Офіційно опубліковано
19.04.2023

Правління Національного банку України

П О С Т А Н О В А

14 квітня 2023 року Київ № 49

Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України

Відповідно до статей 7, 15, 56 Закону України "Про Національний банк України", статті 10 Закону України "Про захист інформації в інформаційно-комунікаційних системах", з метою врегулювання взаємовідносин між Національним банком України і банками України, державними, небанківськими установами, що використовують засоби криптографічного захисту інформації Національного банку України, Правління Національного банку України **постановляє:**

1. Затвердити Положення про використання засобів криптографічного захисту інформації Національного банку України, що додається.

2. Визнати такими, що втратили чинність:

1) постанову Правління Національного банку України від 26 листопада 2015 року № 829 "Про затвердження нормативно-правових актів з питань інформаційної безпеки";

2) постанову Правління Національного банку України від 17 серпня 2017 року № 79 "Про затвердження Змін до Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України";

3) постанову Правління Національного банку України від 05 жовтня 2018 року № 106 "Про внесення змін до Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України";

4) постанову Правління Національного банку України від 13 лютого 2019 року № 38 "Про внесення змін до Положення про порядок перевірки стану

інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України";

5) постанову Правління Національного банку України від 14 лютого 2022 року № 15 "Про затвердження Змін до Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України".

3. Департаменту безпеки (Олександр Паламарчук) після офіційного опублікування довести до відома банків України, їх філій, філій іноземних банків, органів Державної казначейської служби України, інших органів державної влади, небанківських установ, які використовують засоби криптографічного захисту інформації Національного банку України, інформацію про прийняття цієї постанови.

4. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Андрія Пишного.

5. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування.

Голова Андрій ПИШНИЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
14 квітня 2023 року № 49

Положення про використання засобів криптографічного захисту інформації Національного банку України

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про банки і банківську діяльність", "Про захист інформації в інформаційно-комунікаційних системах" і визначає порядок використання (отримання, експлуатації, зберігання, повернення) засобів криптографічного захисту інформації Національного банку України (далі – Національний банк) банками України, їх філіями, філіями іноземних банків, державними установами, небанківськими установами (далі – організація) та здійснення контролю за їх використанням.

2. Терміни та скорочення в цьому Положенні вживаються в такому значенні:

1) адміністратор інформаційної безпеки – працівник, призначений внутрішнім документом організації відповідальним за використання (отримання, експлуатацію, зберігання, повернення) засобів криптографічного захисту інформації Національного банку в цій організації;

2) АРМ-НБУ-інформаційний (далі – АРМ-ІНФ) – інформаційна система Національного банку, призначена для обміну в захищеному вигляді неплатіжною інформацією з обмеженим доступом (крім службової інформації та інформації, яка містить відомості, що становлять державну таємницю);

3) АРМ МГК – інформаційна система Національного банку, призначена для управління ключовими даними засобами модуля генерації ключів криптографічного захисту інформації Національного банку;

4) бібліотека криптографічних функцій (далі – криптобібліотека) – програмний засіб криптографічного захисту інформації Національного банку, призначений для створення і перевірки електронного підпису Національного банку, шифрування та розшифрування інформації в інформаційних системах Національного банку;

5) електронний журнал роботи модуля генерації ключів криптографічного захисту інформації Національного банку (далі – журнал МГК)

– захищений від модифікації протокол роботи модуля генерації ключів криптографічного захисту інформації Національного банку, в якому фіксуються із зазначенням дати та часу всі події управління ключовими даними;

6) ЄДБО – Єдиний договір банківського обслуговування та надання інших послуг Національним банком;

7) засіб криптографічного захисту інформації Національного банку (далі – засіб КЗІ) – програмний, апаратно-програмний або апаратний засіб, призначений для криптографічного захисту інформації, розробником якого є Національний банк або розроблений на замовлення Національного банку;

8) інформаційна система Національного банку – інформаційно-комунікаційна система, створена Національним банком для виконання покладених на нього функцій або для потреб банківської системи України;

9) модуль генерації ключів криптографічного захисту інформації Національного банку (далі – МГК) – апаратно-програмний засіб КЗІ, призначений для генерації ключової пари;

10) організація-замовник – організація, що приєднується до ЄДБО для отримання послуг Національного банку із надання в користування засобів КЗІ та АРМ-ІНФ або укладає договір про використання засобів КЗІ;

11) пара ключів (далі – ключова пара) – особистий ключ та відповідний йому відкритий ключ;

12) СЕП – система електронних платежів Національного банку.

Термін "електронний підпис Національного банку України" вживається у значенні, визначеному в Положенні про застосування електронного підпису та електронної печатки, затвердженому постановою Правління Національного банку України від 14 серпня 2017 року № 78 (у редакції постанови Правління Національного банку України від 25 лютого 2019 року № 42) (зі змінами).

Термін "правила СЕП" вживається у значенні, визначеному в Інструкції про виконання міжбанківських платіжних операцій в Україні в національній валюті, затвердженій постановою Правління Національного банку України від 03 березня 2023 року № 16.

Інші терміни в цьому Положенні вживаються в значеннях, визначених у Законах України "Про електронні документи та електронний документообіг", "Про захист інформації в інформаційно-комунікаційних системах", "Про електронні довірчі послуги", "Про банки та банківську діяльність".

3. Національний банк має право здійснювати контроль за використанням засобів КЗІ відповідно до розділу V цього Положення.

ІІ. Загальні засади використання засобів КЗІ

4. Організація зобов'язана використовувати засоби КЗІ виключно для забезпечення роботи в інформаційних системах Національного банку.

5. Національний банк надає організації такі засоби КЗІ:

1) МГК (основний та резервний);

2) криптобібліотеки.

Національний банк має право надати організації додаткову кількість МГК у разі отримання від організації листа з відповідним обґрунтуванням потреби.

6. Національний банк надає криптобібліотеки організації:

1) як окремі модулі для вбудовування в систему автоматизації організації з метою забезпечення інформаційної взаємодії з інформаційними системами Національного банку;

2) як складові клієнтських частин інформаційних систем Національного банку.

7. Національний банк для забезпечення обміну в захищеному вигляді інформацією з обмеженим доступом (крім службової інформації та інформації, яка містить відомості, що становлять державну таємницю) надає організації АРМ-ІНФ із вбудованою криптобібліотекою.

