

Національний банк України

Рада Системи BankID Національного банку України

ЗАТВЕРДЖЕНО
Рішення Ради Системи BankID
Національного банку України
(протокол від 25.12.2024
№ В/57-0002/163102)

Положення про забезпечення безперервного функціонування
Системи BankID Національного банку України
в умовах особливого періоду

м. Київ

Зміст

I. Загальні положення.....	3
II. Загальні засади забезпечення безперервного функціонування Системи BankID в умовах особливого періоду	4
III. Забезпечення функціонування Системи BankID під час дії режиму підвищеної готовності	5
IV. Забезпечення функціонування Системи BankID під час дії обмеженого режиму	5
V. Забезпечення функціонування Системи BankID під час дії критичного режиму.....	6
Додаток 1 <i>Протокол функціонування Системи BankID у режимі підвищеної готовності</i>	8
Додаток 2 <i>Протокол функціонування Системи BankID в обмеженому режимі</i>	13
Додаток 3 <i>Протокол функціонування Системи BankID у критичному режимі</i>	19
Додаток 4 <i>Рішення голови Ради Системи BankID</i>	25

I. Загальні положення

1. Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про банки і банківську діяльність”, “Про оборону України”, “Про правовий режим воєнного стану”, Положення про Систему BankID Національного банку України, затвердженого постановою Правління Національного банку України (далі – Національний банк) від 17 березня 2020 року № 32, зі змінами (у редакції постанови Правління Національного банку від 01 вересня 2023 року № 105) (далі – Положення № 32), Положення про організацію забезпечення безперебійного функціонування в умовах особливого періоду банківської системи України, діяльності небанківських фінансових установ та інших осіб, які не є фінансовими установами, але мають право надавати окремі фінансові послуги, регулювання та нагляд за діяльністю яких здійснює Національний банк України, затвердженого постановою Правління Національного банку від 14 червня 2024 року № 67 (далі – Положення № 67).

2. Терміни в цьому Положенні вживаються в таких значеннях:

1) договір приєднання до Системи BankID Національного банку (далі – Договір приєднання) – публічна пропозиція Національного банку з метою встановлення з юридичними особами-резидентами приватного або публічного права договірних взаємовідносин щодо роботи в Системі BankID Національного банку (далі – Система BankID);

2) специфікація взаємодії абонентського вузла з центральним вузлом Системи BankID Національного банку (далі – специфікація взаємодії) – документ, який визначає технічні вимоги щодо взаємодії Системи BankID з абонентськими вузлами. У специфікації взаємодії визначаються методи та протоколи інформаційної взаємодії, вимоги до захисту інформації в системі та інші технічні параметри;

3) суб'єкти взаємовідносин у Системі BankID – абоненти та Національний банк.

Інші терміни, що вживаються в цьому Положенні, використовуються в значеннях, визначених законодавством України, нормативно-правовими та розпорядчими актами Національного банку, документами, затвердженими рішеннями Ради Системи BankID.

3. Це Положення визначає загальні засади безперебійного функціонування Системи BankID в умовах особливого періоду.

II. Загальні засади забезпечення безперебійного функціонування Системи BankID в умовах особливого періоду

4. Загальне управління роботою Системи BankID в умовах особливого періоду здійснює Рада Системи BankID, оперативне управління – Рада Системи BankID, а у випадку неможливості зібрати кворум із членів Ради Системи BankID, допускається в обмеженому та критичному режимах прийняття рішення одноосібно головою Ради Системи BankID, або його заступником (у разі відсутності / недоступності голови Ради Системи BankID), за формою, наведеною у додатку 4 до цього Положення. Рішення Ради Системи BankID та голови Ради Системи BankID є обов'язковими до виконання абонентами.

5. Рада Системи BankID у своїй роботі керується законодавством України, у тому числі нормативно-правовими і розпорядчими актами Національного банку, приймає рішення відповідно до цього Положення та з урахуванням обставин, що складаються в країні в особливий період.

6. Порядок забезпечення безперебійного функціонування Системи BankID в умовах особливого періоду залежить від режиму функціонування (далі – режим), введеного відповідно до Положення № 67.

7. Залежно від потенційної загрози та / або фактичного впливу на ринок послуг України, в умовах особливого періоду можуть вводитись наступні режими:

- 1) підвищеної готовності;
- 2) обмежений;
- 3) критичний.

8. Суб'єкти взаємовідносин у Системі BankID в умовах особливого періоду виконують свої функції та обов'язки, передбачені Положенням № 32 та документами, затвердженими рішеннями Ради Системи BankID, із урахуванням виданих Національним банком, відповідно до введеного режиму, нормативно-правових актів та з урахуванням особливостей та вимог, визначених протоколами функціонування Системи BankID, під час дії того чи іншого режиму, наведених у додатках 1-3 до цього Положення.

9. Суб'єкти взаємовідносин у Системі BankID зобов'язані забезпечити можливість оперативного переходу між режимами та адаптації діяльності / інформаційних ресурсів до умов введеного режиму, шляхом удосконалення

системи управління безперебійного функціонування та виконання завчасно розроблених власних протоколів.

