Офіційно опубліковано
28.10.2024

Правління Національного банку України

П О С Т А Н О В А

10 жовтня 2024 року Київ № 123

Про затвердження 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, 19, 26, 66, 81 Закону України “Про платіжні послуги”, статті 21 Закону України “Про фінансові послуги та фінансові компанії”, з метою встановлення вимог до системи управління надавачів фінансових платіжних послуг Правління Національного банку України **постановляє:**

1. Затвердити Положення про вимоги до системи управління надавача фінансових платіжних послуг (далі – Положення), що додається.

2. Платіжні установи (крім малих платіжних установ), установи електронних грошей, оператори поштового зв’язку, які мають право надавати фінансові платіжні послуги, філії іноземних платіжних установ та філії іноземних установ електронних грошей (далі – надавачі фінансових платіжних послуг) зобов’язані привести свою діяльність у відповідність до вимог Положення у терміни, установлені в графіку, що додається.

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

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

Голова Андрій ПИШНИЙ

Інд. 33

Додаток
до постанови Правління
Національного банку України
10 жовтня 2024 року № 123

Графік
приведення діяльності надавача фінансових платіжних послуг у відповідність до вимог Положення про вимоги до системи управління надавача фінансових платіжних послуг

№ з/п	Захід	Термін виконання
1	2	3
1	I. Перший етап – запровадження організаційних заходів	
2	1. Приведення організаційної структури системи внутрішнього контролю у відповідність до вимог Положення про вимоги до системи управління надавача фінансових платіжних послуг (далі – Положення), включаючи:	До 15.11.2024
3	1) створення підрозділу контролю за дотриманням норм (комплаєнс) або покладення виконання відповідних функцій на відповідального працівника;	
4	2) створення підрозділу з управління ризиками або покладення виконання відповідних функцій на відповідального працівника;	
5	3) створення підрозділу внутрішнього аудиту або покладення виконання відповідних функцій на відповідального працівника;	
6	4) визначення персонального розподілу функцій, обов’язків, відповідальності, повноважень членів наглядової ради, виконавчого органу, керівників підрозділів контролю (за наявності), їх підконтрольності та підзвітності, створення належного рівня системи стримування і противаг	
7	2. Надання надавачем фінансових платіжних послуг Національному банку України інформації про виконання першого етапу впровадження вимог Положення	До 01.12.2024
8	II. Другий етап – запровадження документів з питань системи внутрішнього контролю	
9	1. Розроблення / доопрацювання, затвердження та впровадження, включаючи:	До 15.11.2024
10	1) кодекс поведінки (етики);	

Продовження додатка
Продовження таблиці

1	2	3
11	2) політику виявлення, запобігання та управління конфліктами інтересів;	
12	3) положення про систему внутрішнього контролю;	
13	4) положення про підрозділ з управління ризиками або зміни до положення про підрозділ з управління ризиками (у разі створення) / посадову інструкцію головного ризик-менеджера або зміни до посадової інструкції головного ризик-менеджера;	
14	5) положення про підрозділ контролю за дотриманням норм (комплаєнс) або зміни до положення про підрозділ контролю за дотриманням норм (комплаєнс) (у разі створення) / посадову інструкцію головного комплаєнс-менеджера [особи, на яку покладена функція контролю за дотриманням норм (комплаєнс)] або зміни до посадової інструкції головного комплаєнс-менеджера [особи, на яку покладена функція контролю за дотриманням норм (комплаєнс)];	
15	6) положення про підрозділ внутрішнього аудиту або зміни до положення про підрозділ внутрішнього аудиту (у разі створення) / посадову інструкцію внутрішнього аудитора / головного внутрішнього аудитора або зміни до посадової інструкції внутрішнього аудитора / головного внутрішнього аудитора	
16	2. Надання надавачем фінансових платіжних послуг Національному банку України інформації про виконання другого етапу впровадження вимог Положення	До 01.12.2024
17	III. Третій етап – запровадження стратегій, політики, методик і процедур	
18	1. Розроблення / доопрацювання, затвердження та запровадження внутрішніх документів щодо управління ризиками, включаючи:	До 01.12.2024
19	1) політику управління ризиками, включаючи ліміти ризиків;	
20	2) політику управління окремими видами ризиків;	
21	3) положення про контроль за дотриманням норм (комплаєнс);	

Продовження додатка
Продовження таблиці

1	2	3
22	4) стратегію управління ризиками; порядок, форми, наповнення та періодичність надання звітів суб'єктам системи управління ризиками;	
23	5) методи (інструменти) управління виявленими ризиками в межах підходів до управління ризиками	
24	2. Розроблення / доопрацювання, затвердження та запровадження внутрішніх документів щодо управління операційним ризиком:	До 01.12.2024
25	1) політики управління операційним ризиком;	
26	2) політики управління кіберризиками та ризиками безпеки;	
27	3) методології забезпечення безперервності надання платіжних послуг, включаючи політику заходів із забезпечення безперервності надання платіжних послуг, процедуру аналізу впливу негативних факторів на бізнес-процеси надавача фінансових платіжних послуг, план забезпечення безперервності надання платіжних послуг	
28	3. Надання надавачем фінансових платіжних послуг Національному банку України інформації про виконання третього етапу впровадження вимог Положення	До 16.12.2024
29	IV. Четвертий етап – запровадження декларації схильності до ризиків та інших вимог Положення	
30	1. Розроблення, затвердження та запровадження декларації схильності до ризиків	До 16.12.2024
31	2. Розроблення / доопрацювання та затвердження наглядовою радою інших внутрішніх документів щодо управління ризиками та запровадження інших вимог Положення	До 25.12.2024
32	3. Надання надавачем фінансових платіжних послуг Національному банку України інформації про виконання четвертого етапу запровадження Положення	До 31.12.2024

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
10 жовтня 2024 року № 123

Положення
про вимоги до системи управління надавача фінансових платіжних послуг

І. Загальні положення

1. Основні положення та терміни

1. Це Положення розроблене відповідно до вимог Закону України “Про Національний банк України”, Закону України “Про платіжні послуги” (далі – Закон про платіжні послуги), Закону України “Про фінансові послуги та фінансові компанії” (далі – Закон про фінансові послуги) з метою організації та забезпечення належного функціонування системи корпоративного управління, системи внутрішнього контролю та системи управління ризиками (далі – система управління):

1) платіжної установи (крім малої платіжної установи);

2) установи електронних грошей;

3) оператора поштового зв’язку, який має право надавати фінансові платіжні послуги;

4) філії іноземної платіжної установи та філії іноземної установи електронних грошей (далі – філія іноземної платіжної установи).

2. Терміни в цьому Положенні вживаються в такому значенні:

1) агрегування даних щодо ризиків – виявлення, збір та оброблення даних про ризики, включаючи класифікацію, сегментацію, об’єднання чи розподіл даних про ризики, з урахуванням вимог щодо складання звітності про ризики, що дає змогу оцінити діяльність надавача фінансових платіжних послуг з урахуванням ризик-апетиту;

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

3) високий (помаранчевий) рівень критичності – один із критеріїв істотності операційних інцидентів, кіберінцидентів та інцидентів безпеки, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача фінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання платіжних послуг, безпеці (захищеності) критичних даних, внаслідок чого прогнозується значний вплив на національну безпеку і оборону, соціальну сферу, національну економіку та її окремі галузі, припинення виконання функцій та/або надання послуг критичною інфраструктурою, подія може мати транскордонний вплив;

4) внутрішні документи – документи, затверджені або видані уповноваженим органом управління надавача фінансових платіжних послуг у межах його компетенції з урахуванням вимог законодавства України, включаючи політику за окремими напрямами діяльності, положення, стандарти, інструкції, методики, правила, стратегії, розпорядження, рішення, накази або документи, розроблені в іншій формі;

5) декларація схильності до ризиків – внутрішній документ, який визначає сукупну величину ризик-апетиту, види ризиків, які надавач фінансових платіжних послуг прийматиме або уникатиме з метою виконання свого плану діяльності, та рівень ризик-апетиту щодо кожного з таких ризиків (індивідуальний рівень);

6) допустимий рівень ризику – максимальна величина ризику, яку надавач фінансових платіжних послуг у змозі прийняти за всіма видами ризиків з огляду на здатність адекватно та ефективно управляти ризиками, а також з урахуванням обмежень, установлених законодавством України;

7) інформаційна інфраструктура – програмне забезпечення та/або технічні засоби в інформаційній, інформаційно-комунікаційній та комунікаційній системах, що використовуються надавачем фінансових платіжних послуг для здійснення платіжних операцій;

8) інцидент безпеки – подія або низка пов’язаних подій, що виникли під час надання платіжних послуг / виконання платіжних операцій та не були заплановані надавачем фінансових платіжних послуг, що мали або ймовірно матимуть негативний вплив на конфіденційність, цілісність, доступність інформації та/або безперервність надання платіжних послуг;

9) істотний технічний збій або істотні інші невідворотні обставини – неспроможність надавача фінансових платіжних послуг своєчасно та ефективно

надавати фінансові платіжні послуги протягом 24 годин поспіль з моменту настання технічного збою або інших невідворотних обставин, що призвело до порушення надавачем фінансових платіжних послуг вимог законодавства України, включаючи вимогу щодо безперервності надання фінансових платіжних послуг;

10) ключові процеси – дії, операції, завдання, що виконуються структурними підрозділами, окремими працівниками надавача фінансових платіжних послуг, інформаційними системами (включаючи функції, передані на аутсорсинг), що мають безпосередній та істотний вплив на досягнення цілей діяльності надавача фінансових платіжних послуг, та порушення здійснення контрольних заходів щодо таких дій, операцій, завдань може завдати істотних збитків надавачу фінансових платіжних послуг або його користувачам та/або може призвести до порушення вимог законодавства України;

11) комплаєнс-ризик – ризик виникнення збитків та/або санкцій, додаткових втрат або недоотримання запланованих доходів, або втрати репутації внаслідок невиконання надавачем фінансових платіжних послуг вимог законодавства України про діяльність та регулювання діяльності на ринку фінансових послуг, включаючи законодавство України, що регулює діяльність на платіжному ринку, ринкових стандартів, правил добросовісної конкуренції та корпоративної етики, правил платіжних систем, а також внутрішніх документів надавача фінансових платіжних послуг, виникнення конфлікту інтересів або невідповідності діяльності надавача фінансових платіжних послуг таким вимогам;

12) кредитний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок невиконання боржником / контрагентом узятих на себе зобов’язань відповідно до умов договору;

13) критична або важлива функція – функція, припинення чи переривання якої суттєво погіршить фінансову ефективність надавача фінансових платіжних послуг або надійність, або безперервність надання його послуг;

14) критичний (червоний) рівень критичності – один із критеріїв істотності операційних інцидентів, кіберінцидентів та інцидентів безпеки, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача фінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання платіжних послуг, безпеці (захищеності) критичних даних, внаслідок чого виникають реальні загрози для національної безпеки, обороноздатності, економічної

безпеки, зовнішніх відносин, створюється реальна загроза обмеження в наданні основних послуг населенню надавачем фінансових платіжних послуг;

15) культура управління ризиками – дотримання визначених надавачем фінансових платіжних послуг принципів, правил, норм надавача фінансових платіжних послуг, спрямованих на поінформованість усіх працівників надавача фінансових платіжних послуг щодо прийняття ризиків та управління ризиками;

16) ліміти (обмеження) щодо ризиків надавача фінансових платіжних послуг (далі – ліміт ризику) – обмеження (якісні та/або кількісні, єдиним значенням або діапазоном чи межами), установлені для контролю за величиною ризиків, на які наражається надавач фінансових платіжних послуг протягом своєї діяльності, з метою дотримання затвердженого рівня ризик-апетиту;

17) надавачі фінансових платіжних послуг – платіжні установи (крім малих платіжних установ), установи електронних грошей, оператори поштового зв'язку, які мають право надавати фінансові платіжні послуги, філії іноземних платіжних установ;