8. Національний банк створює криптографічну систему (у складі системи інформаційної безпеки) в інформаційній системі Національного банку з урахуванням принципів криптографічного захисту інформаційних систем Національного банку, установлених у пункті 7 розділу І Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95 (далі – Положення № 95). Організація зобов'язана налаштувати криптографічну систему в інформаційній системі Національного банку згідно з вимогами, визначеними у відповідній експлуатаційній документації до інформаційної системи Національного банку та/або правилах СЕП.

9. Організація має право генерувати ключову пару з використанням АРМ МГК згідно з експлуатаційною документацією до АРМ МГК. Особистий ключ має бути захищений паролем відповідальної особи, яка генерує та використовує особистий ключ.

Організація після генерації ключової пари зобов'язана надіслати відкритий ключ до Національного банку для його сертифікації. Залежно від призначення відкритого ключа сертифікація здійснюється в онлайн- або офлайн-режимі. Для здійснення сертифікації в офлайн-режимі організація зобов'язана надсилати відкритий ключ до Національного банку не пізніше ніж за три робочі дні до закінчення строку дії сертифіката такого відкритого ключа.

В онлайн-режимі відкритий ключ сертифікується відразу після його отримання Національним банком. Початком строку дії сертифіката ключа є момент сертифікації відкритого ключа.

В офлайн-режимі відкритий ключ сертифікується не пізніше наступного робочого дня після його отримання Національним банком. Початком строку дії сертифіката ключа є 00.01 наступного календарного дня після дня сертифікації відкритого ключа.

Строк дії сертифіката ключа встановлюється Національним банком залежно від призначення відкритого ключа та становить від 120 діб до 2 років. Національний банк має право змінити строк дії сертифіката ключа у зв'язку з уведенням воєнного стану, настанням кризових та/або надзвичайних ситуацій.

10. Організація зобов'язана забезпечити виконання вимог цього Положення з урахуванням власної політики використання криптографічних засобів для захисту інформації та внутрішніх документів, що описують процес управління ключами, впровадженими організацією.

11. Організації заборонено:

1) передавати МГК іншим установам або організаціям;

2) використовувати засоби КЗІ в системі автоматизації організації, якщо це не обумовлено технологією роботи інформаційних систем Національного банку відповідно до експлуатаційної документації.

12. Організація зобов'язана вжити заходів для усунення загрози втрати МГК в умовах:

1) дії воєнного стану;

2) настання кризових та/або надзвичайних ситуацій.

Організація має право визначити, задокументувати та запровадити тимчасовий порядок експлуатації засобів КЗІ та/або управління ключами в

умовах, що визначені в пункті 12 розділу ІІ цього Положення (далі – тимчасовий порядок). Організація зобов'язана повідомити Національний банк про впровадження та/або скасування дії тимчасового порядку протягом трьох робочих днів із дня, наступного за днем його впровадження та/або скасування.

13. Організація зобов'язана призначити внутрішнім документом адміністратора/адміністраторів інформаційної безпеки та визначити його/їх права, обов'язки, функції, відповідальність за засоби КЗІ в посадовій інструкції. Кількість адміністраторів інформаційної безпеки визначається з урахуванням особливостей діяльності організації. Організація зобов'язана забезпечувати актуальність внутрішніх документів про призначення адміністратора/адміністраторів інформаційної безпеки.

14. Адміністратора інформаційної безпеки заборонено призначати відповідальним за:

1) використання особистого ключа адміністратора АРМ-ІНФ та/або оператора технологічних місць (крім технологічних місць, що пов'язані з виконанням функцій забезпечення інформаційної безпеки) інформаційних систем Національного банку;

2) розроблення або супроводження (адміністрування) системи автоматизації організації;

3) супроводження (адміністрування) інформаційних систем Національного банку.

ІІІ. Порядок отримання і повернення засобів КЗІ

15. Умовами для отримання засобів КЗІ та АРМ-ІНФ є:

1) приєднання організації-замовника до ЄДБО для отримання послуг Національного банку із надання в користування засобів КЗІ та АРМ-ІНФ, крім випадків, якщо організацією-замовником є державна установа. Для державних установ – укладення договору про використання засобів криптографічного захисту інформації Національного банку України (далі – Договір) відповідно до зразка, наведеного в додатку 1 до цього Положення;

2) призначення адміністратора інформаційної безпеки та відповідальних осіб за зберігання та використання особистих ключів;

3) наявність умов зберігання МГК;

4) наявність приміщень, що відповідають вимогам пункту 44 розділу IV цього Положення, в яких будуть розміщені АРМ-ІНФ, АРМ МГК.

Організація після виконання цих умов надсилає Національному банку лист про готовність отримати засоби КЗІ.

16. Національний банк визначає готовність організації до використання засобів КЗІ відповідно до пункту 51 розділу V цього Положення. Національний банк у разі відсутності недоліків за результатами аналізу інформації, отриманої від організації у відповідь на запит, виготовляє МГК та інформує організацію про можливість і спосіб отримання засобів КЗІ.

17. Організація для отримання МГК зобов'язана надіслати до Національного банку засобами системи електронної пошти Національного банку або на офіційну електронну поштову скриньку Національного банку листа, в якому зазначаються номер/дата укладення ЄДБО/Договору, прізвище, ім'я, по батькові (далі – ПІБ) адміністратора інформаційної безпеки, що отримує МГК, реквізити документа, що засвідчує його особу, дата його прибуття до Національного банку (далі – Лист на отримання МГК) та додається копія документа про його призначення адміністратором інформаційної безпеки. Лист на отримання МГК підписується кваліфікованим електронним підписом керівника організації.

Адміністратор інформаційної безпеки зобов'язаний прибути до Національного банку з документом, який засвідчує його особу та в термін, зазначений у Листі на отримання МГК.

18. Національний банк надає шляхом розміщення на сторінці офіційного Інтернет-представництва Національного банку:

1) актуальну інсталяційну версію АРМ-ІНФ із вбудованою криптобібліотекою, останні оновлення до нього, експлуатаційну документацію та інструктивні матеріали щодо технічних питань функціонування АРМ-ІНФ;

2) актуальну інсталяційну версію АРМ МГК, останні оновлення до нього, експлуатаційну документацію;

3) актуальні версії криптобібліотек, супровідну документацію до них.

19. Організації не дозволяється розташовувати і використовувати МГК та АРМ-ІНФ за іншою адресою, ніж це зазначено в додатку 2 до ЄДБО/додатку до Договору. Організація-замовник зобов'язана внести зміни до додатка 2 до ЄДБО/додатка до Договору в разі зміни адреси розташування засобів КЗІ та/або АРМ-ІНФ, крім випадків запровадження тимчасового порядку відповідно до пункту 12 розділу II цього Положення.

