



ЗАТВЕРДЖЕНО
Рішенням Правління
АТ «ТАСКОМБАНК»
Протокол № 36-7
від « 03 » вересня 2019 р.
Голова Правління
АТ «ТАСКОМБАНК»



А.В.Комаріст

**ПОЛОЖЕННЯ
ПРО ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПИСУ В
АКЦІОНЕРНОМУ ТОВАРИСТВІ «ТАСКОМБАНК»**

ЗМІСТ

	ЗМІСТ	2
1.	ЗАГАЛЬНІ ПОЛОЖЕННЯ.....	3
2.	ГЛОСАРІЙ	3
3.	МЕТА ДОКУМЕНТА.....	4
4.	СФЕРА ЗАСТОСУВАННЯ	4
5.	ВИМОГИ ЩОДО ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПISУ ТА ЕЛЕКТРОННОЇ ПЕЧАТКИ	4
6.	ПОРЯДОК ОТРИМАННЯ/ВІДКЛИКАННЯ КВАЛІФІКОВАНИХ ЕП ПРАЦІВНИКАМИ БАНКУ	6
7.	СТВОРЕННЯ І ЗАСВІДЧЕННЯ ЕЛЕКТРОННОЇ КОПІЇ З ПАПЕРОВОГО ДОКУМЕНТА	6
8.	СТВОРЕННЯ І ЗАСВІДЧЕННЯ КОПІЇ НА ПАПЕРІ З ЕЛЕКТРОННОГО ДОКУМЕНТА	7
9.	ВИЯВЛЕННЯ БУДЬ-ЯКИХ ЗМІН В ЕЛЕКТРОННОМУ ДОКУМЕНТІ ТА ЗМІН ЕП ПІСЛЯ ПІДПИСАННЯ В ЕЛЕКТРОННОМУ ДОКУМЕНТІ	7
10.	КОНТРОЛЬ І ВІДПОВІДАЛЬНІСТЬ	7
11.	ЗАКЛЮЧНІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ	8
12.	ДОДАТКИ	8

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про використання електронного підпису в АКЦІОНЕРНОМУ ТОВАРИСТВІ «ТАСКОМБАНК» (далі – Положення) визначає процедури видачі, використання, відкликання кваліфікованого, удосконаленого і простого електронних підписів співробітників і/або клієнтів АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» (далі – Банк).

1.2. Положення розроблене з метою регламентації дій та процедур, направлених на забезпечення роботи з електронними підписами.

1.3. Банк використовує криптографічні алгоритми та протоколи, які затверджено державними та міжнародними стандартами.

1.4. Це Положення розміщується на внутрішньому та зовнішньому сайтах Банку та повинно бути доступним для існуючих та потенційних клієнтів Банку.

1.5. Вимоги цього Положення узгоджуються з Політикою інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» та Положенням про криптографічний захист інформації в АКЦІОНЕРНОМУ ТОВАРИСТВІ «ТАСКОМБАНК».

1.6. Положення розроблено відповідно до вимог чинного законодавства України, нормативно-правових документів Національного банку України. Нормативна база зазначена в Паспорті документу, в Додатку 1 «Паспорт внутрішнього документа нормативного характеру».

1.7. Паспорт документу наведено в Додатку 1 – «Паспорт внутрішнього документа нормативного характеру»

2. ГЛОСАРІЙ

2.1. Терміни та скорочення, що вживаються в цьому документі, використовуються в значеннях, визначених Законом України «Про електронні довірчі послуги» та Положенням про застосування електронного підпису в банківській системі України.

ВК – відкритий ключ.

ТК – таємний (або особистий) ключ.

ТВК – таблиця відкритих ключів.

Компрометація особистого ключа - будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа.

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

Удосконалений ЕП - електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис.

Кваліфікований ЕП - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа.

Електронна ідентифікація — процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи.

Криптобібліотеки – бібліотеки криптографічних функцій – накладання та перевірки електронного підпису, шифрування та дешифрування інформації.

Засіб кваліфікованого електронного підпису чи печатки - апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують

криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам цього Закону.

Контрагент банку - будь-яка юридична чи фізична особа, яка має з банком відносини фінансового характеру. Контрагент може одночасно мати з банком відносини іншого характеру, зокрема трудові.

Підписувач – фізична особа, яка створює електронний підпис.

АЦСК – акредитований центр сертифікації ключів – кваліфікований надавач електронних довірчих послуг, що внесений у перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються (так званий Довірчий список).

