Національний банк України
Оператор Національної платіжної системи
“Український платіжний простір”

ЗАТВЕРДЖЕНО
Рішення Ради Платіжної організації
Національної платіжної системи
“Український платіжний простір”
(протокол від 03.09.2018 № 57/20/2018)

Із змінами, внесеними рішенням
Ради Оператора НПС “ПРОСТІР”:
(протокол від 28.06.2024 № 57/13/2024)

Порядок
роботи з криптографічними ключами
модулів безпеки Національної платіжної системи
“Український платіжний простір”

ПРОСТІР
український платіжний простір

м. Київ

Зміст

1. Загальні положення

1.1. Цей Порядок розроблений згідно із законами України “Про Національний банк України”, “Про банки і банківську діяльність”, “Про платіжні послуги”, Правилами Національної платіжної системи “Український платіжний простір”, затвердженими рішенням Ради Платіжної організації НПС “ПРОСТІР” (протокол від 07.06.2013 № 213/2013), із змінами (далі – Правила), Концепцією розвитку систем криптографічного захисту інформації в Національному банку України, затвердженою рішенням Правління Національного банку України від 20 січня 2017 року № 40, Політикою використання криптографічних засобів захисту інформації в Національному банку України, затвердженою розпорядженням Національного банку України від 20 серпня 2019 року № 419-но, іншими законодавчими актами України та нормативно-правовими актами Національного банку України та документами Оператора Національної платіжної системи “Український платіжний простір” (далі – Оператор).

(пункт 1.1 розділу 1 із змінами, внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024))

1.2. Порядок розроблений з метою запровадження єдиних підходів, спрямованих на забезпечення безпеки криптографічних ключів, зниження ризиків несанкціонованого доступу до них, втрати або порушення цілісності інформації у межах взаємодії учасників Національної платіжної системи “Український платіжний простір” (далі – НПС “ПРОСТІР”) або незалежних процесингових центрів (далі – НПЦ) з Центральним маршрутизатором НПС “ПРОСТІР” (далі – Маршрутизатор).

(пункт 1.2 розділу 1 із змінами, внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024))

1.3. Порядок визначає процедуру взаємодії учасника НПС “ПРОСТІР” (далі – учасник) / НПЦ з офіцерами безпеки НПС “ПРОСТІР” у частині роботи з транспортними ключами ZMK та ключами шифрування ПІН-блоків ZPK.

(пункт 1.3 розділу 1 із змінами, внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024))

1.4. Учасники/НПЦ зобов’язані забезпечити захист даних криптографічних ключів під час їх передачі, використанні, зберіганні та знищенні відповідно до процедур, описаних у цьому Порядку.

(пункт 1.4 розділу 1 із змінами, внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024))

1.5. Організація та проведення робіт із забезпечення захисту даних криптографічних ключів під час їх генерації, передачі, використанні, зберіганні та знищенні повинні здійснюватися відповідно призначеними особами, обов’язком яких є забезпечення контролю за станом організації захисту, проведення проектування, розроблення і модернізації систем захисту, а також учасниками вказаних процесів.

1.6. Терміни в цьому Порядку вживаються в такому значенні:

ключ шифрування ПІН-блоків (ZPK – Zone PIN Key) – криптографічний ключ, призначений для безпечної передачі ПІН-блоків між Маршрутизатором та учасниками/НПЦ. Генерується Маршрутизатором і передається офіцерам безпеки учасників/НПЦ;

криптограма – дані, які зашифровані за допомогою криптографічного алгоритму та криптографічного ключа;

криптографічний ключ (cryptographic key) – унікальна послідовність символів, яка використовується для перетворення даних за допомогою криптографічного алгоритму;

компрометація ключа – втрата довіри до того, що криптографічний ключ забезпечує безпеку інформації, зокрема виявлення власником криптографічного ключа обставин, за яких можливо несанкціоноване використання, підозра на несанкціоноване використання криптографічного ключа неуповноваженими особами тощо;

модуль безпеки НПС “ПРОСТІР” (модуль безпеки, HSM – Hardware Security Module) – апаратний криптографічний пристрій, призначений для генерації, захисту та керування криптографічними ключами;

офіцери безпеки НПС “ПРОСТІР” – призначені рішенням Ради Оператора НПС “ПРОСТІР” працівники Оператора, які супроводжують процеси генерації, зберігання та видачі криптографічних ключів;

офіцери безпеки учасника/НПЦ – працівники учасника/НПЦ, яким надається право отримання, зберігання, імплементації та знищення компонентів транспортного ключа і криптограм ключів шифрування ПІН-блоків;

транспортний ключ (ZMK – Zone Master Key) – криптографічний ключ, призначений для безпечної передачі ключів шифрування ПІН-блоків між Маршрутизатором та учасниками/НПЦ. Генерується Маршрутизатором у вигляді 3 (трьох) компонентів транспортного ключа і передається 3 (трьом) офіцерам безпеки учасника/НПЦ.