18) надзвичайний (чорний) рівень критичності – один із критеріїв істотності операційних інцидентів, кіберінцидентів та інцидентів безпеки, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача фінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання платіжних послуг, безпеці (захищеності) критичних даних, внаслідок чого відбувається невідворотний вплив на повноцінне функціонування держави;

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

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

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

22) орган управління надавача фінансових платіжних послуг – загальні збори учасників (акціонерів) надавача фінансових платіжних послуг (далі – загальні збори), наглядова рада надавача фінансових платіжних послуг (далі – рада) (у разі її створення), одноосібний / колегіальний виконавчий орган надавача фінансових платіжних послуг (далі – виконавчий орган);

23) передавання ризику – використання надавачем фінансових платіжних послуг ресурсів інших осіб для покриття ризику за винагороду зі збереженням наявного рівня ризику;

24) підрозділ внутрішнього аудиту – постійно діючий підрозділ, створений радою (якщо її немає – загальними зборами) (далі – відповідальний орган), який забезпечує виконання функцій внутрішнього аудиту, визначених законодавством України, або внутрішній аудитор / головний внутрішній аудитор;

25) підрозділ з управління ризиками – постійно діючий підрозділ, створений відповідальним органом, який забезпечує виконання функцій з управління ризиками, визначених законодавством України, або головний ризик-менеджер;

26) підрозділ контролю за дотриманням норм (комплаєнс) – постійно діючий підрозділ, створений відповідальним органом, який забезпечує виконання функцій контролю за дотриманням норм (комплаєнс), визначених законодавством України, або головний комплаєнс-менеджер [особа, на яку покладена функція контролю за дотриманням норм (комплаєнс)] (далі – головний комплаєнс-менеджер);

27) підрозділи контролю – підрозділ з управління ризиками, підрозділ контролю за дотриманням норм (комплаєнс), підрозділ внутрішнього аудиту;

28) пом’якшення або зниження ризиків – комплекс заходів, спрямованих на зменшення ймовірності прояву ризику та/або зменшення впливу ризику на результати діяльності надавача фінансових платіжних послуг;

29) посадові особи надавача фінансових платіжних послуг – одноосібний виконавчий орган або члени колегіального виконавчого органу та члени ради (далі – керівники), ключові особи надавача фінансових платіжних послуг (далі – ключова особа);

30) прийняття ризиків – утримання ризиків на рівні, що перебуває в межах визначеного надавачем фінансових платіжних послуг ризик-апетиту або визначеної схильності до ризиків та не створює загрози для користувачів, акціонерів / учасників надавача фінансових платіжних послуг та його фінансового стану;

31) ризик-апетит, або схильність до ризику, – сукупна величина за всіма видами ризиків та окремо за кожним із ризиків, визначена наперед та в межах допустимого рівня ризику, щодо яких надавач фінансових платіжних послуг прийняв рішення про доцільність / необхідність їх утримання з метою досягнення його стратегічних цілей та виконання плану діяльності;

32) ризик безпеки – ризик виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок виникнення під час надання платіжних послуг / виконання платіжних операцій 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 платіжних послуг;

33) ризик контрагента – імовірність невиконання контрагентом договірних зобов’язань;

34) ризик ліквідності – ризик виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок неспроможності надавача фінансових платіжних послуг забезпечувати фінансування зростання активів та/або виконання своїх зобов’язань у належні строки;

35) ринковий ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок несприятливого впливу факторів ринкового ризику, включаючи курси іноземних валют, процентні ставки та/або інші фактори, на вартість / ціну фінансових інструментів;

36) середній (жовтий) рівень критичності – один із критеріїв істотності операційних інцидентів, кіберінцидентів та інцидентів безпеки, який встановлюється до події, що безпосередньо загрожує здійсненню операційної діяльності надавача фінансових платіжних послуг, сталому функціонуванню інформаційної інфраструктури, що використовується для надання платіжних

послуг, внаслідок чого створюються передумови для порушення конфіденційності, цілісності та доступності критичних даних, виникають передумови для порушення безперервності надання платіжних послуг;

37) система внутрішнього контролю – сукупність заходів з внутрішнього аудиту, управління ризиками, комплаєнсу та інших елементів, визначених законодавством України, включаючи це Положення, а також політики, правил і заходів, які забезпечують функціонування, взаємозв'язок та підтримку таких заходів та елементів і спрямовані на досягнення визначених мети, цілей і вимог до діяльності надавача фінансових платіжних послуг та забезпечення безперервності надання платіжних послуг;

38) система стримувань та противаг – розподіл повноважень між органами управління та/або підрозділами надавача фінансових платіжних послуг, який забезпечує взаємну підконтрольність, а також унеможливлює (упереджує) можливість прийняття органами управління надавача фінансових платіжних послуг рішень, що можуть призвести до негативних наслідків у діяльності надавача фінансових платіжних послуг;

39) система управління ризиками – сукупність належним чином задокументованих, затверджених і виданих політики, методик і процедур управління ризиками, розпоряджень, рішень, наказів або документів, розроблених в іншій формі, з урахуванням вимог законодавства України, 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 фінансових платіжних послуг;

40) стрес-тестування – метод вимірювання (оцінки) потенційного впливу ризику як величини збитків, що можуть стати наслідком шокових змін різних факторів ризику, які відповідають виключним (екстремальним), але ймовірним подіям;

41) уникнення ризику – відмова від здійснення певних операцій або припинення ділових відносин, які наражають надавача фінансових платіжних послуг на ризик.

Термін "ключові особи" уживається в цьому Положенні в значенні, наведеному в Положенні про авторизацію надавачів фінансових послуг та умови здійснення ними діяльності з надання фінансових послуг, затвердженому постановою Правління Національного банку України від 29 грудня 2023 року № 199 (зі змінами).

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

Термін “уповноважена посадова особа Національного банку” уживається в цьому Положенні в значенні, наведеному в Положенні про здійснення Національним банком України безвиїзного нагляду на платіжному ринку за небанківськими надавачами платіжних послуг, надавачами обмежених платіжних послуг, затвердженому постановою Правління Національного банку України від 05 травня 2023 року № 60 (зі змінами) (далі – Положення про здійснення безвиїзного нагляду на платіжному ринку).

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

3. Це Положення визначає:

1) вимоги до системи управління надавача фінансових платіжних послуг:

системи корпоративного управління відповідно до вимог, встановлених Законом про платіжні послуги та цим Положенням, включаючи вимоги щодо ключових осіб;

системи внутрішнього контролю, що включає систему управління ризиками, контроль за дотриманням норм (комплаєнс) та внутрішній аудит, згідно з вимогами, встановленими Законом про фінансові послуги, Законом про платіжні послуги та цим Положенням;

2) порядок здійснення контролю Національним банком за дотриманням надавачем фінансових платіжних послуг вимог до системи управління, включаючи порядок складання та подання звітів та іншої інформації до Національного банку щодо системи управління надавача фінансових платіжних послуг.

2. Організація системи управління надавача фінансових платіжних послуг

4. Система управління надавача фінансових платіжних послуг повинна відповідати вимогам, визначеним Законом про платіжні послуги, іншими законами України, цим Положенням та іншими нормативно-правовими актами Національного банку.

5. Надавач фінансових платіжних послуг зобов’язаний організувати та постійно забезпечувати ефективність своєї системи управління, належне

функціонування системи корпоративного управління, системи внутрішнього контролю та належне управління ризиками з урахуванням особливостей виду діяльності, бізнес-моделі, характеру і видів послуг, які він надає, ризиків, притаманних такій діяльності, а також особливостей, встановлених законами з питань регулювання окремих ринків фінансових послуг, Законом України "Про товариства з обмеженою та додатковою відповідальністю" (далі – Закон про товариства з обмеженою та додатковою відповідальністю), Законом України "Про акціонерні товариства" (далі – Закон про акціонерні товариства), Положенням про порядок здійснення авторизації діяльності надавачів фінансових платіжних послуг та обмежених платіжних послуг, затвердженим постановою Правління Національного банку України від 07 жовтня 2022 року № 217 (зі змінами) (далі – Положення про авторизацію надавачів фінансових платіжних послуг), та цим Положенням.

6. Внутрішні документи надавача фінансових платіжних послуг щодо організації системи управління повинні відповідати вимогам законодавства України, включаючи вимоги цього Положення.

7. Порядок організації роботи виконавчого органу, включаючи чіткий розподіл повноважень між головою і членами колегіального виконавчого органу, а також порядок організації роботи ради та комітетів ради, ключових осіб (або осіб, які виконують такі функції) повинні визначатись у внутрішніх документах, що регламентують діяльність виконавчого органу, ради, комітетів ради та ключових осіб. Надавач фінансових платіжних послуг для забезпечення ефективності своєї системи управління переглядає внутрішні документи щодо потреби внесення змін до них не рідше одного разу на рік.

8. Надавач фінансових платіжних послуг (крім філії іноземної платіжної установи) зобов'язаний створити у своїй структурі окремі підрозділи внутрішнього аудиту, з управління ризиками та контролю за дотриманням норм (комплаєнс) або покласти виконання відповідних функцій на внутрішнього аудитора / головного внутрішнього аудитора, головного ризик-менеджера, головного комплаєнс-менеджера та забезпечити їх належними ресурсами для ефективного та належного виконання їхніх функцій.

9. Внутрішній аудитор / головний внутрішній аудитор, головний ризик-менеджер не мають права обіймати будь-які інші посади та виконувати будь-які інші обов'язки в цьому надавачі фінансових платіжних послуг та/або інших юридичних особах.

10. Вимоги, визначені в пункті 9 глави 2 розділу I цього Положення, не застосовуються до материнських та дочірніх компаній надавача фінансових

платіжних послуг, компаній – учасників фінансової групи, до якої належить такий надавач фінансових платіжних послуг, професійних об'єднань на ринку фінансових платіжних послуг, юридичних осіб, кінцевим бенефіціарним власником в яких є кінцевий бенефіціарний власник такого надавача фінансових платіжних послуг.

ІІ. Система корпоративного управління надавача фінансових платіжних послуг

3. Загальні збори надавача фінансових платіжних послуг

11. Загальні збори є вищим органом управління надавача фінансових платіжних послуг.

12. До виключної компетенції загальних зборів належить вирішення питань, віднесених Законом про товариства з обмеженою та додатковою відповідальністю або Законом про акціонерні товариства до виключної компетенції загальних зборів такого товариства.

13. До компетенції загальних зборів надавача фінансових платіжних послуг з урахуванням вимог законів України можуть бути віднесені інші питання діяльності, за винятком тих, які законом України або статутом надавача фінансових платіжних послуг віднесені до виключної компетенції ради, інших органів надавача фінансових платіжних послуг.

Загальні збори з урахуванням вимог законів України уповноважені розглядати і приймати рішення з питань, віднесених законом України або статутом надавача фінансових платіжних послуг до виключної компетенції ради, якщо радою прийнято рішення про внесення відповідного питання на розгляд загальних зборів.

14. Загальні збори з урахуванням вимог законів України, включаючи вимоги Закону про товариства з обмеженою та додатковою відповідальністю та Закону про акціонерні товариства:

1) визначають основні напрями діяльності надавача фінансових платіжних послуг;

2) затверджують / приймають рішення про застосування принципів (кодексу) корпоративного управління надавача фінансових платіжних послуг;

3) вирішують питання про обрання та припинення повноважень членів ради;

4) за відсутності ради вирішують питання про призначення та припинення повноважень (звільнення) голови та членів колегіального виконавчого органу, а також ключових осіб;

5) вирішують інші питання, віднесені до компетенції загальних зборів, відповідно до вимог законодавства України.

4. Рада надавача фінансових платіжних послуг

15. Рада несе відповідальність за забезпечення стратегічного управління надавача фінансових платіжних послуг.

