ПРОЄКТ

Правління Національного банку України

П О С Т А Н О В А

Київ

Про затвердження Положення про вимоги до системи управління ризиками надавача нефінансових платіжних послуг та внесення змін до Положення про вимоги до системи управління надавача фінансових платіжних послуг

Відповідно до статей 7, 15, 55[1], 56 Закону України “Про Національний банк України”, статей 15, 26, 66, 81 Закону України “Про платіжні послуги”, з метою встановлення вимог до системи управління ризиками надавачів нефінансових платіжних послуг Правління Національного банку України **постановляє:**

1. Затвердити Положення про вимоги до системи управління ризиками надавача нефінансових платіжних послуг, що додається.

2. Положення про вимоги до системи управління надавача фінансових платіжних послуг, затверджене постановою Правління Національного банку України від 10 жовтня 2024 року № 123, після пункту 1 глави 1 розділу I доповнити новим пунктом 1[1] такого змісту:

“1[1]. Вимоги цього Положення також поширюються на установи, які зазначені в підпунктах 1, 2, 4 пункту 1 глави 1 розділу I цього Положення, які суміщають діяльність з надання фінансових платіжних послуг з наданням нефінансових платіжних послуг.”.

3. Департаменту методології регулювання діяльності небанківських фінансових установ (Сергій Савчук) після офіційного опублікування довести до відома надавачів платіжних послуг інформацію про прийняття цієї постанови.

4. Постанова набирає чинності з 01 серпня 2025 року.

Голова Андрій ПИШНИЙ

Інд. 33

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Положення
про вимоги до системи управління ризиками надавача нефінансових платіжних послуг

І. Вступні положення

1. Це Положення розроблене відповідно до вимог Закону України “Про Національний банк України”, Закону України “Про платіжні послуги” (далі – Закон про платіжні послуги) з метою організації та забезпечення належного функціонування системи управління кіберризиками та ризиками безпеки як складовими операційного ризику (далі – система управління ризиками) під час провадження діяльності з надання нефінансових платіжних послуг надавачами платіжних послуг з надання відомостей з рахунків та надавачами платіжних послуг з ініціювання платіжних операцій (далі – надавач нефінансових платіжних послуг).

2. Терміни в цьому Положенні вживаються в такому значенні:

1) бізнес-процес – сукупність взаємопов’язаних або взаємозалежних видів діяльності, спрямованих на створення певного продукту або послуги;

2) виконавчий орган – одноосібний / колегіальний виконавчий орган надавача фінансових платіжних послуг надавача нефінансових платіжних послуг;

3) високий (жовтий) рівень критичності – один із критеріїв істотності інцидентів безпеки та кіберінцидентів, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача нефінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання нефінансових платіжних послуг, внаслідок чого створюються передумови для порушення конфіденційності, цілісності та доступності критичних даних, виникають передумови для порушення безперервності надання нефінансових платіжних послуг;

4) внутрішні документи – документи, затверджені або видані уповноваженим органом управління надавача нефінансових платіжних послуг у межах його компетенції з урахуванням вимог законодавства України;

5) інформаційна інфраструктура – програмне забезпечення та/або технічні засоби в інформаційній, інформаційно-комунікаційній та комунікаційній системах, що використовуються надавачем нефінансових платіжних послуг для надання нефінансових платіжних послуг;

6) критичний (червоний) рівень критичності – один із критеріїв істотності інцидентів безпеки та кіберінцидентів, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача нефінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання нефінансових платіжних послуг, безпеці (захищеності) критичних даних, та має негативний вплив на повноцінне функціонування відкритого банкінгу в Україні;

7) небанківський надавач фінансових платіжних послуг – небанківський надавач платіжних послуг, крім надавача нефінансових платіжних послуг;

8) низький (білий) рівень критичності – один із критеріїв істотності інцидентів безпеки та кіберінцидентів, який встановлюється до події, що не загрожує здійсненню операційної діяльності надавача нефінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання нефінансових платіжних послуг, безпеці (захищеності) критичних даних;