20. Організація зобов’язана повернути МГК до Національного банку в разі:

1) розірвання Договору, укладеного відповідно до пункту 15 розділу ІІІ цього Положення;

2) виходу з ладу МГК;

3) на вимогу Національного банку в разі зміни складу засобів КЗІ або технології їх використання.

Криптобібліотеки, АРМ-ІНФ, АРМ МГК поверненню до Національного банку не підлягають.

21. Організація у випадках, передбачених у підпункті 1 пункту 20 розділу ІІІ цього Положення, зобов’язана:

1) ужити заходів щодо знищення на місці ключових даних, АРМ-ІНФ, АРМ МГК, криптобібліотек;

2) ужити заходів щодо передавання до архіву організації журналу обліку засобів КЗІ, журналу МГК;

3) надіслати до Національного банку засобами системи електронної пошти Національного банку або на офіційну електронну поштову скриньку Національного банку листа, підписаного кваліфікованим електронним підписом керівника організації, зазначивши дату виконання заходів, передбачених у підпунктах 1, 2 пункту 21 розділу ІІІ цього Положення , ПІБ працівника організації, що прибуде для повернення МГК, реквізити документа, що засвідчує його особу, дату його прибуття;

4) повернути МГК до Національного банку.

22. Організація у випадках, передбачених у підпунктах 2, 3 пункту 20 розділу ІІІ цього Положення, зобов’язана:

1) надіслати до Національного банку засобами системи електронної пошти Національного банку або на офіційну електронну поштову скриньку Національного банку листа, підписаного кваліфікованим електронним підписом керівника організації, зазначивши ПІБ працівника організації, що прибуде для повернення МГК, реквізити документа, що засвідчує його особу, дату його прибуття;

2) повернути МГК до Національного банку.

Організація має право одночасно під час повернення МГК, що вийшов з ладу, отримати новий МГК за умови виконання підпунктів 1, 2 пункту 35 розділу IV цього Положення.

IV. Правила експлуатації та зберігання засобів КЗІ

23. Організація зобов'язана призначити внутрішнім документом відповідальних осіб за використання та зберігання особистих ключів (далі – відповідальна особа):

1) адміністратора АРМ-ІНФ;

2) операторів технологічних місць інформаційних систем Національного банку.

Кількість відповідальних осіб визначається з урахуванням особливостей діяльності організації, технології/регламенту роботи інформаційних систем Національного банку. Організація має право призначати осіб, які виконуватимуть обов'язки відповідальних осіб у разі їх відсутності.

24. Внутрішній документ організації про призначення відповідальних осіб має містити посаду, ініціали, прізвище працівника, назву технологічного місця інформаційної системи Національного банку, ідентифікатор користувача в інформаційній системі Національного банку. Організація зобов'язана забезпечувати актуальність внутрішніх документів про призначення відповідальних осіб.

25. Керівник організації зобов'язаний забезпечити подання до Національного банку копії документа або виписки з нього в електронній формі про покладання/звільнення від виконання відповідних обов'язків адміністратора інформаційної безпеки, адміністратора АРМ-ІНФ протягом трьох робочих днів із дня, наступного за днем їх покладання/звільнення від виконання.

26. Відповідальні особи повинні підписати зобов'язання відповідно до форми, наведеної в додатку 2 до цього Положення (далі – Зобов'язання).

27. Організація зобов'язана дотримуватися такого порядку допуску відповідальних осіб:

1) допуск до роботи з МГК, АРМ МГК має адміністратор інформаційної безпеки;

2) допуск до роботи з АРМ-ІНФ має адміністратор АРМ-ІНФ;

3) допуск до роботи з особистим ключем має відповідальна особа, однак тільки до свого особистого ключа;

4) допуск до роботи з АРМ МГК тільки для генерації ключової пари і тільки у присутності адміністратора інформаційної безпеки має відповідальна особа;

5) допуск до АРМ-ІНФ тільки для виконання функції контролю і тільки у присутності адміністратора АРМ-ІНФ має адміністратор інформаційної безпеки.

28. Адміністратор інформаційної безпеки зобов'язаний забезпечити умови для генерації ключової пари та доступ до АРМ МГК відповідальній особі за наявності:

1) внутрішнього документа організації про призначення відповідальної особи;

2) підписаного працівником Зобов'язання.

29. Відповідальна особа після отримання доступу до АРМ МГК зобов'язана самостійно генерувати ключову пару на АРМ МГК відповідно до експлуатаційної документації у присутності адміністратора інформаційної безпеки. Усі спроби генерації ключової пари, включаючи й невдалі, фіксуються в журналі МГК в автоматичному режимі.

Адміністратор інформаційної безпеки має право надавати віддалений доступ до АРМ МГК відповідальній особі за умови її ідентифікації та дотримання технологічної дисципліни під час роботи з АРМ МГК.

Організація зобов'язана здійснювати автоматизоване протоколювання всіх подій віддаленого доступу до АРМ МГК у захищених від несанкціонованої модифікації електронних журналах із забезпеченням їх збереження упродовж двох років. Організація має право самостійно визначати засоби (технології) для автоматизації такого процесу. Порядок ідентифікації відповідальної особи, що здійснюється адміністратором інформаційної безпеки перед наданням віддаленого доступу до АРМ МГК, визначається внутрішнім документом, що затверджується керівником організації.

30. Адміністратор інформаційної безпеки зобов'язаний:

1) вести облік МГК під час отримання, заміни та повернення до Національного банку в журналі обліку засобів КЗІ, який повинен містити відомості про серійний номер, дату отримання/повернення, прізвище, ініціали особи, яка отримала засоби МГК (дата, підпис), відмітку про повернення МГК (дата, підпис);

2) вести облік криптобібліотек під час отримання, заміни в журналі обліку засобів КЗІ, який повинен містити відомості про назву та версію криптобібліотеки, дату отримання/заміни, прізвище, ініціали особи, яка отримала кріптобібліотеку (дата, підпис), відмітку про вбудовування/заміну (назва програмного забезпечення, дата, підпис);

3) забезпечувати зберігання МГК та журналу обліку засобів КЗІ;

4) здійснювати тестування МГК;

5) забезпечувати технологічну дисципліну під час роботи АРМ МГК;

6) забезпечувати налаштування комп'ютера з АРМ МГК відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку;

7) забезпечувати умови для своєчасної генерації ключових пар на АРМ МГК та доступ до роботи з АРМ МГК відповідальній особі згідно з експлуатаційною документацією до АРМ МГК;

8) здійснювати ідентифікацію відповідальної особи перед наданням їй віддаленого доступу до АРМ МГК у встановленому порядку;

9) надавати консультації відповідальній особі під час роботи з АРМ МГК з питань генерації ключової пари;

10) забезпечувати надсилання на сертифікацію до Національного банку відкритих ключів;

11) здійснювати резервне копіювання журналу МГК у встановленому порядку;

12) здійснювати контроль за налаштуванням АРМ-ІНФ відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку;

13) здійснювати контроль за дотриманням відповідальними особами цього Положення внутрішнього порядку зберігання особистих ключів;

14) інформувати керівника організації про загрози і випадки компрометації МГК, особистих ключів відповідальних осіб організації та про вихід МГК з ладу.

