Типові зауваження до документів, що подаються до Національного банку України з метою узгодження правил використання електронних грошей, в частині захисту інформації

Зауваження 1: В правилах використання електронних грошей (далі – Правила) здійснюється посилання на нормативно-правові акти, що втратили чинність, або використовуються терміни, що містяться в скасованих нормативно-правових актах.
Коментар: В Правилах необхідно здійснювати посилання тільки на чинні нормативно-правові акти або робити загальні посилання, наприклад: "відповідно до чинного законодавства України". Часто помилково використовуються поняття "ЕЦП", "ЦСК" та інші терміни із Закону України "Про електронний цифровий підпис", який втратив чинність 07.11.2018.

Зазначаємо, що 07.11.2018 набрав чинності Закон України "Про електронні довірчі послуги". Цей Закон запроваджує поняття "кваліфікований електронний підпис" та "удосконалений електронний підпис", які замінили поняття "електронний цифровий підпис". Під час розроблення Правил необхідно звертати увагу на чинність нормативно-правових актів та застосовувати терміни і поняття, визначені чинними нормативно-правовими актами.

Зауваження 2: Врахувати в правилах використання електронних грошей та Інформаційній довідці той факт, що відповідність вимогам стандарту PCI DSS стосується лише забезпечення збереження даних держателів платіжних карток і не гарантує збереження даних по операціям з електронними грошима.
Коментар: Досить частою помилкою банків є те, що, створюючи систему електронних грошей, вони не приділяють увагу вимогам безпеки, помилково вважаючи, що наявність сертифікату PCI DSS автоматично закриває будь-які проблеми із захистом інформації під час використання електронних грошей.

Для розроблення Правил пропонуємо користуватися документом "Рекомендації для підготовки документів, що подаються до Національного банку України з метою узгодження правил використання електронних грошей, в частині захисту інформації".

Зауваження 3: Відповідно до вимог пункту 5.3 розділу 5 Положення про електронні гроші в Україні, затвердженого постановою Правління Національного банку України від 04.11.2010 № 481 (далі – Положення про електронні гроші), для кожного типу інформаційних потоків, які визначені Правилами, необхідно надати опис системи захисту інформації, що застосовується банком-емітентом електронних грошей (далі – банк-емітент) для забезпечення безперервного захисту інформації під час випуску, використання та погашення електронних грошей на всіх етапах їх формування, оброблення, передавання і зберігання.
Коментар: Відповідно до підпункту 2 пункту 2 розділу 6 Положення про електронні гроші банк-емітент повинен надати в Правилах інформацію щодо порядку здійснення операцій між емітентом, оператором, агентами, користувачами та торговцями, який має містити загальну схему всіх інформаційних потоків. Згідно з пунктом 5.3 розділу 5 Положення про електронні гроші для кожного типу інформаційних потоків, які визначені Правилами, необхідно надати опис системи 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.

Така система захисту інформації може складатися із захисту мережі за допомогою захищених мережевих протоколів та захисту даних, що передаються по мережі. Також часто банки-емітенти замість правил використання електронних грошей фактично подають опис порядку діяльності оператора послуг платіжної інфраструктури, який надає інформаційні або технологічні послуги. Фактично наданий опис захисту інформації стосується лише

інформаційних зв'язків Оператора з іншими суб'єктами операцій з електронними грошима і не місить опису інших зв'язків, наприклад, обміну інформацією між користувачами та програмно-технічними комплексами самообслуговування агентів.

Особливу увагу слід приділити опису зв'язку між оператором послуг платіжної інфраструктури та банком-емітентом електронних грошей, оскільки Правила подає виключно банк-емітент і в нього є вся інформація щодо побудови такого інформаційного зв'язку.

