



«ЗАТВЕРДЖЕНО»
Наказом директора
ТОВ «ПУ «ФІН ПЕЙ»
№ 3-ОД від 06.04.2026 р.



Аліна

**ПОЛОЖЕННЯ ПРО ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПISУ ТА
ЕЛЕКТРОННОЇ ПЕЧАТКИ В ТОВ «ПУ «ФІН ПЕЙ»**

Дніпро

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Це Положення про використання електронного підпису та електронної печатки в Товаристві з обмеженою відповідальністю «ПЛАТІЖНА УСТАНОВА «ФІН ПЕЙ» (далі – **Положення**) є внутрішнім нормативним документом Товариства з обмеженою відповідальністю «ПЛАТІЖНА УСТАНОВА «ФІН ПЕЙ» (далі – **Товариство**), що визначає організаційні та правові засади використання електронного підпису та електронної печатки під час здійснення діяльності з надання платіжних послуг, створення, підписання, погодження, оброблення, передавання, зберігання та використання електронних документів, а також під час електронної взаємодії із клієнтами, контрагентами, Національним банком України, органами державної влади та іншими суб'єктами електронної взаємодії.

1.2. Це Положення розроблено відповідно до вимог Законів України «Про Національний банк України», «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги», нормативно-правових актів Національного банку України, зокрема Положення про використання електронного підпису та електронної печатки, затвердженого постановою Правління Національного банку України від 20 грудня 2023 року № 172, а також інших нормативно-правових актів України, що регулюють застосування електронних довірчих послуг та організацію електронного документообігу.

1.3. Вимоги цього Положення є обов'язковими для виконання всіма працівниками Товариства, членами органів управління, іншими особами, які діють від імені Товариства в межах наданих повноважень, а також іншими суб'єктами електронної взаємодії у випадках, передбачених законодавством України, договорами та внутрішніми документами Товариства.

1.4. Це Положення встановлює порядок використання електронного підпису та електронної печатки, визначає права, обов'язки та відповідальність суб'єктів електронної взаємодії, а також організаційні та технічні заходи, спрямовані на забезпечення цілісності, достовірності, конфіденційності, автентичності та юридичної значущості електронних документів.

1.5. Дія цього Положення поширюється на всі інформаційні системи, програмно-технічні комплекси та бізнес-процеси Товариства, у яких створюються, обробляються, передаються, підписуються або зберігаються електронні документи із застосуванням електронного підпису та/або електронної печатки.

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

У цьому Положенні терміни вживаються в таких значеннях:

Автентифікація – процедура перевірки належності особі заявлених ідентифікаційних даних та/або повноважень із використанням одного чи декількох факторів автентифікації відповідно до вимог законодавства України та внутрішніх документів Товариства.

Автентифікаційні дані – сукупність відомостей, реквізитів, кодів, ключів, засобів електронної ідентифікації, електронних підписів, одноразових паролів (ОТР), біометричних даних та інших засобів, що використовуються для підтвердження особи користувача під час отримання платіжних або інших послуг.

Відкритий ключ – параметр криптографічного алгоритму, пов'язаний з особистим ключем, який використовується для перевірки електронного підпису або електронної печатки.

Дистанційні канали обслуговування – визначені Товариством інформаційно-комунікаційні канали взаємодії з Клієнтами, зокрема вебсайт, особистий кабінет, мобільний застосунок, програмний інтерфейс (API), електронна пошта, системи електронного документообігу, інші програмно-технічні засоби, за допомогою яких Клієнт без особистого відвідування Товариства може отримувати платіжні та інші послуги, укладати договори, подавати документи, надавати платіжні інструкції, отримувати інформацію та здійснювати інші дії після проходження процедур електронної ідентифікації та/або автентифікації.

Електронний документ – документ, інформація в якому зафіксована в електронній формі та який містить обов'язкові реквізити відповідно до законодавства України.

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

Кваліфікований електронний підпис (КЕП) – удосконалений електронний підпис, створений із використанням засобу кваліфікованого електронного підпису та кваліфікованого сертифіката відкритого ключа.

Удосконалений електронний підпис, що базується на кваліфікованому сертифікаті відкритого ключа (УЕП) – удосконалений електронний підпис, створений із використанням кваліфікованого сертифіката відкритого ключа без обов'язкового використання засобу кваліфікованого електронного підпису.

Кваліфікована електронна печатка – удосконалена електронна печатка, створена із використанням засобу кваліфікованої електронної печатки та кваліфікованого сертифіката електронної печатки.

Електронна печатка – електронні дані, що додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються з метою підтвердження походження та забезпечення цілісності електронних даних.

Підписувач – фізична особа, яка створює електронний підпис із використанням власного особистого ключа.

Створювач електронної печатки – юридична особа, яка створює електронну печатку із використанням власного засобу електронної печатки.

Особистий ключ – унікальний криптографічний ключ, що використовується підписувачем або створювачем електронної печатки для створення електронного підпису або електронної печатки.

Кваліфікований надавач електронних довірчих послуг (КНЕДП) – юридична особа або фізична особа – підприємець, яка надає одну чи більше електронних довірчих послуг відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та включена до Довірчого списку.

Електронна ідентифікація – процес використання ідентифікаційних даних особи в електронній формі, які однозначно представляють фізичну або юридичну особу чи представника юридичної особи.

Клієнт – фізична особа, фізична особа – підприємець або юридична особа, яка отримує або має намір отримати платіжні чи інші послуги Товариства.

