АКЦІОНЕРНЕ ТОВАРИСТВО
«АКЦІОНЕРНИЙ БАНК «РАДАБАНК»

ЗАТВЕРДЖЕНО

Рішенням Правління АТ «АБ «РАДАБАНК»

Протокол від 16 липня 2019 р. №44/1

Голова Правління

_____ С.Б. Стоянов

ПОРЯДОК
виявлення змін в електронному документі та змін електронного підпису після підписання електронного документа

м. Дніпро
2019 р.

1. Вступ

Порядок виявлення змін в електронному документі та змін електронного підпису після підписання електронного документа (далі – Порядок) описує загальні процедури та покрокові дії під час виконання перевірок електронних документів на предмет виявлення будь-яких можливих змін після накладання електронного підпису та дії під час виконання перевірок на предмет виявлення будь-яких можливих змін в електронних підписах після підписання електронних документів в АТ «АБ «РАДАБАНК».

Порядок розроблено з урахуванням вимог чинного законодавства України та нормативно-правових актів Національного банку України.

Порядок затверджується Головою Правління Банку після погодження документу на засіданні Правління Банку. Банк забезпечує безперешкодний доступ до Порядку своїх клієнтів та потенційних клієнтів Банку.

2. Терміни та визначення

В Порядку використовуються наступні терміни та визначення:

Банк – АКЦІОНЕРНЕ ТОВАРИСТВО «АКЦІОНЕРНИЙ БАНК «РАДАБАНК»;

Електронні дані – будь-яка інформація в електронній формі;

Електронний документ (ЕД) – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов‘язкові реквізити документа (стаття 5 розділ II Закону України «Про електронні документи та електронний документообіг», Відомості Верховної Ради України (ВВР), 2003, №36, ст.275);

Електронний підпис (ЕП) – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис;

Кваліфікований надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;

КЕП Банку – кваліфікована електронна печатка Банку;

НБУ – Національний Банк України;

Підписувач (автор документу) – особа, яка здійснює накладання електронного підпису на електронний документ;

Принцип – при характеристиці різноманітних систем принципи відображають ті суттєві характеристики, що відповідають за правильне функціонування системи, без яких вона не виконувала б свого призначення;

Програмне забезпечення (ПЗ) – сукупність програм системи обробки інформації і програмних документів, необхідних для експлуатації цих програм;

Система Автоматизації Банку (САБ) – призначена для комплексної автоматизації банківської діяльності, є повноцінним інструментом ведення банківського бізнесу та дозволяє автоматизувати широкий спектр бізнес-процесів і фінансових інструментів Банку. Банком використовується САБ «SR–Bank», розробник ТОВ «Софт Ревю Трейд», м.Київ, САБ «Єдине Вікно», розробник АТ «АБ «РАДАБАНК», м.Дніпро;

СЕД – автоматизована система документообігу та управління бізнес-процесами «**AlmexECM**» (розроблена компанією «Алмексофт», м.Київ), скорочена назва - **ІСЕД «AlmexECM»**;

УЕП Банку – удосконалена електронна печатка Банку;

ЦСК АТ «АБ «РАДАБАНК» – «Центр сертифікації ключів «CryptoKDC®» розробки ТОВ «АВТОР».

3. Ціль документа

Ціль Порядку – встановлення порядку дій при роботі з ЕД та ПД, зокрема в частині виявлення будь-яких змін в електронному документі та будь-яких змін ЕП після підписання ЕД з метою забезпечення належного рівня безпеки інформації та дотримання Банком вимог чинного законодавства України при роботі з іншими суб'єктами електронної взаємодії.

4. Сфера застосування

Порядок розповсюджується на всіх співробітників Банку, які згідно своїх посадових обов'язків працюють з ЕД, ЕП, кваліфікованою електронною печаткою та удосконаленою електронною печаткою, а саме:

– оброблюють ЕД, які отримано від контрагентів Банку з використанням кваліфікованого ЕП, удосконаленого ЕП чи ЕП Національного банку;

– оброблюють ЕД, які отримано від контрагентів Банку з використанням кваліфікованого ЕП (на підставі договорів між Банком та підписувачем, які можуть бути укладені як у вигляді паперового так і електронного документу);

– використовують в своїй роботі кваліфіковані та/або удосконалені електронні печатки Банку.