9) операційний інцидент або інцидент безпеки – подія або низка пов’язаних подій, незапланованих надавачем нефінансових платіжних послуг, які мають або ймовірно матимуть негативний вплив на цілісність, доступність, конфіденційність, автентичність та/або безперервність надання нефінансових платіжних послуг (далі – інцидент безпеки);

10) операційний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок виникнення під час надання нефінансових платіжних послуг недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників надавача нефінансових платіжних послуг або інших осіб, збоїв у роботі систем надавача нефінансових платіжних послуг або внаслідок впливу зовнішніх факторів;

11) ризик безпеки – ризик виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок виникнення під час надання нефінансових платіжних послуг подій, обставин, факторів, що можуть нести загрозу порушення виконання вимог щодо захисту інформації та персональних

даних користувачів, автентифікації, зберігання, захисту, використання інформації, що становить таємницю надавача нефінансових платіжних послуг;

12) середній (зелений) рівень критичності – один із критеріїв істотності інцидентів безпеки та кіберінцидентів, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача нефінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання нефінансових платіжних послуг, але не загрожує порушенню конфіденційності, цілісності та доступності критичних даних;

13) система управління ризиками – сукупність належним чином задокументованих, затверджених з урахуванням вимог законодавства України і впроваджених внутрішніх документів, які визначають порядок дій, спрямованих на здійснення систематичного процесу виявлення, вимірювання, моніторингу, контролю, звітування та мінімізацію (зниження до контрольованого рівня) усіх суттєвих ризиків діяльності надавача нефінансових платіжних послуг.

Термін “кіберризик” уживається в цьому Положенні в значенні, наведеному в абзаці другому частини першої статті 66 Закону про платіжні послуги.

Терміни “кіберінцидент”, “критичні дані” уживаються в цьому Положенні в значенні, наведеному в Положенні про захист інформації та кіберзахист учасниками платіжного ринку, затвердженого постановою Правління Національного банку України від 19 травня 2021 року № 43 (зі змінами).

Інші терміни в цьому Положенні вживаються у значеннях, наведених у Законі про платіжні послуги, інших законах України та нормативно-правових актах Національного банку України (далі – Національний банк) з питань регулювання ринку платіжних послуг.

3. Це Положення визначає вимоги до системи управління ризиками таких надавачів нефінансових платіжних послуг:

1) надавача платіжних послуг з надання відомостей з рахунків;

2) надавача платіжних послуг з ініціювання платіжних операцій.

4. Вимоги цього Положення не поширюються на банки, філії іноземних банків та небанківських надавачів фінансових платіжних послуг.

ІІ. Загальні вимоги

5. До компетенції виконавчого органу належить вирішення всіх питань, пов’язаних із забезпеченням належного функціонування системи управління ризиками надавача нефінансових платіжних послуг, крім питань, що належать до виключної компетенції загальних зборів учасників (акціонерів) надавача

нефінансових платіжних послуг, наглядової ради надавача нефінансових платіжних послуг (у разі її створення).

7. Виконавчий орган у межах своїх повноважень відповідає за:

1) безперервність надання нефінансових платіжних послуг;

2) відповідність діяльності надавача нефінансових платіжних послуг законодавству України;

3) належне функціонування механізмів управління операційними ризиками, кіберризиками та ризиками безпеки надавача нефінансових платіжних послуг під час провадження діяльності з надання нефінансових платіжних послуг;

4) актуальність політики управління інцидентами безпеки та кіберінцидентами під час надання нефінансових платіжних послуг та своєчасне повідомлення Національного банку про інциденти безпеки та кіберінциденти.

8. Надавач нефінансових платіжних послуг зобов'язаний призначити головного ризик-менеджера, відповідального за виконання функції з управління операційним ризиком та ризиком безпеки (далі – ризик-менеджер), або покласти виконання відповідних функцій на особу, відповідальну за забезпечення захисту інформації, кіберзахисту та інформаційної безпеки надавача нефінансових платіжних послуг (далі – відповідальна особа).

