**ЗАТВЕРДЖЕНО**

Правління АТ «КОМІНБАНК»

протокол № 11/03-1 від «11» березня 2024 року

**ПОЛОЖЕННЯ**

**про використання електронного підпису в**

**АКЦІОНЕРНОМУ ТОВАРИСТВІ «КОМІНБАНК»**

(версія 1.0)

Київ - 2024

**ОБЛІКОВА КАРТА ВНУТРІШНЬОГО НОРМАТИВНОГО ДОКУМЕНТА**

|  |  |  |  |
| --- | --- | --- | --- |
| **Назва документа** | Положення про використання електронного підпису в АКЦІОНЕРНОМУ ТОВАРИСТВІ «КОМІНБАНК» (версія 1.0) | | |
| **Реєстраційний номер та дата реєстрації** | № 11/03-1 від 11.03.2024 | | |
| **Рішення про затвердження документа** | Протокол засідання Правління АТ «КОМІНБАНК» від  № 11/03-1 від 11.03.2024 | | |
| **Дата набрання чинності** | **з 11 березня 2024 року** | | |
| **Необхідність подання документа до регулюючих та контролюючих органів** | Ні | **Найменування органів** | |
| - | |
| **Підрозділ - розробник документа** | Управління інформаційної безпеки та безперервної діяльності | | |
| **Рівень доступу** | Загальний (для усіх працівників Банку) | | |
| **Назва та номер процесу** |  | | |
| **Перелік пов’язаних ВНД** | Політика інформаційної безпеки АТ «КОМІНБАНК». | | |
| **Перелік документів, що втрачають чинність із вступом в дію даного ВНД** |  | | |
| **Історія документа** | **Версія** | | **Дата** |
| Положення про використання електронного підпису в АКЦІОНЕРНОМУ ТОВАРИСТВІ «КОМІНБАНК» | 1.0 | | 11.03.2024 |

**АРКУШ ПОГОДЖЕННЯ:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Посада** | **Ім’я та ПРІЗВИЩЕ** | **Підпис** | **Дата погодження** |
| Директор Департаменту інформаційних технологій | Андрій ШОСТИК |  |  |
| В.о. Директора Юридичного департаменту | Максим ОВЧИННІКОВ |  |  |
| Директор Департаменту ризик-менеджменту | Ігор КУХАРУК |  |  |
| Начальник Служби комплаєнс-контролю | Наталія ПРОДАН |  |  |
| Заступник начальника Управління загальнобанківської методології | Діна КРАВЕЦЬ |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Підрозділ – розробник** | **Посада, Ім’я та ПРІЗВИЩЕ** | **Підпис** | **Дата** |
| Начальник Управління інформаційної безпеки та безперервної діяльності | Володимир БОРОДАВКІН |  |  |

ЗМІСТ

[1. ЗАГАЛЬНІ ПОЛОЖЕННЯ 5](#_Toc26803463)

[2. НОРМАТИВНА БАЗА 5](#_Toc26803464)

[3. ТЕРМІНИ ТА СКОРОЧЕННЯ 5](#_Toc26803465)

4. ПОРЯДОК ВИКОРИСТАННЯ ЕП……………………………………………………...…...7

[5. КОНТРОЛЬ І ВІДПОВІДАЛЬНІСТЬ 15](#_Toc26803472)

[6. УПРАВЛІННЯ РИЗИКАМИ 15](#_Toc26803473)

[7. ПРИКІНЦЕВІ ПОЛОЖЕННЯ 17](#_Toc26803475)

# ЗАГАЛЬНІ ПОЛОЖЕННЯ

* 1. Положення про використання електронного підпису в АКЦІОНЕРНОМУ ТОВАРИСТВІ «КОМІНБАНК» (далі - Положення), яке регламентує визначення організаційно-методологічних умов застосування в АТ «КОМІНБАНК» (далі - Банк) видів електронних підписів, які використовуються під час створення, оброблення та зберігання електронних документів, а також встановлення порядку дій при роботі з електронними документами, зокрема, в частині виявлення будь-яких змін в електронних документах та/або в електронних підписах після їх підписання з метою забезпечення належного рівня безпеки інформації та дотримання Банком вимог чинного законодавства України.
  2. Метою Положення є встановлення детального та максимально зрозумілого порядку дій Банку під час накладання підписів на електронні документи відповідно до вимог законодавства України, нормативно-правових актів Національного банку України, прийнятих для виконання та відповідно до законів України.
  3. Банк надає можливість безперешкодного ознайомлення з цим Положенням всім учасникам (суб’єктам) електронної взаємодії, які використовують електронний підпис, в тому числі клієнтам та потенційним клієнтам Банку.

# НОРМАТИВНА БАЗА

* 1. При розробці цього Положення були використані такі нормативні документи зовнішнього походження:

|  |  |
| --- | --- |
| № | Найменування документа: |
| 1. | Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене постановою Правління Національного банку України від 28.09.2017 № 95. |
| 2. | Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого постановою Правління Національного банку України від 11.06.2018 №64, із змінами. |
| 3. | Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління Національного банку України від 02.07.2019 №88. |
| 4. | Положення про організацію кіберзахисту в банківській системі України, затверджене постановою Правління Національного банку України від 12.08.2022 №178. |
| 5. | Положення про використання електронного підпису та електронної печатки, затверджене постановою Правління Національного банку України від 20.12.2023 №172. |
| 6. | Інших актів чинного законодавства України, нормативно-правових актів Національного банку України та внутрішніх нормативних документів Банку щодо управління інформаційною безпекою. |

# ТЕРМІНИ ТА СКОРОЧЕННЯ

3.1. У цьому Положенні терміни вживаються в такому значенні:

**Верифікація** – заходи, що вживаються Банком з метою перевірки (підтвердження) належності відповідній особі отриманих Банком ідентифікаційних даних;

**Відкритий мережевий сервіс** – мобільний застосунок, вебсервіс або інше програмне забезпечення, що дає змогу здійснювати обмін повідомленнями між електронними пристроями Банку та користувачів через електронні комунікаційні мережі загального користування;

**Електронна печатка** – електронні дані, що додаються до інших електронних даних або логічно з ними пов’язуються і використовуються для забезпечення достовірності походження пов’язаних електронних даних, або для засвідчення електронних підписів підписувачів на електронних документах, або для засвідчення відповідності копій документів оригіналам та виявлення порушення цілісності;

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

**Електронний підпис Національного банку** **(далі – ЕП Національного банку)** – удосконалений електронний підпис **(далі – УЕП)** або удосконалена електронна печатка, що використовується в створених Національним банком платіжних системах, облікових системах, інформаційних системах;

**Електронний сенсорний пристрій** – електронний пристрій із сенсорним екраном, на якому особа може створити цифровий власноручний підпис;

**Засіб удосконаленого електронного підпису чи печатки** – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки;

**Ідентифікація** – заходи, що вживаються Банком для встановлення особи шляхом отримання її ідентифікаційних даних;

**Кваліфікований надавач електронних довірчих послуг (КНЕДП)**– 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 Закону «Про електронну ідентифікацію та електронні довірчі послуги» та відомості про яку внесені до Довірчого списку;

**Кваліфікована електронна позначка часу** – електронна позначка часу, отримана від кваліфікованого надавача електронних довірчих послуг;

**Кваліфікований електронний підпис (далі - КЕП)** – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. Згідно із цим Положенням використовуються наступні види Кваліфікованого електронного підпису: Кваліфікований електронний підпис Клієнта (КЕП Клієнта) та Кваліфікований електронний підпис Банку (КЕП Банку);

**НКІ** – носій ключової інформації;

**Перевірка цілісності** – процедура, яка дає змогу виявити будь-які зміни в електронному документі та зміни ЕП після підписання електронного документа;

**Підписувач** – фізична особа, зокрема, належним чином уповноважений представник, яка використовує електронний підпис з метою підписання електронного документу;

**Простий електронний підпис** **(далі – простий ЕП)** – будь-який вид ЕП, крім кваліфікованого ЕП (далі - КЕП), цифрового власноручного підпису (далі – ЦВП), УЕП з кваліфікованим сертифікатом, УЕП, ЕП Національного банку;

**Суб’єкт електронної взаємодії** – Національний банк України, Банк, клієнт Банку, контрагент Банку та комерційний агент Банку;

**Удосконалена електронна печатка**, **що базується на кваліфікованому сертифікаті електронної печатки** **(далі – електронна печатка з кваліфікованим сертифікатом)** – удосконалена електронна печатка, створена з використанням кваліфікованого сертифіката електронної печатки, у якому є позначка, що цей сертифікат сформовано як кваліфікований для використання електронної печатки, та немає відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки;

**Удосконалений електронний підпис (далі – УЕП)** – це електронний підпис удосконаленого формату, що являє собою криптографічне поєднання файлу підпису з особистим файловим ключем користувача, який користується УЕП;

**УЕП, що базується на кваліфікованому сертифікаті електронного підпису** **(далі – УЕП з кваліфікованим сертифікатом)** – УЕП, створений з використанням кваліфікованого сертифіката електронного підпису, у якому немає відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки; Центр сертифікації ключів (ЦСК) або надавач електронних довірчих послуг (НЕДП) – це інформаційно-комунікаційна система, яка призначена для обслуговування сертифікатів відкритих ключів користувачів та сервера системи, надання послуг фіксування часу, а також надання (за необхідності) користувачам системи засобів генерації особистих та відкритих ключів;

**Цифровий власноручний підпис (далі – ЦВП)** – електронний підпис, що є власноручним підписом фізичної особи, створеним на екрані електронного сенсорного пристрою.

* 1. Інші терміни та скорочення, що вживаються в цьому Положенні, застосовуються в значеннях, визначених чинним законодавством України.

# ПОРЯДОК ВИКОРИСТАННЯ ЕП

* 1. **Застосовані в Банку ЕП мають юридичну силу незалежно від технологій, що застосовуються для ідентифікації та автентифікації підписувача, та відповідають таким вимогам:**
* логічно пов’язуються з підписаними електронними даними із можливістю перевірити цей зв’язок протягом усього життєвого циклу електронного документа;
* електронні дані, що використовуються для створення ЕП, є унікальними та однозначно пов’язані із підписувачем і не пов’язані з жодною іншою особою;
* дають змогу однозначно ідентифікувати підписувача;
* технологія застосування ЕП забезпечує під час підписання контроль електронних даних, які підписуються, та електронних даних, які використовуються для створення ЕП;
* під час перевірки, здійсненої відповідно до вимог цього Положення, не виявлено будь-яких змін в електронному документі та/або будь-яких змін ЕП після підписання електронного документа;
* на період воєнного стану на території України та протягом шести місяців з дня його припинення чи скасування дозволяється використання електронних підписів чи печаток, що базуються на сертифікатах відкритих ключів, виданих кваліфікованими надавачами електронних довірчих послуг без відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки, користувачами електронних довірчих послуг для здійснення електронної взаємодії, електронної ідентифікації та автентифікації фізичних, юридичних осіб і представників юридичних осіб у випадках, коли законодавством України передбачено використання виключно кваліфікованих електронних підписів чи печаток (засобів кваліфікованого електронного підпису чи печатки, кваліфікованих електронних довірчих послуг) або засобів електронної ідентифікації з високим рівнем довіри, крім вчинення в електронній формі правочинів, що підлягають нотаріальному посвідченню та/або державній реєстрації у випадках, установлених законами України.
  1. **Види електронного підпису, які використовуються в Банку:**

4.2.1.  Простий ЕП Клієнта застосовується в системах дистанційного обслуговування для верифікації Клієнта, підписання електронних документів, підтвердження переказів тощо, та інших системах, у яких потрібне подібне підтвердження. В якості простого ЕП використовуються одноразовий ОТР-пароль, що надсилається Банком Клієнту в повідомленні у відповідному мобільному застосунку або в СМС-повідомленні на фінансовий номер телефону Клієнта або уповноваженої особи Клієнта.