III. Забезпечення функціонування Системи BankID під час дії режиму підвищеної готовності

10. Режим підвищеної готовності зумовлюється тим, що немає системного (повторюваного) впливу прямих загроз для життя та здоров'я людей, цілісності та працездатності інфраструктури, або мінімальним рівнем такого впливу, за якого суб'єкти взаємовідносин у Системі BankID мають змогу в повному обсязі надавати послуги, виконувати свої функції та завдання.

11. Система BankID, у разі настання особливого періоду на території України, уведення воєнного стану в Україні або в окремих її місцевостях, функціонує в режимі підвищеної готовності до введення обмеженого або критичного режиму, або закінчення особливого періоду на території України.

12. Національний банк невідкладно, але не пізніше наступного робочого дня після дня настання особливого періоду, інформує абонентів засобами системи електронного документообігу Національного банку (далі – СЕД АСКОД) або корпоративною електронною поштою Національного банку про перехід Системи BankID до функціонування в режимі підвищеної готовності та активацію Протоколу функціонування Системи BankID в режимі підвищеної готовності (додаток 1 до цього Положення).

13. Абонент зобов'язаний розробити та мати власний протокол (внутрішній документ, що визначає порядок дій абонента для забезпечення надання дистанційних послуг користувачу із використанням Системи BankID) роботи в режимі підвищеної готовності за структурою (відповідним переліком розділів) та з дотриманням вимог, визначених у додатку 1 до цього Положення, та активувати його невідкладно у день отримання повідомлення від Національного банку про перехід Системи BankID до функціонування в режимі підвищеної готовності.

IV. Забезпечення функціонування Системи BankID під час дії обмеженого режиму

14. Обмежений режим зумовлюється наявністю системного впливу прямих загроз для життя та здоров'я людей, цілісності та працездатності інфраструктури або наявністю інформації чи об'єктивних обставин, які несуть потенційну загрозу для життя та здоров'я людей, цілісності та працездатності інфраструктури, за якого можливе надання суб'єктами

взаємовідносин у Системі BankID послуг та виконання завдань і функцій, однак можливі випадки недотримання умов та обсягів надання послуг та / або виконання завдань / функцій так само, як за умови функціонування у режимі підвищеної готовності.

15. Система BankID переходить до функціонування в обмеженому режиму після прийняття Національним банком відповідного рішення.

16. Національний банк невідкладно, але не пізніше наступного робочого дня після дня набрання відповідним рішенням Правління Національного банку чинності, інформує абонентів засобами СЕД АСКОД або корпоративною електронною поштою Національного банку або, за умови їх недоступності, – з використанням інших сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку, про перехід Системи BankID до функціонування в обмеженому режимі та активацію Протоколу функціонування Системи BankID в обмеженому режимі (додаток 2 до цього Положення).

17. Абонент зобов'язаний розробити та мати власний протокол (внутрішній документ, що визначає порядок дій абонента для забезпечення надання дистанційних послуг користувачу із використанням Системи BankID) роботи в обмеженому режимі за структурою (переліком розділів) та з дотриманням вимог, визначених у додатку 2 до цього Положення, та активувати його невідкладно у день отримання повідомлення від Національного банку про перехід Системи BankID до функціонування в обмеженому режиму.

V. Забезпечення функціонування Системи BankID під час дії критичного режиму

18. Критичний режим зумовлюється наявністю системного критичного впливу прямих загроз для життя та здоров'я людей, цілісності та працездатності інфраструктури, недоступності інфраструктури, наявністю критичних безпекових ситуацій (бойові дії, блокування, окупація, зараження територій та місцевостей), за якого можливість надавати послуги та / або виконувати завдання / функції суб'єктами взаємовідносин у Системі BankID є значно обмеженою або який може спричинити зупинення надання послуг та / або виконання завдань / функцій.

19. Система BankID переходить до функціонування в критичному режимі після прийняття Національним банком відповідного рішення.

20. Національний банк невідкладно, але не пізніше наступного робочого дня після дня набрання відповідним рішенням Правління Національного банку чинності, інформує абонентів засобами СЕД АСКОД або корпоративною електронною поштою Національного банку або, за умови їх недоступності, – з використанням інших сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку, про перехід Системи BankID до функціонування в критичному режимі та активацію Протоколу функціонування Системи BankID у критичному режимі (додаток 3 до цього Положення).

21. Абонент зобов'язаний розробити та мати власний протокол (внутрішній документ, що визначає порядок дій абонента для забезпечення надання дистанційних послуг користувачу із використанням Системи BankID) роботи в критичному режимі за структурою (переліком розділів) та з дотриманням вимог, визначених у додатку 3 до цього Положення, та активувати його невідкладно у день отримання повідомлення від Національного банку про перехід Системи BankID до функціонування в критичному режимі.

Голова Ради Системи BankID

Андрій ПОДДЕРЬОГІН

Додаток 1
до Положення про забезпечення
безперебійного функціонування
Системи BankID Національного
банку України в умовах особливого
періоду
(пункт 8 розділу II)

Протокол функціонування Системи BankID у режимі підвищеної готовності

I. Опис послідовності дій та перелік заходів, які повинні здійснюватися для
режиму підвищеної готовності

1. Система BankID під час дії режиму підвищеної готовності функціонує повноцінно у штатному режимі, забезпечує здійснення електронної дистанційної ідентифікації та верифікації фізичних осіб шляхом передавання даних користувачів абонентом-ідентифікатором абоненту-надавачу послуг / абоненту-надавачу послуг зі спеціальним статусом, суб'єкти взаємовідносин у Системі BankID надають послуги та виконують свої функції й завдання в повному обсязі з урахуванням існуючих загроз.