Система електронного документообігу (СЕД) – інформаційна система, визначена Товариством, що забезпечує створення, погодження, підписання, обмін, перевірку, облік, зберігання та архівування електронних документів із використанням електронних довірчих послуг. Товариство може використовувати одну або декілька СЕД (зокрема «Вчасно», М.Е.Doc або інші), що відповідають вимогам законодавства України.

Суб'єкти електронної взаємодії – Товариство, Національний банк України, Клієнти, контрагенти, постачальники послуг, комерційні агенти (за наявності), а також інші особи, які здійснюють електронний документообіг із Товариством.

Дія.Підпис – спосіб накладення кваліфікованого електронного підпису із використанням мобільного застосунку «Дія» відповідно до законодавства України.

Під час надання платіжних послуг Товариство може використовувати КЕП, УЕП, кваліфіковану електронну печатку та інші засоби електронної ідентифікації й автентифікації, застосування яких допускається законодавством України, нормативно-правовими актами Національного банку України та внутрішніми документами Товариства.

Інші терміни, що використовуються у цьому Положенні, застосовуються у значеннях, визначених Законами України «Про Національний банк України», «Про платіжні послуги», «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги», «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», а також Положенням про використання електронного підпису та електронної печатки, затвердженим постановою Правління Національного банку України від 20 грудня 2023 року № 172, та іншими нормативно-правовими актами Національного банку України.

3. ПОРЯДОК СТВОРЕННЯ, ПІДПИСАННЯ, ОБМІНУ ТА ЗБЕРІГАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

3.1. Обмін електронними документами між Товариством, Клієнтами, контрагентами та іншими суб'єктами електронної взаємодії може здійснюватись із використанням систем електронного документообігу (СЕД), визначених Товариством, або інших захищених інформаційних систем, що відповідають вимогам законодавства України.

3.2. Електронний документ повинен містити всі обов'язкові реквізити, встановлені законодавством України, а також реквізити, визначені договором або внутрішніми документами Товариства. Відсутність обов'язкових реквізитів позбавляє документ юридичної сили у випадках, передбачених законодавством.

3.3. Електронні документи, що потребують підписання, підписуються відповідним видом електронного підпису, визначеним законодавством України, цим Положенням, внутрішніми документами Товариства або договором із Клієнтом чи контрагентом.

3.4. Перед прийняттям електронного документа Товариство забезпечує перевірку:

- цілісності електронного документа;
- дійсності електронного підпису та/або електронної печатки;
- чинності кваліфікованого сертифіката відкритого ключа на момент підписання документа;
- відсутності інформації про блокування, скасування або припинення дії сертифіката;
- повноважень підписувача у випадках, передбачених законодавством або договором.

3.5. У разі успішного проходження перевірок електронний документ вважається автентичним та може використовуватися в діяльності Товариства.

3.6. Якщо перевіркою встановлено порушення цілісності документа, недійсність електронного підпису, недійсність сертифіката або інші ознаки компрометації, такий документ не приймається до виконання, про що відповідний суб'єкт електронної взаємодії повідомляється у спосіб, визначений договором або внутрішніми процедурами Товариства.

3.7. Електронний документ вважається підписаним після успішного накладення електронного підпису та/або електронної печатки і підтвердження результату перевірки такого підпису відповідною інформаційною системою.

3.8. У разі необхідності внесення змін до вже підписаного електронного документа зміни оформлюються шляхом створення нового електронного документа або документа про внесення змін відповідно до вимог законодавства та умов договору. Зміна змісту підписаного електронного документа без повторного підписання не допускається.

3.9. Анулювання (скасування) електронного документа здійснюється у випадках та порядку, визначених законодавством України, договором між сторонами або шляхом оформлення окремого електронного документа (акта, угоди чи іншого документа), підписаного сторонами із використанням відповідного електронного підпису.

3.10. Суб'єкти електронної взаємодії забезпечують своєчасне отримання, перевірку, підписання та надсилання електронних документів відповідно до умов договорів та внутрішніх процедур Товариства.

3.11. Товариство забезпечує ведення журналів реєстрації операцій з електронними документами, що містять інформацію про створення, отримання, надсилання, підписання, перевірку, відмову у прийнятті, анулювання та інші дії з електронними документами.

3.12. Електронні документи та пов'язані з ними дані про перевірку електронних підписів, електронних печаток, сертифікатів відкритих ключів, відомості про дату та час їх підписання, а також журнали подій зберігаються протягом строків, установлених законодавством України та внутрішніми документами Товариства.

3.13. Товариство забезпечує захист, резервне копіювання, архівування та відновлення електронних документів відповідно до вимог законодавства України, нормативно-правових актів Національного банку України та внутрішніх документів щодо інформаційної безпеки та безперервності діяльності.

3.14. Кваліфікований електронний підпис має юридичну силу, рівнозначну власноручному підпису, а кваліфікована електронна печатка підтверджує походження електронного документа

від юридичної особи та забезпечує цілісність електронних даних відповідно до вимог законодавства України.

3.15. Електронні документи, підписані відповідно до вимог законодавства України та цього Положення, мають юридичну силу, є належними доказами у правовідносинах між сторонами та можуть використовуватися під час розгляду спорів, у тому числі в суді, якщо інше не встановлено законодавством України.

3.16. Використання удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті відкритого ключа (УЕП), кваліфікованого електронного підпису (КЕП) та електронної печатки

3.16.1. Використання Клієнтом удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті відкритого ключа (УЕП), кваліфікованого електронного підпису (КЕП), а також використання Товариством електронної печатки здійснюється відповідно до вимог законодавства України, нормативно-правових актів Національного банку України, цього Положення та договору, укладеного між Товариством і Клієнтом.