10. Заходами, дотримання яких свідчить про належне функціонування механізмів управління операційними ризиками, кіберризиками та ризиками безпеки надавача нефінансових платіжних послуг, є забезпечення надавачем нефінансових платіжних послуг:

1) повноти та ефективності впровадження внутрішніх документів з питань системи управління ризиками;

2) відповідності внутрішніх документів щодо системи управління ризиками вимогам цього Положення;

3) належного функціонування системи управління ризиками (забезпечує виконавчий орган у межах своїх повноважень);

4) призначення надавачем нефінансових платіжних послуг ризик-менеджера та/або відповідальної особи;

5) відповідальності виконавчого органу, ризик менеджера (у разі призначення) та відповідальної особи за неналежне виконання та/або невиконання ними своїх обов’язків;

6) забезпечення безперервності надання нефінансових платіжних послуг відповідно до вимог, визначених у розділі V цього Положення;

7) створення ефективної системи управління ризиками відповідно до вимог, визначених у розділах III, IV цього Положення.

III. Загальні підходи до системи управління ризиками

11. Надавач нефінансових платіжних послуг створює ефективну та належну систему управління ризиками під час провадження діяльності з надання нефінансових платіжних послуг з урахуванням:

1) особливостей виду діяльності надавача нефінансових платіжних послуг;

2) бізнес-моделі надавача нефінансових платіжних послуг;

3) характеру, виду й обсягів нефінансових платіжних послуг, які надаються надавачем нефінансових платіжних послуг;

4) ризиків, притаманних діяльності надавача нефінансових платіжних послуг;

5) особливостей, встановлених Законом про платіжні послуги, законами з питань регулювання окремих ринків фінансових послуг, законами з питань діяльності господарських товариств та нормативно-правовими актами Національного банку.

12. Ефективна система управління ризиками надавача нефінансових платіжних послуг повинна відповідати таким принципам:

1) ефективність - забезпечення об’єктивної оцінки розміру ризиків надавача нефінансових платіжних послуг та повноти заходів щодо управління ризиками з оптимальним використанням фінансових ресурсів, персоналу та інформаційних систем щодо управління ризиками надавача нефінансових платіжних послуг;

2) своєчасність - забезпечення своєчасного (на ранній стадії) виявлення, вимірювання, моніторингу, контролю, звітування та пом’якшення всіх видів ризиків на всіх організаційних рівнях;

3) структурованість - чіткий розподіл функцій, обов’язків і повноважень з управління ризиками між усіма працівниками надавача нефінансових платіжних послуг та їх відповідальності згідно з таким розподілом;

4) розмежування обов’язків (відокремлення функції контролю від здійснення операцій надавача нефінансових платіжних послуг) - уникнення ситуації, за якої одна й та сама особа здійснює операції надавача нефінансових платіжних послуг та виконує функції контролю;

5) усебічність та комплексність - охоплення всіх видів діяльності надавача нефінансових платіжних послуг на всіх рівнях та в усіх його підрозділах, оцінка взаємного впливу ризиків;

6) пропорційність - відповідність системи управління ризиками розміру надавача нефінансових платіжних послуг, складності, обсягам, видам, характеру здійснюваних надавачем нефінансових платіжних послуг та профілю ризику надавача фінансових платіжних послуг;

7) незалежність - свобода від обставин, що становлять загрозу для неупередженого виконання функцій з управління ризиками;

8) конфіденційність - обмеження доступу до інформації, яка має бути захищеною від несанкціонованого ознайомлення;

9) постійне вдосконалення - постійне поліпшення процедур управління ризиками, моделей та інструментів ідентифікації та вимірювання ризиків, з урахуванням провідних практик, відповідних методів, зазначених у міжнародних стандартах, які мінімізують вплив кіберзагроз на інформаційну інфраструктуру.

13. Система управління ризиками повинна забезпечувати щодо усіх видів ризиків [як наявних (реалізованих, поточних), так і потенційних (нереалізованих)]:

1) виявлення;

2) оцінку (вимірювання);

3) моніторинг;

4) контроль;

5) звітування та мінімізацію (зниження до контрольованого рівня).