31. Адміністратор АРМ-ІНФ зобов'язаний:

1) здійснювати налаштування комп'ютера з АРМ-ІНФ відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку;

2) вбудовувати ключові дані до локального сховища операційної системи комп'ютера з АРМ-ІНФ згідно з експлуатаційною документацією до АРМ-ІНФ.

32. Відповідальна особа зобов'язана:

1) забезпечувати технологічну дисципліну під час роботи в інформаційних системах Національного банку;

2) особисто здійснювати генерацію ключової пари (з урахуванням часу на сертифікацію, установленого в пункті 9 розділу II цього Положення);

3) установлювати пароль до носія особистого ключа та не допускати його розголошення;

4) здійснювати контроль за строком дії сертифіката свого відкритого ключа;

5) зберігати носій особистого ключа у неробочий час і в робочий час, якщо він не використовується в роботі, у спосіб, що виключає можливість несанкціонованого доступу до носія особистого ключа;

6) інформувати адміністратора інформаційної безпеки про загрози і випадки компрометації особистого ключа.

33. Адміністратор інформаційної безпеки після отримання МГК зобов'язаний:

1) зробити відповідний запис у журналі обліку засобів КЗІ;

2) здійснити заміну початкового пароля МГК;

3) здійснити перевірку функціонування МГК шляхом тестової генерації ключової пари.

34. Адміністратор інформаційної безпеки зобов'язаний зберігати МГК у неробочий час і в робочий час, якщо він не використовується в роботі, у спосіб, що виключає можливість несанкціонованого доступу до МГК або втрати МГК.

35. Адміністратор інформаційної безпеки, якщо МГК не працює або пошкоджений з вини персоналу організації, зобов'язаний:

1) повідомити Національний банк засобами системи електронної пошти Національного банку або електронним листом на офіційну електронну поштову скриньку Національного банку протягом трьох робочих днів про такий випадок із зазначенням серійного номера непрацюючого/пошкодженого МГК і причини його непрацездатності;

2) повернути непрацюючий МГК відповідно до підпункту 2 пункту 22 розділу III цього Положення та отримати новий МГК відповідно до пункту 17 розділу III цього Положення;

3) ужити заходів, що передбачені в пункті 33 розділу IV цього Положення.

36. Адміністратор інформаційної безпеки в разі втрати МГК або втрати контролю за місцезнаходженням МГК (уключаючи умови, викладені в пункті 12 розділу II цього Положення) зобов'язаний:

1) повідомити Національний банк засобами системи електронної пошти Національного банку або електронним листом на офіційну електронну поштову скриньку Національного банку протягом одного робочого дня про такий випадок із зазначенням серійного номера втраченого МГК. Після отримання повідомлення Національний банк вживає відповідних заходів щодо неможливості сертифікації відкритих ключів, згенерованих за допомогою такого МГК;

2) замовити новий МГК.

Керівник організації зобов'язаний організувати проведення службового розслідування у випадках, викладених у пункті 36 розділу IV цього Положення, та забезпечити подання до Національного банку висновків за результатами проведення такого розслідування протягом трьох робочих днів із дня, наступного за днем замовлення нового МГК. Національний банк здійснює аналіз отриманих висновків, виготовляє МГК та інформує організацію про можливість і спосіб його отримання.

37. Організація зобов'язана забезпечити зміну паролів до МГК у разі звільнення працівника організації від обов'язків адміністратора інформаційної безпеки або компрометації пароля МГК.

38. Організація має право використовувати як носій особистого ключа під час роботи в інформаційних системах Національного банку (крім АРМ-ІНФ):

1) пристрій, який має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього ключових даних від несанкціонованого

доступу та від безпосереднього ознайомлення із значенням параметрів особистого ключа;

2) файловий контейнер ключа за умови запровадження організаційних та технічних заходів, спрямованих на забезпечення захисту від несанкціонованого доступу до нього.

Національний банк має право встановлювати вимоги до носіїв особистих ключів, що використовуються організацією під час роботи в інформаційних системах Національного банку, виклавши їх в експлуатаційній документації до АРМ МГК.

Організація має право використовувати носії особистих ключів, зазначені в підпункті 1 пункту 38 розділу IV цього Положення, для розв'язання інших завдань організації (зберігання інших особистих ключів, обмеження доступу до комп'ютерів, приміщень).

39. Відповідальна особа має право створити копії особистого ключа для запобігання зупиненню роботи організації в інформаційних системах Національного банку за умови наявності документа організації, який визначає порядок створення копій особистого ключа та відповідальних за їх використання та зберігання осіб. На копії особистого ключа поширюються всі вимоги щодо використання, як і на основний особистий ключ.

40. Організація зобов'язана розробити та затвердити внутрішній порядок зберігання особистих ключів залежно від конкретних умов її функціонування, забезпечивши дотримання вимог цього Положення.

Організація, що є банком, повинна розробити такий внутрішній порядок зберігання особистих ключів з урахуванням внутрішніх документів, що описують процес управління ключами відповідно до пункту 45 розділу IV Положення № 95.

41. Організація зобов'язана вести архів журналу МГК протягом двох років. Організація, що є учасником системи електронних платежів Національного банку, повинна зберігати журнал МГК відповідно до Положення про порядок формування, зберігання та знищення відокремлених електронних даних, отриманих за результатами роботи інформаційних систем у Національному банку України і банках України, затвердженого постановою Правління Національного банку України від 14 вересня 2018 року № 99.