3.16.2. Право використання УЕП, КЕП або іншого допустимого законодавством засобу електронного підпису під час отримання платіжних та інших послуг виникає після:

- укладення між Товариством та Клієнтом відповідного договору;
- проведення ідентифікації, верифікації та, за необхідності, належної перевірки Клієнта відповідно до вимог законодавства України у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення;
- погодження сторонами порядку використання відповідного виду електронного підпису.

3.16.3. Договір про використання електронного підпису може бути укладений:

- у паперовій формі шляхом підписання власноручними підписами сторін;
- у формі електронного документа, підписаного КЕП або іншим видом електронного підпису, використання якого допускається законодавством України та погоджене сторонами;
- у процесі дистанційного встановлення ділових відносин відповідно до законодавства України та внутрішніх документів Товариства.

3.16.4. Якщо між Товариством та Клієнтом вже укладено договір, який передбачає використання електронного підпису, будь-які додаткові договори, заяви, повідомлення, платіжні інструкції, акти, додаткові угоди та інші електронні документи можуть оформлюватися із застосуванням погодженого сторонами виду електронного підпису без необхідності повторного укладення окремого договору щодо його використання, якщо інше не встановлено законодавством України або договором.

3.16.5. Товариство забезпечує перевірку чинності сертифіката відкритого ключа, належності електронного підпису відповідному підписувачу, а також цілісності електронного документа перед його прийняттям до виконання.

3.17. Вимоги до використання удосконаленого та кваліфікованого електронного підпису

3.17.1. Якщо порядок використання електронного підпису визначений договором про надання платіжних або інших послуг між Товариством та Клієнтом, укладення окремого договору щодо використання кваліфікованого електронного підпису (КЕП) або кваліфікованої електронної печатки не вимагається.

3.17.2. Товариство використовує УЕП, КЕП та кваліфіковану електронну печатку відповідно до законодавства України, нормативно-правових актів Національного банку України, цього Положення та внутрішніх документів Товариства.

3.17.3. УЕП застосовується у випадках, визначених законодавством України, договором із Клієнтом та внутрішніми документами Товариства.

3.17.4. До прийняття електронного документа, підписаного УЕП, Товариство забезпечує перевірку:

- цілісності електронного документа;
- належності електронного підпису підписувачу;
- чинності кваліфікованого сертифіката відкритого ключа;

- статусу сертифіката на момент підписання документа;
- відсутності ознак компрометації електронного підпису.

3.17.5. Електронний документ вважається підписаним належним чином після успішного завершення всіх процедур перевірки відповідно до вимог законодавства України.

3.18. Використання кваліфікованого електронного підпису

3.18.1. Кваліфікований електронний підпис створюється із використанням засобу кваліфікованого електронного підпису та кваліфікованого сертифіката відкритого ключа, виданого кваліфікованим надавачем електронних довірчих послуг.

3.18.2. Кваліфікований електронний підпис має юридичну силу, еквівалентну власноручному підпису, та користується презумпцією його відповідності власноручному підпису відповідно до законодавства України.

3.18.3. Товариство забезпечує приймання, реєстрацію, перевірку, оброблення, зберігання та архівування електронних документів, підписаних КЕП, із використанням інформаційних систем, що відповідають вимогам законодавства України.

3.18.4. Під час оформлення електронних копій паперових документів у процесі ідентифікації та верифікації Клієнтів Товариство застосовує КЕП та/або кваліфіковану електронну печатку, а також електронну позначку часу у випадках, передбачених законодавством або внутрішніми процедурами.

3.18.5. Перевірка КЕП здійснюється із використанням засобів перевірки електронного підпису відповідно до вимог законодавства України.

3.18.6. Підписувач зобов'язаний використовувати лише чинний кваліфікований сертифікат відкритого ключа та невідкладно повідомити кваліфікованого надавача електронних довірчих послуг у разі втрати контролю над особистим ключем або виникнення підозри щодо його компрометації.

3.18.7. Представник юридичної особи використовує кваліфікований сертифікат відкритого ключа, що містить відомості, необхідні для його ідентифікації як представника відповідної юридичної особи, відповідно до вимог законодавства України.

3.18.8. Забороняється створення електронного підпису із використанням нечинного, заблокованого, скасованого або такого сертифіката відкритого ключа, статус якого неможливо перевірити.

3.18.9. Товариство забезпечує ведення журналів перевірки електронних підписів, фіксацію результатів перевірки, а також зберігання відповідних записів протягом строків, визначених законодавством України та внутрішніми документами.

3.19. Порядок використання кваліфікованої електронної печатки

3.19.1. Товариство має право використовувати кваліфіковану електронну печатку під час:

- створення, підписання та засвідчення електронних документів;
- електронної взаємодії з Клієнтами, контрагентами, Національним банком України, органами державної влади та іншими суб'єктами електронної взаємодії;
- надання платіжних та інших послуг в електронній формі;
- автоматизованого формування документів, довідок, повідомлень, витягів та інших електронних документів.

3.19.2. Кваліфікована електронна печатка застосовується у випадках, коли це передбачено законодавством України, нормативно-правовими актами Національного банку України, договорами або внутрішніми документами Товариства.

3.19.3. Використання удосконаленої електронної печатки, що базується на кваліфікованому сертифікаті електронної печатки, допускається у випадках, визначених законодавством України та договором між суб'єктами електронної взаємодії.