14. Система управління ризиками надавача нефінансових платіжних послуг охоплює управління операційними ризиками, кіберризиками, ризиками безпеки, а також іншими суттєвими ризиками, які притаманні його діяльності (у разі їх визначення).

15. Надавач нефінансових платіжних послуг має право розширювати перелік суттєвих видів ризиків, визначений у пункті 14 розділу ІІІ цього Положення, самостійно встановлювати критерії, за якими визначатиметься суттєвість інших видів ризиків діяльності надавача нефінансових платіжних послуг і визначати порядок виявлення таких ризиків.

Перелік суттєвих видів ризиків має бути визначений у внутрішніх документах надавача нефінансових платіжних послуг (у разі їх визначення).

16. Надавач нефінансових платіжних послуг оцінює операційні ризики, кіберризики та ризики безпеки з урахуванням їх взаємозв'язку та впливу на інші ризики, що притаманні діяльності надавача нефінансових платіжних послуг та/або визначені надавачем нефінансових платіжних послуг як такі (за наявності).

17. Надавач нефінансових платіжних послуг зобов'язаний мінімізувати вплив кіберризиків та ризиків безпеки шляхом застосування відповідних стратегій, політики, процедур, протоколів та інструментів, потрібних для належного та адекватного захисту інформаційної інфраструктури, включаючи програмне та апаратне забезпечення, сервери.

18. Надавач нефінансових платіжних послуг зобов'язаний мінімізувати вплив кіберризиків та ризиків безпеки для захисту всіх компонентів інфраструктури, таких як приміщення, центри обробки даних і виділені зони, щоб гарантувати, що інформаційна інфраструктура належним чином захищена від ризиків, включаючи пошкодження та несанкціонований доступ.

19. Надавач нефінансових платіжних послуг для вимірювання (оцінки) операційних ризиків, кіберризиків та ризиків безпеки зобов'язаний використовувати дані, що є достовірними, повними та точними, а також використовувати ефективні моделі та інструменти.

20. Результати здійснення надавачем нефінансових платіжних послуг процедур виявлення, оцінки (вимірювання), моніторингу, контролю, звітування та мінімізації (зниження до контрольованого рівня) операційних ризиків, кіберризиків та ризиків безпеки повинні бути задокументовані.

21. Надавач нефінансових платіжних послуг має право включити до внутрішніх документів щодо управління операційними ризиками, кіберризиками

та ризиками безпеки інші положення, додатково до тих, що встановлюються цим Положенням та які не суперечать вимогам цього Положення.

22. Надавач нефінансових платіжних послуг своєчасно та періодично переглядає (не рідше одного разу на рік) та оновлює (актуалізує) внутрішні документи з питань управління операційними ризиками, кіберризиками та ризиками безпеки, включаючи у разі змін у законодавстві України, дія яких поширюється на надавача нефінансових платіжних послуг, змін у профілі ризику надавача нефінансових платіжних послуг, та з урахуванням інших внутрішніх чи зовнішніх подій та/або обставин.

Зміни в системі управління ризиками надавача нефінансових платіжних послуг, а також причини таких змін повинні бути задокументовані і підлягають затвердженню уповноваженим органом управління.

23. Внутрішні документи з питань управління операційними ризиками, кіберризиками та ризиками безпеки надавача нефінансових платіжних послуг повинні бути доступними для Національного банку для проведення відповідних оцінок ефективності системи управління ризиками, включаючи їх надання на письмову вимогу Національного банку.

24. Надавач нефінансових платіжних послуг зобов’язаний забезпечувати постійне вдосконалення системи управління ризиками.

25. Надавач нефінансових платіжних послуг зобов’язаний:

1) доводити до відома працівників зміст внутрішніх документів щодо управління ризиками;

2) письмово фіксувати кожен факт ознайомлення працівника з такими документами у спосіб, що дає змогу підтвердити факт та дату такого ознайомлення, включаючи ознайомлення під підпис або в інший спосіб, що забезпечує підтвердження ознайомлення.