42. Відповідальна особа в разі компрометації особистого ключа зобов'язана припинити використання такого особистого ключа і невідкладно повідомити про таку подію адміністратору інформаційної безпеки.

Адміністратор інформаційної безпеки в разі отримання повідомлення про компрометацію особистого ключа зобов'язаний невідкладно:

1) забезпечити скасування відповідного сертифіката відкритого ключа;

2) забезпечити генерацію нової ключової пари і надсилання на сертифікацію до Національного банку відкритого ключа;

3) провести службове розслідування, висновки за результатами якого подати до Національного банку протягом трьох робочих днів із дня, наступного за днем завершення такого розслідування.

43. Адміністратор інформаційної безпеки зобов'язаний забезпечити скасування відповідних сертифікатів відкритих ключів, якщо відповідальна особа, яка має особистий ключ для будь-якого робочого місця інформаційної системи Національного банку, звільняється від виконання відповідних функціональних обов'язків.

44. Організація зобов'язана розмістити АРМ-ІНФ, АРМ МГК в окремих приміщеннях та виключити можливість несанкціонованого доступу до цих приміщень. Дозволяється розміщувати АРМ-ІНФ у серверному приміщенні, якщо АРМ-ІНФ працює в автоматичному режимі.

Організація зобов'язана внутрішнім документом призначити працівників, які мають допуск до приміщень з АРМ-ІНФ, АРМ МГК.

Організація зобов'язана повідомляти Національний банк про зміни свого місцезнаходження або зміни місцезнаходження МГК, АРМ-ІНФ, АРМ МГК протягом трьох робочих днів із наступного дня за датою настання таких змін.

V. Контроль за використанням засобів КЗІ

45. Адміністратор інформаційної безпеки забезпечує контроль за дотриманням вимог цього Положення, внутрішнього порядку зберігання особистих ключів в організації.

46. Національний банк здійснює контроль за використанням організаціями засобів КЗІ (далі – контроль засобів КЗІ) шляхом:

1) безвиїзних заходів контролю методом аналізу інформації, документів, звітів, отриманих від організацій, відповідно до вимог, визначених у пунктах 36, 42 розділу IV, пунктах 47, 48, 51 розділу V цього Положення;

2) виїзних заходів контролю у формі перевірок.

47. Національний банк має право вимагати від організації надання інформації для здійснення контролю шляхом надсилання запиту.

Керівник організації зобов'язаний забезпечити надання на запит Національного банку достовірної інформації у вигляді письмових пояснень, документів в електронній (уключаючи журнал МГК) формі у строк, в обсязі, згідно з форматом та структурою, визначеними в такому запиті.

48. Керівник організації зобов'язаний забезпечити подання звіту щодо використання засобів криптографічного захисту інформації Національного банку України (далі – Звіт) за формою, визначеною в додатку 3 до цього Положення.

Керівник організації забезпечує надання організацією повної та достовірної інформації у Звіті.

Звіт подається організаціями до Національного банку один раз на рік протягом одного місяця, наступного за звітним періодом (рік), в електронній формі у форматі pdf, підписаний кваліфікованим електронним підписом керівника організації. Звіт разом із супровідним листом надсилається засобами системи електронної пошти Національного банку або на офіційну електронну поштову скриньку Національного банку.

49. Національний банк забезпечує нерозголошення інформації, отриманої ним під час здійснення контролю, третім особам, за винятком випадків, передбачених законодавством України.

50. Національний банк здійснює контроль за дотриманням банками цього Положення під час здійснення заходів контролю, передбачених у розділі II Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затвердженого постановою Правління Національного банку України від 16 січня 2021 року № 4.

51. Національний банк визначає готовність організації до використання засобів КЗІ за результатами аналізу інформації про готовність до використання засобів криптографічного захисту інформації Національного банку України (додаток 4), отриманої у відповідь на запит Національного банку.

52. Керівник організації зобов'язаний забезпечити надання на запит Національного банку достовірної інформації у строк, в обсязі та згідно з форматом і структурою, визначеними в такому запиті.

Додаток 1
до Положення про використання
засобів криптографічного захисту
інформації Національного банку
(підпункт 1 пункту 15 розділу III)

Зразок

Договір № _____
про використання засобів криптографічного захисту інформації Національного банку України

Київ "____" _____ 20___року

Національний банк України (далі – Виконавець) в особі _____ _____,
(найменування посади) (прізвище, власне ім'я, по батькові)
який діє на підставі_____ від _____ № ____,
(назва документа)
та_____(далі – Замовник)
(найменування організації)
в особі _____, який діє на
(найменування посади, прізвище, власне ім'я, по батькові)
підставі _____ від _____ № ____ (далі – Сторони),
(назва документа)
уклали цей договір про використання засобів криптографічного захисту інформації Національного банку України (далі – договір) про таке.

I. Предмет договору

1. Виконавець зобов'язується надати Замовнику та його установам, визначеним у додатку до цього договору, такі послуги:

1) надати в користування засоби криптографічного захисту інформації Національного банку України (далі – засоби КЗІ) для використання їх в інформаційних системах Національного банку України, а саме:

модулі генерації ключів криптографічного захисту інформації Національного банку України (далі – МГК) разом з інформаційною системою Національного банку України, що призначена для управління ключовими даними засобами МГК (далі – АРМ МГК);

криптобібліотеки;

2) надати в користування інформаційну систему Національного банку України, що призначена для обміну неплатіжною інформацією (далі – АРМ-ІНФ), із вбудованою криптобібліотекою, а також послуги з її супроводження.

2. Отримання, експлуатація, зберігання та повернення засобів КЗІ здійснюються відповідно до нормативно-правових актів Національного банку України з питань використання засобів КЗІ.

II. Строки виконання зобов'язань за договором

3. Виконавець зобов'язується протягом дії цього договору надавати Замовнику послуги, визначені в пункті 1 розділу I цього договору.

4. Замовник має здійснити оплату за надані послуги в порядку та на умовах, визначених цим договором.

III. Загальна вартість за договором

5. Вартість послуг за цим договором, ураховуючи всі витрати Виконавця, визначається згідно з тарифами, встановленими нормативно-правовим актом Національного банку України з питань затвердження тарифів на послуги (операції), що надаються (здійснюються) Національним банком України.

6. У разі внесення Національним банком України змін до тарифів розмір оплати змінюється з дати набрання чинності такими змінами шляхом укладення Сторонами додаткового договору.