16. Рада в межах своїх повноважень з урахуванням компетенції, визначеної відповідно законом України та статутом, несе відповідальність за:

1) безпеку та фінансову стійкість надавача фінансових платіжних послуг;

2) відповідність діяльності надавача фінансових платіжних послуг законодавству України;

3) упровадження стратегічних цілей надавача фінансових платіжних послуг відповідно до основних напрямів діяльності, визначених загальними зборами, та плану діяльності надавача фінансових платіжних послуг;

4) забезпечення ефективної організації корпоративного управління;

5) функціонування та контроль за ефективністю системи внутрішнього контролю, системи управління ризиками та контролю за дотриманням норм (комплаєнс), системи внутрішнього аудиту надавача фінансових платіжних послуг;

6) призначення голови та членів колегіального виконавчого органу, а також ключових осіб.

17. Рада затверджує організаційну структуру надавача фінансових платіжних послуг, що відповідає його потребам, розміру, особливостям діяльності надавача фінансових платіжних послуг, характеру й обсягам фінансових платіжних та інших послуг, профілю ризику надавача фінансових платіжних послуг, надає змогу раді та виконавчому органу виконувати свої обов’язки належним чином відповідно до вимог законодавства України та сприяє ефективному прийняттю рішень кожним з органів управління і належному управлінню надавачем фінансових платіжних послуг у цілому. Організаційна

структура містить у собі визначення персонального розподілу функцій, обов'язків, відповідальності, повноважень членів ради, виконавчого органу, ключових осіб, їх підконтрольності та підзвітності, а також забезпечує наявність системи стримування і противаг.

18. Рада має право внести на розгляд загальних зборів питання, яке законом України або статутом надавача фінансових платіжних послуг віднесене до її виключної компетенції.

19. Рада має право утворювати постійні чи тимчасові комітети з числа осіб, які входять до її складу, для попереднього вивчення і підготовки до розгляду на засіданні питань, що належать до компетенції ради.

20. Рада має право утворити постійно діючі комітети (далі – комітети ради):

1) комітет з питань аудиту (аудиторський комітет) з урахуванням вимог до аудиторського комітету, передбачених Законом України "Про аудит фінансової звітності та аудиторську діяльність";

2) комітет з управління ризиками;

3) комітет з питань винагороди та призначень.

21. Рада в межах компетенції визначає обсяг повноважень комітетів ради, контролює та регулює їхню діяльність.

22. Загальні збори або орган, визначений статутом надавача фінансових платіжних послуг, здійснюють повноваження ради, якщо її не створено.

5. Виконавчий орган надавача фінансових платіжних послуг

23. До компетенції виконавчого органу належить вирішення всіх питань, пов'язаних з керівництвом поточною діяльністю надавача фінансових платіжних послуг, крім питань, що належать до виключної компетенції загальних зборів та ради.

Виконавчі або невиконавчі члени (директори) можуть обиратися до складу колегіального виконавчого органу. Невиконавчий член здійснює функції нагляду, управління ризиками та контролю за діяльністю товариства та виконавчих членів колегіального виконавчого органу.

24. Виконавчий орган у межах своїх повноважень відповідає за:

1) безпеку та фінансову стійкість надавача фінансових платіжних послуг;

2) безперервність надання платіжних послуг;

3) відповідність діяльності надавача фінансових платіжних послуг законодавству України;

4) забезпечення поточного управління надавачем фінансових платіжних послуг;

5) виконання рішень загальних зборів та ради;

6) щоденне управління та контроль за операціями надавача фінансових платіжних послуг;

7) реалізацію стратегії надавача фінансових платіжних послуг, плану діяльності надавача фінансових платіжних послуг;

8) відповідність діяльності надавача фінансових платіжних послуг декларації схильності до ризиків.

ІІІ. Система внутрішнього контролю

6. Загальні засади побудови системи внутрішнього контролю

25. Надавач фінансових платіжних послуг зобов’язаний створити комплексну, адекватну та ефективну систему внутрішнього контролю, що включає систему управління ризиками, контроль за дотриманням норм (комплаєнс) та внутрішній аудит, відповідно до вимог Закону про платіжні послуги, Положення про авторизацію надавачів фінансових платіжних послуг та цього Положення.

26. Система внутрішнього контролю повинна забезпечувати:

1) виконання функцій управління ризиками, контролю за дотриманням норм (комплаєнс) та внутрішнього аудиту з урахуванням розміру надавача фінансових платіжних послуг, складності, обсягів, видів, характеру здійснюваних надавачем фінансових платіжних послуг операцій, організаційної структури та профілю ризику надавача фінансових платіжних послуг;

2) досягнення надавачем фінансових платіжних послуг операційних, інформаційних цілей та комплаєнс-цілей, стратегічних цілей, визначених у його внутрішніх документах та плані діяльності.

27. Операційні цілі діяльності надавача фінансових платіжних послуг передбачають:

1) забезпечення спрямованості процедур контролю на ефективність управління активами, зобов'язаннями та позабалансовими позиціями надавача фінансових платіжних послуг з метою досягнення показників плану діяльності з одночасним уникненням або обмеженням втрат внаслідок впливу негативних внутрішніх та зовнішніх факторів;

2) здійснення систематичного процесу виявлення, вимірювання (оцінювання), моніторингу, контролю, звітування та мінімізації (зниження до контрольованого рівня) усіх видів ризиків у діяльності надавача фінансових платіжних послуг на всіх організаційних рівнях.

28. Інформаційні цілі діяльності надавача фінансових платіжних послуг можуть передбачати:

1) забезпечення цілісності, повноти та достовірності фінансової, управлінської та іншої інформації, що використовується для прийняття управлінських рішень;

2) забезпечення обміну інформацією як за вертикаллю, так і за горизонталлю організаційної структури надавача фінансових платіжних послуг.

29. Інформація, визначена в підпункті 1 пункту 28 глави 6 розділу III цього Положення, охоплює звітність надавача фінансових платіжних послуг з фінансових та нефінансових питань, що подається зовнішнім та внутрішнім користувачам.

30. Комплаєнс-цілі діяльності надавача фінансових платіжних послуг повинні передбачати забезпечення організації діяльності надавача фінансових платіжних послуг та виконання надавачем фінансових платіжних послуг вимог:

1) законодавства України про діяльність та регулювання діяльності на ринку фінансових послуг, включаючи законодавство України, що регулює діяльність на платіжному ринку;

2) ринкових стандартів;

3) правил добросовісної конкуренції та корпоративної етики;

4) правил платіжних систем;

5) щодо врегулювання конфлікту інтересів;

6) внутрішніх документів надавача фінансових платіжних послуг або відповідності діяльності надавача фінансових платіжних послуг таким вимогам.

31. Надавач фінансових платіжних послуг має право у своїх внутрішніх документах визначати додаткові цілі системи внутрішнього контролю.

32. Система внутрішнього контролю надавача фінансових платіжних послуг повинна містити такі компоненти:

1) контрольне середовище, вимоги до якого встановлені в пункті 37 глави 6 розділу III цього Положення;

2) система управління ризиками, вимоги до якої встановлені в пункті 39 глави 6 розділу III та в розділі VI цього Положення;

3) контрольна діяльність, вимоги до якої встановлені в главі 12 розділу III цього Положення;

4) контроль за інформаційними потоками та комунікаціями, вимоги до якого встановлені в главі 13 розділу III цього Положення;

5) моніторинг ефективності системи внутрішнього контролю, вимоги до якого встановлені в главі 14 розділу III цього Положення.

33. Надавач фінансових платіжних послуг визначає у своїх внутрішніх документах опис кожного з компонентів системи внутрішнього контролю, визначених у пункті 32 глави 6 розділу III цього Положення.

34. Надавач фінансових платіжних послуг запроваджує систему внутрішнього контролю шляхом:

1) прийняття внутрішніх документів із дотриманням вимог пунктів 53–57, 59 глави 10 розділу III цього Положення;

2) побудови організаційної структури надавача фінансових платіжних послуг з урахуванням вимог розділу ІІІ цього Положення;

3) впровадження компонентів системи внутрішнього контролю, визначених у пункті 32 глави 6 розділу ІІІ цього Положення.

35. Надавач фінансових платіжних послуг зобов'язаний після запровадження системи внутрішнього контролю забезпечувати її постійне та ефективне функціонування.

36. Суб'єктами внутрішнього контролю надавача фінансових платіжних послуг є:

1) відповідальний орган;

2) комітети ради;

3) виконавчий орган / невиконавчий член колегіального виконавчого органу;

4) підрозділи, безпосередньо залучені до процесу надання платіжних послуг (бізнес-підрозділи), та підрозділи підтримки діяльності надавача фінансових платіжних послуг;

5) підрозділ з управління ризиками;

6) підрозділ контролю за дотриманням норм (комплаєнс);

7) підрозділ внутрішнього аудиту.

37. Заходами, дотримання яких свідчить про належне впровадження та функціонування контрольного середовища як компонента системи внутрішнього контролю надавача фінансових платіжних послуг, є такі:

1) надавачем фінансових платіжних послуг затверджено, доведено до відома всіх працівників відповідно до пункту 58 глави 10 розділу ІІІ цього Положення та контролюється дотримання і належне виконання внутрішніх документів, що визначають стандарти етичної поведінки працівників, порядок здійснення внутрішніх та зовнішніх комунікацій;

2) надавачем фінансових платіжних послуг визначено порядок дій та повноваження осіб, відповідальних за здійснення контролю за діяльністю

структурних підрозділів / осіб, на яких покладено виконання окремих функцій у системі трьох ліній захисту, щодо належного функціонування системи внутрішнього контролю надавача фінансових платіжних послуг;

3) створено організаційну структуру надавача фінансових платіжних послуг, яка забезпечує побудову системи внутрішнього контролю, у межах якої визначено та розподілено функції, обов'язки, повноваження, відповідальність, визначено підзвітність та підконтрольність суб'єктів внутрішнього контролю, а також забезпечує належний рівень системи стримування і противаг;

4) надавач фінансових платіжних послуг з урахуванням цілей його діяльності забезпечує створення умов, потрібних для залучення компетентних осіб, які володіють необхідним досвідом, професійними навичками та якостями для виконання функцій та обов'язків, забезпечує їх належними ресурсами для ефективного та належного виконання їх функцій та забезпечує навчання таких працівників шляхом опису відповідних процесів у внутрішніх документах та виділення необхідних коштів (за потреби);

5) рада (якщо її не створено – орган, визначений статутом надавача фінансових платіжних послуг) забезпечує функціонування та контроль за ефективністю комплексної та адекватної системи внутрішнього контролю;

6) виконавчий орган у межах своїх повноважень забезпечує виконання рішень ради (якщо її не створено – органу, визначеного статутом надавача фінансових платіжних послуг) щодо забезпечення організації та функціонування системи внутрішнього контролю надавача фінансових платіжних послуг;

7) суб'єкти внутрішнього контролю надавача фінансових платіжних послуг несуть відповідальність за неналежне виконання та/або невиконання ними своїх обов'язків.

38. Надавач фінансових платіжних послуг створює комплексну та адекватну систему управління ризиками як компонент системи внутрішнього контролю, що відповідає вимогам, визначеним у розділі VI цього Положення.

39. Заходами з управління ризиками, дотримання яких свідчить про впровадження та ефективність, комплексність та адекватність функціонування системи управління ризиками як компонента системи внутрішнього контролю надавача фінансових платіжних послуг, є:

1) відповідність затверджених радою стратегії управління ризиками та декларації схильності до ризиків надавача фінансових платіжних послуг його загальним стратегічним цілям розвитку;

2) відповідність профілю ризику надавача фінансових платіжних послуг затвердженому радою рівню ризик-апетиту;

3) повнота та ефективність впровадження внутрішніх документів з питань управління ризиками;

4) створення та дотримання культури управління ризиками, включаючи забезпечення обізнаності та залучення членів ради та членів колегіального виконавчого органу, а також інших працівників надавача фінансових платіжних послуг до управління ризиками, шляхом проведення періодичних засідань ради, комітетів ради за участю головного ризик-менеджера / працівників підрозділу з управління ризиками, документування таких засідань, навчання працівників надавача фінансових платіжних послуг з питань управління ризиками;

5) відповідність внутрішніх документів щодо управління ризиками вимогам цього Положення;

6) наявність у головного ризик-менеджера та головного комплаєнс-менеджера належного статусу та відповідної кваліфікації для виконання покладених на них функцій з управління ризиками, контролю за дотриманням норм (комплаєнс).

