо), це також повинно бути зазначено разом з алгоритмами шифрування та довжинами ключів.

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

4.3. Процедура автентифікації

Оскільки будь-який обмін інформацією при використанні відкритих мереж повинен розпочинатися із взаємної автентифікації (якщо тільки одна сторона доводить свою справжність, автентифікація одностороння), має бути описано цей процес. Рекомендовано вказати яка автентифікація застосовується (одностороння чи двостороння, однофакторна чи двофакторна). Якщо для автентифікації 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, необхідно зазначити вимоги до парольної політики, порядок встановлення, заміни та передачі паролів користувачів та уповноважених осіб агентів. У випадках, коли замість паролю передається його ґеш-функція, необхідно вказати алгоритм ґешування та довжину ґеш-функції. Якщо пароль до логіну є динамічним (наприклад, при використанні двофакторної автентифікації), необхідно це зазначити.

4.4. Використання електронного підпису

Відповідно до законів України “Про платіжні системи та переказ коштів в Україні” та “Про електронні документи та електронний документообіг” електронний документ повинен мати електронний підпис. В документах банка-емітента, що подаються для узгодження правил використання електронних грошей, необхідно зазначити вид електронного підпису (кваліфікований або удосконалений електронний підпис, MAC), який використовується для підпису електронних документів (щодо операцій з електронними грошима) та під час створення архівів електронних документів. Потрібно описати на якому етапі, яким способом, за допомогою яких засобів та ким створюється електронний підпис, де здійснюється перевірка цього підпису, яким чином відбувається перевірка цілісності, достовірності та авторства електронного документу.

Необхідно вказати які криптографічні алгоритми та з якою довжиною ключів будуть використовуватись.

4.5. Надання копій дозвільних документів на використання засобів захисту

Під час проведення операцій з електронними грошима для захисту інформації, вимоги щодо захисту якої встановлено законодавством України (електронних документів, архівів електронних документів, а також для шифрування їх під час передавання засобами телекомунікаційного зв'язку), використовуються засоби технічного та криптографічного захисту інформації. На такі засоби захисту інформації необхідно надати копії чинних експертних висновків уповноваженого органу. Вказані експертні висновки мають бути чинними на момент подання документів для узгодження правил використання електронних грошей Національним банком. Для засобів технічного захисту інформації допускається чинність на момент побудови системи захисту інформації.

Якщо експертний висновок містить вимоги до умов експлуатації сертифікованого засобу, має бути надана копія сторінок з цими вимогами. При цьому в описі відповідної ланки Схеми має бути вказано, що такі вимоги мають виконуватися. У випадку наявності особливих вимог до мережевого обладнання, які не співпадають з вимогами до умов експлуатації, потрібно надати опис цих вимог.

5. Система управління ключовою інформацією

Оскільки криптографічні ключі, що використовуються для захисту інформації, під час свого життєвого циклу генеруються, вводяться в експлуатацію, пересилаються, зберігаються, архівуються, відновлюються та знищуються, 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, опис повинен містити 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 сертифікація. У випадку пересилання відкритого ключа на сертифікацію рекомендуємо описати механізм, за допомогою якого програмно-технічний комплекс або надавач електронних довірчих послуг зможе ідентифікувати власника ключа.

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

6. Розмежування прав доступу до інформаційних ресурсів під час використання електронних грошей

Необхідно описати вимоги щодо розподілу обов'язків персоналу, який займається розробленням, тестуванням, налаштуванням та експлуатацією програмно-апаратних комплексів та програмного забезпечення. Слід навести перелік ролей (в тому числі конкретизувати чи існують ролі адміністраторів АРМ, технічних працівників, працівників служби підтримки тощо).

Також потрібно зазначити механізм та засоби для розмежування прав доступу (локального та віддаленого) до програмно-апаратних комплексів, серверів баз даних та іншого призначення, особистого кабінету користувача, автоматизованого аудиту, протоколювання. Потрібно описати яким чином захищені від фальсифікацій та несанкціонованого доступу журнали реєстрації подій, у яких записуються дії користувачів (адміністраторів), збої та події інформаційної безпеки оператора тощо.

7. Доступ до приміщень обмеженого доступу

В описі системи захисту інформації необхідно вказати загальні вимоги до приміщень обмеженого доступу, які використовуються, (уключаючи вимоги щодо доступу, протоколювання доступу, наявності відеоспостереження тощо) та/або 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.

В документах рекомендовано навести вимоги як до фізичного доступу, так і до віддаленого доступу до серверів. Також рекомендовано надати вимоги до конфігурації серверів, що працюють (можуть працювати) у віртуальному та/або "хмарному" середовищі.

8. Створення архівів електронних документів

В процесі формування, використання та зберігання архівів електронних документів, які створюються під час здійснення операцій з електронними грошима (далі – електронні архіви), необхідно забезпечити їх цілісність, достовірність та авторство. Для цього використовуються електронний підпис або інші надійні механізми.

В Правилах необхідно описати вищевказані процедури перевірки цілісності, достовірності та авторства електронних архівів. Також необхідно описати процедуру перевірки цілісності, достовірності та авторства даних на носіях інформації під час копіювання електронних документів на/з цих носіїв. Рекомендуємо зазначити, які засоби захисту інформації, криптографічні

алгоритми та довжини ключів при цьому використовуються. У випадку використання засобів електронного підпису необхідно також надати копії чинних експертних висновків Держспецзв'язку на ці засоби.

9. Заходи та засоби для виявлення, запобігання, протидії шахрайству та несанкціонованим операціям

Рекомендуємо надати короткий опис щодо використання організаційних, процедурних заходів безпеки та технічних засобів для виявлення, запобігання, протидії шахрайству та несанкціонованим операціям. При цьому використання деяких заходів та засобів може визначатися окрім положень правил використання електронних грошей також внутрішніми документами банку-емітента, що регулюють питання проведення моніторингу операцій з електронними грошима.

Опис може містити такі складові:

порядок антивірусного захисту;

порядок здійснення резервного копіювання баз даних та інших важливих даних;

порядок блокування та відновлення проведення операцій з електронними грошима;

порядок скасування операцій з електронними грошима (у випадку виявлення технічних, операційних помилок, а також виявлення операцій, що містять ознаки шахрайських дій);

система моніторингу та захисту від проникнень у внутрішній мережі;

система виявлення несанкціонованих операцій;

система сповіщення про виявлені загрози;

системи збору та збереження журналів реєстрації поведінки складових програмно-апаратних комплексів;

система збору та збереження журналів успішної або не успішної авторизації;

система контролю цілісності системних файлів;

система синхронізації точного часу тощо.

Перелік законодавчих та нормативно-правових актів України, які необхідно використовувати під час розроблення правил використання електронних грошей

Закони України:

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

Нормативно-правові акти:

- Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 (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 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).