IV. Політика, порядки та процедури управління операційними ризиками, кіберризиками та ризиками безпеки

26. Надавач нефінансових платіжних послуг розробляє і впроваджує такі окремі внутрішні документи щодо управління операційними ризиками, кіберризиками та ризиками безпеки:

1) політика управління операційними ризиками, кіберризиками та ризиками безпеки;

2) порядок управління операційними ризиками, кіберризиками та ризиками безпеки;

3) процедури управління операційними ризиками, кіберризиками та ризиками безпеки.

Надавач нефінансових платіжних послуг має право виокремити компоненти політики, порядку, процедур управління операційними ризиками, кіберризиками та ризиками безпеки в окремі документи.

27. Політика управління операційними ризиками, кіберризиками та ризиками безпеки повинна містити:

1) мету, завдання та принципи управління операційними ризиками, кіберризиками та ризиками безпеки;

2) організаційну структуру процесу управління операційними ризиками, кіберризиками та ризиками безпеки (визначені учасники процесу, їх повноваження, відповідальність та порядок взаємодії);

3) підходи щодо виявлення, оцінки (вимірювання), моніторингу, контролю, звітування та мінімізації (зниження до контрольованого рівня) операційних ризиків, кіберризиків та ризиків безпеки;

4) критерії визначення значних подій операційного ризику, порядок їх дослідження та ескалації інформації щодо таких подій керівникам надавача нефінансових платіжних послуг;

5) перелік та формат (інформаційне наповнення) форм управлінської звітності щодо операційних ризиків, включаючи кіберризики та ризики безпеки, та обґрунтування таких критеріїв;

7) внутрішні правила щодо ефективного зниження та контролю за операційними ризиками, кіберризиками та ризиками безпеки, пов’язаними з наданням нефінансових платіжних послуг, які повинні також містити процедури забезпечення безпеки надання нефінансових платіжних послуг, реагування на інциденти безпеки, здійснення моніторингу та ведення бази даних інцидентів безпеки та кіберінцидентів;

8) опис можливих наслідків недотримання політики управління операційними ризиками, кіберризиками та ризиками безпеки персоналом надавача нефінансових платіжних послуг, третіми особами, які мають доступ до інформаційної інфраструктури надавача нефінансових платіжних послуг [включаючи третіх (юридичних) осіб, які залучаються надавачем нефінансових платіжних послуг на договірній основі для виконання окремих операційних

функцій, пов’язаних із наданням нефінансових платіжних послуг, постачальників послуг технічного характеру, що супроводжують надання нефінансових платіжних послуг], технологічних операторів платіжних послуг (далі – треті особи).

28. Порядок та процедури управління операційними ризиками, кіберризиками та ризиками безпеки повинні містити:

1) порядок та процедури щодо виявлення, оцінки (вимірювання), моніторингу, контролю, звітування та мінімізації (зниження до контрольованого рівня) операційних ризиків, кіберризиків та ризиків безпеки;

2) процедури контролю за повнотою та якістю даних про події операційного ризику, включаючи кіберризику та ризику безпеки, включаючи інструменти, що використовуються для такого контролю;

3) порядок та критерії класифікації подій операційного ризику, включаючи кіберризику та ризику безпеки, за типами подій;

4) правила визначення критеріїв значних подій операційних ризиків, кіберризиків та ризиків безпеки, порядок їх класифікації, процедури їх оброблення, аналізу, дослідження, ескалації інформації та звітування керівникам надавача нефінансових платіжних послуг;

5) порядок та процедури реагування на операційні ризики, кіберризики та ризики безпеки;

6) визначення та опис основних інструментів, що використовуються під час управління операційними ризиками, кіберризиками та ризиками безпеки, а також порядок їх використання;

7) порядок управління операційними ризиками, кіберризиками та ризиками безпеки, що властиві процесу співпраці з третіми особами;

8) порядок обміну інформацією між учасниками процесу управління операційними ризиками, кіберризиками та ризиками безпеки, включаючи види, форми і терміни надання інформації.