Зауваження 4: В Правилах не конкретизовані вимоги до захисту інформації на ланках обміну інформаційними повідомленнями.
Коментар: Типовою є ситуація, коли в Правилах замість конкретних вимог до захисту інформації на певних ланках інформаційних повідомлень наявні лише фрази загального характеру. Наприклад: "забезпечується високий рівень захисту", "інформація шифрується за допомогою надійних алгоритмів", "захист інформації на цій ланці здійснюється відповідно до міжнародної практики та законодавства України".

В Правилах необхідно конкретизувати вимоги до захисту інформації на всіх ланках обміну інформаційними повідомленнями, вказати алгоритми, методи захисту інформації. Рекомендації щодо вимог до захисту інформації зазначені в документі "Рекомендації для підготовки документів, що подаються до Національного банку України з метою узгодження правил використання електронних грошей, в частині захисту інформації".

Зауваження 5: В Правилах відсутній порядок реєстрації уповноважених працівників банка-емітента і Оператора та отримання ними персоналізованих логінів і початкових паролів доступу до програмно-апаратних комплексів Оператора.
Коментар: Відповідно до підпункту 2 пункту 2 розділу 6 Положення про електронні гроші банк-емітент має надати в Правилах інформацію про систему розмежування прав доступу до інформаційних ресурсів під час використання електронних грошей. Рекомендується надати в Правилах порядок доступу до програмно-апаратних комплексів, що здійснюють облік електронних грошей, різних категорій осіб: користувачів, відповідальних осіб агентів, працівників, які адмініструють програмно-апаратні комплекси.

Зауваження 6: В правилах використання електронних грошей відсутній порядок встановлення та заміни паролів користувачів, уповноважених осіб агентів, відсутні вимоги щодо парольної політики.
Коментар: З метою забезпечення розмежування прав доступу до інформаційних ресурсів під час використання електронних грошей одним із способів автентифікації користувачів або уповноважених осіб агентів може використовуватися автентифікація за допомогою паролів. В такому випадку необхідно в Правилах передбачити процедури одержання початкового паролю, передачі паролів та їх заміни. Рекомендується передбачити зберігання в програмно-апаратних комплексах інформаційних ресурсів не самого паролю, а ґеш-функції від нього з додаванням певної додаткової інформації ("солі"). Також необхідно розробити парольну політику для уникнення використання слабких паролів.

Зауваження 7: В Правилах не визначені основні вимоги щодо розмежування прав доступу до програмно-технічного комплексу Оператора в частині того, які функціональні ролі забороняється поєднувати одному користувачу (посадовій особі Оператора).
Коментар: Відповідно до підпункту 2 пункту 2 розділу 6 Положення про електронні гроші банк-емітент має надати в Правилах інформацію про систему розмежування прав доступу до інформаційних ресурсів під час використання електронних грошей. Інформація про систему розмежування прав доступу має включати в себе правила поєднання різних функціональних ролей посадових осіб Оператора, які здійснюють функції обліку електронних грошей.

Зауваження 8: Під час виконання операцій з електронними грошима та зберігання інформації щодо таких операцій не передбачено перевірку цілісності інформації.
Коментар: Відповідно до вимог пункту 5.2 розділу 5 Положення про електронні гроші банк-емітент зобов'язаний забезпечити фіксування всіх трансакцій електронних грошей між користувачами, торговцями, агентами, емітентом і Оператором за допомогою технічних засобів, а також зберігання інформації щодо них у формі, яка дозволяє перевірити цілісність інформації. Банк-емітент повинен надати опис процедури перевірки цілісності як окремих трансакцій, так і загальної інформації щодо всіх здійснених трансакцій.