7. Вартість послуг за цим договором становить ____ грн __ коп. (сума словами _____ гривень ____ копійок), у тому числі 20% ПДВ: ____ грн __ коп. (сума словами _____ гривень ____ копійок).

IV. Права та обов'язки Сторін

8. Виконавець має право:

1) здійснювати контроль за Замовником та його установами, які отримали засоби КЗІ згідно з додатком до цього договору, щодо виконання ними порядку використання (отримання, експлуатації, зберігання, повернення) засобів КЗІ, установленого Національним банком України;

2) зупиняти обслуговування Замовника та/або його установ у разі порушень ним правил використання (отримання, експлуатації, зберігання, повернення) засобів КЗІ або передавання (навіть тимчасово) отриманих Замовником та його установами МГК іншим установам, організаціям;

3) запроваджувати нові програмно-технічні та технологічні засоби, розроблені для поліпшення послуг, що надаються Замовнику.

9. Замовник та його установи, визначені в додатку до цього договору, мають право:

1) користуватися наданими засобами КЗІ в інформаційних системах Національного банку України згідно з діючою технологією;

2) отримувати від Виконавця консультації з питань, пов'язаних з експлуатацією і зберіганням засобів КЗІ та експлуатації АРМ-ІНФ.

10. Виконавець бере на себе зобов'язання:

1) належним чином та своєчасно надавати Замовнику та його установам, визначеним у додатку до цього договору, засоби КЗІ, у тому числі оновлені, з потрібною документацією до них;

2) надавати консультації з питань користування засобами КЗІ та експлуатації АРМ-ІНФ;

3) своєчасно інформувати Замовника про зміни, які планується вносити до систем криптографічного захисту інформації Національного банку України;

4) забезпечувати своєчасну заміну МГК у разі їх пошкодження або виходу з ладу, крім випадків, зазначених у пункті 16 розділу VI цього договору.

11. Замовник бере на себе зобов'язання:

1) не передавати (навіть тимчасово) отримані ним МГК іншим установам, організаціям;

2) дотримуватися технологічної дисципліни в роботі із засобами КЗІ, забезпечувати їх використання згідно з вимогами Виконавця. Негайно інформувати Виконавця про виникнення порушень умов використання засобів КЗІ і вживати заходів для їх усунення;

3) дотримуватися технологічної дисципліни в роботі з АРМ-ІНФ, АРМ МГК;

4) утримувати МГК в належному стані;

5) не використовувати надані засоби КЗІ для завдань, які не обумовлені наявними інструкціями та експлуатаційною документацією;

6) забезпечувати транспортування МГК до адреси розташування Замовника та Виконавця в разі заміни/повернення;

7) своєчасно здійснювати оплату Виконавцю за надані послуги;

8) забезпечувати виконання нормативно-правових актів Національного банку України з питань використання засобів КЗІ;

9) дотримуватися строків подання звіту щодо використання засобів КЗІ;

10) передавати (повертати) Виконавцю МГК протягом трьох робочих днів після припинення дії цього договору.

V. Порядок розрахунків

12. Виконавець щомісяця до 26 числа надсилає Замовнику засобами системи електронної пошти Національного банку України акт про надані послуги в електронному вигляді, підписаний кваліфікованим електронним підписом відповідальної особи Виконавця (далі – акт про надані послуги), згідно з тарифами, встановленими нормативно-правовим актом Національного банку України з питань затвердження тарифів на послуги (операції), що надаються (здійснюються) Національним банком України.

Замовник має здійснити оплату (у тому числі пені) протягом 10 робочих днів із дня отримання засобами системи електронної пошти Національного банку України акта про надані послуги або надіслати протягом трьох робочих днів із дня отримання акта про надані послуги мотивовану відмову від оплати. У разі неподання Замовником зауважень/заперечень щодо акта про надані послуги у визначений в договорі термін послуги є прийнятими в повному обсязі і такими, що підлягають оплаті, а акт про надані послуги є таким, що підписаний обома Сторонами договору.

Продовження додатка 1

На вимогу Замовника паперова копія електронного акта про надані послуги надсилається засобами поштового зв'язку протягом двох робочих днів із дня його підписання.

Оплата здійснюється за рахунок коштів бюджетної програми КПКВК _____ за КЕКВ _____, код ДК _____.

13. Розрахунок за надані послуги за неповний робочий місяць (у разі укладення, розірвання договору) здійснюється за фактичний час наданих послуг.

14. У разі несплати Замовником грошових коштів відповідно до пункту 12 розділу V цього договору строком більше ніж один календарний місяць Виконавець має право тимчасово зупинити надання послуг на користь Замовника до моменту погашення ним заборгованості.

VI. Відповідальність Сторін

15. Виконавець несе відповідальність перед Замовником за правильне та своєчасне надання засобів КЗІ Замовнику та його установам, визначеним у додатку до цього договору, для забезпечення можливості роботи в інформаційних системах Національного банку України.

16. Замовник відшкодовує Виконавцю збитки, завдані ним у зв'язку з порушенням умов використання засобів КЗІ.

17. За невиконання або неналежне виконання однією зі Сторін своїх зобов'язань, передбачених цим договором та/або законодавством України, винна Сторона несе відповідальність згідно з умовами цього договору та законодавством України.

18. Сторона, яка порушила зобов'язання, узяті на себе за цим договором, повинна усунути ці порушення в найкоротший строк.

19. У разі несвоєчасної оплати наданих послуг Замовник сплачує Виконавцю:

1) суму боргу з урахуванням установленого індексу інфляції за весь час прострочення та три відсотки річних із простроченої суми;

2) пеню в розмірі подвійної облікової ставки Національного банку України, що діяла в період, за який сплачується пеня, від суми несвоєчасно перерахованих коштів за кожний день прострочення.

20. Сплата штрафних санкцій (пені) не звільняє Сторони від виконання договірних зобов'язань.

VII. Форс-мажор

21. Сторони звільняються від відповідальності за часткове або повне невиконання будь-якого з положень цього договору, якщо це невиконання стало наслідком причин, що перебувають поза сферою контролю Сторони, яка його не виконала. Такі причини включають стихійне лихо, надзвичайні погодні умови, пожежі, війни, страйки, військові дії, громадські заворушення, але не обмежуються ними (далі – форс-мажор). Період звільнення від відповідальності починається з часу оголошення однією Стороною форс-мажору і закінчується, якщо ця Сторона вжила заходів, яких вона і справді могла б ужити для виходу з форс-мажору. Форс-мажор автоматично продовжує строк виконання зобов'язань на весь період його дії та ліквідації наслідків. Про настання форс-мажорних обставин Сторони мають інформувати одна одну невідкладно. Якщо ці обставини триватимуть більше ніж шість місяців, то кожна зі Сторін матиме право відмовитися від подальшого виконання зобов'язань за цим договором і в такому разі жодна зі Сторін не матиме права на відшкодування іншою Стороною можливих збитків.