4.2.2. Цифровий власноручний підпис (ЦВП) Клієнта застосовується в системах дистанційного обслуговування для верифікації Клієнта, підписання електронних документів, підтвердження переказів, тощо, та інших системах, у яких потрібне подібне підтвердження. На документ в електронній формі одразу після його підписання ЦВП клієнта накладається кваліфікована електронна позначка часу.

4.2.3. КЕП Банку та кваліфікована електронна печатка Банку застосовується для: відправки звітності та листів в електронній формі до Національного банку України, Державної податкової служби України, Пенсійного фонду України тощо; підписання інших документів в електронній формі відповідно до повноважень, наданих працівникам Банку; підписання платежів та інформаційних повідомлень в системі «Клієнт-Банк».

4.2.3.1. КЕП Клієнта використовується для підписання електронних документів в системі «Клієнт-Банк», в програмних комплексах або WEB-сервісах електронного документообігу з метою підписання електронних документів та здійснення електронної взаємодії між Банком та Клієнтом.

4.2.3.2. КЕП Банку – КЕП працівника Банку, уповноваженого на укладення від імені Банку правочинів та підписання відповідних документів, в тому числі під час електронної взаємодії з Клієнтом.

4.2.4. Умови електронної взаємодії між Клієнтом та Банком зазначаються у відповідному договорі (у випадах та в обсязі, визначеному відповідно до чинного законодавства України).

4.2.5. ЕП НБУ застосовується для забезпечення роботи з інформаційними задачами НБУ, підписання та відправки платежів та інформаційних повідомлень Банку в системі електронних платежів НБУ.

4.2.6. УЕП з кваліфікованим сертифікатом Банку та електронна печатка з кваліфікованим сертифікатом Банку застосовується для: відправки звітності та листів в електронні формі до Національного банку України, Державної податкової служби України, Пенсійного фонду України тощо; підписання інших документів в електронній формі відповідно до повноважень, наданих працівникам Банку; підписання платежів та інформаційних повідомлень в системі «Клієнт-Банк».

4.2.7. УЕП Банку та електронна печатка Банку застосовується для підписання документів в електронній формі відповідно до повноважень, наданих працівникам Банку; підписання платежів та інформаційних повідомлень тільки в межах програмного забезпечення інформаційних систем Банку.

* 1. **Порядок отримання ЕП.**

4.3.1. Порядок отримання ЕП визначається:

* для Простого ЕП – відповідними умовами договорів, укладених між Банком та контрагентом (Клієнтом);
* для ЦВП – відповідними умовами договорів, укладених між Банком та контрагентом (Клієнтом);
* для КЕП та кваліфікованої електронної печатки – відповідно до регламенту роботи та вимог КНЕДП;
* для УЕП з кваліфікованим сертифікатом та електронної печатки з кваліфікованим сертифікатом – відповідно до регламенту роботи та вимог КНЕДП;
* для УЕП та електронної печатки – відповідно до регламенту роботи, настанов та інструкцій ЦСК;
* для ЕП НБУ – відповідними нормативними документами НБУ та умовами договору, укладеного між Банком та НБУ.
  1. **Порядок виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа:**

4.4.1. ЕП є обов’язковим реквізитом електронного документа. Накладанням ЕП завершується створення електронного документа.

4.4.2. Електронний документ вважається створеним, якщо ЕП додається до підписаних електронних даних та логічно пов’язується з ними. В цьому випадку є можливість перевірити цей зв'язок протягом усього життєвого циклу електронного документу: від його створення до знищення, або під час постійного зберігання.

4.4.3. Підписувач, який здійснює накладення ЕП на електронний документ, цим самим засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, не має заперечень до тексту документа і свідомо застосував свій підпис у контексті, передбаченому документом (підписав, погодив, засвідчив, підтвердив тощо).

4.4.4. Виявлення будь-яких змін в електронному документі здійснюється шляхом перевірки цілісності ЕП, наявності та актуальності ЕП на момент підписання або логічного додавання до електронного документу.

* 1. **Порядок виявлення будь-яких змін ЕП після підписання електронного документу.**

4.5.1. Перевірка цілісності електронного документу та виявлення будь-яких змін ЕП після підписання електронного документу забезпечується:

* для Простого ЕП - в автоматичному режимі при обробці даних в системах дистанційного обслуговування та інших системах, у яких створюються, обробляються та зберігаються електронні документи. Простий ЕП є таким, що пройшов перевірку, якщо перевірку ЕП здійснено згідно з процедурою, наведеною в договорі між учасниками (суб’єктами) електронної взаємодії.
* для КЕП та кваліфікованої електронної печатки - порядок виявлення будь-яких змін ЕП визначається та здійснюється у відповідності до регламенту роботи, настанов та інструкцій КНЕДП, який здійснив випуск відповідних КЕП. Результатом перевірки КЕП та кваліфікованої електронної печатки є висновок (відповідь), отримана від відповідного сервісу КНЕДП.
* для УЕП з кваліфікованим сертифікатом та електронної печатки з кваліфікованим сертифікатом - порядок виявлення будь-яких змін ЕП визначається та здійснюється у відповідності до регламенту роботи, настанов та інструкцій КНЕДП, який здійснив випуск відповідних УЕП. Результатом перевірки УЕП з кваліфікованим сертифікатом та електронної печатки з кваліфікованим сертифікатом є висновок (відповідь), отримана від відповідного сервісу КНЕДП.
* для УЕП та електронної печатки - порядок виявлення будь-яких змін ЕП визначається та здійснюється у відповідності до регламенту роботи, настанов та інструкцій ЦСК, який здійснив випуск відповідних УЕП. Результатом перевірки УЕП та електронної печатки є висновок (відповідь), отримана від відповідного сервісу ЦСК.
* для ЕП НБУ – в автоматичному режимі при обробці даних в інформаційних системах Банку та інформаційних задачах НБУ. Порядок виявлення будь-яких змін в ЕП НБУ визначається нормативними документами НБУ.