3. МЕТА ДОКУМЕНТА

- 3.1. Метою Положення є впорядкування та визначення наступних процедур:
- створення і засвідчення копій з електронних та паперових документів;
 - виявлення будь-яких змін в електронному документі
 - виявлення будь-яких змін ЕП після підписання електронного документа;
 - роботи з удосконаленим електронним підписом;
 - визначення бізнес-процесів в яких використовується ЕП;
 - визначення мінімальних вимог до договорів із контрагентами Банку для взаємодії за допомогою ЕП (простих, удосконалених та кваліфікованих).

4. СФЕРА ЗАСТОСУВАННЯ

4.1. Вимоги цього Положення поширюються на усіх працівників Банку, які у своїй роботі використовують та взаємодіють з електронними підписами.

5. ВИМОГИ ЩОДО ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПISУ ТА ЕЛЕКТРОННОЇ ПЕЧАТКИ

5.1. Електронний документ, підписаний електронним підписом, має таку саму юридичну силу, як і паперовий, який підписала власноруч відповідальна особа.

5.2. Види електронних підписів які застосовуються в Банку: простий електронний підпис, удосконалений електронний підпис, кваліфікований електронний підпис і електронний підпис Національного банку України.

5.3. Порядок використання в Банку електронного підпису Національного банку України визначено в «Інструкції про роботу з засобами захисту інформації Національного банку України в АТ "ТАСКОМБАНК"».

5.4. Вимоги до використання простого ЕП.

- Простий ЕП – це будь-який вид ЕП, крім кваліфікованого ЕП, удосконаленого ЕП, ЕП Національного банку. Може використовуватись фізичними особами, які не є суб'єктами підприємницької діяльності.
- Простий ЕП може використовуватись за умови, що Банк забезпечує доведення цілісності, достовірності та авторства електронного документа із створеним простим ЕП. Бізнес-процеси, у яких використовується простий ЕП, визначаються внутрішніми документами нормативного характеру, що регламентують кожен з цих процесів.
- Фізична особа, яка не є суб'єктом підприємницької діяльності, має право використовувати простий ЕП у разі дотримання таких вимог:
 - електронна взаємодія фізичної особи здійснюється виключно з Банком і з використанням технології, визначеної Банком;
 - використання простого ЕП здійснюється на підставі договору між Банком і клієнтом, який укладається в письмовій формі (у вигляді паперового документа

з власноручними підписами сторін або як електронний документ із кваліфікованим ЕП) після проведення ідентифікації та верифікації клієнта відповідно до вимог законодавства України.

- Простий ЕП має забезпечувати однозначну ідентифікацію особи підписувача.
- Доведення цілісності електронних даних із створеним простим ЕП може забезпечуватися засобами інформаційної системи, у якій здійснюється створення, оброблення, зберігання електронних документів.
- Банк забезпечує доведення цілісності, достовірності та авторства електронного документа із створеним простим ЕП.
- Банк у разі недотримання зазначеної вимоги несе відповідальність за шкоду, заподіяну фізичній особі, яка не є суб'єктом підприємницької діяльності.

5.5. Вимоги до використання удосконаленого ЕП.

- Удосконалений ЕП – служить для ідентифікації клієнтів та працівників Банку, забезпечує авторство та цілісність електронних документів. Може використовуватись на підставі договору між банком і клієнтом, який укладається в письмовій формі.
- Банк та його клієнти під час вчинення правочинів у вигляді електронних документів мають право використовувати удосконалений ЕП на підставі договору у вигляді паперового документа з власноручними підписами сторін або як електронний документ із кваліфікованим ЕП після проведення ідентифікації та верифікації клієнта відповідно до вимог законодавства України. Бізнес-процеси, у яких використовується удосконалений ЕП, визначаються внутрішніми документами нормативного характеру, що регламентують кожен з цих процесів.
- Банк визначає технологію використання удосконаленого ЕП та засоби удосконаленого електронного підпису чи печатки, що використовуються під час взаємодії банку з клієнтом.
- Суб'єкти електронної взаємодії використовують удосконалений ЕП без сертифіката відкритого ключа або чинність відкритого ключа підписувача засвідчується сертифікатом відкритого ключа на договірних засадах, або чинність відкритого ключа підписувача засвідчується надавачем електронних довірчих послуг згідно з вимогами законодавства України у сфері електронних довірчих послуг, нормативно-правових актів Національного банку України.
- Удосконалений ЕП є таким, що пройшов перевірку, якщо перевірку удосконаленого ЕП здійснено згідно з процедурою, зазначеною в договорі, укладеному між учасниками електронної взаємодії.