3.19.4. Товариство самостійно визначає порядок застосування електронної печатки, перелік документів, які можуть засвідчуватися електронною печаткою, а також інформаційні системи та програмно-технічні засоби, у яких вона використовується. Кваліфікована електронна печатка може використовуватися, зокрема, для:

- засвідчення походження електронних документів від Товариства;
- підтвердження цілісності електронних документів;

- засвідчення електронних копій документів відповідно до вимог законодавства України;
- автоматизованого формування та засвідчення довідок, повідомлень, виписок, реєстрів, квитанцій, звітності та інших електронних документів;
- інших випадків, передбачених законодавством України або внутрішніми документами Товариства.

3.19.5. До прийняття електронного документа, засвідченого електронною печаткою, Товариство забезпечує перевірку:

- чинності кваліфікованого сертифіката електронної печатки;
- цілісності електронного документа;
- справжності електронної печатки;
- статусу сертифіката на момент створення електронної печатки.

3.19.6. Особистий ключ електронної печатки Товариства зберігається із застосуванням засобів криптографічного захисту інформації, що відповідають вимогам законодавства України. Доступ до використання особистого ключа надається виключно уповноваженим особам або автоматизованим інформаційним системам Товариства відповідно до встановлених прав доступу.

3.19.7. У разі втрати контролю над особистим ключем електронної печатки, виникнення підозри щодо його компрометації, закінчення строку чинності або скасування кваліфікованого сертифіката електронної печатки Товариство невідкладно припиняє використання відповідної електронної печатки, забезпечує блокування або скасування сертифіката та оформлює новий кваліфікований сертифікат у встановленому законодавством порядку.

3.20. Усі операції із використанням кваліфікованої електронної печатки підлягають журналюванню в інформаційних системах Товариства та повинні забезпечувати можливість подальшого аудиту, підтвердження автентичності та відстеження історії використання електронної печатки.

3.21. Кваліфікована електронна печатка використовується лише у випадках, коли її застосування відповідає вимогам законодавства України, нормативно-правових актів Національного банку України, договорів із Клієнтами та внутрішніх документів Товариства.

3.22. Накладання кваліфікованої електронної печатки здійснюється уповноваженими працівниками Товариства або автоматизованими інформаційними системами Товариства відповідно до наданих повноважень та встановлених прав доступу.

3.23. Товариство та інші юридичні особи – суб'єкти електронної взаємодії мають право використовувати кваліфіковану електронну печатку під час надання або отримання послуг в електронній формі, здійснення електронного документообігу та інформаційного обміну відповідно до вимог законодавства України.

3.24. Кваліфікований сертифікат електронної печатки повинен відповідати вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та містити відомості, необхідні для використання кваліфікованої електронної печатки.

3.25. До використання кваліфікованої електронної печатки Товариство забезпечує автоматизовану або ручну перевірку:

- чинності кваліфікованого сертифіката електронної печатки;
- статусу сертифіката (чинний, заблокований, скасований, строк дії закінчився);
- цілісності електронного документа;
- справжності кваліфікованої електронної печатки.

3.26. Товариство може використовувати одну або декілька кваліфікованих електронних печаток залежно від організаційної структури, функціонального призначення інформаційних систем, бізнес-процесів та вимог інформаційної безпеки.

3.27. Забороняється використання кваліфікованої електронної печатки у разі:

- закінчення строку чинності кваліфікованого сертифіката;
- блокування або скасування сертифіката;
- неможливості перевірки статусу сертифіката;
- втрати контролю над особистим ключем або виникнення підозри щодо його компрометації.

4. УПРАВЛІННЯ ОСОБИСТИМИ КЛЮЧАМИ ТА СЕРТИФІКАТАМИ

4.1. Товариство забезпечує управління життєвим циклом особистих ключів, кваліфікованих сертифікатів відкритих ключів, кваліфікованих електронних підписів та кваліфікованих електронних печаток відповідно до вимог законодавства України, нормативно-правових актів Національного банку України та внутрішніх документів Товариства.

4.2. Управління особистими ключами здійснюється з дотриманням принципів конфіденційності, цілісності, доступності, автентичності та простежуваності.

4.3. Отримання та використання особистих ключів

4.3.1. Особисті ключі та кваліфіковані сертифікати відкритих ключів отримуються виключно у кваліфікованих надавачів електронних довірчих послуг відповідно до вимог законодавства України.

4.3.2. Особистий ключ є конфіденційною інформацією та перебуває під виключним контролем його власника.

4.3.3. Забороняється:

- передавати особистий ключ іншим особам;
- копіювати особистий ключ, якщо це не передбачено вимогами законодавства або засобами кваліфікованого електронного підпису;
- повідомляти пароль або інші дані доступу до особистого ключа третім особам;
- використовувати особистий ключ після закінчення строку дії сертифіката або після його блокування чи скасування.

4.4. Зберігання особистих ключів

4.4.1. Особисті ключі зберігаються із використанням засобів кваліфікованого електронного підпису або інших захищених носіїв відповідно до вимог законодавства України.

4.4.2. Товариство забезпечує організаційні та технічні заходи щодо захисту особистих ключів від втрати, компрометації, несанкціонованого доступу, копіювання або використання.

4.4.3. Доступ до засобів кваліфікованого електронного підпису або електронної печатки надається лише уповноваженим особам відповідно до їх службових повноважень.