2. Національний банк для забезпечення функціонування Системи BankID під час дії режиму підвищеної готовності забезпечує:

1) надання послуг у Системі BankID абонентам та здійснення організаційно-технологічних функцій в Системі BankID відповідно до Положення № 32.

У разі настання негативних факторів Національний банк забезпечує оперативне відновлення процесів та переключення на резервні локації за недоступності основної. При переключенні на резервну локацію має забезпечуватись ведення у повному обсязі журналу аудиту центрального вузла Системи BankID;

2) розвиток Системи BankID з метою ефективного та надійного управління нею;

3) проведення взаєморозрахунків між комерційними абонентами у день розрахунків.

У разі настання негативних факторів, з метою забезпечення виконання міжабонентських розрахунків у день розрахунків, Радою Системи BankID може прийматись рішення щодо перенесення дня розрахунків на інший день;

4) проведення розрахунків за наданими Національним банком абонентам послугами у Системі BankID.

У разі настання негативних факторів, з метою забезпечення виконання білінгу в день білінгу, Радою Системи BankID може прийматись рішення щодо перенесення дня білінгу на інший день;

5) оперативне відновлення функціонування основного / використання резервного каналу телекомунікаційного зв'язку у разі порушення його роботи або виникнення позаштатних ситуацій.

3. Абонент зобов'язаний:

1) забезпечити надання послуг користувачам із використанням Системи BankID відповідно до Положення № 32 та документів, затверджених рішеннями Ради Системи BankID;

2) забезпечити безперервну роботу інформаційної інфраструктури, інформаційних та електронних комунікаційних систем, що використовуються для забезпечення надання дистанційних послуг користувачу із використанням Системи BankID, шляхом, зокрема використання в центрі обробки даних резервних джерел електроживлення, дизельних електростанцій та наявності ресурсів / палива для їх роботи не менше ніж сім діб із постійним поповненням запасів із надійних джерел;

3) забезпечити максимально можливу безперебійність роботи своїх систем і каналів зв'язку з урахуванням вірогідного тимчасового обмеження надання електронних комунікаційних послуг та постачання електроенергії строком не менше ніж сім діб;

4) підтримувати в актуальному стані резервування об'єктів інформаційної інфраструктури, каналів зв'язку, здійснювати їх оперативне переключення з основної локації на резервну, у тому числі з використанням надавачів хмарних послуг, та забезпечувати створення, зберігання та оперативне відновлення з резервних копій даних відповідних інформаційних систем;

5) забезпечити виконання підготовчих робіт для підтримання роботи власних абонентських вузлів / порталів послуг у належному стані відповідно до вимог, визначених Положенням № 32 та документів, затверджених рішеннями Ради Системи BankID;

6) забезпечити стабільне підключення власних каналів зв'язку до центрального вузла Системи BankID, а також мати змогу здійснити

підключення на резервній локації за недоступності основної. При переключенні на резервну локацію має забезпечуватись ведення в повному обсязі журналу аудиту абонентських вузлів;

7) забезпечити готовність до запровадження обмеженого та критичного режимів;

8) протягом трьох годин у робочий час та протягом 48 годин у неробочий час із моменту виявлення повідомити в порядку, визначеному Договором приєднання, Національний банк про:

виникнення позаштатних ситуацій у роботі абонентського вузла / порталу послуг;

будь-яке порушення або невідповідність роботи Системи BankID у цілому та (або) окремих її частин, роботи абонентських вузлів / порталів послуг вимогам Положення № 32 та / або специфікації взаємодії та / або інших документів, затверджених рішеннями Ради Системи BankID;

виявлені факти порушення цілісності даних, що передаються з використанням Системи BankID;

виявлені факти несанкціонованих дій щодо інформації, отриманої з використанням Системи BankID;

порушення інформаційної безпеки власного абонентського вузла;

припинення роботи абонентського вузла Системи BankID, причини та прогностні терміни відновлення його роботи.

II. Перелік відповідальних осіб за організацію, контроль і виконання запланованих для режиму підвищеної готовності дій та завдань

4. Перелік відповідальних осіб Національного банку України за організацію, контроль і виконання запланованих для забезпечення функціонування Системи BankID дій та завдань (з класифікацією та розподілом ролей) під час дії режиму підвищеної готовності затверджується окремим рішенням Ради Системи BankID.

III. Порядок взаємодії та способи комунікації між керівниками, працівниками, підрозділами Національного банку, а також між абонентами та Національним банком

5. Порядок взаємодії та способи комунікації між працівниками Національного банку, задіяними в процесі розвитку, супроводження та забезпечення діяльності Системи BankID, а також з іншими працівниками Національного банку з метою виконання своїх функціональних обов'язків, під час дії режиму підвищеної готовності здійснюється як і при звичайному

режимі: засобами СЕД АСКОД, корпоративною електронною поштою Національного банку та засобами телекомунікаційного зв'язку.

6. Взаємодія та комунікація між Національним банком та абонентами під час дії режиму підвищеної готовності здійснюється засобами СЕД АСКОД, корпоративною електронною поштою Національного банку та засобами телекомунікаційного зв'язку.