5.6. Вимоги до використання кваліфікованого ЕП.

- Кваліфікований ЕП створюється з використанням засобу кваліфікованого електронного підпису та базується на кваліфікованому сертифікаті відкритого ключа, що виданий кваліфікованим надавачем електронних довірчих послуг – одним із акредитованих центрів сертифікації ключів (надалі – АЦСК). Використання кваліфікованих ЕП врегульовано Законом України «Про електронні довірчі послуги». Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Укладення окремого договору щодо використання кваліфікованого ЕП не вимагається. Бізнес-процеси, у яких використовується кваліфікований ЕП, визначаються внутрішніми документами нормативного характеру, що регламентують кожен з цих процесів.

5.7. Вимоги до використання удосконаленої електронної печатки.

- Удосконалена електронна печатка – використовується в разі, якщо:
 - потрібно засвідчити дійсність удосконаленого підпису на електронних документах;
 - проставити печатку для засвідчення відповідності копій документів оригіналам;
 - підтвердити повноваження представника юридичної особи на застосування ЕП у контексті, передбаченому документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення)
 - може використовуватись на підставі договору між банком і клієнтом, який

укладається в письмовій формі (у вигляді паперового документа з власноручними підписами сторін або як електронний документ із кваліфікованим ЕП) після проведення ідентифікації та верифікації клієнта відповідно до вимог законодавства України.

5.8. Вимоги до використання кваліфікованої електронної печатки.

- Кваліфікована електронна печатка – використовується в разі, якщо:
 - потрібно засвідчити дійсність кваліфікованого підпису на електронних документах;
 - проставити печатку для засвідчення відповідності копій документів оригіналам;
 - підтвердити повноваження представника юридичної особи на застосування ЕП у контексті, передбаченому документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення). Укладення окремого договору щодо використання кваліфікованої електронної печатки не вимагається.

5.9. Для збереження конфіденційності таємних ключів рекомендується їх зберігання на захищених носіях. Щодо кваліфікованих електронних підписів і кваліфікованих електронних печаток їх створення та зберігання виконується з використанням засобів кваліфікованого електронного підпису.

6. ПОРЯДОК ОТРИМАННЯ/ВІДКЛИКАННЯ КВАЛІФІКОВАНИХ ЕП ПРАЦІВНИКАМИ БАНКУ

6.1. У разі необхідності отримання кваліфікованого ЕП, працівник Банку подає заявку в системі звернень до технічної підтримки, з аргументуванням службової необхідності. В копію ставиться Департамент інформаційної безпеки.

6.2. Відповідальний працівник Департаменту інформаційної безпеки готує пакет документів згідно з вимогами кваліфікованого надавача електронних довірчих послуг та в разі необхідності ініціює сплату рахунків за послуги.

6.3. Документи підписує Голова Правління банку (або особа призначена тимчасово виконуючою обов'язки Голови Правління).

6.4. Працівник отримує у відповідального працівника Департаменту інформаційної безпеки пакет документів з підписом Голови Правління, захищений носій ТК та подальші інструкції щодо генерації ТК.

6.5. Генерація ТК проводиться працівником особисто в представництві кваліфікованого надавача електронних довірчих послуг, відповідно до пункту 2 статті 22 Закону України "Про електронні довірчі послуги".

6.6. Працівник повідомляє відповідальному працівнику Департаменту інформаційної безпеки дату отримання кваліфікованого ЕП. Відповідальний працівник Департаменту інформаційної безпеки вносить інформацію в реєстр ЕП, що використовуються в Банку.

6.7. Відповідальний працівник Департаменту інформаційної безпеки відслідковує відомості про звільнення працівників банку та якщо працівник який звільняється має діючий кваліфікований ЕП від Банку, ініціює відкликання кваліфікованого ЕП у відповідальному АЦСК.

7. СТВОРЕННЯ І ЗАСВІДЧЕННЯ ЕЛЕКТРОННОЇ КОПІЇ З ПАПЕРОВОГО ДОКУМЕНТА

7.1. Створення електронної копії з паперового документа виконується через сканування та збереження документа.

7.2. Засвідчення електронної копії виконується шляхом накладання на електронну копію ЕП співробітника, уповноваженого належним чином на підписання даного документа в паперовому вигляді.