4.5. Контроль чинності сертифікатів

4.5. 1. Перед використанням кваліфікованого електронного підпису або кваліфікованої електронної печатки здійснюється перевірка:

- чинності кваліфікованого сертифіката;
- строку його дії;
- статусу сертифіката;
- цілісності електронного документа.

4.5.2. Товариство забезпечує використання лише чинних кваліфікованих сертифікатів відкритих ключів.

4.6 Компрометація особистого ключа

4.6.1. У разі втрати, викрадення, пошкодження носія особистого ключа, втрати контролю над ним або виникнення обґрунтованої підозри щодо його компрометації власник особистого ключа зобов'язаний невідкладно:

- припинити використання особистого ключа;
- повідомити безпосереднього керівника та відповідальний структурний підрозділ Товариства;
- звернутися до кваліфікованого надавача електронних довірчих послуг щодо блокування або скасування сертифіката.

4.6.2. До моменту отримання нового кваліфікованого сертифіката використання скомпрометованого особистого ключа забороняється.

4.6 3. Усі випадки компрометації особистих ключів підлягають реєстрації відповідно до внутрішніх процедур управління інцидентами інформаційної безпеки.

4.7. Заміна та припинення використання сертифікатів

4.7.1. Заміна кваліфікованого сертифіката здійснюється у разі:

- закінчення строку його чинності;
- зміни персональних або реєстраційних даних власника;
- зміни повноважень підписувача;

- компрометації особистого ключа;
- інших випадків, визначених законодавством України.

4.7.2. У разі припинення трудових відносин або припинення повноважень працівника Товариство забезпечує припинення використання відповідного особистого ключа та вживає заходів щодо блокування або скасування сертифіката відкритого ключа.

4.8. Контроль та аудит

4.8.1. Товариство забезпечує ведення журналів використання кваліфікованих електронних підписів та електронних печаток, а також облік операцій із сертифікатами відкритих ключів.

4.8.2. Використання особистих ключів, кваліфікованих сертифікатів та електронних печаток підлягає періодичному контролю в межах системи внутрішнього контролю, управління ризиками та інформаційної безпеки.

4.8.3. Результати перевірок та виявлені порушення документуються, а за потреби є підставою для вжиття заходів реагування відповідно до внутрішніх документів Товариства.

5. СТВОРЕННЯ ТА ЗАСВІДЧЕННЯ ЕЛЕКТРОННОЇ КОПІЇ ПАПЕРОВОГО ДОКУМЕНТА

5.1. Електронна копія паперового документа створюється шляхом сканування, фотографування або іншого способу оцифрування паперового документа, що забезпечує повне та достовірне відтворення його змісту, реквізитів і візуальної форми.

5.2. Електронна копія повинна бути придатною для візуального сприйняття, містити всі сторінки документа та забезпечувати можливість однозначної ідентифікації його змісту.

5.3. Відповідність електронної копії паперового документа його оригіналу засвідчується шляхом накладення кваліфікованого електронного підпису (КЕП) або удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті відкритого ключа (УЕП), уповноваженою особою Товариства відповідно до вимог законодавства України та внутрішніх документів Товариства.

5.4. У випадках, визначених законодавством України або внутрішніми документами Товариства, електронна копія паперового документа додатково засвідчується кваліфікованою електронною печаткою Товариства та/або електронною позначкою часу.

5.5. Право створення та засвідчення електронних копій паперових документів надається працівникам Товариства, визначеним наказом або іншим розпорядчим документом керівника Товариства.

5.6. Створення електронних копій паперових документів здійснюється із забезпеченням цілісності, достовірності, конфіденційності та захисту інформації відповідно до вимог законодавства України та внутрішніх документів Товариства з питань інформаційної безпеки.

5.7. Електронні копії паперових документів зберігаються в інформаційних системах Товариства протягом строків, установлених законодавством України та внутрішніми документами Товариства, із забезпеченням їх цілісності, доступності та можливості перевірки електронного підпису й електронної печатки.

5.8. На вимогу Клієнта Товариство надає:

- документ, оформлений у паперовій формі, якщо це передбачено законодавством або договором;
- паперову копію електронного документа;
- електронний примірник оригіналу електронного документа або його копію в електронній формі у форматі, що забезпечує можливість перевірки електронного підпису та/або електронної печатки.

5.9. Надання електронних копій або примірників електронних документів здійснюється способом, що забезпечує захист інформації, автентичність документів та дотримання вимог законодавства України щодо захисту інформації та персональних даних.

6. СТВОРЕННЯ ТА ЗАСВІДЧЕННЯ ПАПЕРОВОЇ КОПІЇ ЕЛЕКТРОННОГО ДОКУМЕНТА

6.1. Паперова копія електронного документа є його візуальним поданням на паперовому носії,

створеним шляхом друку електронного документа та засвідченим відповідно до вимог законодавства України і цього Положення.

6.2. Перед створенням паперової копії Товариство забезпечує перевірку:

- цілісності електронного документа;
- чинності та коректності електронного підпису та/або електронної печатки;
- чинності кваліфікованого сертифіката відкритого ключа на момент підписання документа;
- можливості підтвердження автентичності електронного документа.

6.3. Після успішної перевірки електронний документ може бути відтворений на паперовому носії шляхом друку.

6.4. Паперова копія електронного документа засвідчується керівником Товариства або уповноваженою ним особою шляхом проставлення:

- відмітки «Копія» (за потреби);
- напису про засвідчення копії;
- найменування посади особи, яка засвідчує копію;
- особистого підпису;
- власного імені та прізвища;
- дати засвідчення копії.