7. Три лінії захисту

40. Надавач фінансових платіжних послуг створює та впроваджує систему внутрішнього контролю, що ґрунтується на розподілі обов’язків між відповідальними за певний процес у межах системи внутрішнього контролю особами та/або структурними підрозділами надавача фінансових платіжних послуг з урахуванням вимог цього Положення.

41. Надавач фінансових платіжних послуг зобов’язаний забезпечити розподіл обов’язків між структурними підрозділами надавача фінансових платіжних послуг, що ґрунтується на системі трьох ліній захисту, яка передбачає, що:

1) до першої лінії захисту належать підрозділи, безпосередньо залучені до процесу надання платіжних послуг (бізнес-підрозділи), підрозділи підтримки діяльності надавача фінансових платіжних послуг, а також працівники цих

підрозділів (далі – суб'єкти першої лінії), які ініціюють, здійснюють або відображають господарські операції, приймають ризики в процесі своєї діяльності та відповідають за поточне управління цими ризиками, здійснюють заходи з контролю в межах своєї компетенції;

2) до другої лінії захисту належать структурні підрозділи / особи, на яких покладено виконання функцій з управління ризиками, контролю за дотриманням норм (комплаєнс) (далі – суб'єкти другої лінії), які забезпечують ефективність впроваджених першою лінією захисту заходів із контролю та управління ризиками, їх відповідність вимогам законодавства України та внутрішнім документам надавача фінансових платіжних послуг;

3) до третьої лінії захисту належить структурний підрозділ / окрема посадова особа, визначений / визначена відповідальним органом для проведення внутрішнього аудиту, що здійснює оцінювання ефективності діяльності першої та другої ліній захисту, загальне оцінювання ефективності системи внутрішнього контролю в межах виконання функції внутрішнього аудиту надавача фінансових платіжних послуг (далі – суб'єкти третьої лінії).

42. Відокремлені підрозділи надавача фінансових платіжних послуг залежно від їх розміру, функцій та повноважень, якими вони наділені відповідно до внутрішніх документів надавача фінансових платіжних послуг, можуть бути віднесені надавачем фінансових платіжних послуг до першої лінії захисту та/або мати у своїй структурі розподіл функцій за трьома лініями захисту.

43. Надавач фінансових платіжних послуг зобов'язаний забезпечити розподіл функцій у межах системи трьох ліній захисту з дотриманням обмежень щодо конфлікту інтересів на рівні керівників, підрозділів, працівників першої, другої і третьої ліній захисту, а також незалежність другої та третьої ліній захисту.

8. Відповідальність та функції органів управління надавача фінансових платіжних послуг щодо функціонування системи внутрішнього контролю

44. Рада як суб'єкт внутрішнього контролю відповідно до виключної компетенції:

1) затверджує та контролює реалізацію стратегічних цілей та плану діяльності надавача фінансових платіжних послуг;

2) затверджує організаційну структуру надавача фінансових платіжних послуг, а також структури підрозділів з управління ризиками, контролю за дотриманням норм (комплаєнс), внутрішнього аудиту;

3) затверджує внутрішні документи, віднесені до компетенції ради, включаючи документи, згідно з якими відбувається делегування повноважень ради в процесі здійснення внутрішнього контролю (крім повноважень, що належать до виключної компетенції ради), які передбачають право головного ризик-менеджера та головного комплаєнс-менеджера накладати заборону (вето) на рішення виконавчого органу та встановлення підстав (випадків) такої заборони, а також здійснює контроль за їх упровадженням, дотриманням та своєчасним оновленням (актуалізацією);

4) приймає рішення про обрання та припинення повноважень осіб, які входять до складу виконавчого органу, призначення та припинення повноважень (звільнення) ключових осіб;

5) забезпечує функціонування та контроль за ефективністю комплексної та адекватної системи внутрішнього контролю надавача фінансових платіжних послуг, включаючи розгляд звітів про результати здійснення моніторингу ефективності організації системи внутрішнього контролю, проведеного в межах діяльності другої та третьої ліній захисту, та прийняття за результатами розгляду рішення про здійснення / нездійснення відповідних заходів; розгляд звітів про результати виконання заходів, спрямованих на підвищення ефективності системи внутрішнього контролю, звітів про проведення щорічної самооцінки ефективності діяльності та прийняття рішення про досягнення або недосягнення поставлених у рішенні завдань, а також рішення щодо додаткових заходів у таких випадках.

45. Виконавчий орган як суб’єкт внутрішнього контролю в межах вирішення питань, пов’язаних з управлінням поточною діяльністю надавача фінансових платіжних послуг, крім питань, що належать до виключної компетенції загальних зборів та ради:

1) забезпечує діяльність надавача фінансових платіжних послуг, спрямовану на належне функціонування системи управління надавача фінансових платіжних послуг, безперервність надання платіжних послуг;

2) забезпечує функціонування інформаційних систем, що сприяють функціонуванню системи управління надавача фінансових платіжних послуг та здійснення внутрішнього контролю;

3) забезпечує суб’єктів першої – третьої ліній захисту ресурсами, потрібними для належного виконання повноважень;

4) здійснює поточне управління підпорядкованими суб’єктами системи внутрішнього контролю надавача фінансових платіжних послуг;

5) забезпечує впровадження стратегії та політики управління ризиками (включаючи ліміти ризиків), декларації схильності до ризиків, культури управління ризиками, включаючи дотримання надавачем фінансових платіжних послуг установленого рівня ризик-апетиту та лімітів ризиків;

6) ураховує в процесі прийняття рішень інформацію, отриману в межах системи управління ризиками;

7) забезпечує підготовку та надання раді, комітетам ради пропозицій щодо необхідності внесення змін до внутрішніх документів, затверджених радою;

8) розглядає та оцінює результати здійснення внутрішнього контролю, інформацію про виявлені в системі внутрішнього контролю порушення / недоліки, розробляє заходи щодо оперативного усунення недоліків, урахування рекомендацій та зауважень, наданих підрозділом внутрішнього аудиту, суб’єктами аудиторської діяльності, Національним банком та іншими контролюючими органами щодо функціонування системи управління ризиками;

9) приймає рішення про здійснення заходів щодо усунення / мінімізації порушень / недоліків, виявлених у системі внутрішнього контролю суб’єктами всіх ліній захисту, суб’єктами аудиторської діяльності та/або Національним банком;

10) здійснює поточний контроль за виконанням рішень про застосування заходів щодо усунення / мінімізації порушень / недоліків, виявлених у системі внутрішнього контролю уповноваженими суб’єктами першої – третьої ліній внутрішнього контролю, зовнішніми аудиторами та/або Національним банком.

46. Суб’єкти трьох ліній захисту надавача фінансових платіжних послуг зобов’язані:

1) дотримуватися вимог законодавства України, внутрішніх документів надавача фінансових платіжних послуг, у межах повноважень виконувати рішення про застосування заходів щодо усунення / мінімізації порушень / недоліків, виявлених у системі внутрішнього контролю

уповноваженими суб’єктами першої – третьої ліній захисту, суб’єктами аудиторської діяльності та/або Національним банком;

2) діяти в межах своїх повноважень, виконувати покладені на них виконавчим органом, радою обов’язки щодо внутрішнього контролю;

3) проходити навчання, призначене / організоване надавачем фінансових платіжних послуг із метою підвищення рівня кваліфікації у сфері внутрішнього контролю, порядок, умови та періодичність проведення якого визначає надавач фінансових платіжних послуг у своїх внутрішніх документах.

47. Головний комплаєнс-менеджер та головний ризик-менеджер у межах забезпечення виконання своїх функцій зобов’язані бути присутніми на засіданнях виконавчого органу, мають право дорадчого голосу, а також можуть накладати заборону (вето) на рішення виконавчого органу з питань, що стосуються / впливають на:

1) бізнес-модель надавача фінансових платіжних послуг;

2) систему внутрішнього контролю, систему управління ризиками;

3) тарифну політику надавача фінансових платіжних послуг;

4) встановлений ризик-апетит та/або затверджені ліміти ризику;

5) дотримання вимог законодавства України;

6) інші випадки, встановлені у внутрішніх документах надавача фінансових платіжних послуг.

48. Головний комплаєнс-менеджер та головний ризик-менеджер у разі використання дорадчого голосу або накладення заборони (вето) на рішення виконавчого органу невідкладно інформують комітет з управління ризиками (у разі створення) або відповідальний орган про такі рішення.

49. Головний ризик-менеджер у межах забезпечення виконання функції управління ризиками:

1) має право бути присутнім на засіданнях комітетів ради та надавати обов’язкові до розгляду пропозиції та/або зауваження до рішень цих органів, якщо реалізація таких рішень призведе / може призвести до порушення встановленого ризик-апетиту та/або затверджених лімітів ризику;

2) має право накладати заборону (вето) на рішення цих органів з підстав (у випадках), установлених цим Положенням, відповідальним органом, якщо таке право встановлено у внутрішніх документах;

3) невідкладно інформує комітет з управління ризиками або відповідальний орган про такі пропозиції та/або зауваження, заборону (вето) на рішення.

9. Функції та повноваження ліній захисту

50. Суб'єкти першої лінії захисту в межах компетенції:

1) здійснюють виконання покладених на них обов'язків та повноважень відповідно до внутрішніх документів надавача фінансових платіжних послуг, забезпечують дотримання вимог, визначених внутрішніми документами, законодавством України;

2) регулярно здійснюють заходи з контролю, обов'язок із виконання яких визначено у внутрішніх документах надавача фінансових платіжних послуг, та відповідають за їх належне і своєчасне виконання;

3) здійснюють заходи з виявлення та інформування про ризики, пов'язані з діяльністю суб'єктів першої лінії захисту, відповідно до вимог цього Положення;

4) мають право ініціювати / брати участь у періодичному перегляді / розробленні процесу внутрішнього контролю.

51. Суб'єкти другої лінії захисту в межах повноважень під час виконання функцій із контролю за дотриманням норм (комплаєнс) та функції з управління ризиками надавача фінансових платіжних послуг:

1) надають пропозиції щодо вибору та визначення виконавчим органом видів контрольної діяльності;

2) консультують виконавчий орган з питань розроблення / перегляду внутрішніх документів, які визначають процес здійснення кожного з видів діяльності в межах системи управління, та окремих процедур внутрішнього контролю;

3) забезпечують організацію, здійснюють контроль та моніторинг впровадження внутрішніх документів, включаючи документи з питань культури

управління ризиками, та виконання суб'єктами першої лінії захисту покладених на них функцій, включаючи виконання заходів із контролю;

4) здійснюють контроль за виявленням та своєчасним інформуванням про виявлені ризики, пов'язані з їх діяльністю;

5) контролюють дотримання лімітів ризиків та встановленого ризик-апетиту;

6) ураховують під час прийняття рішень інформацію, отриману в межах системи управління ризиками;

7) забезпечують складання та своєчасне подання звітності, підготовка якої належить до компетенції відповідного підрозділу;

8) здійснюють контроль за дотриманням вимог законодавства України про захист прав споживачів фінансових послуг, внутрішніх документів та процесів;

9) здійснюють контрольну діяльність за інформаційними системами і технологіями, надають рекомендації щодо їх вдосконалення, усунення виявлених недоліків у їх роботі виконавчому органу;

10) перевіряють відповідність внутрішніх документів надавача фінансових платіжних послуг законодавству України;

11) перевіряють відповідність здійснюваних суб'єктами першої лінії захисту заходів із контролю внутрішнім документам надавача фінансових платіжних послуг;

12) здійснюють контрольну діяльність з недопущення конфлікту інтересів;

13) відповідають за належне та своєчасне інформування суб'єктів внутрішнього контролю щодо внутрішніх документів та внесених до них змін, які визначають процедури здійснення кожного з видів контрольної діяльності та окремих процедур внутрішнього контролю;

14) складають звіти в межах компетенції щодо реалізації контрольної діяльності / моніторингу, які повинні подаватися для оцінки та розгляду відповідальному органу, виконавчому органу / органу, визначеному статутом / комітетам ради / іншим користувачам, які приймають рішення відповідно до внутрішніх документів з питань системи управління ризиками.