Зауваження 9: В Правилах містяться помилки в описі криптографічних алгоритмів або протоколів.
Коментар: В описах захисту інформації на кожній ланці обміну інформаційними повідомленнями зустрічаються помилки, пов'язані з поняттями щодо захисту інформації та криптографії. Наприклад, криптографічний алгоритм ґешування (ґеш-функцію) SHA-1 визначено як "асиметричний криптографічний алгоритм", асиметричний алгоритм шифрування RSA названо "симетричним алгоритмом блочного шифрування", довжина ключів криптографічного алгоритму вказана не правильно (не передбачена стандартами для цього алгоритму). З метою зменшення помилок та спрощення процедури погодження документів рекомендується не надавати блок-схеми криптографічних алгоритмів, опис алгоритмів, якщо вони вже описані у відповідних стандартах, або якщо оператор послуг платіжної інфраструктури не є їх розробником.

Зауваження 10: Правила використання електронних грошей не містять положень щодо забезпечення безперервності захисту інформації під час використання електронних грошей.
Коментар: Відповідно до вимог пункту 5.3 розділу 5 Положення про електронні гроші банк-емітент має здійснювати безперервний захист інформації під час випуску, використання та погашення електронних грошей на всіх етапах її формування, оброблення, передавання і зберігання. Опис системи захисту інформації повинен включати в себе захист інформації на кожній ланці обміну інформаційними потоками.

Однією з типових помилок є використання проміжної ланки при взаємодії між користувачем та інформаційними системами, що здійснюють облік інформації по операціям з електронними грошима. На цій проміжній ланці можлива модифікація інформації без погодження з користувачем. Тому пропонуємо не використовувати проміжні ланки під час такої взаємодії або, якщо такі ланки використовуються, забезпечити їх захист від атаки "людина посередині".

Також правила використання електронних грошей повинні містити опис захисту інформації щодо операцій з електронними грошима від навмисної чи ненавмисної модифікації під час передачі та зберігання такої інформації.

Зауваження 11: Правилами використання електронних грошей передбачено зберігання електронних документів на носіях інформації, однак не надано опис порядку проведення перевірки цілісності, достовірності та авторства даних на цих носіях під час копіювання та зберігання електронних документів відповідно до вимог статті 19 Закону України "Про платіжні системи та переказ коштів в Україні".
Коментар: Стаття 19 Закону України "Про платіжні системи та переказ коштів в Україні" передбачає, що електронні документи зберігаються на носіях інформації у формі, що дозволяє перевірити цілісність, достовірність та авторство електронних документів на цих носіях. Крім того, при копіюванні електронного документа з носія інформації обов'язково має бути виконана перевірка цілісності, достовірності та авторства даних на цьому носії. Банк-емітент повинен передбачити виконання такої перевірки та надати її опис.

Також 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, визначено, що для криптографічного захисту інформації, вимога щодо захисту якої встановлена законом, повинні використовуватися засоби, що мають чинний експертний висновок Держспецзв'язку.

Зауваження 12: В правилах електронних грошей міститься інформація щодо використання користувачами системи електронних платежів Національного банку (СЕП), яка не є частиною системи електронних грошей банка-емітента.
Коментар: Окремі банки-емітенти в систему розрахунків електронними грошима включають використання платіжних систем, наприклад, міжнародних карткових платіжних систем або державної системи електронних платежів – СЕП. Однак надавати в Правилах або Інформаційній довідці інформацію щодо роботи цих платіжних систем не потрібно. Адже такі платіжні системи повинні мати власну ліцензію одержану від Національного банку України. В цьому випадку правила роботи таких платіжних систем вже розглянуто під час їх погодження.

Зауваження 13: В Правилах не вказано, яким чином забезпечується виконання вимог до умов експлуатації засобу захисту мережі.
Коментар: Під час побудови захисту інформації в системі розрахунків електронними грошима банк-емітент повинен передбачити безперервність захисту інформації на всіх етапах її передавання та зберігання. Для цього можуть використовуватися технічні засоби захисту інформації. Надійність таких засобів підтверджується свідоцтвом, сертифікатом відповідності або експертним висновком, виданими компетентними органами. Зазвичай у сертифікаційних документах вказуються вимоги до умов експлуатації цих засобів, до яких входить порядок налаштування та використання.