За наявності та у випадках, передбачених законодавством України або внутрішніми документами Товариства, паперова копія додатково засвідчується відбитком печатки Товариства.

6.5. Якщо паперова копія використовується виключно для внутрішнього документообігу Товариства, її засвідчення може здійснюватися без використання печатки, якщо інше не встановлено законодавством України або внутрішніми документами Товариства.

6.6. Якщо паперова копія складається з двох і більше аркушів, вони можуть бути пронумеровані та скріплені у спосіб, що унеможлиблює підміну окремих аркушів. У випадках, визначених законодавством України або внутрішніми документами Товариства, на місці скріплення робиться відповідна відмітка із зазначенням кількості аркушів та засвідчується підписом уповноваженої особи.

6.7. У разі засвідчення кожного аркуша паперової копії окремо прошивання багатосторінкового документа не є обов'язковим, якщо інше не передбачено законодавством України.

6.8. На вимогу суду, Національного банку України, органів державної влади, правоохоронних органів, аудиторів або інших осіб, які мають відповідні повноваження згідно із законодавством України, Товариство забезпечує надання належним чином засвідченої паперової копії електронного документа.

6.9. Засвідчення паперової копії електронного документа не змінює юридичного статусу його електронного оригіналу. Оригіналом документа залишається електронний документ, підписаний відповідно до вимог законодавства України із застосуванням електронного підпису та/або електронної печатки.

7. КОНТРОЛЬ ЦІЛІСНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ТА ВИЯВЛЕННЯ ЗМІН

7.1. Товариство забезпечує контроль цілісності електронних документів та електронних копій паперових документів протягом усього строку їх зберігання та використання.

7.2. Для виявлення змін в електронному документі або електронній копії паперового документа здійснюється перевірка:

- цілісності електронного документа;
- дійсності електронного підпису та/або електронної печатки;
- чинності кваліфікованого сертифіката відкритого ключа;
- електронної позначки часу (у разі її використання).

7.3. Перевірка електронного підпису та електронної печатки здійснюється із використанням засобів перевірки, що відповідають вимогам законодавства України у сфері електронної ідентифікації та електронних довірчих послуг.

7.4. Інформаційні системи та системи електронного документообігу, що використовуються Товариством, повинні забезпечувати:

- збереження історії змін електронних документів (за наявності механізму версійності);

- фіксацію дати і часу створення, підписання, отримання, зміни статусу та інших дій щодо електронного документа;
- ідентифікацію особи або автоматизованої системи, яка здійснила відповідну дію;
- ведення журналів подій (audit logs), достатніх для проведення внутрішнього контролю та аудиту.

7.5. Якщо під час перевірки встановлено порушення цілісності електронного документа або неможливість підтвердження дійсності електронного підпису чи електронної печатки, такий документ не приймається до виконання до з'ясування причин та проведення відповідної перевірки.

7.6. Виявлені випадки порушення цілісності електронних документів, недійсності електронних підписів або електронних печаток, а також інші інциденти, пов'язані з електронним документообігом, підлягають обов'язковій реєстрації та розгляду відповідно до внутрішніх документів Товариства щодо управління інцидентами інформаційної безпеки.

7.7. Будь-яке внесення змін до електронного документа після його підписання призводить до порушення його цілісності, що виявляється під час перевірки електронного підпису та/або електронної печатки. У такому випадку підтвердити автентичність документа неможливо до усунення причин невідповідності.

7.8. У разі необхідності внесення змін до змісту вже підписаного електронного документа створюється новий електронний документ або документ про внесення змін, який підписується відповідно до вимог законодавства України та цього Положення.

8. ПЕРЕВІРКА ЕЛЕКТРОННОГО ПІДПISУ ПІСЛЯ ПІДПISАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТА

8.1. Після накладення електронного підпису та/або електронної печатки Товариство забезпечує можливість перевірки їх дійсності протягом усього строку зберігання електронного документа.

8.2. Перевірка електронного підпису здійснюється шляхом перевірки:

- цілісності електронного документа;
- автентичності електронного підпису та/або електронної печатки;
- чинності кваліфікованого сертифіката відкритого ключа;
- статусу сертифіката на момент підписання документа;
- електронної позначки часу (за наявності).

8.3. Для перевірки електронного підпису Товариство використовує засоби перевірки електронних довірчих послуг, що відповідають вимогам законодавства України та забезпечують можливість підтвердження дійсності електронного підпису і кваліфікованої електронної печатки.

8.4. Інформаційні системи та системи електронного документообігу Товариства повинні забезпечувати:

- збереження інформації про накладені електронні підписи та електронні печатки;
- фіксацію дати і часу підписання;
- журналювання операцій із підписання, перевірки та використання електронних документів;
- можливість проведення аудиту дій користувачів.

8.5. Якщо під час перевірки встановлено порушення цілісності електронного документа або неможливість підтвердження дійсності електронного підпису чи електронної печатки, такий документ не приймається до виконання до завершення перевірки причин виявленої невідповідності.

8.6. Будь-які зміни до змісту електронного документа після його підписання призводять до порушення його цілісності та виявляються під час перевірки електронного підпису або електронної печатки. У такому випадку результати перевірки не підтверджують дійсність електронного підпису щодо зміненого документа.

8.7. Усі випадки негативного результату перевірки електронного підпису або електронної печатки підлягають реєстрації, аналізу та розгляду відповідно до внутрішніх документів Товариства з питань управління інцидентами інформаційної безпеки.