7. Національний банк залишає за собою право використовувати альтернативні засоби електронної комунікації або паперові носії інформації для забезпечення безперебійного функціонування Системи BankID та доведення рішень Ради Системи BankID / голови Ради Системи BankID або його заступника (у разі відсутності голови Ради Системи BankID) до абонентів у разі виникнення технічних проблем із СЕД АСКОД та / або з корпоративною електронною поштою Національного банку під час дії режиму підвищеної готовності.

IV. Порядок активації та деактивації протоколу

8. Протокол функціонування Системи BankID у режимі підвищеної готовності активується у разі настання особливого періоду на території України, введення воєнного стану в Україні або в окремих її місцевостях.

9. Протокол функціонування Системи BankID у режимі підвищеної готовності деактивується у разі:

введення обмеженого або критичного режиму;

закінчення особливого періоду на території України.

10. Національний банк невідкладно, але не пізніше наступного робочого дня після дня настання / закінчення особливого періоду на території України, інформує абонентів засобами СЕД АСКОД або корпоративною електронною поштою Національного банку про активацію / деактивацію Протоколу функціонування Системи BankID у режимі підвищеної готовності.

V. Порядок виконання дій та завдань для режиму підвищеної готовності

11. Дії та завдання під час дії режиму підвищеної готовності здійснюються та виконуються працівниками Національного банку, відповідальними за розвиток, супроводження та забезпечення діяльності Системи BankID, відповідно до своїх функціональних обов'язків, згідно із

затвердженими регламентами та внутрішніми протоколами Національного банку.

VI. Перелік необхідних ресурсів для забезпечення функціонування Системи BankID

12. Перелік необхідних ресурсів Національного банку України (включно і людських) для забезпечення функціонування Системи BankID під час дії режиму підвищеної готовності затверджується окремим рішенням Ради Системи BankID.

Додаток 2
до Положення про забезпечення
безперебійного функціонування
Системи BankID Національного
банку України в умовах особливого
періоду
(пункт 8 розділу II)

Протокол функціонування Системи BankID в обмеженому режимі

I. Опис послідовності дій та перелік заходів, які повинні здійснюватися для обмеженого режиму

1. Система BankID під час дії обмеженого режиму функціонує з урахуванням наявності системного впливу прямих загроз (життю / здоров'ю людей та цілісності / працездатності інфраструктури) та об'єктивних обставин, за яких можливі випадки недотримання умов та обсягів надання послуг та / або виконання функцій суб'єктами взаємовідносин у Системі BankID.

2. Національний банк для забезпечення функціонування Системи BankID під час дії обмеженого режиму:

1) забезпечує надання послуг у Системі BankID абонентам та здійснення організаційно-технологічних функцій в Системі BankID відповідно до Положення № 32.

У разі настання негативних факторів Національний банк забезпечує оперативне, у терміни можливі з урахуванням наявності прямих загроз життю / здоров'ю людей або необхідності та можливості відновлення цілісності та працездатності інфраструктури, відновлення процесів та переключення на резервні локації за недоступності основної. При переключенні на резервну локацію має забезпечуватись ведення у повному обсязі журналу аудиту центрального вузла Системи BankID;

2) здійснює посилений моніторинг за роботою Системи BankID для своєчасної ідентифікації подій, настання яких може вплинути на штатне функціонування Системи BankID, із метою своєчасного реагування на них;

3) забезпечує проведення взаєморозрахунків між комерційними абонентами у день розрахунків.

Якщо Система BankID або окремі її модулі непрацездатні або відповідальні працівники Національного банку не можуть виконати свої функції через загрозу їх життю / здоров'ю, або через інші чинники, які

заважають працівникам забезпечити виконання міжабонентських розрахунків у день розрахунків, Радою Системи BankID / головою Ради Системи BankID або його заступником (у разі відсутності / недоступності голови Ради Системи BankID) приймається рішення щодо перенесення дня розрахунків на інший день;

4) забезпечує проведення розрахунків за наданими Національним банком абонентам послугами в Системі BankID.

Якщо Система BankID або окремі її модулі непрацездатні або відповідальні працівники Національного банку не можуть виконати свої функції через загрозу їх життю / здоров'ю, або через інші чинники, які заважають працівникам забезпечити виконання білінгу в день білінгу, Радою Системи BankID / головою Ради Системи BankID або його заступником (у разі відсутності / недоступності голови Ради Системи BankID) приймається рішення щодо перенесення дня білінгу на інший день;

5) забезпечує оперативне відновлення функціонування основного / використання резервного каналу телекомунікаційного зв'язку у разі порушення його роботи або виникнення позаштатних ситуацій;

б) здійснює моніторинг динаміки зміни кількості електронних запитів на електронну дистанційну ідентифікацію в Системі BankID (навантаження). У разі зростання кількості електронних запитів на електронну дистанційну ідентифікацію до рівня, наближеного до максимальної пропускну здатності Системи BankID, обмеженої працездатності Системи BankID, у відповідності до рішень Ради Системи BankID / голови Ради Системи BankID або його заступника (у разі відсутності / недоступності голови Ради Системи BankID), з метою забезпечення виконання соціально значущої функції Системи BankID, здійснює тимчасове зупинення (блокування в Системі BankID) роботи абонента та / або абонентського вузла та / або передавання даних користувачів до контрагентів абонента-надавача послуг зі спеціальним статусом.