4.5.2. Результати автоматизованого накладання/додавання ЕП відображаються у базах даних відповідних інформаційних систем.

4.5.3. Перевірка на предмет виявлення будь-яких змін в електронному документі та ЕП після підписання електронного документу, в т.ч. на предмет забезпечення їх цілісності, може бути здійснена незалежною третьою стороною.

* 1. **Порядок роботи з Простим ЕП.**

4.6.1. Клієнт – фізична особа, яка отримує або має намір отримати банківські та/або фінансові послуги, не пов'язані з підприємницькою діяльністю, під час підписання документів/відомостей має право використовувати Простий ЕП на підставі договору між Банком і Клієнтом, що укладається в письмовій формі (у вигляді паперового документа з власноручними підписами сторін або електронного документа з використанням КЕП).

4.6.2. При укладенні договору здійснюється ідентифікація Клієнта-фізичної особи, його автентифікація. В договорі обов’язково визначаються умови використання Клієнтом Простого ЕП:

* при ідентифікації та автентифікації користувача (Клієнта);
* для надання санкціонованого доступу до програмного забезпечення, з використанням якого здійснюється доступ до вищезазначених систем;
* для підтвердження переказів, транзакцій за рахунками Клієнта;
* при відправленні повідомлень Клієнтом засобами комунікативного зв’язку у вищезазначених системах;
* при підписанні електронних документів.

4.6.3. Правильність всіх наданих даних Клієнтом для здійснення Банком ідентифікації під час укладення договору (згідно з умовами якого здійснюється користування системою дистанційного обслуговування) підтверджується та засвідчується Клієнтом особистим підписом.

4.6.4. У випадку якщо один з параметрів для ідентифікації чи автентифікації Клієнта не співпадає, операція буде відхилена, а електронні дані не будуть вважатися електронним документом та не будуть опрацьовані інформаційними системами.

4.6.5. Для забезпечення перевірки Простого ЕП та логічного зв’язку Простого ЕП з електронним документом, Геш-функція отриманого Простого ЕП заноситься у відповідне поле бази даних систем.

4.6.6. Джерелом(-ами) формування Простого ЕП є:

* для системи дистанційного обслуговування - програмне забезпечення системи, яке формує одноразовий OTP-пароль, який направляється Клієнту в повідомленні у відповідному мобільному застосунку або в СМС повідомленні;
* для інших систем дистанційного обслуговування, також PIN і OTP-пароль, який направляється Клієнту в повідомленні у відповідному мобільному застосунку або в СМС повідомленні.

4.6.7. При здійсненні будь-яких операцій та правочинів між Клієнтом та Банком за допомогою Простого ЕП, підтвердження Клієнтом здійснення операції або укладення правочину здійснюється шляхом введення у відповідне поле інтерфейсу мобільного застосунку або сайту Банку цифрової послідовності, яка повністю ідентична надісланому Банком ОТР на фінансовий номер телефону Клієнта.

4.6.8. Прості ЕП приймаються до обробки тільки в межах програмного забезпечення інформаційних систем Банку.

4.6.9. Документи, підписані Простим ЕП, що надійшли засобами електронної пошти, або іншими шляхами, але поза технологічними процесами інформаційних систем Банку, до обробки не приймаються.

4.6.10. Банк може використовувати й інші види Простого ЕП відповідно до розроблених ним технологій та зміни функціональних можливостей програмного забезпечення та сервісів Банку, зокрема: ОТР, QR-код, кнопки «Підпис», «Підписав», «Підтверджую», «Ознайомився» тощо у програмних комплексах, мобільному застосунку та/ або на офіційному сайті Банку у мережі Інтернет, де Клієнту надається технічна можливість ознайомитися з умовами надання відповідної послуги та підписати відповідний договір та/або дати доручення Банку на здійснення операції з переказу коштів тощо, або якщо інтерфейс відповідного програмного комплексу Банку надає клієнту змогу зробити однозначний висновок про суть операції, доручення на здійснення якої клієнт надає Банку шляхом підписання способами, визначеними цим Положенням.

4.6.11. Правочини у вигляді електронних документів із використанням простих ЕП є дійсними та обов’язковими для суб'єктів електронного документообігу та такими, що не потребують додаткового підтвердження.