52. Суб’єкти третьої лінії захисту:

1) здійснюють оцінювання ефективності діяльності першої та другої ліній захисту, загальне оцінювання ефективності системи внутрішнього контролю, оцінювання обраних та визначених у внутрішніх документах надавача фінансових платіжних послуг заходів із контролю, а саме: здійснення перевірки щодо того, чи належним чином вони регламентовані, виконуються уповноваженими суб’єктами внутрішнього контролю, відповідають цілям надавача фінансових платіжних послуг, є ефективними та достатніми для їх реалізації, шляхом проведення внутрішнього аудиту, складення звітів та подання їх на розгляд ради та для ознайомлення виконавчому органу;

2) надають пропозиції з питань розроблення / перегляду процесу здійснення заходів із контролю та/або окремих процедур внутрішнього контролю.

10. Внутрішні документи з питань системи внутрішнього контролю

53. Надавач фінансових платіжних послуг зобов’язаний визначити у внутрішніх документах письмовий опис процесів, які забезпечують організацію та функціонування системи внутрішнього контролю, включаючи завдання, порядок та етапи здійснення заходів із контролю, відповідальних осіб, а також способи досягнення результатів щодо кожного процесу.

54. Положення про систему внутрішнього контролю надавача фінансових платіжних послуг повинно містити:

1) мету, завдання та принципи побудови системи внутрішнього контролю надавача фінансових платіжних послуг;

2) організаційну структуру системи внутрішнього контролю з урахуванням розподілу функціональних обов’язків між учасниками процесу, їх повноваження, відповідальність та порядок взаємодії;

3) принципи та підходи щодо впровадження компонентів системи внутрішнього контролю у надавачі фінансових платіжних послуг;

4) порядок, види, періодичність підготовки та розгляду звітів;

5) процедуру здійснення відповідних коригувальних заходів щодо виправлення виявлених недоліків.

55. Відповідальний орган або орган, визначений статутом надавача фінансових платіжних послуг, затверджує та регулярно (не рідше одного разу на рік) переглядає положення про систему внутрішнього контролю надавача фінансових платіжних послуг.

56. Відповідальний орган затверджує та регулярно (не рідше одного разу на рік) переглядає внутрішні документи, які передбачають право головного ризик-менеджера та головного комплаєнс-менеджера накладати заборону (вето) на рішення виконавчого органу та встановлення підстав (випадків) такої заборони.

57. Перелік питань щодо внутрішнього контролю, які повинні врегульовуватися у внутрішніх документах надавача фінансових платіжних послуг, зазначено в додатку 1 до цього Положення.

Надавач фінансових платіжних послуг має право об'єднувати окремі внутрішні документи щодо побудови та організації системи внутрішнього контролю в один або кілька документів, не порушуючи вимог цього Положення щодо їх розроблення, наповнення, затвердження, перегляду та інших вимог.

58. Надавач фінансових платіжних послуг зобов'язаний:

1) доводити до відома працівників зміст внутрішніх документів;

2) письмово фіксувати кожен факт ознайомлення працівника з такими документами у спосіб, що дає змогу підтвердити факт такого ознайомлення, включаючи ознайомлення під власноручний підпис або шляхом накладання кваліфікованого електронного підпису (далі – КЕП) працівника та особи, яка забезпечила проведення ознайомлення.

59. Надавач фінансових платіжних послуг визначає у внутрішніх документах процедури та заходи з контролю, які застосовуються підрозділами кожної з трьох ліній захисту, а також порядок та процедури:

1) вертикальної взаємодії, що застосовуються під час здійснення внутрішнього контролю між структурними підрозділами / окремими посадовими особами / суб'єктами різних ліній захисту, органами управління надавача фінансових платіжних послуг;

2) горизонтальної взаємодії, що застосовуються в разі здійснення внутрішнього контролю в межах одного структурного підрозділу / функції та/або між структурними підрозділами / окремими посадовими особами / функціями однієї лінії захисту.

11. Кодекс поведінки (етики) та запобігання конфліктам інтересів

60. Відповідальний орган з метою дотримання керівниками та іншими працівниками надавача фінансових платіжних послуг корпоративних цінностей затверджує та не рідше одного разу на рік переглядає:

1) кодекс поведінки (етики);

2) політику виявлення, запобігання та управління конфліктами інтересів.

Відповідальний орган разом із підрозділом контролю за дотриманням норм (комплаєнс) здійснює контроль за дотриманням документів, визначених у підпунктах 1, 2 пункту 60 глави 11 розділу III цього Положення.

61. Кодекс поведінки (етики) має чітко визначати:

1) загальнообов'язкові норми поведінки для керівників та інших працівників надавача фінансових платіжних послуг, а також відповідальність за порушення цих норм;

2) заборону на здійснення незаконної діяльності:

адміністративні правопорушення відповідно до Кодексу України про адміністративні правопорушення; посадовий злочин, економічний злочин (шахрайство);

порушення санкцій;

легалізація (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення;

неконкурентна практика;

3) заборону на подання недостовірної фінансової та регуляторної звітності;

4) заборону надання послуг чи консультацій користувачам та контрагентам, спрямованих на уникнення ними чи їх контрагентами сплати податків або уникнення виконання встановлених законодавством України або договірними умовами інших зобов'язань;

5) вимоги щодо дотримання культури управління ризиками;

6) порядок дій керівників та інших працівників надавача фінансових платіжних послуг для запобігання завданню шкоди майну надавача фінансових платіжних послуг;

7) заходи із запобігання порушенню прав споживачів;

8) заборону на використання службового становища керівниками та іншими працівниками надавача фінансових платіжних послуг з метою отримання несправедливих персональних переваг або надання таких переваг третім особам;

9) заходи із запобігання корупційним діям та хабарництву;

10) обмеження щодо дарування та отримання подарунків;

11) гарантії рівності відносин між надавачем фінансових платіжних послуг та його користувачами, працівниками, постачальниками та конкурентами, заборону дискримінації;

12) механізм конфіденційного повідомлення про неприйнятну поведінку в надавачі фінансових платіжних послуг / порушення в діяльності надавача фінансових платіжних послуг, який передбачає забезпечення захисту заявників;

13) порядок дослідження випадків неприйнятної поведінки в надавачі фінансових платіжних послуг / порушення в діяльності надавача фінансових платіжних послуг.

62. Кодекс поведінки (етики) може визначати інші вимоги та/або обмеження додатково до встановлених у пункті 61 глави 11 розділу ІІІ цього Положення.

63. Відповідальний орган, посадові особи зобов’язані вживати заходів для запобігання виникненню конфліктів інтересів у надавачі фінансових платіжних послуг та сприяти їх виявленню та врегулюванню.

64. Політика виявлення, запобігання та управління конфліктами інтересів повинна містити:

1) організаційні механізми, які визначають повноваження та відповідальність осіб, відповідальних за виявлення, запобігання та управління конфліктами інтересів;

2) інформацію про обставини, що свідчать або можуть свідчити про наявність конфлікту інтересів;

3) обов’язки керівників, ключових осіб та працівників надавача фінансових платіжних послуг щодо:
запобігання, виявлення та управління конфліктами інтересів;

оперативного повідомлення про обставини, що можуть спричинити або вже спричинили конфлікт інтересів, і порядок такого повідомлення;

4) процедуру перевірки керівників, ключових осіб надавача фінансових платіжних послуг до початку виконання ними посадових обов'язків для запобігання виникненню конфлікту інтересів під час виконання ними своїх обов'язків;

5) процедуру розгляду керівником отриманої інформації про потенційний або реальний конфлікт інтересів, визначення впливу цього конфлікту інтересів на профіль ризику надавача фінансових платіжних послуг та прийняття рішення про вжиття відповідних заходів;

6) обов'язок керівника щодо утримання від голосування з будь-якого питання, яке може спричинити конфлікт інтересів або зашкодити об'єктивному ставленню чи належному виконанню таким керівником обов'язків перед надавачем фінансових платіжних послуг;

7) порядок відсторонення керівника від голосування або участі іншим чином у прийнятті надавачем фінансових послуг будь-якого рішення, щодо якого в нього є конфлікт інтересів;

8) процедури та заходи з контролю для управління конфліктом інтересів, забезпечення вжиття заходів у разі виникнення конфлікту інтересів, процедури документування випадків виникнення (чи загрози виникнення) та управління конфліктами інтересів, розкриття інформації про конфлікт інтересів членами (або кандидатами в члени) органів управління, іншими працівниками;

9) порядок і періодичність здійснення перевірки потенційних і реальних конфліктів інтересів у надавачі фінансових платіжних послуг, що включає анкетування керівників, ключових осіб та працівників надавача фінансових платіжних послуг та подання керівниками, ключовими особами запевнень щодо відсутності конфлікту інтересів;

10) процедуру врегулювання конфлікту інтересів, включаючи вжиття заходів у разі виявлення порушення вимог порядку запобігання, виявлення та управління конфліктами інтересів у надавачі фінансових платіжних послуг;

11) порядок повідомлення Національного банку про конфлікти інтересів у надавачі фінансових платіжних послуг та заходи, вжиті для врегулювання конфліктів інтересів, якщо такі конфлікти не були врегульовані самостійно надавачем фінансових платіжних послуг.

65. Політика виявлення, запобігання та управління конфліктами інтересів може містити інші обов’язки, процедури додатково до встановлених у пункті 64 глави 11 розділу ІІІ цього Положення.

12. Контрольна діяльність надавача фінансових платіжних послуг

66. Надавач фінансових платіжних послуг здійснює контрольну діяльність у межах системи внутрішнього контролю з метою забезпечення досягнення надавачем фінансових платіжних послуг цілей його діяльності шляхом:

1) запровадження та виконання заходів із контролю щодо всіх процесів та на всіх організаційних рівнях;

2) розгляду звітів, підготовлених за результатами здійснення заходів із контролю.

67. Надавач фінансових платіжних послуг розробляє та контролює виконання внутрішніх документів, що встановлюють:

1) види, періодичність та порядок здійснення заходів із контролю;

2) перелік структурних підрозділів / працівників, відповідальних за проведення заходів із контролю;

3) види, періодичність та порядок підготовки звітності (управлінської, фінансової, регуляторної, податкової, іншої);

4) періодичність та порядок розгляду звітів;

5) перелік осіб / органів управління надавача фінансових платіжних послуг, що уповноважені здійснювати розгляд звітів;

6) процедури здійснення надавачем фінансових платіжних послуг відповідних коригувальних заходів щодо виправлення виявлених недоліків.

68. Надавач фінансових платіжних послуг зобов’язаний:

1) здійснювати заходи з контролю з метою запобігання, виявлення та усунення порушень законодавства України та внутрішніх документів надавача фінансових платіжних послуг;

2) забезпечити розроблення, впровадження та застосування механізмів внутрішнього контролю під час організації внутрішніх процесів, а також у разі залучення третіх осіб до надання та/або рекламування послуг за умови дотримання законодавства України.