За відсутності зв'язку з Радою Системи BankID / головою Ради Системи BankID або його заступником (у разі відсутності / недоступності голови Ради Системи BankID) блокування в Системі BankID здійснюється в такій послідовності:

а) комерційні абоненти-надавачі послуг / комерційні абоненти-надавачі послуг зі спеціальним статусом (або їх абонентські вузли);

б) некомерційні абоненти-надавачі послуг (крім державних сервісів, визначених окремим рішенням Ради Системи BankID як важливі);

в) абоненти-ідентифікатори (окрім системно важливих банків);

7) здійснює оперативну комунікацію з абонентами (за наявності потреби) щодо їх роботи в Системі BankID. Запитує та отримує інформацію від абонентів у разі виникнення сумнівів стосовно відповідності їхньої діяльності або діяльності їхніх контрагентів (для абонентів-надавачів послуг зі спеціальним статусом) вимогам законодавства України, Положення № 32, специфікації взаємодії, Договору приєднання, а також інших документів, затверджених рішеннями Ради Системи BankID, та / або безпечності передавання ними даних користувачів.

3. Абонент зобов'язаний:

1) забезпечити надання послуг користувачам із використанням Системи BankID відповідно до Положення № 32 та документів, затверджених рішеннями Ради Системи BankID;

2) забезпечити безперервну роботу інформаційної інфраструктури, інформаційних та електронних комунікаційних систем, що використовуються для забезпечення надання дистанційних послуг користувачу із використанням Системи BankID, шляхом, зокрема використання в центрі обробки даних резервних джерел електроживлення, дизельних електростанцій та наявності ресурсів / палива для їх роботи не менше ніж сім діб із постійним поповненням запасів із надійних джерел;

3) забезпечити максимально можливу безперебійність роботи своїх систем і каналів зв'язку з урахуванням вірогідного тимчасового обмеження надання електронних комунікаційних послуг та постачання електроенергії строком не менше ніж сім діб;

4) підтримувати в актуальному стані резервування об'єктів інформаційної інфраструктури, каналів зв'язку, здійснювати їх оперативне переключення з основної локації на резервну, у тому числі з використанням надавачів хмарних послуг, та забезпечувати створення, зберігання та оперативне відновлення з резервних копій даних відповідних інформаційних систем;

5) забезпечити виконання підготовчих робіт для підтримання роботи власних абонентських вузлів / порталів послуг у належному стані відповідно до вимог, визначених Положенням № 32 та документами, затвердженими рішеннями Ради Системи BankID;

6) забезпечити стабільне підключення власних каналів до центрального вузла Системи BankID, а також мати змогу здійснити підключення на резервній локації за недоступності основної. При переключенні на резервну

локацію має забезпечуватись ведення у повному обсязі журналу аудиту абонентських вузлів ;

7) забезпечити готовність до запровадження критичного режиму ;

8) протягом трьох годин із моменту виявлення або відновлення можливості комунікації (якщо засоби зв'язку були недоступні або існувала загроза життю / здоров'ю людей) повідомити будь-яким доступним способом Національний банк про:

виникнення позаштатних ситуацій у роботі абонентського вузла / порталу послуг;

будь-яке порушення або невідповідність роботи Системи BankID у цілому та (або) окремих її частин, роботи абонентських вузлів / порталів послуг вимогам Положення № 32 та / або специфікації взаємодії та / або інших документів, затверджених рішеннями Ради Системи BankID;

виявлені факти порушення цілісності даних, що передаються з використанням Системи BankID;

виявлені факти несанкціонованих дій щодо інформації, отриманої з використанням Системи BankID;

порушення інформаційної безпеки власного абонентського вузла;

припинення роботи абонентського вузла Системи BankID, причини та прогнози терміни відновлення його роботи.

4. Абонент-надавач послуг / абонент-надавач послуг зі спеціальним статусом забезпечує надання послуг користувачам із використанням Системи BankID, а абонент-ідентифікатор – виконання функцій ідентифікації, автентифікації та верифікації клієнтів, які є користувачами, за технічної можливості та відсутності впливу прямих загроз життю / здоров'ю їх працівників та за умови виконання вимог щодо захисту, конфіденційності та цілісності інформації під час її оброблення на власних абонентських вузлах.

5. Абонент, у разі настання обставин, що унеможливають надання послуги користувачу та / або виконання ним функцій, протягом цього ж робочого дня інформує про це Національний банк електронною поштою, засобами телекомунікаційного зв'язку та, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку, із зазначенням таких обставин і відновлює надання послуг користувачам та виконання своїх функцій у Системі BankID у найкоротший можливий строк.

6. Національний банк має право в односторонньому порядку за рішенням Ради Системи BankID тимчасово зупинити (блокувати в Системі BankID) роботу абонента та / або абонентського вузла та / або передавання

даних користувачів до контрагентів абонента-надавача послуг зі спеціальним статусом без розірвання договірних відносин із абонентом, у разі виявленого порушення роботи абонентського вузла в Системі BankID, порушення вимог щодо захисту, конфіденційності та цілісності інформації під час її оброблення на власних абонентських вузлах або виявлення обґрунтованої загрози, до моменту усунення таких порушень / загроз.