5. Предмет документа та опис дій

5.1. Опис принципів використання кваліфікованого ЕП.

5.1.1. Види ЕП

Використовуючи більш спрощені визначення, не беручі до уваги формальні визначення, види електронних підписів для накладання на електронні документи можна описати наступним чином:

1. Електронний підпис – це будь-яка електронна форма даних, що використовується підписувачем як підпис, і не обов'язково захищений.

2. Удосконалений електронний підпис – це підпис, сформований з використанням засобів криптографії, але при цьому не обов'язково з використанням сертифіката, а якщо й з використанням, то не обов'язково, щоб сертифікат був кваліфікованим.

3. Кваліфікований електронний підпис – має бути заснований на криптографії, і відкритий ключ має бути підтверджений сертифікатом, і сам сертифікат повинен бути кваліфікованим. Кваліфікований ЕП може бути накладений з використанням особистого ключа отриманого виключно у кваліфікованих надавачів електронних довірчих послуг.

Крім електронного підпису, Закон України «Про електронні довірчі послуги» запроваджує поняття й електронної печатки. Електронна печатка також може бути удосконаленою та кваліфікованою – критерії видів цих електронних печаток аналогічні відповідним критеріям видів електронних підписів. Відмінність полягає в тому, що електронним підписом може користуватися як юридична, так і фізична особа, а електронною печаткою – тільки юридична особа. У функціональному ж змісті суттєвої різниці між електронним підписом і

електронною печаткою немає.

5.1.2. Забезпечення цілісності та автентичності

Застосування кваліфікованого ЕП при електронній взаємодії дозволяє здійснити:

1) Контроль цілісності переданого ЕД – при будь-якій випадковій або навмисній зміні ЕД електронний підпис стане недійсним, тому що він обчислений на підставі вихідного стану початкового ЕД і відповідає лише йому;

2) Захист від змін (підроблення) ЕД – гарантія виявлення підробки при контролі цілісності робить підроблення недоцільним у більшості випадків;

3) Неможливість відмовитись від авторства – створення коректного кваліфікованого ЕП можливе виключно з використанням особистого ключа, а він повинен бути відомим виключно власнику особистого ключа (підписувачу). Відповідно підписувач не може відмовитись від свого ЕП під ЕД;

Електронний підпис є певною послідовністю символів, отриманою в результаті певного перетворення початкового ЕД за допомогою спеціального ПЗ. Будь-яка зміна вихідного ЕД робить ЕП недійсним, а на практиці він є унікальним для кожного ЕД і не може бути перенесений на інший ЕД.

5.1.3. Забезпечення надійності кваліфікованого ЕП

Забезпечення надійності кваліфікованого ЕП здійснюється залученням до процесу отримання особистих ключів, накладання кваліфікованого ЕП та перевірки його дійсності – кваліфікованих надавачів електронних довірчих послуг.

При розгляді даного питання особливу увагу слід приділити термінам «особистий ключ» та «сертифікат». Криптографічний захист електронних підписів заснований, як правило, на шифруванні, яке передбачає використання пари «відкритий ключ – особистий ключ». Відкритий ключ доступний для кореспондентів і для підписувача, а особистий ключ має перебувати тільки в підписувача (ця асиметрія між ключами, до речі, і лежить в основі терміна «асиметричне криптографічне перетворення»). При цьому пара цих ключів створюється таким чином, що присвоїти електронному документу електронний підпис можна тільки за допомогою особистого ключа, але перевірити підпис можна за допомогою відкритого ключа, що відповідає особистому ключу. Кореспондент, отримавши документ з удосконаленим ЕП, може, у загальному випадку, покладатися на те, що це присвоєння було зроблено власником особистого ключа. Крім того, під час створення підпису відбувається співвіднесення даних про документ і даних, що містяться в самому підписі, таким чином, що якщо після підписання змінити в документі що-небудь, то він перестане відповідати підпису й кореспондент має змогу це виявити.