7.3. У разі необхідності додаткового підтвердження повноважень особи, що накладає ЕП, на електронній копії документа, допускається застосування печатки (за вимогою). Перелік працівників, яким надається право створення кваліфікованих електронних печаток для електронних документів затверджено розпорядчим документом Банку.

8. СТВОРЕННЯ І ЗАСВІДЧЕННЯ КОПІЇ НА ПАПЕРІ З ЕЛЕКТРОННОГО ДОКУМЕНТА

8.1. Створення копії на папері з електронного документа виконується після перевірки цілісності електронного документа та ЕП накладеного на електронний документ, шляхом роздрукування електронного документа.

8.2. Для засвідчення копії на папері відповідальна особа, уповноважена організаційно-розпорядчим документом внутрішнім Банку (де буде визначено перелік посад) на підписання такого документа в паперовому вигляді, накладає на документ свій власноручний підпис та відмітку «Згідно з оригіналом».

8.3. У разі необхідності додаткового підтвердження повноважень особи, що накладає власноручний підпис на документ, допускається застосування печатки (за вимогою).

8.4. На паперову копію наноситься інформація про те, що даний документ – копія з електронного документа і що електронний документ підписаний ЕП, П.І.Б. підписанта, дата та час накладання підпису.

9. ВИЯВЛЕННЯ БУДЬ-ЯКИХ ЗМІН В ЕЛЕКТРОННОМУ ДОКУМЕНТІ ТА ЗМІН ЕП ПІСЛЯ ПІДПИСАННЯ В ЕЛЕКТРОННОМУ ДОКУМЕНТІ

9.1. Для виявлення будь-яких змін в електронному документі та змін ЕП після підписання електронного документа проводиться перевірка цілісності електронного документа та ЕП.

9.2. Перевірка цілісності електронних документів підписаних кваліфікованим ЕП виконується за допомогою програмних комплексів, які використовують криптографічні алгоритми та протоколи, що відповідають чинному законодавству України, про що є експертний висновок, затверджений в Державній службі спеціального зв'язку України.

9.3. Для перевірки цілісності електронних документів підписаних кваліфікованим ЕП також дозволяється використовувати Державні онлайн ресурси, які використовують криптографічні алгоритми та протоколи, що відповідають чинному законодавству України, про що є експертний висновок, затверджений в Державній службі спеціального зв'язку України.

9.4. Перевірка цілісності електронних документів підписаних простим або удосконаленим ЕП забезпечується засобами інформаційної системи, у якій здійснюється створення, оброблення, зберігання електронних документів.

10. КОНТРОЛЬ І ВІДПОВІДАЛЬНІСТЬ

10.1. Відповідальність за підтримання цього Положення в актуальному стані, за своєчасне внесення змін та доповнень до нього несе Департамент інформаційної безпеки.

10.2. Працівники Банку, які у своїй роботі використовують електронний підпис, несуть персональну відповідальність за збереження і правильне використання ТК, програмних засобів захисту інформації і за зміст електронних документів, підписаних їх електронним підписом.

10.3. Працівники Банку, які у своїй роботі використовують електронний підпис, несуть персональну відповідальність за несвоєчасну генерацію власного ТК у зв'язку із

закінченням його строку дії.

10.4. Працівники Банку, які у своїй роботі використовують електронний підпис та взаємодіють з електронними підписами, можуть бути притягнуті до відповідальності згідно з чинним законодавством за порушення цього Положення.

10.5. **Власник процесу.** Відповідальність за організацію, забезпечення та контроль виконання вимог Положення покладено на відділ методології і контролю процесів інформаційної безпеки та кіберзахисту Департаменту інформаційної безпеки, який є власником процесу (Положення).

10.6. **Контроль процесу.** Відповідальність за контроль організації, забезпечення виконання вимог Положення та результату процесу покладається на директора Департаменту інформаційної безпеки, якому відповідно до організаційної структури Банку підпорядковується відділ методології і контролю процесів інформаційної безпеки та кіберзахисту.

11. ЗАКЛЮЧНІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

11.1. Положення набуває чинності з моменту прийняття відповідного рішення Правлінням Банку та діє до моменту скасування його дії.

11.2. Положення переглядається за необхідністю, але не менш ніж один раз на три роки.

11.3. Відповідальність за підтримання Положення в актуальному стані, за своєчасне внесення змін та доповнень до нього несе Департамент інформаційної безпеки.

12. ДОДАТКИ

Додаток 1 – Паспорт внутрішнього нормативного документу.