(пункт 1.6 розділу 1 із змінами, внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024))

2. Процедура генерації та передачі криптографічних ключів

2.1. Маршрутизатор, здійснює генерацію компонентів транспортного ключа та криптограми ключа шифрування ПІН-блоків для учасника/НПЦ:

1) на підставі заяви учасника/НПЦ (додаток 1);

2) у випадку позапланової заміни криптографічних ключів на підставі заяви учасника/НПЦ (додаток 5);

3) у разі завершення строку дії криптографічних ключів (2 роки від дати генерації криптографічних ключів).

За результатом генерації транспортного ключа ZMK для учасника/НПЦ друкуються компоненти ключа в захищених ПІН-конвертах.

(пункт 2.1 розділу 2 викладено в новій редакції згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

2.2. Офіцери безпеки НПС "ПРОСТІР" здійснюють передачу захищених ПІН-конвертів з компонентами транспортного ключа ZMK офіцерам безпеки учасника/НПЦ з оформленням акта приймання-передавання криптографічних ключів (додаток 2). Кожний компонент транспортного ключа передається окремому відповідальному офіцеру безпеки учасника/НПЦ.

(пункт 2.2 розділу 2 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

2.3. Криптографічний ключ шифрування ПІН-блоків ZPK, який зашифрований транспортним ключем ZMK учасника/НПЦ, направляється захищеними каналами НПС "ПРОСТІР" офіцерам безпеки учасника/НПЦ.

(пункт 2.3 розділу 2 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

2.4. Зберігання криптографічних ключів дозволяється тільки в модулі безпеки НПС "ПРОСТІР". У разі необхідності зберігання роздрукованих криптографічних ключів, до моменту передачі офіцерам безпеки учасника/НПЦ, вони зберігаються у сейфі в приміщенні з обмеженим доступом у офіцерів безпеки НПС "ПРОСТІР".

(пункт 2.4 розділу 2 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

2.5. Новий криптографічний ключ повинен бути імплементований офіцерами безпеки учасника/НПЦ протягом 3 (трьох) робочих днів з моменту його отримання.

(пункт 2.5 розділу 2 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

2.6. Передавання ПІН-конвертів з компонентами транспортного ключа ZMK за актом приймання-передавання відбувається на території Національного банку за адресою визначеною Оператором.

(розділ 2 доповнено новим пунктом 2.6 згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

3. Анулювання дії криптографічних ключів

3.1. Анулювання дії криптографічних ключів означає припинення використання транспортного ключа ZMK та ключів шифрування ПІН-блоків ZPK, виданих учаснику/НПЦ.

(пункт 3.1 розділу 3 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

3.2. Анулювання дії криптографічних ключів здійснюється в таких випадках:

за заявою учасника/НПЦ про анулювання дії криптографічних ключів (додаток 3) із зазначенням причини анулювання;

у зв'язку із завершенням терміну дії криптографічних ключів;

за поданням Оператора НПС "ПРОСТІР" у разі виявлення порушень Правил та вимог цього Порядку;

у зв'язку із компрометацією криптографічних ключів.

(пункт 3.2 розділу 3 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

3.3. Оператор НПС "ПРОСТІР" опрацьовує заяву учасника/НПЦ про анулювання дії криптографічних ключів у строк не пізніше 1 (одного) робочого дня, наступного за робочим днем, протягом якого було подано заяву.

(пункт 3.3 розділу 3 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

3.4. В інших випадках Оператор НПС "ПРОСТІР" направляє учаснику/НПЦ офіційний лист про анулювання дії криптографічних ключів з повідомленням причин анулювання.

(пункт 3.2 розділу 3 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

4. Планова заміна криптографічних ключів

4.1. Процедура планової заміни криптографічних ключів здійснюється офіцерами безпеки НПС "ПРОСТІР" та офіцерами безпеки учасника/НПЦ.

(пункт 4.1 розділу 4 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

4.2. Процедура планової заміни криптографічних ключів ініціюється Оператором за 1 (один) місяць до закінчення терміну дії криптографічних ключів.

(пункт 4.2 розділу 4 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

4.3. Планова заміна криптографічних ключів виконується в два етапи:

генерація нових криптографічних ключів та анулювання старих криптографічних ключів.

5. Позапланова заміна криптографічних ключів

5.1. Позапланова заміна криптографічних ключів здійснюється в таких випадках:

у разі компрометації криптографічних ключів;

якщо учасник/НПЦ за будь-яких обставин не зміг здійснити планову заміну криптографічних ключів у встановлені для цієї процедури строки;

в інших випадках, викликаних форс-мажорними обставинами.