Для мінімізації такого ризику, у схему було введено ще один елемент: третя сторона, яка перевіряє особу підписувача й, упевнившись, що дані відкритого ключа відповідають особистим даним підписувача, видає «сертифікат» – спеціальний набір даних, асоційований із відкритим ключем, що засвідчується. В цьому разі кореспондент, одержавши підписаний електронний документ, який пов’язаний не тільки з відкритим ключем, а і з сертифікатом, може покладатися на те, що особа, яка застосувала кваліфікований електронний підпис, є тим, чий це електронний підпис. При цьому якщо згадана третя сторона – засвідчувач внесена до спеціального Довірчого списку, то сертифікат, що видається нею, є кваліфікованим сертифікатом, і сама вона має статус кваліфікованого надавача електронних довірчих послуг. Слід зауважити, що Закон України «Про електронні довірчі послуги» спеціально наголошує на ідентифікації – її проведення обов'язкове, якщо відповідна послуга є кваліфікованою.

5.1.4. Принцип створення ЕД з накладанням кваліфікованого ЕП

При підписанні ЕД його початковий зміст не змінюється, а додається блок даних, так званий «Електронний підпис». Отримання цього блоку можна розділити на два етапи:

1) На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток документу». Цей відбиток має такі властивості:

– фіксовану довжину, незалежно від довжини документу;
– унікальність відбитку для кожного документу;
– неможливість відновлення документу за його відбитком.

Таким чином, якщо ЕД був модифікований, то зміниться і його відбиток, що відобразиться при перевірці накладеного кваліфікованого ЕП.

2) На другому етапі відбиток електронного документу шифрується за допомогою програмного забезпечення і особистого ключа підписувача (автора). Розшифрувати кваліфікований ЕП і одержати початковий відбиток, який відповідатиме даному документу, можна тільки використовуючи «сертифікат» відкритого ключа підписувача.

Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем підписувача підтверджує авторство електронного документу.

5.1.5. Принцип перевірки кваліфікованого ЕП створеного ЕД

Перевірка кваліфікованого ЕП створеного ЕД, в результаті виконання процедури підписання ЕД, проводиться декількома етапами:

1) На першому етапі адресат за допомогою спеціалізованого програмного забезпечення «сертифікатом» відкритого ключа підписувача розшифровує підписаний відбиток документу і одержує відбиток початкового документа (оригінального ЕД на який підписувач власноручно з використанням особистого ключа наклав кваліфікований ЕП);

2) За допомогою програмного забезпечення і спеціальної математичної функції з документу, який був одержаний (мається на увазі ЕД з накладеним кваліфікованим ЕП), обчислюється його відбиток;

3) При перевірці кваліфікованого ЕП порівнюються відбитки початкового і одержаного електронних документів. Результат виконання такої перевірки може бути лише одна з відповідей: «вірний» чи «невірний».

Для повноцінного функціонування системи електронної взаємодії, у т.ч. перевірки належності відкритого ключа відповідному підписувачу, Банк використовує спеціальні захищені довідники сертифікатів відкритих ключів, які ведуться кваліфікованими надавачами електронних довірчих послуг, як то АЦСК Органів Юстиції України, АЦСК «Україна», АЦСК ІДД ДФС, АЦСК ПАТ «НДУ», тощо.

5.2. Порядок виявлення будь–яких змін в електронному документі.

Перевірка цілісності ЕД проводиться шляхом перевірки ЕП підписувача (ст. 12 Закону України «Про електронні документи та електронний документообіг»).

Процес виявлення наявності будь-яких змін в ЕД у разі необхідності здійснюється Банком з використанням відповідного програмного забезпечення в якому є відповідні «інструменти» для виконання такої перевірки. Процедури використання таких «інструментів» визначаються розробником програмного забезпечення.