II. Перелік відповідальних осіб за організацію, контроль і виконання запланованих для обмеженого режиму дій та завдань

7. Перелік відповідальних осіб Національного банку України за організацію, контроль і виконання запланованих для забезпечення функціонування Системи BankID дій та завдань (з класифікацією та розподілом ролей) під час дії обмеженого режиму затверджується окремим рішенням Ради Системи BankID.

III. Порядок взаємодії та способи комунікації між керівниками, працівниками, підрозділами Національного банку, а також між абонентами та Національним банком

8. Порядок взаємодії та способи комунікації між працівниками Національного банку, задіяними в процесі розвитку, супроводження та забезпечення діяльності Системи BankID, а також з іншими працівниками Національного банку з метою виконання своїх функціональних обов'язків, під час дії обмеженого режиму здійснюється засобами СЕД АСКОД, корпоративною електронною поштою Національного банку, засобами телекомунікаційного зв'язку та, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку.

9. Взаємодія та комунікація між Національним банком та абонентами під час дії обмеженого режиму здійснюється засобами СЕД АСКОД, корпоративною електронною поштою Національного банку, засобами телекомунікаційного зв'язку та, за умови їх недоступності – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку.

10. Національний банк залишає за собою право використовувати альтернативні засоби електронної комунікації або паперові носії інформації для забезпечення безперебійного функціонування Системи BankID та доведення рішень Ради Системи BankID / голови Ради Системи BankID або його заступника (у разі відсутності / недоступності голови Ради Системи BankID) до абонентів у разі виникнення технічних проблем із СЕД АСКОД

та / або корпоративною електронною поштою Національного банку під час дії обмеженого режиму.

IV. Порядок активації та деактивації протоколу

11. Протокол функціонування Системи BankID в обмеженому режимі:

активується у разі прийняття Правлінням Національного банку рішення про введення обмеженого режиму;

деактивується у разі прийняття Правлінням Національного банку рішення про скасування обмеженого режиму.

12. Національний банк невідкладно, але не пізніше наступного робочого дня після дня набрання відповідним рішенням Правління Національного банку чинності, інформує абонентів засобами СЕД АСКОД або корпоративною електронною поштою Національного банку, або, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку, про активацію / деактивацію Протоколу функціонування Системи BankID в обмеженому режимі.

V. Порядок виконання дій та завдань для обмеженого режиму

13. Дії та завдання під час дії обмеженого режиму здійснюються та виконуються працівниками Національного банку, відповідальними за розвиток, супроводження та забезпечення діяльності Системи BankID, відповідно до своїх функціональних обов'язків, згідно з затвердженими регламентами та внутрішніми протоколами Національного банку, з урахуванням технічної можливості та відсутності впливу прямих загроз життю / здоров'ю працівників.

VI. Перелік необхідних ресурсів для забезпечення функціонування Системи BankID

14. Перелік необхідних ресурсів Національного банку України (включно і людських) для забезпечення функціонування Системи BankID під час дії обмеженого режиму затверджується окремим рішенням Ради Системи BankID.

Додаток 3
до Положення про забезпечення
безперебійного функціонування
Системи BankID Національного
банку України в умовах особливого
періоду
(пункт 8 розділу II)

Протокол функціонування Системи BankID у критичному режимі

I. Опис послідовності дій та перелік заходів, які повинні здійснюватися для критичного режиму

1. Система BankID під час дії критичного режиму функціонує з урахуванням наявності системного критичного впливу прямих загроз (життю / здоров'ю людей та цілісності / працездатності / недоступності інфраструктури), безпекових ситуацій, за яких можливість надання послуг та / або виконання функцій / завдань суб'єктами взаємовідносин в Системі BankID є значно обмеженою або навіть може бути зупинена.

2. Національний банк, для забезпечення функціонування Системи BankID під час дії критичного режиму:

1) забезпечує надання послуг у Системі BankID абонентам та здійснення організаційно-технологічних функцій в Системі BankID відповідно до Положення № 32.

У разі настання негативних факторів Національний банк забезпечує оперативне, у терміни можливі з урахуванням наявності прямих загроз життю / здоров'ю людей або необхідності та можливості відновлення цілісності та працездатності інфраструктури або усунення інших безпекових ситуацій, відновлення процесів та переключення на резервні локації за недоступності основної. При переключенні на резервну локацію має забезпечуватись ведення у повному обсязі журналу аудиту центрального вузла Системи BankID;

2) здійснює посилений моніторинг за роботою Системи BankID для своєчасної ідентифікації подій, настання яких може вплинути на штатне функціонування Системи BankID, із метою своєчасного реагування на них;

3) забезпечує проведення взаєморозрахунків між комерційними абонентами у день розрахунків.

Якщо Система BankID або окремі її модулі непрацездатні або відповідальні працівники Національного банку не можуть виконати свої

функції через загрозу їх життю / здоров'ю, або через інші чинники, які заважають працівникам забезпечити виконання міжабонентських розрахунків у день розрахунків, Радою Системи BankID / головою Ради Системи BankID або його заступником (у разі відсутності / недоступності голови Ради Системи BankID) приймається рішення щодо перенесення дня розрахунків на інший день;

4) забезпечує проведення розрахунків за наданими Національним банком абонентам послугами у Системі BankID.