(пункт 5.1 розділу 5 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

5.2. Для позапланової заміни криптографічних ключів учасник/НПЦ направляє Оператору НПС "ПРОСТІР" заяву про позапланову заміну криптографічних ключів з поясненням причин позапланової заміни (додаток 4).

(пункт 5.2 розділу 5 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

5.3. Позапланова заміна криптографічних ключів виконується у два етапи: генерація нових криптографічних ключів та анулювання старих криптографічних ключів.

6. Компрометація криптографічних ключів

6.1. Компрометація криптографічних ключів може відбутись за таких обставин:

втрата носіїв криптографічних ключів та/або його компонентів;

звільнення працівників, які мали доступ до криптографічних ключів;

інші обставини, які прямо або опосередковано вказують на можливість несанкціонованого доступу до криптографічних ключів сторонніх осіб.

6.2. У випадку компрометації криптографічних ключів офіцер безпеки учасника/НПЦ будь-якими доступними засобами зв'язку протягом 1 (однієї) години з моменту виявлення компрометації повідомляє офіцерові безпеки НПС "ПРОСТІР" про факт компрометації криптографічних ключів та направляє до Оператора НПС "ПРОСТІР" заяву на позапланову заміну криптографічних ключів із зазначенням компрометації у якості причин позапланової заміни.

(пункт 6.2 розділу 6 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

6.3. У разі компрометації криптографічних ключів проводиться процедура позапланової заміни криптографічних ключів.

7. Строк дії криптографічних ключів

7.1. Строк дії криптографічного транспортного ключа ZMK і ключа шифрування ПІН-блоків ZPK, виданих учаснику, однаковий та складає – 2 (два) роки.

(пункт 7.1 розділу 7 із змінами, внесеними згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

7.2. Період дії криптографічних ключів починається з дати і часу їх генерації.

8. Знищення криптографічних ключів

8.1. Офіцери безпеки учасника, після успішного формування транспортного ключа ZMK із компонентів отриманих у захищених ПІН-конвертах та захищеного збереження його учасником/НПЦ, для уникнення можливості несанкціонованого доступу до компонентів та/або використання транспортного ключа ZMK, здійснюють його знищення шляхом фізичного знищення отриманих ПІН-конвертів з компонентами.

(пункт 8.1 розділу 8 викладено в новій редакції згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

8.2. Знищення ПІН-конвертів з компонентами транспортного ключа ZMK, здійснюється зі складанням акту про знищення криптографічних ключів за формою згідно з додатком 6 до цього Порядку, із обов'язковим зазначенням членів комісії, місця та часу знищення.

(розділ 8 доповнено новим пунктом 8.2 згідно з рішенням Ради Оператора НПС "ПРОСТІР" (протокол від 28.06.2024 № 57/13/2024))

Голова Ради,
директор Департаменту платіжних систем
та інноваційного розвитку Андрій ПОДДЄРЬОГІН

Додаток 1
до Порядку роботи з криптографічними ключами модулів безпеки Національної платіжної системи “Український платіжний простір”
(Додаток 1 із змінами внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024

ЕЛЕКТРОННЕ ПОВІДОМЛЕННЯ

Назва учасника/НПЦ

__.__.20__ р. №___

Національний банк України
Оператор НПС “ПРОСТІР”
Департамент платіжних систем та інноваційного розвитку

ЗАЯВА
про генерацію компонент транспортного ключа та криптограми ключа шифрування ПІН-блоків

На підставі договору приєднання до Національної платіжної системи “Український платіжний простір” / участі в Національній платіжній системі “Український платіжний простір” від _____ № _____ просимо вас здійснити генерацію та видачу криптографічних ключів.

Реквізити учасника/НПЦ: код ЕДРПОУ _____,
Місцезнаходження (поштова адреса) _____
Контактна інформація:
Посада, прізвище, ім’я, по батькові осіб, уповноважених отримати криптографічні ключі:_____
_____
_____

Посада, прізвище, ім’я, по батькові працівника (ів), учасника/НПЦ, відповідального(их) за роботу з криптографічними ключами: _____
Номер контактного телефону, факсу_____.
E-mail:_____.

Керівник учасника/НПЦ _____ _____
(посада) (ініціали, прізвище)

Додаток 2 до Порядку роботи з криптографічними ключами модулів безпеки Національної платіжної системи “Український платіжний простір”
(Додаток 2 із змінами внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024)

Акт приймання-передавання криптографічних ключів № ____

“___” _____ 20__

Цей акт укладений між Національним банком України та *назва учасника/НПЦ* далі – Сторони) про таке.

Національний банк України передав, а *назва учасника/НПЦ* отримав першу/другу/третю компоненту 3-компонентного криптографічного ключа ZMK для роботи в системі Центрального маршрутизатора та розрахунковоклірингового центру Національної платіжної системи “Український платіжний простір” (далі – НПС “ПРОСТІР”) з використанням електронних платіжних засобів НПС “ПРОСТІР”.