За допомогою «інструментів» виконується перевірка ЕП (в друкованій копії такого

ЕД це поле може мати назву «штам», «сертифікат» чи відображатись як інша унікальна послідовність символів), що має наступні особливості:

– ЕП має фіксовану довжину незалежно від обсягу інформації в ЕД. Довжина підпису визначається розробником програмного забезпечення;

– унікальність ЕП для кожного ЕД всередині всієї інформаційної системи електронної взаємодії. ЕП нерозривно пов'язаний з конкретним документом і тільки з ним;

– неможливість відновлення секретного ключа чи інших таємних компонентів по ЕП на ЕД;

– тощо.

Накладений ЕП дозволяє здійснити контроль цілісності кожного ЕД, оскільки при будь-якій випадковій або навмисній зміні електронного документа, ЕП стане недійсним, тому що він (електронний підпис) обчислений на підставі вихідного стану документа і відповідає лише йому.

Відповідно, якщо ЕД був модифікований, то перевірка цілісності цього ЕД виявить невідповідність накладеному ЕП, що буде свідчить про негативний результат – відповідь «невірний» (див. підпункт 3 пункту 5.1.5. Порядку). Такий ЕД буде вважатися не дійсним. Позитивний результат перевірки цілісності ЕД – відповідь «вірний» (див. підпункт 3 пункту 5.1.5. Порядку) буде підтвердженням відсутності будь-яких змін у створеному і підписаному (за допомогою електронного підпису) електронному документі.

5.3. Порядок виявлення будь-яких змін ЕП після підписання ЕД.

5.3.1. Принципи виявлення будь-яких змін ЕП після підписання ЕД

Оскільки ЕП, як було зазначено раніше, це якась послідовність символів, яка отримана в результаті певного перетворення початкового документа (або будь-якої іншої інформації в електронному вигляді) за допомогою спеціального програмного забезпечення, то будь-яка зміна вихідного документа робить ЕП недійсним, а на практиці він є унікальним для кожного ЕД і не може бути перенесений на інший ЕД. Неможливість підробки ЕП забезпечується дуже великим обсягом математичних обчислень, необхідних для його підбору. Таким чином, при отримані документа, підписаного ЕП, одержувач може бути впевненим у авторстві і незмінності змісту даного документа.

Аналіз можливостей підробки ЕП називається криптоаналіз. Спробу сфальсифікувати підпис або підписаний ЕД криптоаналітики називають «атака». На даний момент часу актуальними є наступні моделі атак:

– атака з використанням відкритого ключа. Криптоаналітик має тільки відкритий ключ;

– атака на основі відомих ЕД з накладеним ЕП. Криптоаналітик володіє допустимими підписами набору ЕД, які йому відомі, але які він не має змоги обрати сам;

– адаптивна атака на основі вибраних ЕД. Криптоаналітик може отримати підписи ЕД, які він обирає сам.

Саме особистий ключ є найбільш вразливим компонентом всієї криптосистеми ЕП. Шахрай, який може заволодіти особистим ключем підписувача, може створити дійсний цифровий підпис будь-якого ЕД від імені цього підписувача, але при умові що знатиме пароль доступу до особистого ключа. Тому в Банку особлива увага приділяється способам зберігання особистих ключів – всі особисті ключі які використовуються Банком зберігаються на захищених носіях ключової інформації, а паролі доступу до особистих ключів відомі виключно власникам таких ключів.

5.3.2. Порядок виявлення будь-яких змін ЕП після підписання ЕД з використанням сертифікату відкритого ключа підписувача.

У Банку при роботі з ЕД на які накладено кваліфікований ЕП встановлений наступний порядок виявлення будь-яких змін ЕП після підписання ЕД:

1) При роботі з ЕД якими обмінюються через інформаційну систему «Мій електронний документ» (ІС «M.E.Doc») відповідальні співробітники Банку, за допомогою штатних «інструментів» у ІС «M.E.Doc» перевіряють, чи дійсно ЕП відповідає документу та відкритому ключу, зазначеному у сертифікаті. За наявності будь-яких змін в ЕП результати перевірки вважаються негативними і такий ЕД визначається Банком не дійсним. Позитивний результат підтверджує цілісність ЕП;

