ЗАТВЕРДЖЕНО

Рішенням Наглядової ради
АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»
Протокол від 23.04.2026 р. № 50

ПОГОДЖЕНО

Рішенням Правління
АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»
Протокол від 22.04.2026 р. № 34

…

ВИТЯГ ІЗ ПОЛІТИКИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»

1. ПРИНЦИПИ ОРГАНІЗАЦІЇ КРИПТОГРАФІЧНОГО ЗАХИСТУ

1.1. Криптографічний захист в Банку організовується за дотримання наступних принципів:

забезпечення нормативної відповідності – криптографічний захист організовано у відповідності до вимог нормативно-правових актів України, Національного банку України стандартів з питань інформаційної безпеки, вимог міжнародних та внутрідержавних платіжних систем та систем переказу коштів, внутрішніх нормативних документів;

системної діяльності - діяльність із забезпечення криптографічного захисту проводиться в рамках СУІБ, є системною, має циклічний характер, відповідає моделі циклічності Демінга "PDCA" (Plan– Do– Check– Act, Плануй-Виконуй-Перевіряй-Дій);

персональної відповідальності – за реалізацію та виконання визначених заходів та вимог криптографічного захисту передбачена персональна відповідальність, об’єм якої визначається внутрішніми нормативними/розпорядчими документами Банку. Персональна відповідальність за реалізацію та виконання вимог криптографічного захисту є складовою частиною Кодексу корпоративної етики**;**

виправданості витрат – об’єм ресурсів залучених/запланованих для криптографічного захисту має відповідати наявним/прогнозованим загрозам і не повинен перевищувати об’єм збитків, що можуть виникнути внаслідок Інцидентів безпеки/реалізації Загроз;

достатньої компетенції – персонал Банку та Постачальника послуг мають рівень обізнаності достатній для: адекватного реагування на інциденти, ефективної протидії загрозам інформаційної безпеки та дотримання вимог криптографічного захисту. В Банку проводиться навчання з інформаційної безпеки та контроль рівня знань Персоналу в галузі криптографічного захисту;

забезпечення конфіденційності – використання шифрування інформації для захисту інформації з обмеженим доступом, як збереженої, так і тієї, що передається;

забезпечення цілісності/автентичності – використання електронних підписів або кодів аутентифікації повідомлення для захисту автентичності та цілісності збереженої інформації з обмеженим доступом або тієї, що передається;

забезпечення неспростовності – використання криптографічних методів для отримання доказів виникнення або не виникнення факту застосування СКЗІ, які будуються на основі засобів КЗІ, що мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи в сфері КЗІ.

забезпечення безперервності – в Банку діє процес управління безперервністю діяльності, який забезпечує безперебійну роботу СКЗІ.

….

7. ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПИСУТА ПЕЧАТКИ

7.1. Електронний підпис виступає невід'ємним та обов'язковим елементом (реквізитом) будь-якого електронного документа. Банк впроваджує технічні рішення, що дозволяють підтвердити автентичність та незмінність (цілісність) даних в електронних документах, сформованих у внутрішніх системах.

7.2. Накладанням ЕП підписант підтверджує повне ознайомлення зі змістом документа, його однозначне розуміння та відсутність зауважень (або фіксацію таких зауважень у спеціальному полі). Використання ЕП є свідомим актом підтвердження волевиявлення (затвердження, візування або погодження) у межах контексту документа.

7.3. У взаємодії з клієнтами та партнерами Банк впроваджує інформаційні системи з інтегрованими механізмами захисту, що гарантують незмінність підписаних файлів. Процеси формування та архівації електронної документації в Банку побудовані таким чином, щоб за потреби незалежна третя сторона (узгоджена з Банком) могла провести перевірку автентичності та цілісності даних.

7.4. У разі підписання документа кількома сторонами, ЕП накладаються у чіткій послідовності, визначеній відповідним технологічним процесом, договором. Технологія обробки розробляється згідно з нормами законодавства, а формування документа вважається завершеним лише після накладання останнього необхідного ЕП.

7.5. Порядок надання, відкликання та моніторингу прав доступу до систем Банку, що задіяні в обігу електронних документів, регулюється окремими внутрішніми нормативними документами. Створення кваліфікованих/удосконалених підписів/печаток для застосування в роботі здійснюють працівники Банку, які мають на це відповідні повноваження.

7.6. Під час роботи з електронними документами (приймання, обробка, архівація) Банк суворо дотримується принципу мінімальних привілеїв: користувачі отримують лише той обсяг повноважень, що необхідний для виконання їхніх функцій. Використовувані ІТ-системи повністю відповідають стандартам інформаційної безпеки НБУ (зокрема Положенню №95), вимогам законодавства України та внутрішнім нормативним документам з інформаційної безпеки.

7.7. Порядок доступу до ресурсів Банку, що забезпечують повний життєвий цикл електронного документа (від реєстрації до зберігання), деталізується в нормативних документах Банку.

7.8. В Банку під час створення, оброблення та зберігання електронних документів використовуються:

1) кваліфікований ЕП (КЕП);
2) УЕП з кваліфікованим сертифікатом;
3) ЕП Національного банку України;
4) простий ЕП;
5) кваліфікована електронна печатка;
6) удосконалена електронна печатка;
7) ЦВП цифровий власноручний підпис.