Якщо Система BankID або якщо окремі її модулі непрацездатні або відповідальні працівники Національного банку не можуть виконати свої функції через загрозу їх життю / здоров'ю, або через інші чинники, які заважають працівникам забезпечити виконання білінгу в день білінгу, Радою Системи BankID / головою Ради Системи BankID або його заступником (у разі відсутності / недоступності голови Ради Системи BankID) приймається рішення щодо перенесення дня білінгу на інший день;

5) забезпечує оперативне відновлення функціонування основного / використання резервного каналу телекомунікаційного зв'язку у разі порушення його роботи або виникнення позаштатних ситуацій у строк, можливий з урахуванням критичного впливу прямих загроз життю / здоров'ю людей та цілісності / працездатності / недоступності інфраструктури;

б) здійснює моніторинг динаміки зміни кількості ЕЗІ в Системі BankID (навантаження). У разі зростання кількості операцій до рівня, наближеного до максимальної пропускної здатності Системи BankID, обмеженої працездатності Системи BankID, у відповідності до рішень Ради Системи BankID / голови Ради Системи BankID або його заступника (у разі відсутності / недоступності голови Ради Системи BankID), з метою забезпечення виконання соціально значущої функції системи, здійснює тимчасове зупинення (блокування в Системі BankID) роботи абонента та / або абонентського вузла та / або передавання даних користувачів до контрагентів абонента-надавача послуг зі спеціальним статусом.

У разі відсутності зв'язку з Радою Системи BankID / головою Ради Системи BankID або його заступником (у разі відсутності / недоступності голови Ради Системи BankID) блокування в Системі BankID здійснюється в такій послідовності:

а) комерційні абоненти-надавачі послуг / комерційні абоненти-надавачі послуг зі спеціальним статусом (або їх абонентські вузли);

б) некомерційні абоненти-надавачі послуг (крім державних сервісів, визначених окремим рішенням Ради Системи BankID як важливі);

в) абоненти-ідентифікатори (окрім системно-важливих банків);

7) здійснює оперативну комунікацію з абонентами (за наявності потреби) щодо їх роботи в Системі BankID. Запитує та отримує інформацію від абонентів у разі виникнення сумнівів стосовно відповідності їхньої діяльності або діяльності їхніх контрагентів (для абонентів-надавачів послуг зі спеціальним статусом) вимогам законодавства України, Положення № 32, специфікації взаємодії, Договору приєднання, а також інших документів, затверджених рішеннями Ради Системи BankID, та / або безпечності передавання ними даних користувачів.

3. Абонент зобов'язаний:

1) забезпечити надання послуг користувачам із використанням Системи BankID відповідно до Положення № 32 та документів, затверджених рішеннями Ради Системи BankID;

2) забезпечити безперервну роботу інформаційної інфраструктури, інформаційних та електронних комунікаційних систем, що використовуються для забезпечення надання дистанційних послуг користувачу із використанням Системи BankID, шляхом, зокрема використання в центрі обробки даних резервних джерел електроживлення, дизельних електростанцій та наявності ресурсів / палива для їх роботи не менше ніж сім діб із постійним поповненням запасів із надійних джерел;

3) забезпечити максимально можливу безперебійність роботи своїх систем і каналів зв'язку з урахуванням вірогідного тимчасового обмеження надання електронних комунікаційних послуг та постачання електроенергії строком не менше ніж сім діб;

4) підтримувати в актуальному стані резервування об'єктів інформаційної інфраструктури, каналів зв'язку, здійснювати їх оперативне переключення з основної локації на резервну, у тому числі з використанням надавачів хмарних послуг, та забезпечувати створення, зберігання та оперативне відновлення з резервних копій даних відповідних інформаційних систем;

5) забезпечити виконання підготовчих робіт для підтримання роботи власних абонентських вузлів / порталів послуг у належному стані відповідно до вимог, визначених Положенням № 32 та документами, затвердженими рішеннями Ради Системи BankID;

6) забезпечити стабільне підключення власних каналів до центрального вузла Системи BankID, а також мати змогу здійснити підключення на

резервній локації за недоступності основної. При переключенні на резервну локацію має забезпечуватись ведення у повному обсязі журналу аудиту абонентських вузлів;

7) у найкоротший термін із моменту виявлення або відновлення можливості комунікації (якщо засоби зв'язку були недоступні або існувала загроза життю / здоров'ю людей) повідомити будь-яким доступним способом Національний банк про:

виникнення позаштатних ситуацій у роботі абонентського вузла / порталу послуг;

будь-яке порушення або невідповідність роботи Системи BankID у цілому та (або) окремих її частин, роботи абонентських вузлів / порталів послуг вимогам Положення № 32 та / або специфікації взаємодії та / або інших документів, затверджених рішеннями Ради Системи BankID;

виявлені факти порушення цілісності даних, що передаються з використанням Системи BankID;

виявлені факти несанкціонованих дій щодо інформації, отриманої з використанням Системи BankID;

порушення інформаційної безпеки власного абонентського вузла;

припинення роботи абонентського вузла Системи BankID, причини та прогностні терміни відновлення його роботи.