* 1. **Порядок роботи з ЦВП.**
     1. Клієнт – фізична особа, яка отримує або має намір отримати банківські та/або фінансові послуги, не пов'язані з підприємницькою діяльністю, під час підписання документів/відомостей має право використовувати ЦВП. Використання ЦВП Клієнтом не вимагає наявності попередньо укладеного договору між Банком та Клієнтом.
     2. Технологія створення електронних документів, які клієнт підписує ЦВП, визначається Банком. Банк забезпечує гарантію того, що клієнт підписав саме той документ, з текстом якого він ознайомився. Клієнт підписує ЦВП документ в неперервному технологічному процесі (сеансі обслуговування), що гарантує підписання саме того документу, з яким Клієнт ознайомлювався та який підписував.
     3. На електронному сенсорному пристрої уповноваженого працівника Банку або Клієнта генерується електронний документ, на якому Клієнт ознайомлюється із текстом документу та після натискання на кнопку «Підписати» власноруч виконує підпис на сенсорному екрані пристрою способом, аналогічним виконанню підпису на паперовому носії. На документ в електронній формі одразу після його підписання ЦВП Клієнта накладається кваліфікована електронна позначка часу.
     4. Для забезпечення перевірки ЦВП та логічного зв’язку ЦВП з електронним документом, Геш-функція отриманого ЦВП заноситься у відповідне поле бази даних систем.
     5. Джерелом(-ами) формування ЦВП є сенсорний екран системи, яка формує зображення ЦВП, що створюється Клієнтом власноруч.
     6. ЦВП приймаються до обробки тільки в межах програмного забезпечення інформаційних систем Банку та/або уповноважених на здійснення ідентифікації та верифікації осіб.

4.7.7. Документи, підписані ЦВП, що надійшли засобами електронної пошти або іншими шляхами, але поза технологічними процесами інформаційних систем Банку, до обробки не приймаються.

* 1. **Порядок роботи з КЕП та кваліфікованою електронною печаткою.**
     1. КЕП має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Укладення окремого договору щодо використання КЕП не вимагається.

4.8.2. Кваліфікована електронна печатка створюється, якщо:

* відповідно до законодавства України потрібно засвідчити дійсність підпису на електронних документах;
* відповідно до законодавства України проставлення печатки вимагається для засвідчення відповідності копій документів оригіналам;
* потрібно підтвердити повноваження представника юридичної особи на застосування ЕП у контексті, передбаченому документом.

4.8.3. Банк має право використовувати більш, ніж одну кваліфіковану електронну печатку. Юридична особа – суб’єкт електронної взаємодії має право використовувати більш, ніж одну кваліфіковану електронну печатку.

4.8.4. Створювачу КЕП та/або кваліфікованої електронної печатки забороняється створювати кваліфіковану електронну печатку, якщо кваліфікований сертифікат електронної печатки є нечинним або одержати інформацію про його статус неможливо.

4.8.5. Для забезпечення виконання вимог законодавства України, в тому числі, але не виключно, нормативно-правових актів Кабінету Міністрів України, Національного банку України, Міністерства доходів та зборів України, своєчасного подання звітності в Банку призначаються відповідальні особи, відповідно до їх функціональних обов’язків.

4.8.6. Проставляння КЕП Банку та створення кваліфікованої електронної печатки на електронних документах здійснюється працівниками Банку, які мають на це повноваження відповідно до розпорядчого документу Банку, в межах, передбачених відповідною довіреністю (у разі, якщо складення довіреності вимагається згідно з законодавством України).

4.8.7. Уповноважені особи Банку використовують кваліфіковані електронні печатки в програмних комплексах відповідно до інструкцій цих програмних комплексів. Відповідно до вимог чинного законодавства України, Банк здійснює приймання, реєстрацію та обробку повідомлень, що надходять до Банку із накладеними КЕП.

4.8.8. При надходженні вхідного електронного повідомлення на поштову скриньку Банку, додаток до якого є електронний документ, підписаний КЕП, таке повідомлення проходить перевірку на наявність шкідливого програмного забезпечення, а також перевіряється справжність зазначеного ЕП (в т.ч. здійснюється перевірка цілісності електронних даних, що підписуються ЕП та ідентифікація Підписувача).

4.8.9. За відсутності шкідливого програмного забезпечення та визначення справжності ЕП (в т.ч. проходження перевірки на предмет цілісності електронних даних, що підписуються, та на предмет ідентифікації Підписувача), повідомлення реєструється у встановленому порядку в Банку та приймається до опрацювання відповідними підрозділами Банку, яких стосується вказане звернення, відповідно до встановленого порядку.

* 1. **Порядок роботи з УЕП** **з кваліфікованим сертифікатом та електронної печатки з кваліфікованим сертифікатом.**
     1. УЕП з кваліфікованим сертифікатом має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Укладення окремого договору щодо використання УЕП з кваліфікованим сертифікатом не вимагається.
     2. Електронна печатка з кваліфікованим сертифікатом створюється, якщо:
* Відповідно до законодавства України потрібно засвідчити дійсність підпису на електронних документах;
* Відповідно до законодавства України проставлення печатки вимагається для засвідчення відповідності копій документів оригіналам;
* Потрібно підтвердити повноваження представника юридичної особи на застосування ЕП у контексті, передбаченому документом.
  + 1. Банк має право використовувати більш, ніж одну електронну печатку з кваліфікованим сертифікатом. Юридична особа – суб’єкт електронної взаємодії має право використовувати більш, ніж одну електронну печатку з кваліфікованим сертифікатом.
    2. Створювачу УЕП з кваліфікованим сертифікатом та/або електронної печатки з кваліфікованим сертифікатом забороняється створювати електронну печатку з кваліфікованим сертифікатом, якщо кваліфікований сертифікат електронної печатки є нечинним або одержати інформацію про його статус неможливо.
    3. Для забезпечення виконання вимог законодавства України, в тому числі, але не виключно, нормативно-правових актів Кабінету Міністрів України, Національного банку України, Міністерства доходів та зборів України, своєчасного подання звітності в Банку призначаються відповідальні особи, відповідно до їх функціональних обов’язків.
    4. Проставляння УЕП з кваліфікованим сертифікатом Банку та створення електронної печатки з кваліфікованим сертифікатом на електронних документах здійснюється працівниками Банку, які мають на це повноваження відповідно до розпорядчого документу Банку. в межах, передбачених відповідною довіреністю (у разі, якщо складення довіреності вимагається згідно з законодавством України).
    5. Уповноважені особи Банку використовують електронні печатки з кваліфікованим сертифікатом в програмних комплексах відповідно до інструкцій цих програмних комплексів. Відповідно до вимог чинного законодавства України, Банк здійснює приймання, реєстрацію та обробку повідомлень, що надходять до Банку із накладеними КЕП.
    6. При надходженні вхідного електронного повідомлення на поштову скриньку Банку, додаток до якого є електронний документ, підписаний УЕП з кваліфікованим сертифікатом, таке повідомлення проходить перевірку на наявність шкідливого програмного забезпечення, а також перевіряється справжність зазначеного ЕП (в т.ч. здійснюється перевірка цілісності електронних даних, що підписуються ЕП та ідентифікація Підписувача).
    7. За відсутності шкідливого програмного забезпечення та визначення справжності ЕП (в т.ч. проходження перевірки на предмет цілісності електронних даних, що підписуються, та на предмет ідентифікації Підписувача), повідомлення реєструється у встановленому порядку в Банку та приймається до опрацювання відповідними підрозділами Банку, яких стосується вказане звернення, відповідно до встановленого порядку.