Відповідно до вимог пункту 5.3 розділу 5 Положення про електронні гроші, банк-емітент електронних грошей зобов'язаний забезпечити запровадження організаційних, процедурних заходів та використання технічних засобів з метою виявлення, запобігання, перешкоджання та протидії шахрайству. Тому банк-емітент має передбачити запровадження таких організаційних та процедурних заходів. Також необхідно надати їх опис, зокрема опис щодо виконання вимог до умов експлуатації засобу захисту мережі.

Зауваження 14: В Правилах не надано опис захисту вебсерверу від атак із зовнішньої мережі та захисту внутрішньої мережі Оператора у випадку успішної зовнішньої атаки на вебсервер.
Коментар: Розповсюдженим способом забезпечення можливості використання електронних грошей є надання користувачам електронних грошей доступу до свого облікового запису через вебсайт або за допомогою вебсервісів. В такому випадку вебсервер повинен бути доступним із мереж загального користування і має бути забезпечено захист цього вебсерверу від атак з таких мереж.

Якщо вебсервер розміщений у внутрішній мережі Оператора, суттєво спрощується можливість здійснення атак на внутрішню мережу Оператора з використанням цього вебсерверу. З метою усунення такої вразливості необхідно передбачити використання засобів захисту мережі між вебсервером та іншими серверами Оператора у внутрішній мережі, тобто передбачити розміщення вебсерверу в окремій демілітаризованій зоні.

Відповідно до вимог 5.3 розділу 5 Положення про електронні гроші, банк-емітент електронних грошей зобов'язаний забезпечити запровадження організаційних, процедурних заходів та використання технічних засобів з метою виявлення, запобігання, перешкоджання та протидії шахрайству. Тому в Правилах необхідно надати опис засобів та технологій захисту вебсерверу від зовнішніх мережевих атак.

Зауваження 15: Надана Інформаційна довідка про принципи технічної реалізації здійснення розрахунків із використанням електронних грошей не відповідає правилам використання електронних грошей.
Коментар: Пунктом 2 розділу 6 Положення про електронні гроші передбачено узгодження з Національним банком двох документів: Інформаційної довідки про принципи технічної реалізації здійснення розрахунків і правил використання електронних грошей. Досить часто зустрічається ситуація, коли вказані документи не відповідають один одному. Така невідповідність може полягати у використанні різної термінології для одних і тих же понять або використанні одного терміну для різних понять, у несумісності схем інформаційних потоків, різному порядку взаємодії суб'єктів тощо.

Зауваження 16: В описі HTTPS-з'єднання не вказано параметри шифрування (алгоритм ґешування, ключ шифрування та його довжину, не зазначено видавців сертифікатів).
Коментар: Сам по собі протокол HTTPS не забезпечує надійності захисту інформації без використання стійких до атак криптографічних алгоритмів. Тому у випадку використання цього протоколу необхідно вказати також його параметри.

Зауваження 17: В Правилах не вказано версію протоколу SSL/TLS.
Коментар: SSL/TLS є сімейством протоколів, яке час від часу доповнюється новими версіями, що враховують виявлені нові типи атак на такий протокол. Виходячи з цього, необхідно використовувати (та вказувати це в Правилах) мінімально допустиму версію цього протоколу. Це має бути версія TLS не нижче 1.2.

Зауваження 18: Поданий пакет документів оформлено неналежним чином.
Коментар: Часто буває ситуація, коли подані пакети документів не можуть бути проаналізовані на відповідність чинному законодавству України з технічних причин. Зокрема:

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

– при друкуванні схем, що на екрані виглядають якісно, друкуються з відображенням окремих частин, в неправильному кодуванні тощо (це – наслідок використання неправильного формату при збереженні документів);

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

– наявні посилання на неіснуючі в документі пункти або сторінки;

– помилково замість актуальних подано застарілі версії документів.