69. Критерії, що свідчать про впровадження та здійснення контрольної діяльності як компонента системи внутрішнього контролю надавача фінансових платіжних послуг, уключають:

1) обрання та впровадження заходів із контролю, що забезпечують пом'якшення ризиків діяльності надавача фінансових платіжних послуг до прийнятного рівня;

2) забезпечення рівня контролю за вибором та використанням / застосуванням інформаційних систем та технологій, що використовуються надавачем фінансових платіжних послуг, на рівні, потрібному для забезпечення досягнення цілей його діяльності;

3) визначення заходів із контролю у внутрішніх документах надавача фінансових платіжних послуг, визначення очікуваних результатів та порядку здійснення таких заходів.

70. Надавач фінансових платіжних послуг має враховувати під час розроблення та перегляду заходів із контролю:

1) зміни в ринковому середовищі та законодавстві України, включаючи зміни в законодавстві України про захист прав споживачів фінансових послуг;

2) адекватність установлених заходів із контролю щодо кожного зі суттєвих видів ризиків, визначених у пунктах 127, 128 глави 23 розділу VI цього Положення;

3) ефективність застосованих у минулих періодах окремих видів заходів із контролю;

4) можливість моніторингу здійснення певного виду контролю.

71. Система внутрішнього контролю надавача фінансових платіжних послуг може включати здійснення таких видів заходів із контролю:

1) залежно від моменту здійснення контролю:
попередній – передує виконанню дії або операції;

поточний – здійснюється під час виконання дії або операції;

подальший – здійснюється після виконання дії або операцій та спрямований на виявлення недоліків, виправлення допущених помилок;

2) залежно від призначення контролю:

превентивний – спрямований на попередження порушень та ризиків;

виявляючий – спрямований на виявлення ризиків;

коригуючий – спрямований на уникнення / пом'якшення реалізованих ризиків та їх наслідків у майбутньому;

3) залежно від суб'єкта контролю:

самостійний – здійснюється працівником самостійно;

колективний – здійснюється двома (або більше) працівниками;

колегіальний – здійснюється колегіальним органом;

автоматизований – здійснюється автоматизованою системою;

4) залежно від періодичності здійснення:

функціональний (постійний) – проводиться щоденно;

періодичний – проводиться згідно з установленою у внутрішніх документах періодичністю;

5) залежно від обсягів контролю:

повний – охоплює весь обсяг відповідного процесу надавача фінансових платіжних послуг;

портфельний – проводиться за групами функцій, операцій, договорів;

вибірковий – проводиться за окремими відібраними елементами відповідного процесу надавача фінансових платіжних послуг.

72. Надавач фінансових платіжних послуг забезпечує послідовне поєднання попереднього, поточного і подальшого видів контролю, визначених у підпункті 1 пункту 71 глави 12 розділу III цього Положення, з метою підвищення дієвості та ефективності контролю.

73. Надавач фінансових платіжних послуг обирає та впроваджує заходи з контролю за інформаційними системами та технологіями, що використовуються у надавачі фінансових платіжних послуг, з метою забезпечення безперервності надання платіжних послуг надавачем фінансових платіжних послуг, що визначається у внутрішніх документах.

74. Заходи, зазначені в пункті 73 глави 12 розділу III цього Положення, включають:

1) контроль за збереженням цілісності та доступності інформації, що використовується в діяльності надавача фінансових платіжних послуг, яка зберігається з використанням інформаційних систем і технологій, що має право забезпечуватися шляхом резервування (копіювання) такої інформації / даних, відновлення функцій інформаційних систем і технологій, що були пошкоджені / знищені / втрачені;

2) управління доступами до систем, технологій та/або інформації, що використовуються надавачем фінансових платіжних послуг, а також до інших даних, інформаційних систем (системне програмне забезпечення), мереж, програмних додатків. Ці заходи здійснюються з метою захисту інформаційних систем надавача фінансових платіжних послуг від несанкціонованого використання та зловживань;

3) контроль за інформаційними системами та технологіями під час їх придбання, розроблення або супроводження впроваджується з метою забезпечення відповідних процедур, що регламентують придбання, розроблення та супроводження інформаційних систем і технологічних рішень, вимоги до їх документації, тестування та подальше технічне обслуговування. Ці процедури забезпечують контроль за змінами в інформаційних системах та технологіях і можуть передбачати необхідність авторизації запитів на зміни, узгоджень і результатів тестування.

75. Надавач фінансових платіжних послуг визначає осіб, відповідальних за здійснення заходів із контролю, підготовку та опрацювання звітів про результати здійснення заходів із контролю за горизонтальною та вертикальною взаємодією та з урахуванням принципу недопущення конфлікту інтересів.

76. Надавач фінансових платіжних послуг зобов’язаний у строки, визначені у внутрішніх документах надавача фінансових платіжних послуг, проводити щорічну самостійну оцінку відповідності системи внутрішнього контролю надавача фінансових платіжних послуг (далі – щорічна самооцінка) його цілям, розміру, видам діяльності, вимогам законодавства України, включаючи вимоги цього Положення, з обов’язковим урахуванням результатів здійснення контрольної діяльності та заходів з моніторингу ефективності системи внутрішнього контролю надавача фінансових платіжних послуг.

Результати проведеної щорічної самооцінки повинні викладатися у формі звіту за підписом уповноваженого працівника надавача фінансових платіжних послуг / керівника підрозділу, відповідального за складення такого звіту.

Звіт про результати щорічної самооцінки повинен містити оцінку за кожним компонентом системи внутрішнього контролю, визначеним у пункті 32 глави 6 розділу ІІІ цього Положення. Звіт про результати щорічної самооцінки може

містити іншу інформацію, обов’язковість включення якої визначено у внутрішньому документі надавача фінансових платіжних послуг.

13. Контроль за інформаційними потоками та комунікаціями

77. Надавач фінансових платіжних послуг у межах системи внутрішнього контролю визначає у внутрішніх документах порядок здійснення суб’єктами внутрішнього контролю зовнішніх та внутрішніх комунікацій, порядок використання, отримання та надання інформації.

78. Заходами, дотримання яких свідчить про впровадження та ефективне функціонування контролю за інформаційними потоками та комунікаціями як компонента системи внутрішнього контролю надавача фінансових платіжних послуг, є такі:

1) використання у своїй діяльності у визначеному внутрішніми документами порядку інформації, що відповідає принципам, які свідчать про забезпечення якості інформації, визначеним у пункті 79 глави 13 розділу ІІІ цього Положення;

2) проведення внутрішніх комунікацій, що потрібні для забезпечення ефективного функціонування системи внутрішнього контролю;

3) проведення зовнішніх комунікацій щодо питань, пов’язаних з ефективним функціонуванням системи внутрішнього контролю.

79. Надавач фінансових платіжних послуг забезпечує якість інформації, що створюється, використовується та отримується надавачем фінансових платіжних послуг під час його діяльності, ґрунтуючись на таких принципах:

1) актуальність, що передбачає забезпечення надавачем фінансових платіжних послуг внесення змін до інформації та повідомлення заінтересованих осіб про такі зміни протягом строку, визначеного законодавством України, нормативно-правовими актами Національного банку, внутрішніми документами надавача фінансових платіжних послуг;

2) коректність, що передбачає забезпечення надавачем фінансових платіжних послуг достовірності та повноти інформації;

3) цілісність, що передбачає обов’язок надавача фінансових платіжних послуг вживати заходів, включаючи використання інформаційних систем і

технологій, які спрямовані на захист інформації від викривлення, пошкодження, втрати або знищення;

4) збереження, що передбачає збереження інформації протягом усього строку її використання надавачем фінансових платіжних послуг, але не менше строків, визначених законодавством України та внутрішніми документами надавача фінансових платіжних послуг;

5) доступність, що передбачає визначення надавачем фінансових платіжних послуг у внутрішніх документах переліків інформації, яка є:

загальнодоступною;

з обмеженим доступом – може бути отримана та/або використана суб'єктами внутрішнього контролю виключно в межах їх повноважень;

6) достатність, що передбачає забезпечення надавачем фінансових платіжних послуг рівня деталізації інформації, яка відповідає потребам внутрішніх та зовнішніх користувачів.

80. Надавач фінансових платіжних послуг зобов'язаний визначити у внутрішніх документах порядок проведення перевірки якості інформації, включаючи її відповідність принципам, визначеним у пункті 79 глави 13 розділу ІІІ цього Положення, достовірність джерел походження такої інформації.

Перевірка якості інформації має здійснюватися уповноваженими суб'єктами внутрішнього контролю.

81. Надавач фінансових платіжних послуг зобов'язаний забезпечити суб'єктам внутрішнього контролю можливість використовувати інформаційні системи та технології, функціональні можливості яких дають змогу проведення перевірки дотримання принципів якості інформації, визначених у пункті 79 глави 13 розділу ІІІ цього Положення.

82. Надавач фінансових платіжних послуг визначає у внутрішніх документах порядок і способи здійснення внутрішніх та зовнішніх комунікацій з урахуванням різних напрямів та учасників комунікацій, характеру комунікацій, питань, щодо яких здійснюються комунікації, та вимог законодавства України.

83. Надавач фінансових платіжних послуг для забезпечення функціонування комплексної, адекватної та ефективної системи внутрішнього контролю зобов'язаний запровадити внутрішню систему повідомлення працівниками (включаючи повідомлення конфіденційно) про виявлені ризики, порушення вимог законодавства України та внутрішніх документів надавача фінансових платіжних послуг. Порядок роботи такої системи повинен бути

визначений внутрішніми документами та доведений до відома всіх працівників надавача фінансових платіжних послуг.

84. Надавач фінансових платіжних послуг визначає у внутрішніх документах заходи з контролю під час здійснення зовнішніх комунікацій, включаючи порядок отримання інформації від зовнішніх користувачів, її перевірки та передавання цієї інформації в межах організаційної структури надавача фінансових платіжних послуг.

85. Суб'єкти внутрішнього контролю, уповноважені здійснювати зовнішні комунікації, зобов'язані дотримуватися вимог законодавства України та внутрішніх документів надавача фінансових платіжних послуг щодо нерозголошення інформації з обмеженим доступом.

86. Надавач фінансових платіжних послуг, здійснюючи внутрішні та зовнішні комунікації, зобов'язаний дотримуватися принципів якості інформації, визначених у пункті 79 глави 13 розділу ІІІ цього Положення.

87. Надавач фінансових платіжних послуг має право встановити у внутрішніх документах порядок проведення оцінювання якості та ефективності внутрішніх та зовнішніх комунікацій, їх впливу на ефективне функціонування системи внутрішнього контролю та на досягнення цілей його діяльності.

14. Моніторинг ефективності системи внутрішнього контролю

88. Надавач фінансових платіжних послуг здійснює моніторинг ефективності системи внутрішнього контролю відповідно до вимог цього Положення та внутрішніх документів надавача фінансових платіжних послуг з метою:

1) оцінювання якості роботи системи внутрішнього контролю за певний період часу;

2) визначення здатності системи внутрішнього контролю забезпечити досягнення цілей його діяльності, включаючи визначення ймовірності виникнення та оцінку суттєвості потенційно можливих недоліків системи внутрішнього контролю, що можуть спричинити негативний вплив на досягнення цілей;

3) розроблення заходів, спрямованих на мінімізацію негативного впливу, з метою вдосконалення системи внутрішнього контролю.

89. Надавач фінансових платіжних послуг обирає види заходів з моніторингу системи внутрішнього контролю, включаючи моніторинг ефективності процедур із контролю та оцінку ефективності системи внутрішнього контролю, як комбінацію поточних та періодичних заходів з моніторингу з урахуванням установлених цілей діяльності надавача фінансових платіжних послуг, характеру, обсягу та складності його операцій, кількості та складності видів контролю, ймовірності виникнення недоліків, а також кваліфікації та досвіду працівників надавача фінансових платіжних послуг.

90. Надавач фінансових платіжних послуг має право визначати у внутрішніх документах, крім суб'єктів третьої лінії захисту, також інших працівників надавача фінансових платіжних послуг, уповноважених здійснювати моніторинг ефективності внутрішнього контролю.