29. Надавач нефінансових платіжних послуг зобов’язаний розробляти, документувати та впроваджувати порядок і процедури управління операційними ризиками, кіберризиками та ризиками безпеки надавача нефінансових платіжних послуг з метою забезпечення безпеки інформаційної інфраструктури, забезпечення відповідних гарантій захисту від вторгнень і неправомірного використання інформації, збереження її конфіденційності, цілісності,

доступності, автентичності та гарантувати точну й оперативну передачу інформації без невиправданих затримок.

30. Надавач нефінансових платіжних послуг забезпечує впровадження задокументованих і затверджених процесів та процедур щодо:

1) забезпечення безперервності функціонування інформаційної інфраструктури;

2) управління інцидентами безпеки та кіберінцидентами / проблемами інформаційно-комунікаційних технологій для їх моніторингу та реєстрації, включаючи процедури визначення, відстеження, реєстрації, категоризації та класифікації за пріоритетом на основі критичності процесів, а також процедури реагування;

3) управління змінами для забезпечення контролю за всіма змінами в системах та сервісах інформаційно-комунікаційних технологій, включаючи процедури реєстрації, тестування, оцінювання, затвердження, упровадження і верифікації змін.

31. Процедура забезпечення безпеки надавача нефінансових платіжних послуг повинна включати всі зазначені нижче елементи:

1) обмеження доступу до інформаційної інфраструктури з урахуванням установлених прав та ролей;

2) визначення базової конфігурації для критичних компонентів інформаційної інфраструктури з урахуванням провідних практик, відповідних методів, зазначених у міжнародних стандартах, які мінімізують вплив кіберзагроз на інформаційну інфраструктуру, а також заходів для регулярної перевірки того, що заходи безпеки ефективно впроваджені;

3) визначення заходів захисту від шкідливого коду;

4) визначення заходів безпеки для забезпечення використання лише дозволених носіїв інформації та систем для передачі та зберігання даних надавача нефінансових платіжних послуг;

5) процес безпечного видалення локальних або збережених зовні даних, які надавачу нефінансових платіжних послуг більше не потрібно обробляти;

6) процес безпечної утилізації або виведення з експлуатації пристроїв зберігання локальних або збережених зовні даних, що містять інформацію з обмеженим доступом;

7) визначення та впровадження заходів безпеки для запобігання втраті та витоку даних для систем і кінцевих пристроїв;

8) упровадження технічних та організаційних заходів безпеки щодо облікових даних, які використовуються для доступу до хмарних ресурсів користувача, під час використання хмарних послуг.

32. Надавач нефінансових платіжних послуг розробляє та впроваджує процедури контролю за повнотою та якістю даних про події операційного ризику, включаючи кіберризик та ризик безпеки, надавача нефінансових платіжних послуг, що передбачають:

1) розподіл обов'язків та відповідальності щодо контролю за повнотою та якістю даних про події операційного ризику, включаючи кіберризик та ризик безпеки, надавача нефінансових платіжних послуг під час їх збору, унесення до бази внутрішніх подій операційного ризику, включаючи кіберризик та ризик безпеки, та подальшої перевірки;

2) заходи поточного (під час збору та внесення даних до бази внутрішніх подій операційного ризику, включаючи кіберризик та ризик безпеки) та подальшого контролю за повнотою та якістю даних про події операційного ризику, включаючи кіберризик та ризик безпеки, включаючи автоматизовані та/або ручні перевірки щодо того, що немає помилок та суперечливості даних, відповідності обліковим, фінансовим, статистичним даним та даним управлінської звітності надавача нефінансових платіжних послуг.

V. Безперервність надання нефінансових платіжних послуг

33. Надавач нефінансових платіжних послуг із метою забезпечення належного управління операційними ризиками, кіберризиками та ризиками безпеки розробляє методологію забезпечення безперервності надання нефінансових платіжних послуг, яка включає:

1) політику заходів із забезпечення безперервності надання нефінансових платіжних послуг;

2) процедуру аналізу впливу негативних факторів на бізнес-процеси надавача нефінансових платіжних послуг (далі – аналіз впливу);

3) план забезпечення безперервності надання нефінансових платіжних послуг.