22. Сторона, яка не може виконати своїх зобов'язань унаслідок надзвичайних обставин, передбачених у пункті 21 розділу VII цього договору, повинна письмово повідомити про це іншу Сторону протягом трьох робочих днів із часу виникнення таких обставин. Невиконання цієї вимоги не дає жодній із Сторін права посилатися надалі на вищезазначені обставини.

23. Належним доказом наявності обставин непереборної сили є сертифікат Торгово-промислової палати України.

VIII. Порядок зміни умов та розірвання договору

24. Зміни до цього договору вносяться в письмовій формі шляхом укладання додаткових договорів.

25. Додатковий договір стає невід'ємною частиною договору і набирає чинності з дня підписання обома Сторонами.

26. Сторона, яка вважає за потрібне змінити чи розірвати цей договір, надсилає пропозиції про це другій Стороні.

27. Сторона, яка одержала пропозицію про зміну чи розірвання цього договору, у двадцятиденний строк після одержання пропозиції повідомляє другу Сторону про результати її розгляду.

28. Якщо Сторони не досягли згоди щодо зміни (розірвання) цього договору або в разі неодержання відповіді у встановлений строк з урахуванням часу поштового обігу, то зацікавлена Сторона має право передати вирішення спору до суду.

29. У разі зміни однією зі Сторін будь-яких реквізитів, зазначених у розділі XII цього договору, Сторона, яка змінила реквізити, у строк до 30 днів після їх зміни письмово повідомляє про це другу Сторону. Сторона, яка одержала таке повідомлення, має письмово повідомити другу Сторону про його одержання.

IX. Порядок розгляду спорів

30. Спори, що виникають протягом дії цього договору, вирішуються шляхом переговорів.

31. У разі недосягнення згоди шляхом переговорів спори вирішуються в судовому порядку.

X. Строк дії договору

32. Цей договір уважається укладеним і набирає чинності з дати його укладення Сторонами і діє до _____ 20___ року, але в будь-якому разі до повного виконання Сторонами своїх зобов'язань за цим договором.

33. Закінчення строку дії цього договору не звільняє Сторони від відповідальності за його порушення, яке мало місце під час дії цього договору.

XI. Інші умови договору

34. Цей договір укладено в двох примірниках українською мовою по одному примірнику для кожної зі Сторін. Обидва примірники мають однакову юридичну силу.

35. Відносини Сторін, що виникають під час дії цього договору і які не врегульовані ним, регулюються законодавством України.

Продовження додатка 1

36. Для розв’язання всіх питань, пов’язаних із виконанням цього договору, відповідальними представниками є:

від Виконавця:
_____, _____;
(найменування посади, прізвище, власне ім’я, по батькові) (номер телефону)

від Замовника:
_____, _____.
(найменування посади, прізвище, власне ім’я, по батькові) (номер телефону)

XII. Місцезнаходження (поштові адреси), платіжні реквізити і підписи Сторін

Юридична адреса:	Юридична адреса:
Поштова адреса:	Поштова адреса:
UA_____ у Національному банку України Отримувач – Національний банк України Код за ЄДРПОУ _____ Індивідуальний податковий номер _____	UA_____ _____ _____ _____ Код за ЄДРПОУ _____ Індивідуальний податковий номер _____
Від Національного банку України	Від Замовника_____ _____
Виконавець	Замовник
_____ (особистий підпис)	_____ (особистий підпис)

Продовження додатка 1

Пояснення щодо заповнення договору про використання засобів криптографічного захисту інформації Національного банку України

1. Під час укладення договору Сторони використовують зразок договору, проте мають право вносити до нього зміни, зумовлені особливостями конкретної ситуації та засобів КЗІ, про передавання яких йдеться в договорі.

2. Організації, які не мають підпорядкованих установ або територіальних органів, укладають договір за зразком договору, виключивши з нього підпункти і слова, що стосуються установ Замовника.

Додаток
до договору про використання засобів криптографічного захисту інформації Національного банку України

Перелік
установ Замовника, які отримують засоби криптографічного захисту інформації Національного банку України та АРМ-НБУ інформаційний

№ з/п	Найменування установи	Адреса розташування МГК	Адреса розташування АРМ МГК	Адреса розташування АРМ-НБУ інформаційний
1	2	3	4	5
1				
2				

Від Національного банку України _____

Виконавець _____
(особистий підпис)

Від Замовника _____

Замовник _____
(особистий підпис)

Додаток 2
до Положення про використання
засобів криптографічного захисту
інформації Національного банку
(пункт 26 розділу IV)

Зобов’язання

Я, _____, який призначений
(найменування посади, прізвище, власне ім’я, по батькові)

згідно з внутрішнім документом _____
(найменування організації)

від “___” _____ 20__ року №___ відповідальною особою за зберігання та використання особистого ключа

_____,

(ідентифікатор користувача в інформаційній системі Національного банку)

ознайомлений з Положенням про використання засобів криптографічного захисту інформації Національного банку України (далі – Положення), і зобов’язуюся:

1) виконувати вимоги Положення;

2) не передавати іншим особам для використання особистий ключ та носій особистого ключа;

3) здійснювати контроль за строком дії сертифіката свого відкритого ключа;

4) не розголошувати паролі входу до інформаційних систем Національного банку України, пароля до носія особистого ключа;

5) у разі компрометації особистого ключа або виникнення такої загрози негайно повідомляти про це адміністратора інформаційної безпеки організації або керівника організації.

Я, _____,
(прізвище, власне ім’я, по батькові)

попереджений про те, що я є підписувачем електронних документів, на які накладений електронний підпис Національного банку України з використанням мого особистого ключа.