9. КОНТРОЛЬ ЦІЛІСНОСТІ ЕЛЕКТРОННОЇ ПЕЧАТКИ ТА ВИЯВЛЕННЯ ЗМІН ПІСЛЯ ЇЇ ВИКОРИСТАННЯ

9.1. Після накладення кваліфікованої електронної печатки або удосконаленої електронної печатки, що базується на кваліфікованому сертифікаті, Товариство забезпечує можливість перевірки їх дійсності та цілісності електронного документа протягом усього строку його зберігання.

9.2. Для виявлення змін після накладення електронної печатки здійснюється перевірка:

- цілісності електронного документа;
- автентичності електронної печатки;
- чинності кваліфікованого сертифіката електронної печатки;
- статусу сертифіката на момент створення електронної печатки;
- електронної позначки часу (у разі її використання).

9.3. Перевірка електронної печатки здійснюється із застосуванням засобів перевірки електронних довірчих послуг, що відповідають вимогам законодавства України.

9.4. Інформаційні системи та системи електронного документообігу Товариства повинні забезпечувати:

- журналювання операцій із використання електронної печатки;
- фіксацію дати та часу накладення електронної печатки;
- збереження інформації про використаний сертифікат електронної печатки;
- ведення історії змін електронних документів (за наявності механізму версійності);
- можливість проведення аудиту дій користувачів та автоматизованих процесів.

9.5. Якщо під час перевірки встановлено порушення цілісності електронного документа або неможливість підтвердження дійсності електронної печатки, такий документ не приймається до виконання до завершення перевірки причин виявленої невідповідності.

9.6. Будь-які зміни до електронного документа після накладення електронної печатки призводять до порушення його цілісності та виявляються під час перевірки електронної печатки. У такому випадку результати перевірки не підтверджують дійсність електронної печатки щодо зміненого документа.

9.7. Усі випадки негативного результату перевірки електронної печатки, порушення цілісності електронних документів або інших інцидентів, пов'язаних із використанням електронної печатки, підлягають обов'язковій реєстрації, аналізу та розгляду відповідно до внутрішніх документів Товариства щодо управління інцидентами інформаційної безпеки.

10. УПРАВЛІННЯ РИЗИКАМИ ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПISУ ТА ЕЛЕКТРОННОЇ ПЕЧАТКИ

10.1. Товариство застосовує ризик-орієнтований підхід до використання електронного підпису та електронної печатки відповідно до вимог законодавства України, нормативно-правових актів Національного банку України, внутрішніх документів з управління ризиками та інформаційною безпекою.

10.2. Управління ризиками здійснюється протягом усього життєвого циклу електронного документа, включаючи його створення, підписання, передавання, отримання, оброблення, зберігання, архівування та знищення.

10.3. Під час організації електронної взаємодії Товариство забезпечує належний рівень захисту інформації відповідно до категорії інформаційних активів, рівня ризику та критичності бізнес-процесу.

10.4. Ідентифікація ризиків

Товариство здійснює постійну ідентифікацію ризиків, пов'язаних із використанням електронного підпису та електронної печатки, зокрема:

- компрометація особистих ключів;
- несанкціоноване використання електронного підпису або електронної печатки;
- використання прострочених, заблокованих або відкликаних сертифікатів;
- підроблення або модифікація електронних документів;
- відсутність можливості перевірки електронного підпису;

- несанкціонований доступ до засобів КЕП;
- відмова інформаційних систем;
- кібератаки;
- внутрішнє шахрайство;
- помилки працівників;
- використання неавторизованого програмного забезпечення;
- порушення вимог законодавства щодо електронної взаємодії.

10.5.Оцінка ризиків

Оцінка ризиків здійснюється із врахуванням:

- ймовірності виникнення події;
- можливого фінансового впливу;
- впливу на безперервність діяльності;
- впливу на права клієнтів;
- регуляторних наслідків;
- репутаційних втрат;
- впливу на інформаційну безпеку.

За результатами оцінки ризику класифікуються як:

- низькі;
- помірні;
- значні;
- критичні.

10.6. Заходи контролю

Для мінімізації ризиків Товариство забезпечує:

- використання виключно чинних сертифікатів;
- багаторівневу автентифікацію користувачів інформаційних систем;
- розмежування прав доступу;
- принцип мінімально необхідних повноважень;
- застосування електронної позначки часу;
- журналювання усіх операцій;
- контроль використання ключової інформації;
- резервне копіювання;
- шифрування інформації;
- моніторинг аномальної активності;
- регулярний перегляд прав доступу;
- контроль використання службових облікових записів;
- контроль використання електронної печатки автоматизованими системами.

10.7. Моніторинг

Товариство здійснює безперервний моніторинг:

- використання електронних підписів;
- використання електронних печаток;
- спроб несанкціонованого використання;
- компрометації ключів;
- змін сертифікатів;
- інцидентів інформаційної безпеки;
- журналів аудиту;
- працездатності сервісів електронних довірчих послуг.

Моніторинг здійснюється відповідно до внутрішніх процедур Платіжної установи та з використанням наявних організаційних, технічних і програмних засобів контролю.

10.8. Управління інцидентами

У разі виявлення:

- компрометації особистого ключа;
- втрати носія ключової інформації;
- використання недійсного сертифіката;

- несанкціонованого підписання документа;
- порушення цілісності електронного документа;
- порушення роботи сервісів електронних довірчих послуг;

Товариство забезпечує:

- негайне блокування використання відповідного ключа;
- повідомлення відповідальних осіб;
- реєстрацію інциденту;
- оцінку впливу;
- проведення службового розслідування;
- визначення коригувальних заходів;
- повідомлення компетентних органів та Національного банку України у випадках, передбачених законодавством.