34. Політика заходів із забезпечення безперервності надання нефінансових платіжних послуг повинна містити:

1) ключові цілі надавача нефінансових платіжних послуг щодо забезпечення безперервності надання нефінансових платіжних послуг;

2) принципи та підходи надавача нефінансових платіжних послуг щодо здійснення аналізу впливу негативних факторів на бізнес-процеси надавача нефінансових платіжних послуг;

3) принципи та підходи надавача нефінансових платіжних послуг щодо розроблення та приведення в дію плану забезпечення безперервності надання нефінансових платіжних послуг;

4) принципи та підходи надавача нефінансових платіжних послуг щодо моніторингу ефективності та вдосконалення плану забезпечення безперервності надання нефінансових платіжних послуг.

35. Аналіз впливу включає визначення рівнів критичності бізнес-процесів, систем та сервісів інформаційно-комунікаційних технологій, інших ресурсів (працівники, приміщення, техніка) із урахуванням:

1) цільового часу на відновлення процесів та систем, що обслуговують цей процес, після переривання діяльності;

2) максимально допустимого проміжку часу, за який можлива втрата критичних даних надавачем нефінансових платіжних послуг у разі відмови систем та сервісів інформаційно-комунікаційних технологій.

36. Аналіз впливу повинен охоплювати всі процеси та підрозділи надавача нефінансових платіжних послуг з урахуванням їх взаємозалежності.

37. Надавач нефінансових платіжних послуг у межах здійснення аналізу впливу забезпечує послідовний та комплексний аналіз вразливості процесів, систем та сервісів інформаційно-комунікаційних технологій надавача нефінансових платіжних послуг до різних типів імовірних сценаріїв переривання діяльності, включаючи сценарій кібератаки, відсутності / обмеження доступу в режимі реального часу до рахунків користувачів. Надавач нефінансових платіжних послуг здійснює кількісну та якісну оцінку ймовірного фінансового, операційного та репутаційного впливу сценаріїв на діяльність надавача нефінансових платіжних послуг, використовуючи внутрішні та зовнішні дані.

38. Надавач нефінансових платіжних послуг використовує результати аналізу впливу негативних факторів на процеси надавача нефінансових

платіжних послуг для встановлення цілей і пріоритетів під час розроблення плану забезпечення безперервності надання нефінансових платіжних послуг.

39. Надавач нефінансових платіжних послуг розробляє план забезпечення безперервності надання нефінансових платіжних послуг, який уключає:

1) стратегічні цілі та пріоритети надавача нефінансових платіжних послуг щодо забезпечення безперервності надання нефінансових платіжних послуг у розрізі процесів надавача нефінансових платіжних послуг;

2) процедури та заходи з виявлення і усунення загрози безперервності надання нефінансових платіжних послуг, реагування на інциденти безпеки та кіберінциденти, порушення безперервності надання нефінансових платіжних послуг;

3) заходи в разі порушення безперервності надання нефінансових платіжних послуг щодо внутрішніх комунікацій, а також зовнішніх комунікацій надавача нефінансових платіжних послуг із користувачами, контрагентами надавача нефінансових платіжних послуг, Національним банком, іншими регуляторними, контролюючими органами та органами державної влади;

4) заходи з відновлення діяльності для критичних процесів надавача нефінансових платіжних послуг, включаючи відновлення постійного доступу в режимі реального часу до рахунків користувача;

5) заходи з відновлення систем та сервісів інформаційно-комунікаційних технологій після збоїв.

VI. Інциденти безпеки, кіберінциденти

40. Залежно від ступеня негативних наслідків, що можуть настати в результаті інцидентів безпеки та кіберінцидентів установлюються такі критерії істотності інцидентів безпеки та кіберінцидентів (далі – рівні критичності):

1) низький (білий);

2) середній (зелений);

3) високий (жовтий);

4) критичний (червоний).