**4.10. Порядок роботи з УЕП** **та електронною печаткою.**

4.10.1. Джерелом формування УЕП та електронною печатки є ЦСК, який формує УЕП та електронну печатку, що створюється користувачем власноруч.

4.10.2. Технологія створення електронних документів, які клієнт підписує УЕП або електронною печаткою, визначається Банком. Банк забезпечує гарантію того, що користувач підписав саме той документ, з текстом якого він ознайомився. Користувач підписує УЕП або електронною печаткою документ в неперервному технологічному процесі (сеансі обслуговування), що гарантує підписання саме того документу, з яким користувач ознайомлювався та який підписував.

4.10.3. УЕП та електронна печатка приймаються до обробки тільки в межах програмного забезпечення інформаційних систем Банку.

**4.11. Вимоги до зберігання криптографічних ключів.**

4.11.1. Зберігання ключів повинно виконуватися згідно з такими вимогами:

* для зберігання особистих ключів мають використовуватися НКІ;
* відкриті ключі можуть зберігатися у відкритому вигляді з контролем цілісності;
* у випадку використання криптографічних засобів інформації, архітектура якої вимагає зберігання особистих ключів у вигляді файлів на жорстких магнітних дисках інформаційної системи, адміністратор системи обмежує доступ до цих ключів на рівні файлової системи, доступ до якої у відповідній частині мають виключно власники ключів;
* паролі для особистих ключів повинні знати тільки власники особистих ключів.

4.11.2. Підписувач, який здійснює накладення ЕП будь-якого виду, відповідальний за безпеку зберігання та використання особистого ключа ЕП або іншого компоненту ЕП, володіння яким носить виключний характер і є невід’ємною частиною ЕП. Підписувачу, що є володільцем особистого ключа ЕП або іншого компонента ЕП, заборонено передавати його будь-яким третім особам.

4.11.3. Забезпечення належних умов зберігання та використання ключів ЕП, що належать Банку, покладається на Банк, а інших Підписувачів – на самих володільців (власників) ключів.

**4.12. Створення і засвідчення електронної копії з паперового документа.**

4.12.1. Копія документа в електронній формі (електронна копія) створюється шляхом сканування виключно з оригіналу документа у паперовій формі.

4.12.2. Для засвідчення копії документа в електронній формі працівник Банку, уповноважений на підписання такого документа в паперовій формі або на засвідчення копій документів, накладає на документ свій ЕП.

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

4.12.4. Електронна копія документа без ЕП прирівнюється за статусом до незавіреної електронної копії оригіналу документу у паперовій формі.

4.12.5. Електронна копія документу у паперовій формі, засвідчена ЕП уповноваженого працівника Банку, є електронним документом, статус якого прирівнюється до завіреної електронної копії оригіналу документу у паперовій формі.

**4.13. Створення і засвідчення копії на папері з електронного документу.**

4.13.1. У разі створення копії на папері з електронного документу працівник Банку, який створює таку копію, проводить обов’язкову перевірку цілісності електронного документу засобами перевірки ЕП, вбудованих в програмні комплекси (WEB-сервіси в мережі Інтернет) електронного документообігу або WEB-сервіси в мережі Інтернет на офіційному сайті кваліфікованого надавача електронних довірчих послуг. Електронний документ вважається справжнім у разі одержання позитивного результату перевірки його цілісності.

4.13.2. Створення копії на папері з електронного документа виконується шляхом роздрукування електронного документа.

4.13.3. Для засвідчення копії на папері працівник Банку, уповноважений на підписання такого документа в паперовій формі або на засвідчення копій документів, накладає на документ свій власноручний підпис та відмітку «Згідно з оригіналом».

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

4.13.5. 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.

# КОНТРОЛЬ І ВІДПОВІДАЛЬНІСТЬ

5.1. Підписувач, який здійснює накладання ЕП на електронний документ, цим самим засвідчує та несе відповідальність, що:

* ознайомився з текстом документа;
* зрозумів його зміст;
* не має заперечень до тексту документа;
* свідомо застосував свій підпис у контексті, передбаченому документом (підписав, погодив, засвідчив тощо).

5.2. Використання ЕП НБУ учасниками (суб'єктами) електронної взаємодії дозволяється тільки у випадках, прямо передбачених нормативно-правовими актами Національного банку України, і з обов'язковим використанням засобів захисту інформації Національного банку України. Підписувач, який здійснює накладення ЕП НБУ на електронний документ, несе особисту відповідальність за достовірність та повноту інформації, що міститься в реквізитах електронного документа.