Літерно-цифрове зображення першого/другого/третього компонента 3-компонентного криптографічного ключа ZMK надано в паперовому вигляді в запечатаному та захищеному ПІН-конверті. ПІН-конверт не має слідів розкриття.

Цей акт складено в двох примірниках, по одному для кожної зі Сторін.

Передав	Прийняв
Відповідальна особа з боку Національного банку України: *посада*	Відповідальна особа з боку учасника/НПЦ *назва учасника/НПЦ*: *посада*
_____/ *ПІБ*	_____/ *ПІБ*

Додаток 3
до Порядку роботи з криптографічними ключами модулів безпеки Національної платіжної системи “Український платіжний простір”
(Додаток 3 із змінами внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024

ЕЛЕКТРОННЕ ПОВІДОМЛЕННЯ

Назва учасника/НПЦ

__.__.20__ р. №___

Національний банк України
Оператор НПС “ПРОСТІР”
(Департамент платіжних систем та інноваційного розвитку)

ЗАЯВА
про анулювання дії криптографічних ключів

На підставі договору приєднання / участі в Національній платіжній системі “Український платіжний простір” до Національної платіжної системи “Український платіжний простір” від _____ № _____ просимо вас здійснити анулювання дії криптографічних ключів.

Причина анулювання: _____
_____

Контактна інформація:

Посада, прізвище, ім’я, по батькові працівника(ів) учасника/НПЦ, відповідального(их) за роботу з криптографічними ключами:
_____
_____

Номер контактного телефону _____
E-mail: _____

Керівник учасника/НПЦ _____ _____
(посада) (ініціали, прізвище)

(Додаток 4 виключено згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024

Додаток 5
до Порядку роботи з криптографічними ключами модулів безпеки Національної платіжної системи “Український платіжний простір”
(Додаток 5 із змінами внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024

ЕЛЕКТРОННЕ ПОВІДОМЛЕННЯ

Назва учасника/НПЦ

__.__.20__ р. №___

Національний банк України
Оператор НПС “ПРОСТІР”
(Департамент платіжних систем та інноваційного розвитку)

ЗАЯВА
про позапланову заміну криптографічних ключів

На підставі договору приєднання до Національної платіжної системи “Український платіжний простір”/участі в Національній платіжній системі “Український платіжний простір” від _____ № _____ просимо вас здійснити позапланову заміну криптографічних ключів шляхом генерації нових криптографічних ключів та анулювання старих криптографічних ключів.

Причина позапланової заміни: _____
_____

Контактна інформація:
Посада, прізвище, ім’я, по батькові осіб, уповноважених отримати криптографічні ключі: _____
_____
Посада, прізвище, ім’я, по батькові працівника (ів), відповідального (их) за цей напрям роботи в учасника/НПЦ: _____

Номер контактного телефону _____.

E-mail:_____.

Керівник _____ _____
(посада) (ініціали, прізвище)

Додаток 6
до Порядку роботи з криптографічними ключами модулів безпеки Національної “Український платіжний простір”
(Додаток 6 із змінами внесеними згідно з рішенням Ради Оператора НПС “ПРОСТІР” (протокол від 28.06.2024 № 57/13/2024

АКТ про знищення криптографічних ключів № __

“___” _____ 20___ р.

Цей акт укладено про те, що комісією, призначеною наказом від __.__.20__ р. № ___, у складі: Голова комісії – *повна посада, прізвище, ім’я та по батькові Голови комісії,* члени комісії: *повна посада, прізвище, ім’я та по батькові членів комісії* в період з __.__.20__ р. до __.__.20__ р. у *місце знищення* проведено відбір на знищення таких матеріальних носіїв інформації, які складають банківську таємницю:

№ з/п	Найменування матеріальних носіїв інформації	Обліковий номер	Прим. №	Кількість аркушів	Зауваження
1	ПІН-конверт з першою частиною криптографічного ключа ZMK	Зазначається обліковий №	1	1	
2	ПІН-конверт з другою частиною криптографічного ключа ZMK	Зазначається обліковий №	1	1	
…	…	…	…	…	…

Разом *(вказується кількість найменувань)* найменування.

Перевірку наявності та відповідності, відібраних на знищення матеріальних носіїв інформації з обліковими даними виконано, носії _____*(зазначається чи в наявності носії)*.

Підстава для знищення: *зазначається підстава (пошкодження ПІН-конверту тощо).*

Відібрані носії знищені шляхом *(вказати спосіб, яким було знищено криптографічні ключі: перероблені через знищувач документів, спалені тощо)*.

Голова комісії *підпис, прізвище та ініціали*

Члени комісії: *підпис, прізвище та ініціали*