_____
(дата, особистий підпис)

Додаток 3
до Положення про використання
засобів криптографічного захисту
інформації Національного банку
(пункт 48 розділу V)

Звіт
щодо використання засобів криптографічного захисту інформації
Національного банку України

_____
(найменування організації)

за 20___ рік

№ з/п	Запитувана інформація	Відповідь
1	2	3
1	Назва, дата (число, місяць, рік) та номер чинного внутрішнього документа (документів) про призначення адміністратора інформаційної безпеки відповідно до пункту 13 розділу II Положення про використання засобів криптографічного захисту інформації Національного банку України (далі – Положення) та відповідальних осіб відповідно до пункту 23 розділу IV Положення	
2	Інформація про місцезнаходження АРМ-ІНФ, МГК, АРМ МГК (адреса розташування, номер приміщення)	
3	Чи є робочі місця відповідальних осіб, які розташовані за іншою адресою, ніж зазначена в колонці 2 рядка 2 цього звіту (так чи ні)? Якщо так, додати до цього звіту опис процедури генерації ключових пар такими відповідальними особами	
4	Чи взяті та оформлені всіма відповідальними особами зобов'язання відповідно до пункту 26 розділу IV та додатка 2 до Положення (так чи ні)? Якщо ні, зазначити причину	
5	Чи є призначення або повноваження адміністратора інформаційної безпеки,	

Продовження додатка 3
Продовження таблиці

1	2	3
	заборонені згідно з пунктом 14 розділу II Положення (так чи ні)? Якщо так, зазначити, які саме є призначення або повноваження та причину їх наявності	
6	Чи виконує адміністратор інформаційної безпеки в повному обсязі обов'язки, визначені в розділі IV Положення (так чи ні)? Якщо ні, зазначити перелік обов'язків, що не виконує адміністратор інформаційної безпеки, та причини їх невиконання	
7	Чи здійснюють відповідальні особи особисто генерацію ключових пар (так чи ні)? Якщо ні, зазначити причину. Чи використовується віддалений доступ до АРМ МГК для відповідальних осіб для генерації ключових пар? Якщо так, зазначити назву та реквізити внутрішнього документа, що регламентує ідентифікацію відповідальних осіб перед наданням віддаленого доступу до АРМ МГК (пункт 29 розділу IV Положення)	
8	Чи здійснюють відповідальні особи контроль за строком дії сертифікатів особистих ключів (так чи ні)? Якщо ні, зазначити причину	
9	Чи є внутрішній порядок зберігання особистих ключів відповідно до пункту 40 розділу IV Положення (так чи ні)? Якщо так, зазначити назву та реквізити такого документа. Якщо ні, зазначити причину	
10	Чи ознайомлені відповідальні особи з внутрішнім порядком зберігання особистих ключів (так чи ні)? Якщо ні, зазначити причину	
11	Чи забезпечено налаштування комп'ютера з АРМ-ІНФ, комп'ютера з АРМ МГК відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку (так чи ні)? Якщо ні, зазначити причину	
12	Чи забезпечено дотримання порядку доступу відповідальних осіб до засобів КЗІ відповідно до пункту 27 розділу IV	

Продовження додатка 3

Продовження таблиці

1	2	3
	Положення (так чи ні)? Якщо ні, зазначити причину	
13	Кількість випадків заміни МГК за звітний період, зазначити причину заміни	
14	Кількість випадків компрометації особистих ключів за звітний період	
15	Кількість сеансів генерацій ключових пар за звітний період (за кожним МГК окремо)	
16	Кількість особистих ключів (на останній робочий день звітного періоду), що використовуються в організації	
17	Чи є в організації архів електронного журналу МГК (так чи ні)? Якщо ні, зазначити причину	
18	Чи забезпечено розміщення АРМ-ІНФ, АРМ МГК відповідно до пункту 44 розділу IV Положення (так чи ні)? Якщо ні, зазначити причину	
19	Чи є внутрішній документ про призначення працівників, які мають доступ до приміщень з АРМ-ІНФ, АРМ МГК відповідно до пункту 44 розділу IV Положення (так чи ні)? Якщо так, зазначити назву та реквізити такого документа. Якщо ні, зазначити причину	
20	Зазначте умови зберігання МГК (пункт 34 розділу IV Положення)	
21	Чи впроваджувався в організації тимчасовий порядок експлуатації засобів КЗІ та/або управління ключами в умовах, що визначені в пункті 12 розділу II Положення?	
22	Які носії для зберігання особистих ключів використовуються (пункт 38 розділу IV Положення)?	

Додаток 4
до Положення про використання
засобів криптографічного захисту
інформації Національного банку
(пункт 51 розділу V)

зразок

Інформація про готовність
до використання засобів криптографічного захисту інформації
Національного банку України

_____
(найменування організації)

№ з/п	Запитувана інформація	Відповідь
1	2	3
1	Зазначте мету використання АРМ-ІНФ (стислий опис завдань, що будуть вирішені з використанням АРМ-НБУ-інформаційний)	
2	Які інформаційні системи Національного банку будуть впроваджені в організації?	
3	Інформація про розташування комп'ютерів для АРМ-ІНФ, АРМ МГК (адреса розташування, номер приміщення)	
4	Чи забезпечено розміщення АРМ-ІНФ, АРМ МГК відповідно до пункту 44 розділу IV Положення про використання засобів криптографічного захисту інформації Національного банку України (далі – Положення) (так чи ні)? Якщо ні, зазначити причину	
5	У який спосіб забезпечено виконання вимоги щодо виключення можливості несанкціонованого доступу до приміщень АРМ-ІНФ, АРМ МГК (пункт 44 розділу IV Положення)	
6	Опишіть умови, що створені для зберігання МГК (пункт 34 розділу IV Положення)	
7	Чи є внутрішній документ про призначення працівників, які мають доступ до приміщень з АРМ-ІНФ, АРМ МГК відповідно до пункту 44 розділу IV Положення (так чи ні)? Якщо так,	

Продовження додатка 4
Продовження таблиці

1	2	3
	зазначити назву та реквізити такого документа. Якщо ні, зазначити причину	
8	Назва, дата (число, місяць, рік) та номер чинного внутрішнього документа (документів) про призначення адміністратора інформаційної безпеки відповідно до пункту 13 розділу II Положення та відповідальних осіб відповідно до пункту 23 розділу IV Положення	
9	Чи взяті та оформлені всіма відповідальними особами зобов'язання відповідно до пункту 26 розділу IV та додатка 2 до Положення (так чи ні)? Якщо ні, зазначити причину	
10	Які носії для зберігання особистих ключів будуть використовуватися (пункт 38 розділу IV Положення)?	

Пояснення щодо надання інформації про готовність до використання засобів криптографічного захисту інформації Національного банку України

1. Під час складання запиту Національний банк використовує цей зразок, проте має право вносити до нього зміни, зумовлені особливостями конкретної організації.