5.3. Відповідно до вимог Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління НБУ від 02.07.2019 № 88, Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого постановою Правління НБУ від 11.06.2018 № 64 (зі змінами) та внутрішніх нормативних документів у Банку впроваджена система внутрішнього контролю під час забезпечення інформаційної безпеки, що ґрунтується на розподілі обов'язків між підрозділами Банку із застосуванням моделі трьох ліній захисту, а саме:

**Перша лінія захисту** - на рівні бізнес-підрозділів та підрозділів підтримки, що задіяні в процесі використання електронного підпису, опис якого визначений цим Положенням. Зазначені структурні підрозділи здійснюють функції, визначені цим Положенням, приймають ризики в процесі своєї діяльності та несуть відповідальність за поточне управління цими ризиками, здійснюють заходи контролю у порядку, визначеному цим Положенням та іншими внутрішніми нормативними документами Банку.

На цій лінії захисту внутрішній контроль здійснюється за наступними видами контролів:

* залежно від суб’єкта контролю – подвійний контроль, який здійснюється двома (або більше) працівниками (принцип «двох пар очей») під час здійснення дій, щодо використання електронного підпису, визначених розділом 4 цього Положення (здійснюється бізнес-підрозділами та підрозділами підтримки, що задіяні в процесі використання електронного підпису); колегіальний контроль – здійснюється Правлінням Банку під час затвердження внутрішніх нормативних документів, що регламентують порядок забезпечення безпеки інформаційних систем;
* залежно від періодичності здійснення – функціональний (постійний) контроль, який проводиться на регулярній основі керівниками підрозділів, задіяних у процесі використання електронного підпису згідно цього Положення;
* залежно від моменту здійснення контролю – попередній, який передує процесу використання електронного підпису та полягає у впровадженні заходів з забезпечення безпеки інформаційних систем; поточний – здійснюється під час виконання дії процесу використання електронного підпису та полягає у виконанні усіх заходів з забезпечення безпеки інформаційних систем, відповідно до вимог цього Положення та чинного законодавства України. Поточний контроль здійснюється бізнес-підрозділами та підрозділами підтримки, що задіяні в процесі використання електронного підпису із залученням за необхідності Управління інформаційної безпеки та безперервної діяльності, Департаменту ІТ та/або Комітету з інформаційної безпеки та безперервної діяльності; подальший контроль - здійснюється після виконання дій процесу і спрямований на виявлення недоліків у виконанні усіх заходів з забезпечення безпеки інформаційних систем при використанні електронного підпису, перегляді та удосконаленні системи управління інформаційною безпекою у частині впровадження нових заходів з забезпечення безпеки інформаційних систем при використанні електронного підпису. Подальший контроль здійснюється відповідальними працівниками Управління інформаційної безпеки та безперервної діяльності із залученням за необхідності Комітету з інформаційної безпеки та безперервної діяльності, працівників Департаменту ІТ та інших структурних підрозділів Головного офісу Банку.

**Друга лінія захисту** - на рівні Департаменту ризик-менеджменту та Служби комплаєнс-контролю, мінімальні вимоги щодо діяльності яких встановлені в Положенні про організацію системи управління ризиками в банках України та банківських групах, затвердженому постановою Правління НБУ від 11.06.2018 №64 (зі змінами) та Положенні про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженому постановою НБУ від 02.07.2019 №88, зокрема: контроль за виявленням, вимірюванням та оцінкою інформаційного ризику (у т.ч. кіберризику), який є складовою операційного ризику, та інших ризиків, що виникають в процесі використання електронного підпису (Департамент ризик-менеджменту); контроль за дотриманням норм законодавства та внутрішніх нормативних документів Банку (Служба комплаєнс-контролю) та виконання інших функцій контролю у відповідності до функцій Департаменту ризик-менеджменту та Служби комплаєнс-контролю, визначених внутрішніми нормативними документами з питань управління ризиками.

На другій лінії захисту Департамент ризик-менеджменту та Служба комплаєнс-контролю аналізують, оцінюють, узагальнюють, складають звітність щодо результатів моніторингу ефективності системи внутрішнього контролю (СВК), проведеного бізнес-підрозділами та підрозділами підтримки на першій лінії захисту, з наданням відповідних рекомендацій. Моніторинг ефективності СВК, документальне оформлення його результатів, строки подання на засідання Правління Банку та Наглядової ради на розгляд та погодження звіту про результати моніторингу СВК здійснюється у порядку, визначеному внутрішньою Процедурою здійснення моніторингу ефективності системи внутрішнього контролю в АТ «КОМІНБАНК».

**Третя лінія захисту** - на рівні Служби внутрішнього аудиту, яка здійснює незалежну оцінку ефективності діяльності першої та другої ліній захисту та загальну оцінку ефективності системи внутрішнього контролю з урахуванням вимог, установлених Положенням про організацію внутрішнього аудиту в банках України, затвердженим постановою Правління НБУ від 10.05.2016 №311 (зі змінами), Положенням про організацію системи управління ризиками в банках України та банківських групах, затвердженим постановою Правління НБУ від 11.06.2018 №64 (зі змінами), Положенням про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженим постановою НБУ від 02.07.2019 №88.

5.4. Керівники структурних підрозділів Банку, що задіяні в процесі використання електронного підпису, забезпечують контроль за виконанням підлеглими працівниками посадових обов’язків, передбачених посадовими інструкціями, цим Положенням та іншими внутрішніми нормативними документами Банку.