91. Заходами, дотримання яких свідчить про впровадження та функціонування моніторингу ефективності внутрішнього контролю як компонента системи внутрішнього контролю надавача фінансових платіжних послуг, є такі:

1) визначення у внутрішніх документах порядку здійснення поточних та періодичних перевірок відповідності законодавству України та внутрішнім документам, якості та ефективності системи внутрішнього контролю;

2) забезпечення належного здійснення уповноваженими суб'єктами внутрішнього контролю оцінювання компонентів системи внутрішнього контролю та своєчасного повідомлення керівників надавача фінансових платіжних послуг про виявлені недоліки системи внутрішнього контролю та/або допущені суб'єктами внутрішнього контролю порушення і причини їх вчинення, відповідальних за прийняття рішення про здійснення коригувальних заходів, усунення порушення та/або внесення змін до внутрішніх документів.

92. Суб'єкти третьої лінії захисту (підрозділ внутрішнього аудиту / внутрішній аудитор / головний внутрішній аудитор) зобов'язані здійснювати загальну оцінку ефективності системи внутрішнього контролю в межах виконання функції внутрішнього аудиту надавача фінансових платіжних послуг.

93. Надавач фінансових платіжних послуг здійснює обов'язкові поточні та періодичні заходи з моніторингу ефективності системи внутрішнього контролю.

Поточні заходи з моніторингу здійснюються з метою оперативного виявлення та усунення недоліків системи внутрішнього контролю.

Відповідальність за проведення таких заходів можуть нести суб'єкти другої лінії захисту в межах повноважень.

Періодичні заходи з моніторингу / перевірки, включаючи оцінювання ефективності системи внутрішнього контролю, здійснюються суб'єктами третьої лінії захисту з метою виявлення недоліків після встановлення факту події.

94. Суб'єкти третьої лінії захисту (підрозділ внутрішнього аудиту / внутрішній аудитор / головний внутрішній аудитор) зобов'язані за результатами здійснення моніторингу / перевірки ефективності системи внутрішнього контролю складати звіти, що подаються на розгляд ради (якщо її немає, − на розгляд органу згідно з компетенцією, визначеною в статуті надавача фінансових платіжних послуг).

Звіти, що подаються раді або органу, визначеному статутом надавача фінансових платіжних послуг, повинні містити інформацію про виявлені недоліки системи внутрішнього контролю та порушення, аналіз причин їх виникнення, ймовірні наслідки, до яких можуть призвести ці недоліки, рекомендації / пропозиції щодо підвищення ефективності функціонування системи внутрішнього контролю, процес контролю за станом виконання рекомендацій / пропозицій, затверджених раніше.

95. Надавач фінансових платіжних послуг забезпечує подання звітів щодо результатів моніторингу ефективності системи внутрішнього контролю також працівникам, які відповідають за здійснення коригувальних заходів, та керівникам надавача фінансових платіжних послуг у межах визначених повноважень.

IV. Функція контролю за дотриманням норм (комплаєнс)

15. Загальні вимоги до організації функції контролю за дотриманням норм (комплаєнс) у надавачі фінансових платіжних послуг

96. Надавач фінансових платіжних послуг зобов'язаний забезпечити ефективне виконання функції контролю за дотриманням норм (комплаєнс) у надавачі фінансових платіжних послуг відповідно до вимог цього Положення.

97. Підрозділ контролю за дотриманням норм (комплаєнс) надавача фінансових платіжних послуг забезпечує виконання ключової функції контролю за дотриманням норм (комплаєнс) надавача фінансових платіжних послуг щодо організації забезпечення відповідності діяльності надавача фінансових платіжних послуг вимогам законодавства України, внутрішнім документам надавача фінансових платіжних послуг, стандартам професійних об'єднань, дія яких поширюється на надавача фінансових платіжних послуг, оцінювання

можливого впливу будь-яких змін, що вносяться до законодавства, на діяльність надавача фінансових платіжних послуг, а також визначення і оцінювання ризику недотримання норм та інших функцій, визначених цим Положенням.

98. Підрозділ контролю за дотриманням норм (комплаєнс) діє відповідно до вимог цього Положення та на підставі положення, що затверджується відповідальним органом, організаційно не залежить від інших підрозділів надавача фінансових платіжних послуг, не підпорядковується таким підрозділам і підпорядковується головному комплаєнс-менеджеру. Головний комплаєнс-менеджер діє відповідно до вимог цього Положення та на підставі положення, що затверджується відповідальним органом, організаційно не залежить від інших підрозділів надавача фінансових платіжних послуг, не підпорядковується таким підрозділам і підпорядковується відповідальному органу та звітує перед ним (ними).

16. Функції підрозділу контролю за дотриманням норм (комплаєнс) у надавачі фінансових платіжних послуг

99. Виконання підрозділом контролю за дотриманням норм (комплаєнс) у надавачі фінансових платіжних послуг функції контролю за дотриманням норм (комплаєнс) у надавачі фінансових платіжних послуг передбачає:

1) організацію контролю за дотриманням надавачем фінансових платіжних послуг норм законодавства України, внутрішніх документів надавача фінансових платіжних послуг і стандартів професійних об’єднань, дія яких поширюється на надавача фінансових платіжних послуг;

2) моніторинг змін у законодавстві України, стандартах професійних об’єднань, дія яких поширюється на надавача фінансових платіжних послуг, оцінку впливу таких змін на процеси та процедури, запроваджені в надавачі фінансових платіжних послуг, а також контроль за імплементацією відповідних змін у внутрішні документи надавача фінансових платіжних послуг;

3) контроль за комплаєнс-ризиком, що виникає у взаємовідносинах надавача фінансових платіжних послуг з користувачами та контрагентами;

4) управління ризиками, пов’язаними з конфліктом інтересів, та в разі виявлення будь-яких фактів, що свідчать про наявність конфлікту інтересів у надавача фінансових платіжних послуг, інформування ради / загальних зборів;

5) організацію контролю за дотриманням надавачем фінансових платіжних послуг норм щодо своєчасності подання та достовірності звітності, включаючи фінансову;

6) організацію контролю за захистом персональних даних відповідно до законодавства України;

7) надання роз'яснень, консультацій керівникам надавача фінансових платіжних послуг на їхні запити з питань контролю за дотриманням норм (комплаєнс);

8) своєчасне виявлення, вимірювання (оцінка), моніторинг, контроль, звітування і надання рекомендацій щодо пом'якшення комплаєнс-ризику;

9) контроль за дотриманням норм щодо визначення переліку пов'язаних осіб надавача фінансових платіжних послуг, підготовку висновків стосовно комплаєнс-ризику для ухвалення рішень щодо операцій з такими особами;

10) контроль за відповідністю процедур притягнення до дисциплінарної відповідальності працівників вимогам законодавства України;

11) підготовку та подання звіту щодо комплаєнс-ризику відповідальному органу або органу, визначеному статутом надавача фінансових платіжних послуг, комітету з управління ризиками з урахуванням вимог цього Положення;

12) розроблення внутрішніх документів з питань дотримання норм (комплаєнс);

13) проведення навчання, регулярних тренінгів для працівників надавача фінансових платіжних послуг, включаючи працівників, які займають посади з високою відповідальністю або залучені до діяльності з високим ризиком, щодо дотримання норм законодавства України, внутрішніх документів та стандартів професійних об'єднань, вимоги яких поширюються на надавача фінансових платіжних послуг, кодексу поведінки (етики);

14) інформування відповідального органу, комітету з управління ризиками та виконавчого органу щодо надмірних комплаєнс-ризиків, надання пропозицій відповідальному органу, комітету з управління ризиками та виконавчому органу щодо заходів пом'якшення впливу комплаєнс-ризиків, а також забезпечення координації роботи з питань управління комплаєнс-ризиками між структурними підрозділами та/або працівниками надавача фінансових платіжних послуг;

15) забезпечення безперервності роботи підрозділу контролю за дотриманням норм (комплаєнс) надавача фінансових платіжних послуг.

100. Головний комплаєнс-менеджер відповідає за:

1) виконання функції контролю за дотриманням норм (комплаєнс);

2) виконання підрозділом контролю за дотриманням норм (комплаєнс) (у разі його створення) покладених на нього функцій.

101. Головний комплаєнс-менеджер повинен відповідати вимогам до професійної придатності та ділової репутації, визначеним Положенням про авторизацію надавачів фінансових платіжних послуг.

102. Надавач фінансових платіжних послуг має право прийняти рішення про одночасне виконання функцій головного комплаєнс-менеджера та відповідального працівника надавача фінансових платіжних послуг за проведення фінансового моніторингу на умовах суміщення з урахуванням вимог цього Положення та Положення про авторизацію надавачів фінансових платіжних послуг.

17. Внутрішні документи з питань дотримання норм (комплаєнс)

103. Надавач фінансових платіжних послуг розробляє та періодично (не рідше одного разу на рік) переглядає положення про контроль за дотриманням норм (комплаєнс) і політику управління комплаєнс-ризиком, яке затверджується відповідальним органом або органом, визначеним статутом надавача фінансових платіжних послуг, і не може суперечити вимогам цього Положення.

104. Положення про контроль за дотриманням норм (комплаєнс) у надавачі фінансових платіжних послуг документально закріплює процес здійснення функції контролю за дотриманням норм (комплаєнс) і враховує вимоги цього Положення.

105. Політика управління комплаєнс-ризиком повинна обов’язково містити:

1) процедури щодо виявлення, вимірювання, моніторингу, контролю, звітування та пом’якшення комплаєнс-ризику, включаючи інструменти / індикатори, що використовуються;

2) процедури та процеси забезпечення відповідності діяльності надавача фінансових платіжних послуг вимогам законодавства України, включаючи

законодавство у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення та внутрішніх документів під час діяльності надавача фінансових платіжних послуг;

3) процедуру забезпечення контролю за достовірністю фінансової та статистичної звітності;

4) чітке розмежування функцій управління комплаєнс-ризиком та операційним ризиком із метою уникнення їх дублювання;

5) порядок обміну інформацією між учасниками процесу управління комплаєнс-ризиком, включаючи види, форми і терміни подання інформації.

18. Звіт щодо комплаєнс-ризику надавача фінансових платіжних послуг

106. Головний комплаєнс-менеджер складає та подає звіт щодо комплаєнс-ризику відповідальному органу або органу, визначеному статутом надавача фінансових платіжних послуг, комітету з управління ризиками не рідше одного разу на квартал або частіше у випадках, установлених законодавством України або статутом надавача фінансових платіжних послуг.

107. Звіт щодо комплаєнс-ризику надавача фінансових платіжних послуг повинен містити інформацію про:

1) види діяльності, процеси, що піддають надавача фінансових платіжних послуг значному комплаєнс-ризику та в разі його реалізації впливають на діяльність надавача фінансових платіжних послуг, а також пропозиції щодо уникнення чи пом’якшення цього ризику;

2) випадки порушень вимог законодавства України, ринкових стандартів, правил добросовісної конкуренції та корпоративної етики, правил платіжних систем та внутрішніх документів під час діяльності надавача фінансових платіжних послуг, а також застосованих заходів впливу до надавача фінансових платіжних послуг або інших негативних наслідків через такі порушення;

3) зміни в законодавстві України та про їх потенційні наслідки для надавача фінансових платіжних послуг;

4) випадки конфлікту інтересів;

5) проведені навчання працівників надавача фінансових платіжних послуг з питань, що належать до функцій підрозділу контролю за дотриманням норм (комплаєнс);

6) випадки порушень працівниками надавача фінансових платіжних послуг правил корпоративної етики, результати досліджень їх причин та про заходи щодо запобігання таким подіям надалі.

V. Функція внутрішнього аудиту надавача фінансових платіжних послуг

19. Загальні вимоги до організації функції внутрішнього аудиту в надавачі фінансових платіжних послуг

108. Надавач фінансових платіжних послуг (крім філії іноземної платіжної установи) зобов'язаний забезпечити ефективне виконання функції внутрішнього аудиту в надавачі фінансових платіжних послуг відповідно до вимог Закону про платіжні послуги, Закону про фінансові послуги та цього Положення.