7.9. Питання щодо застосування типу ЕП в процесах Банку визначається власником процесу з урахуванням законодавчих та нормативних вимог в сфері електронного документообігу, інформаційної безпеки та кіберзахисту.

7.10. Особливості використання ЕП в конкретних процесах Банку визначаються шляхом:

1) внесення таких особливостей власником процесу до внутрішніх нормативних документів банку, що визначають вимоги до відповідного процесу або описують процес, або
2) створення окремого порядку використання ЕП в визначеному процесі.

7.11. Електронні підписи, які інтегровані в бізнес-процеси Банку, мають повну юридичну силу. Це не залежить від конкретних методів ідентифікації підписувача, за умови дотримання таких критеріїв:

1) логічно пов'язуються з підписаними електронними даними із можливістю перевірити цей зв'язок протягом усього життєвого циклу електронного документа;

2) електронні дані, що використовуються для створення ЕП, є унікальними та однозначно пов'язані із Підписувачем і не пов'язані з жодною іншою особою;

3) дають змогу однозначно ідентифікувати Підписувача;

4) перевірка ЕП виконана виключно відповідним до виду ЕП засобом КЗІ окремим чи вбудованим в платіжну чи інформаційну систему (Удосконалений ЕП, Кваліфікований ЕП, УЕП з кваліфікованим сертифікатом, ЕП НБУ, Удосконалена електронна печатка, Кваліфікована електронна печатка) або за допомогою засобу перевірки ЕП інформаційної системи, у якій здійснюється створення, оброблення, зберігання електронних документів (простий ЕП);

5) технологія застосування ЕП забезпечує під час підписання контроль електронних даних, які підписуються, та електронних даних, які використовуються для створення ЕП;

6) під час перевірки, не виявлено будь-яких змін в електронному документі та/або будь-яких змін ЕП після підписання електронного документа.

7.12. Процедура виявлення будь-яких змін в електронному документі, цифровій копії паперового оригіналу або самому ЕП після моменту підписання реалізується через перевірку валідності підпису. Залежно від типу ЕП, цей процес здійснюється внутрішніми інструментами інформаційної системи (для Простих ЕП) або спеціалізованими засобами КЗІ (для інших видів). Якщо підпис не проходить перевірку, такий документ автоматично відхиляється від подальшого опрацювання.

7.13. Перевірка цілісності документів та їхніх цифрових копій, завірених Удосконаленим ЕП (зокрема з кваліфікованим сертифікатом) або Кваліфікованим ЕП, проводиться з використанням криптографічного захисту. Ці засоби відповідають законодавству, нормативним актам НБУ та враховуючи умови п.7.11. Успішне підтвердження цілісності гарантує, що зміст документа залишився незмінним з моменту його підписання.

7.14. В разі, якщо функціоналом автоматизованої системи Банка не передбачена перевірка електронного підпису/ печатки необхідно виконати перевірку в ручному режимі.

7.15. Для уніфікації процесу перевірки КЕП на електронному документі, перевірки цілісності документу, наявності всіх необхідних реквізитів та властивостей підписаного документу, працівник Банку повинен скористатися, наприклад, WEB-ресурсом Центрального засвідчувального органу Міністерства цифрової трансформації України (далі – ЦЗО): https://czo.gov.ua/verify. Під час перевірки документу у WEB-ресурсі, наприклад ЦЗО працівник Банку встановлює, що документ підписаний, цілісний, підписаний кваліфікованим ЕП і є можливість вивантажити протокол перевірки. В протоколі перевірки має обов'язково значитися інформація:

1) Дата та час перевірки;
2) Назва файлу з підписом;
3) Розмір файлу з підписом;
4) Назва файлу без підпису;
5) Розмір файлу без підпису;
6) Результат перевірки підпису: «Файл успішно перевірено. Усі дані цілі»;
7) П.І.Б. підписувача.

Якщо підписувач (контрагент/клієнт Банку) діє від імені юридичної особи, протокол перевірки має додатково містити:

1) РНОКПП і назву юридичної особи
2) Код ЄДРПОУ юридичної особи;
3) Час підпису (має бути підтверджено кваліфікованою позначкою часу для підпису від Надавача);
4) Тип носія на якому був КЕП/Печатка;
5) Ким виданий кваліфікований сертифікат (назву КНЕДП, де підписувач отримав КЕП/Печатку);
6) Серійний номер сертифікату;
7) Застосований алгоритм підпису (наприклад ДСТУ-4145);
8) Тип підпису, наприклад кваліфікований або удосконалений;
9) Тип контейнера, наприклад: підпис та дані в одному файлі (CAdES enveloped);
10) Формат підпису: з повними даними ЦСК для перевірки (CAdES-X Long);
11) Тип сертифікату, наприклад «Кваліфікований».

За необхідності, працівник може зберегти протокол перевірки підпису у якості свідчення проведення перевірки документа.

7.16. Моніторинг незмінності документів, підписаних Простим ЕП, ЦВП покладається на функціонал тієї інформаційної системи, де відбувається життєвий цикл документа (створення, обіг, архівування). Процес має відповідати безпековим вимогам, викладеним у пункті 7.11 цього документа.

7.17. Всі працівники Банку, що приймають участь у процесах із використанням ЕП, мають ознайомлюються з даною Політикою та особливостями використання ЕП в конкретних процесах Банку, які визначені внутрішніми нормативними документами.