2) При роботі з ЕД якими обмінюються із використанням звичайного файлообміну відповідальні співробітники Банку, за допомогою штатних «інструментів» офіційного Інтернет-ресурсу «АЦСК Органів Юстиції України» https://ca.informjust.ua/verify або спеціалізованого ПЗ «Користувач АЦСК ІДД ДФС» наданого АЦСК ІДД ДФС перевіряють, чи дійсно ЕП відповідає документу та відкритому ключу, зазначеному у сертифікаті. За наявності будь-яких змін в ЕП результати перевірки вважаються негативними і такий ЕД визначається Банком не дійсним. Позитивний результат підтверджує цілісність ЕП;

3) При роботі з ЕД в інформаційній системі електронного документообігу «AlmexECM» достовірність електронного підпису перевіряється штатними «інструментами» ІСЕД «AlmexECM» у автоматичному режимі. При цьому перевірка відповідності ЕП відкритому ключу здійснюється з використанням довідника сертифікатів відкритих ключів ЦСК АТ «АБ «РАДАБАНК»;

4) При роботі з ЕД в системі дистанційного обслуговування рахунків «ВЕБ-банкінг для корпоративних клієнтів» достовірність електронного підпису перевіряється штатними «інструментами» у автоматичному режимі. При цьому перевірка відповідності ЕП відкритому ключу здійснюється з використанням довідника сертифікатів відкритих ключів серверу СДОР Банку.

5.3.3. Порядок виявлення будь-яких змін ЕП після підписання ЕД без використання сертифікату відкритого ключа підписувача.

Банк за допомогою «інструментів» у спеціалізованого програмному забезпеченню здійснює перевірку простого ЕП підписувача у автоматичному режимі згідно з процедурою, передбаченою у договорі між Банком і підписувачем. За результатами перевірки підтверджується відповідність простого ЕП певному ЕД.

За допомогою програмно-технічних комплексів, в яких здійснюється створення, обробка та зберігання ЕД клієнтів Банку (фізичних осіб, які не є суб‘єктами підприємницької діяльності) Банк забезпечує цілісність, достовірність та авторство електронного документа, на який накладено простий ЕП, який забезпечує однозначну ідентифікацію особи підписувача. У разі необхідності за допомогою «інструментів» у спеціалізованому програмному забезпеченню в будь-який час можна виконати перевірку відповідності простого ЕП конкретному ЕД з чітким визначенням дати та часу накладання простого ЕП та чіткої ідентифікації особи підписувача.

Вся службова інформація (електронні дані в базах даних, логи, протоколи, тощо), що стосується створення, оброблення, зберігання таких ЕД надійно захищена від модифікації та доступність до неї чітко регламентується вимогами Системи управління інформаційною безпекою Банку.

6. Ролі та відповідальності

Всі співробітники Банку, які обробляють ЕД з накладеними ЕП для виконання своїх посадових обов‘язків, повинні дотримуватись процедур даного Порядку, інших внутрішніх нормативних документів Банку та чинного законодавства України і несуть особисту відповідальність за їх порушення.

Співробітники відділу інформаційної безпеки та Адміністратори інформаційної безпеки Банку (які призначені виконувати свої функціональні обов‘язки згідно Наказів керівництва Банку) відповідають за підтримку стабільної роботи інформаційних систем і виконання належного контролю за дотриманням співробітниками вимог даного Порядку для забезпечення своєчасного виявлення недоліків чи слабких місць та їх швидке усунення.

Керівництво Банку здійснює всебічну підтримку для забезпечення стабільного та безвідмовного функціонування інформаційних систем, в яких виконується робота з ЕД, для забезпечення необхідного рівня конфіденційності та інформаційної безпеки відповідно до вимог Системи управління інформаційною безпекою Банку.

7. Перегляд документу

Порядок переглядається за необхідністю. Причинами внесення змін до Порядку є зміни в інформаційної інфраструктурі та/або впровадженні нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах, що стосуються застосування ЕП та обігу ЕД.