4. Суб'єкти взаємодії в Системі BankID забезпечують надання послуг із використанням Системи BankID та виконання своїх функцій до настання обставин, що унеможливають надання послуг та / або виконання функцій (за технічної можливості та відсутності впливу прямих загроз життю / здоров'ю їх працівників, безпекових ситуацій).

5. Абонент, у разі настання обставин, що унеможливають надання послуги користувачу та / або виконання ним функцій, протягом цього ж робочого дня інформує про це Національний банк електронною поштою, засобами телекомунікаційного зв'язку та, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку, із зазначенням таких обставин і відновлює надання послуг користувачам та виконання своїх функцій у Системі BankID у найкоротший можливий строк.

6. Національний банк має право в односторонньому порядку за рішенням Ради Системи BankID тимчасово зупинити (блокувати в Системі BankID) роботу абонента та / або абонентського вузла та / або передавання даних користувачів до контрагентів абонента-надавача послуг зі спеціальним статусом без розірвання договірних відносин із абонентом, який зазнав впливу негативних факторів, що призвело до порушення роботи

абонентського вузла в Системі BankID, порушення вимог щодо захисту, конфіденційності та цілісності інформації під час її оброблення на власних абонентських вузлах, або існує така загроза, до моменту усунення таких порушень / загроз.

II. Перелік відповідальних осіб за організацію, контроль і виконання запланованих для критичного режиму дій та завдань

7. Перелік відповідальних осіб Національного банку України за організацію, контроль і виконання запланованих для забезпечення функціонування Системи BankID дій та завдань (з класифікацією та розподілом ролей) під час дії критичного режиму затверджується окремим рішенням Ради Системи BankID.

III. Порядок взаємодії та способи комунікації між керівниками, працівниками, підрозділами Національного банку, а також між абонентами та Національним банком

8. Порядок взаємодії та способи комунікації між працівниками Національного банку, задіяними в процесі розвитку, супроводження та забезпечення діяльності Системи BankID, а також з іншими працівниками Національного банку з метою виконання своїх функціональних обов'язків, під час дії критичного режиму здійснюється засобами СЕД АСКОД, корпоративною електронною поштою Національного банку, засобами телекомунікаційного зв'язку та, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку.

9. Взаємодія та комунікація між Національним банком та абонентами під час дії критичного режиму здійснюється засобами СЕД АСКОД, корпоративною електронною поштою Національного банку, засобами телекомунікаційного зв'язку та, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку.

10. Національний банк залишає за собою право використовувати альтернативні засоби електронної комунікації або паперові носії інформації для забезпечення безперебійного функціонування Системи BankID та доведення рішень Ради Системи BankID / голови Ради Системи або його заступника (у разі відсутності / недоступності голови Ради Системи BankID) BankID до абонентів у разі виникнення технічних проблем з СЕД АСКОД та / або корпоративною електронною поштою Національного банку під час дії критичного режиму.

IV. Порядок активації та деактивації протоколу

11. Протокол функціонування Системи BankID у критичному режимі:

активується у разі прийняття Правлінням Національного банку рішення про введення критичного режиму;

деактивується у разі прийняття Правлінням Національного банку рішення про скасування критичного режиму.

12. Національний банк невідкладно, але не пізніше наступного робочого дня після дня набрання відповідним рішенням Правління Національного банку чинності, інформує абонентів засобами СЕД АСКОД або корпоративною електронною поштою Національного банку, або, за умови їх недоступності, – з використанням сервісів обміну повідомленнями в мережі Інтернет, незаборонених до використання розпорядчими актами Національного банку про активацію / деактивацію Протоколу функціонування Системи BankID у критичному режимі.

V. Порядок виконання дій та завдань для критичного режиму

13. Дії та завдання під час дії критичного режиму здійснюються та виконуються працівниками Національного банку, відповідальними за розвиток, супроводження та забезпечення діяльності Системи BankID, відповідно до своїх функціональних обов'язків, згідно із затвердженими регламентами та внутрішніми протоколами Національного банку, з урахуванням технічної можливості та відсутності впливу прямих загроз життю / здоров'ю працівників, до настання обставин, що унеможливають виконання тих чи інших дій чи завдань.

VI. Перелік необхідних ресурсів для забезпечення функціонування Системи BankID

14. Перелік необхідних ресурсів Національного банку України (включно і людських) для забезпечення функціонування Системи BankID під час дії критичного режиму затверджується окремим рішенням Ради Системи BankID.

Додаток 4
до Положення про забезпечення
безперебійного функціонування
Системи BankID Національного
банку України в умовах особливого
періоду
(пункт 4 розділу II)

НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

Рішення голови Ради Системи BankID
для забезпечення безперебійного функціонування
Системи BankID в умовах особливого періоду

Дата _____

м. Київ

№ _____

Відповідно до вимог статті 28 та частини другої статті 35¹ Закону України “Про запобігання корупції” та з урахуванням вимог розпорядчих актів Національного банку України повідомляю про відсутність конфлікту інтересів, пов’язаного з прийняттям цього рішення.

Порядок денний:

ВИРІШЕНО (УХВАЛЕНО):

Підстава для одноосібного прийняття рішення:

Підстава:

Контроль за виконанням покласти на:

Термін виконання:

Дата набрання чинності рішенням:

Голова Ради Системи BankID

_____ [Ім’я ПРИЗВИЩЕ]
(особистий підпис)