10.10. Відповідальність

Керівники структурних підрозділів забезпечують виконання вимог цього Положення.

Працівники Товариства несуть персональну відповідальність за:

- збереження особистих ключів;
- нерозголошення автентифікаційних даних;
- дотримання вимог інформаційної безпеки;
- своєчасне повідомлення про компрометацію ключів або інші інциденти.

Головний ризик-менеджер здійснює оцінку ризиків використання електронних підписів та електронних печаток.

Відповідальна особа з інформаційної безпеки здійснює контроль технічних засобів захисту, моніторинг кіберінцидентів та контроль виконання вимог цього Положення.

Головний внутрішній аудитор (за наявності) здійснює незалежну оцінку ефективності системи контролю використання електронних підписів та електронних печаток відповідно до затвердженого плану аудиту.

11. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

11.1. Це Положення є внутрішнім нормативним документом Товариства та є обов'язковим для виконання всіма працівниками, посадовими особами, членами органів управління, а також іншими особами, які в межах своїх повноважень використовують електронний підпис, електронну печатку або беруть участь у процесах електронного документообігу.

11.2. Керівник Товариства забезпечує організацію системи використання електронних підписів та електронних печаток, визначає відповідальних осіб, забезпечує необхідні організаційні, технічні та фінансові ресурси для виконання вимог цього Положення.

11.3. Керівники структурних підрозділів забезпечують виконання вимог цього Положення працівниками відповідних підрозділів, здійснюють контроль за дотриманням встановлених процедур та невідкладно повідомляють про виявлені порушення.

11.4. Працівники Товариства несуть персональну відповідальність за:

- належне використання електронних підписів та електронних печаток;
- збереження особистих ключів та засобів кваліфікованого електронного підпису;
- нерозголошення автентифікаційних даних;
- дотримання вимог законодавства України, цього Положення та інших внутрішніх документів Товариства.

11.5. Використання електронних підписів та електронних печаток є складовою системи внутрішнього контролю, системи управління ризиками та системи управління інформаційною безпекою Товариства.

11.6. Товариство застосовує ризик-орієнтований підхід до організації процесів електронного документообігу, використання електронних підписів та електронних печаток, а також забезпечує постійний моніторинг відповідних ризиків, оцінку ефективності контрольних заходів та впровадження необхідних коригувальних заходів.

11.7. Контроль за дотриманням вимог цього Положення здійснюється відповідно до моделі трьох ліній захисту:

- перша лінія захисту — структурні підрозділи та працівники, які використовують електронні підписи та електронні печатки;
- друга лінія захисту — підрозділи з управління ризиками, комплаєнсу та інформаційної безпеки в межах своїх повноважень;
- третя лінія захисту — підрозділ внутрішнього аудиту (у разі його створення) шляхом проведення незалежної оцінки ефективності системи внутрішнього контролю.

11.8. Товариство забезпечує ознайомлення та, за необхідності, навчання працівників з питань:

- використання електронних підписів та електронних печаток;
- вимог законодавства України у сфері електронної ідентифікації та електронних довірчих послуг;
- інформаційної та кібербезпеки;
- управління операційними ризиками та ризиками інформаційної безпеки;
- реагування на інциденти, пов'язані з використанням електронних підписів та електронних печаток.

Порядок, періодичність та форми проведення такого навчання або ознайомлення визначаються внутрішніми документами Товариства.

11.9. Це Положення переглядається не рідше одного разу на рік, а також у разі:

- внесення змін до законодавства України або нормативно-правових актів Національного банку України;
- зміни організаційної структури або бізнес-процесів Товариства;
- впровадження нових інформаційних систем або технологій;
- виникнення суттєвих інцидентів інформаційної чи кібербезпеки;
- виявлення недоліків під час внутрішнього контролю, внутрішнього аудиту, перевірок Національного банку України або зовнішнього аудиту.

11.10. Зміни до цього Положення затверджуються уповноваженим органом управління Товариства відповідно до його внутрішніх документів.

11.11. Якщо окремі положення цього Положення суперечать вимогам законодавства України внаслідок внесення до нього змін, застосовуються норми законодавства України до моменту внесення відповідних змін до цього Положення.

11.12. Товариство забезпечує захист інформації, персональних даних, ключової інформації та інших інформаційних активів відповідно до вимог законодавства України, нормативно-правових актів Національного банку України, внутрішніх документів із питань інформаційної безпеки та кіберзахисту.

11.13. Документи, журнали подій, інформація про використання електронних підписів та електронних печаток, результати перевірок, журнали аудиту та інші матеріали, пов'язані з електронним документообігом, зберігаються протягом строків, установлених законодавством України та внутрішніми документами Товариства.

11.14. Товариство забезпечує взаємодію з кваліфікованими надавачами електронних довірчих послуг, державними органами, Національним банком України, контрагентами та іншими суб'єктами електронної взаємодії з метою забезпечення безперервності, сумісності та безпеки електронного документообігу.

11.15. Використання електронних підписів та електронних печаток у Товаристві здійснюється з дотриманням принципів законності, безперервності діяльності, ризик-орієнтованого підходу, інформаційної безпеки, конфіденційності, цілісності, автентичності, доступності інформації та простежуваності дій користувачів.