41. Надавач нефінансових платіжних послуг зобов’язаний у довільній формі негайно (у найкоротший строк) повідомляти Національний банк про інциденти

безпеки та кіберінциденти, які відповідають високому (жовтому) та критичному (червоному) рівням критичності, та про неможливість / перепони у постійному доступі в режимі реального часу до рахунків користувачів та/або до прикладних програмних інтерфейсів надавача платіжних послуг з обслуговування рахунку в спосіб, визначений у пункті 44 розділу VII цього Положення.

VII. Порядок обміну інформацією та контролю Національного банку за дотриманням вимог до системи управління ризиками надавача нефінансових платіжних послуг

42. Національний банк здійснює контроль відповідно до вимог Закону про платіжні послуги та інших законів України за дотриманням надавачем нефінансових платіжних послуг вимог цього Положення та здійснює оцінку організації та належного функціонування системи управління ризиками у порядку, визначеному Положенням про проведення перевірок небанківських надавачів платіжних послуг, надавачів обмежених платіжних послуг, затвердженим постановою Правління Національного банку України від 06 квітня 2023 року № 47 (зі змінами), Положенням про здійснення безвиїзного нагляду на платіжному ринку, затвердженим постановою Правління Національного банку України від 05 травня 2023 року № 60 (зі змінами). Національний банк під час здійснення контролю та оцінки має право використовувати професійне судження.

43. Офіційна комунікація Національного банку із надавачем нефінансових платіжних послуг, його працівниками здійснюється засобами корпоративної електронної пошти (e-mail) Національного банку (шляхом надсилання повідомлення з офіційної електронної поштової скриньки Національного банку nbu@bank.gov.ua).

Така комунікація може включати:

1) запитування додаткової інформації, документів і пояснень;

2) отримання інформації, пояснень, додаткових документів щодо дотримання вимог цього Положення у вигляді електронних документів та/або електронних копій документів.

44. Надавач нефінансових платіжних послуг подає необхідні документи до Національного банку в один із таких способів:

1) на паперових носіях з одночасним поданням електронних копій цих документів без накладання кваліфікованого електронного підпису (далі – КЕП) (далі - електронні копії документів);

2) у формі електронного документа, підписаного шляхом накладання КЕП, або електронної копії документа, засвідченої відповідно КЕП керівника надавача нефінансових платіжних послуг, - на офіційну електронну поштову скриньку Національного банку nbu@bank.gov.ua або іншими засобами електронного зв'язку, які використовуються Національним банком для електронного документообігу.

Документи на вимогу Національного банку також подаються в електронній формі у форматі, визначеному Національним банком.

45. Національний банк для оцінки достатності заходів з управління ризиками проводить:

1) аналіз діяльності надавача нефінансових платіжних послуг, внутрішніх документів щодо управління операційними ризиками, кіберризиками, ризиками безпеки;

2) перевірку процесів, операцій, інструментів з управління ризиками;

3) інтерв'ю з керівниками, ризик-менеджером та/або відповідальною особою, аукціонером / учасником надавача нефінансових платіжних послуг та іншими працівниками надавача нефінансових платіжних послуг;

4) оцінку відповідності внутрішніх документів щодо управління операційними ризиками, кіберризиками, ризиками безпеки надавача нефінансових платіжних послуг вимогам цього Положення;

5) оцінку відповідності внутрішніх процесів надавача нефінансових платіжних послуг вимогам внутрішніх документів надавача нефінансових платіжних послуг.

46. Застосування Національним банком заходів впливу в разі порушення вимог цього Положення та/або в разі недостатності заходів з управління ризиками, що вживаються для захисту інтересів споживачів платіжних послуг, здійснюється в порядку, визначеному Законом про платіжні послуги та Положенням про застосування Національним банком України заходів впливу за порушення вимог законодавства, що регулює діяльність на платіжному ринку, затвердженим постановою Правління Національного банку України від 22 вересня 2022 року № 206 (зі змінами).