# УПРАВЛІННЯ РИЗИКАМИ

* 1. Процесу використання електронного підпису, що виконується згідно з цим Положенням, притаманні наступні види ризиків:
* **Ризик інформаційної безпеки, як складова операційного ризику** - управління даним видом ризику ґрунтується на принципах контролю в частині ризиків інформаційної безпеки, здійснення аналізу та оцінки операційного інциденту за фактом виникнення (або підозри на виникнення) подій, які можуть нанести значну шкоду Банку шляхом порушення конфіденційності, цілісності, доступності інформації: отримання несанкціонованого доступу до ІС, несанкціоноване підвищення привілеїв користувача у ІС, несанкціоноване підключення до або відключення від ІС носіїв інформації та інших пристроїв, передача великого об’єму інформації з критичної ІС за межі мережі Банку, виявлення численних шкідливих програм на серверах та/або робочих станціях, здійснення мережевої атаки з використанням існуючих у ІС технічних вразливостей, вимкнення заходів безпеки ІС (антивірусних програм, брандмауерів) тощо.
* **Ризик інформаційно-комунікаційних технологій, як складова операційного ризику** - управління даним видом ризику ґрунтується на принципах контролю в частині ризиків інформаційно-комунікаційних технологій, здійснення аналізу та оцінки операційного інциденту за фактом виникнення (або підозри на виникнення) подій, які можуть нанести значну шкоду Банку шляхом порушення функціонування інформаційних систем та інших інформаційних ресурсів банку та управління ними тощо.
* **Кіберризик, як складова ризику інформаційної безпеки** - управління даним видом ризику ґрунтується на принципах контролю в частині кіберризиків, здійснення аналізу та оцінки операційного інциденту за фактом виникнення (або підозри на виникнення) подій, які можуть нанести значну шкоду Банку шляхом порушення функціонування у кіберпросторі інформаційних систем та інших інформаційних ресурсів банку та управління ними тощо.
* **Ризик репутації** - управління ризиком репутації полягає в зниженні можливих фінансових втрат, збереженні та підтримці ділової репутації Банку перед діючими та потенційними клієнтами, контрагентами, акціонерами, учасниками фінансового ринку та контролюючими організаціями. Управління репутаційним ризиком в частині цього Положення досягається шляхом збереження конфіденційної інформації, захисту інформаційних систем.
* **Комплаєнс-ризик** – управління даним видом ризику здійснюється шляхом дотримання вимог законодавства, враховуючи вимоги нормативно-правових актів НБУ, відповідних стандартів професійних об’єднань, дія яких поширюється на Банк, та внутрішніх нормативних документів Банку; управління конфліктами інтересів тощо.

Перелік зазначених вище видів ризиків, що виникають за процесом, визначеним цим Положенням, не є вичерпним.

Дотримання вимог законодавства, враховуючи вимоги нормативно-правових актів НБУ, відповідних стандартів професійних об’єднань, дія яких поширюється на Банк, здійснюється шляхом:

* розробки внутрішніх нормативних документів, які регламентують процес використання електронного підпису;
* розподілу в межах організаційної структури Банку повноважень, обов’язків та відповідальності між підрозділами, задіяними в процесі використання електронного підпису;
* регламентації та забезпечення контролю за дотриманням відповідальними працівниками підрозділів, задіяних в процесі використання електронного підпису, встановленої цим Положенням процедури використання електронного підпису, інформуванням керівників Банку відповідного рівня, підрозділу комплаєнс-контролю про виявлені порушення, помилки і недоліки;
* контролю за інформаційними системами та технологіями Банку під час їх придбання, налаштування та супроводження та інші процедури контролю, запроваджені внутрішніми нормативними документами Банку, згідно з вимогами Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління НБУ від 02.07.2019 №88.

Зазначений перелік не є вичерпним та може доповнюватися за результатами проведення додаткової оцінки ризиків згідно установленого в Банку порядку.

* 1. Управління ризиками, притаманними процесу використання електронного підпису, який регламентує це Положення, здійснюється відповідно до внутрішніх нормативних документів Банку, зокрема: Стратегії управління ризиками АТ «КОМІНБАНК», Кодексу поведінки (етики) АТ «КОМІНБАНК», Політики з управління операційним ризиком (в тому числі ризиком ІСТ та ризиком інформаційної безпеки) АТ «КОМІНБАНК», Політики управління комплаєнс-ризиком в АТ «КОМІНБАНК», Політики запобігання конфліктам інтересів в АТ «КОМІНБАНК», Методики управління операційним ризиком АТ «КОМІНБАНК» та іншими документами, що регламентують питання управління ризиками.
  2. З метою ефективного управління та мінімізації ризиків, зазначених у пункті 6.1 цього Положення, здійснюється комплекс заходів, спрямованих на зниження ймовірності настання подій та обставин, що призводять до операційних збитків та/або на зменшення розмірів потенційних операційних збитків.

# ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Положення набуває чинності з моменту його затвердження Правлінням Банку.
2. Зміни та доповнення до цього Положення затверджуються Правлінням Банку та оформлюються шляхом викладення нової редакції Положення або окремими змінами до нього. Прийняття нової редакції Положення автоматично призводить до припинення дії попереднього документа. Причинами внесення змін до Положення є зміни інформаційної інфраструктури та/або впровадження нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.
3. У разі невідповідності будь-якої частини Положення чинному законодавству України або нормативно-правовим актам НБУ, у тому числі у зв’язку з прийняттям нових актів законодавства України або нормативно-правових актів НБУ, це Положення буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України або нормативно-правовим актам Національного банку України. До внесення відповідних змін до Положення відповідальні працівники Банку в своїй роботі повинні керуватися нормами чинного законодавства України та нормативно-правових актів НБУ.
4. Положення підлягає регулярному перегляду для його постійного вдосконалення.
5. У разі зміни найменувань структурних підрозділів, які задіяні в процедурах, що описані в цьому Положенні, при незмінності функцій, Положення вважається дійсним щодо їх нового найменування.