109. Виконання ключової функції внутрішнього аудиту надавача фінансових платіжних послуг забезпечує підрозділ внутрішнього аудиту.

110. Підрозділ внутрішнього аудиту діє відповідно до вимог Закону про платіжні послуги, Закону про фінансові послуги, цього Положення.

Підрозділ внутрішнього аудиту на підставі положення, що затверджується відповідальним органом, організаційно не залежить від інших підрозділів надавача фінансових платіжних послуг, не підпорядковується таким підрозділам і підпорядковується головному внутрішньому аудитору.

Головний внутрішній аудитор організаційно не залежить від інших підрозділів надавача фінансових платіжних послуг, підпорядковується відповідальному органу та звітує перед ним.

Головний внутрішній аудитор повинен відповідати вимогам до професійної придатності та ділової репутації, визначеним Положенням про авторизацію надавачів фінансових платіжних послуг.

111. Виконання функції внутрішнього аудиту надавача фінансових платіжних послуг передбачає здійснення внутрішніх аудиторських перевірок надавача фінансових платіжних послуг відповідно до річного плану проведення аудиторських перевірок на звітний рік, який затверджується відповідальним органом. За потреби для забезпечення оцінки тих сфер діяльності надавача фінансових платіжних послуг, в яких є (виникли) значні ризики протягом звітного року, підрозділ внутрішнього аудиту може проводити перевірки, які не включені до річного плану перевірок.

112. Річний план проведення внутрішніх аудиторських перевірок надавача фінансових платіжних послуг та зміни до нього складаються головним внутрішнім аудитором на основі ризик-орієнтованого підходу та з урахуванням пропозицій і завдань, отриманих від ради або виконавчого органу, спеціальних вимог Національного банку і за потреби може переглядатися (принаймні один раз на рік або частіше) для забезпечення оцінки тих сфер діяльності надавача фінансових платіжних послуг, в яких є значні ризики.

113. Головний внутрішній аудитор подає річний план (зміни до плану) проведення внутрішніх аудиторських перевірок надавача фінансових платіжних послуг на наступний рік на затвердження відповідальному органу до 10 грудня року, що передує звітному. Відповідальний орган має затвердити річний план проведення внутрішніх аудиторських перевірок не пізніше 25 грудня року, що передує звітному.

20. Функції підрозділу внутрішнього аудиту

114. Підрозділ внутрішнього аудиту під час виконання функції внутрішнього аудиту надавача фінансових платіжних послуг здійснює:

1) оцінку відповідності діяльності надавача фінансових платіжних послуг вимогам законодавства України, ефективності процесів делегування повноважень між структурними підрозділами надавача фінансових платіжних послуг та розподілу обов’язків між ними, ефективності використання наявних у надавача фінансових платіжних послуг ресурсів, ефективності використання та мінімізації ризиків від використання інформаційних систем і технологій, достатності і ефективності заходів, спрямованих на зменшення ризиків та усунення недоліків, виявлених державними органами, зовнішніми аудиторами або підрозділом внутрішнього аудиту надавача фінансових платіжних послуг;

2) перевірку правильності ведення та достовірності бухгалтерського обліку, фінансової та регуляторної звітності, що складається надавачем фінансових платіжних послуг, їх повноти та вчасності надання, включаючи подання таких звітів до Національного банку, органів державної влади та органів управління надавача фінансових платіжних послуг, які в межах компетенції здійснюють нагляд за діяльністю надавача фінансових платіжних послуг;

3) оцінку надійності, ефективності та цілісності управління інформаційними системами надавача фінансових платіжних послуг;

4) річне планування завдань підрозділу внутрішнього аудиту, включаючи складання та виконання плану проведення внутрішніх аудиторських перевірок надавача фінансових платіжних послуг;

5) реалізацію завдань згідно із затвердженим планом проведення внутрішніх аудиторських перевірок надавача фінансових платіжних послуг;

6) проведення планового та позапланового внутрішнього аудиту надавача фінансових платіжних послуг;

7) подання керівникам структурних підрозділів (учасникам процесів, які підлягали внутрішній аудиторській перевірці надавача фінансових платіжних послуг), виконавчому органу та раді звітів за результатами проведення внутрішніх аудиторських перевірок та повідомлення про виявлені під час проведення такого внутрішнього аудиту порушення, недоліки та ризики, а також надані рекомендації за результатами проведеного внутрішнього аудиту для прийняття ними відповідних організаційних (коригувальних) заходів;

8) моніторинг виконання структурними підрозділами надавача фінансових платіжних послуг рекомендацій;

9) подання відповідальному органу не рідше ніж один раз на рік інформації (звіт) про стан реалізації, включаючи невиконання, виконавчим органом та керівниками структурних підрозділів надавача фінансових платіжних послуг рекомендацій (пропозицій) з усунення порушень і недоліків у діяльності надавача фінансових платіжних послуг, виявлених за результатами внутрішнього аудиту;

10) складання та подання відповідальному органу звіту про виконання річного плану проведення аудиторських перевірок надавача фінансових платіжних послуг із наданням підтвердження щодо організаційної незалежності підрозділу внутрішнього аудиту надавача фінансових платіжних послуг;

11) підготовку письмового повідомлення Національному банку в спосіб, визначений в пункті 230 глави 37 розділу VIII цього Положення, про виявлені під час проведення внутрішньої аудиторської перевірки випадки формування недостовірної фінансової та регуляторної звітності надавача фінансових платіжних послуг, порушення, недоліки, а також будь-які події в діяльності та роботі надавача фінансових платіжних послуг, які можуть негативно вплинути на платоспроможність надавача фінансових платіжних послуг, якщо виконавчий орган своєчасно не вжив заходів щодо усунення цих порушень та недоліків, а відповідальний орган не розглянув звернення головного внутрішнього аудитора

щодо бездіяльності виконавчого органу та за результатами розгляду цього звернення не вжив відповідних заходів;

12) виявлення сфер потенційних збитків для надавача фінансових платіжних послуг, сприятливих умов для шахрайства, зловживань і незаконного присвоєння активів надавача фінансових платіжних послуг;

13) взаємодію із зовнішніми аудиторами, органами державної влади та управління, які в межах компетенції здійснюють нагляд за діяльністю надавача фінансових платіжних послуг, включаючи взаємодію з Національним банком;

14) аналіз висновків зовнішніх аудиторів та здійснення моніторингу виконання рекомендацій зовнішніх аудиторів;

15) взаємодію з іншими підрозділами надавача фінансових платіжних послуг у сфері організації контролю і моніторингу системи управління надавача фінансових платіжних послуг;

16) участь у службових розслідуваннях та інформування ради і виконавчого органу про результати таких розслідувань;

17) розроблення та впровадження програм оцінки і підвищення якості внутрішнього аудиту;

18) забезпечення безперервності роботи підрозділу внутрішнього аудиту надавача фінансових платіжних послуг та проведення внутрішнього аудиту відповідно до вимог, визначених у главі 20 розділу V цього Положення, інших нормативно-правових актів Національного банку, положення про внутрішній аудит надавача фінансових платіжних послуг;

19) забезпечення безперервності професійної підготовки та навчання головного внутрішнього аудитора, працівників підрозділу внутрішнього аудиту надавача фінансових платіжних послуг (не рідше двох разів на рік), включаючи проходження відповідного навчання в навчальних закладах, що надають послуги з підвищення кваліфікації внутрішніх аудиторів, включаючи вивчення теорії та практики застосування міжнародних стандартів внутрішнього аудиту, освоєння принципів прогнозування та управління ризиками фінансової установи, запобігання шахрайству, методик проведення внутрішніх аудиторських перевірок;

20) забезпечення внутрішніх періодичних перевірок щодо дотримання надавачем фінансових платіжних послуг вимог законодавства у сфері

запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення [включаючи вимоги щодо достатності вжитих надавачем фінансових платіжних послуг заходів з управління ризиками легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення].

115. Підрозділ внутрішнього аудиту під час виконання функції внутрішнього аудиту надавача фінансових платіжних послуг зобов'язаний:

1) не розголошувати та не використовувати конфіденційну інформацію, яка стала відома їм під час виконання функцій, на свою користь чи на користь третіх осіб та забезпечити збереження і своєчасне повернення одержаних від керівників або структурних підрозділів надавача фінансових платіжних послуг документів та інформації на всіх носіях;

2) не брати участі в створенні та організації, включаючи разом зі структурними підрозділами надавача фінансових платіжних послуг, будь-яких заходів та процесів, що забезпечують діяльність надавача фінансових платіжних послуг або сприймаються як такі, що впливають на неупередженість та об'єктивність внутрішніх аудиторів;

3) не брати участі в розробленні внутрішніх документів надавача фінансових платіжних послуг (крім випадків надання внутрішніми аудиторами консультаційних послуг, які передбачені функцією внутрішнього аудиту) та не візувати внутрішніх документів надавача фінансових платіжних послуг.

116. Головний внутрішній аудитор / працівники підрозділу внутрішнього аудиту надавача фінансових платіжних послуг під час виконання своїх функціональних обов'язків з метою реалізації функцій внутрішнього аудиту має / мають право:

1) отримувати необхідну інформацію та документи, які стосуються внутрішнього аудиту і є в надавача фінансових платіжних послуг;

2) ініціювати комунікацію / взаємодію з керівниками та з будь-якими працівниками надавача фінансових платіжних послуг, з керівниками структурних підрозділів надавача фінансових платіжних послуг, включаючи відокремлені підрозділи надавача фінансових платіжних послуг, що забезпечують здійснення діяльності з надання платіжних послуг, незалежно від їх місцезнаходження, отримувати доступ до будь-яких документів та інформації надавача фінансових платіжних послуг, його афілійованих осіб, архівів, даних і

об’єктів надавача фінансових платіжних послуг, управлінської інформації, документів із прийняття рішень органами управління надавача фінансових платіжних послуг;

3) залучати за потреби працівників інших структурних підрозділів надавача фінансових платіжних послуг (за згодою керівників таких структурних підрозділів) та/або зовнішніх експертів, консультантів, аудиторів (за погодженням із радою) для виконання поставлених перед підрозділом внутрішнього аудиту завдань;

4) на безперешкодний доступ до інформаційних систем надавача фінансових платіжних послуг та до всіх приміщень надавача фінансових платіжних послуг, а також до приміщень, що використовуються для зберігання документів, матеріальних цінностей, на отримання інформації, яка зберігається в паперовій формі та на електронних носіях;

5) отримувати необхідні пояснення в письмовій чи усній формі від працівників надавача фінансових платіжних послуг з питань, що виникають під час проведення внутрішньої аудиторської перевірки та за її результатами;

6) робити копії з наданих для перевірки документів (у разі надання їх на паперових носіях), робити копії електронних документів, що зберігаються на електронних носіях та є необхідними для проведення аудиторської перевірки;

7) уносити на розгляд ради пропозиції щодо вдосконалення діяльності підрозділу внутрішнього аудиту.

117. Головний внутрішній аудитор зобов’язаний вести облік і зберігати документи та інші матеріальні носії, що містять інформацію, зібрану під час проведення внутрішнього аудиту в надавачі фінансових платіжних послуг, інформацію про всі перевірені сфери, виявлені проблеми та надані рекомендації надавачу фінансових платіжних послуг протягом семи років з дати їх складання / затвердження для забезпечення підтвердження ефективності здійснення функції внутрішнього аудиту в надавачі фінансових платіжних послуг.

21. Положення про внутрішній аудит надавача фінансових платіжних послуг

118. Надавач фінансових платіжних послуг розробляє та періодично (не рідше одного разу на рік) переглядає положення про внутрішній аудит надавача фінансових платіжних послуг, яке затверджується відповідальним органом і яке

не може суперечити вимогам Закону про платіжні послуги, Закону про фінансові компанії та цього Положення.

119. Положення про внутрішній аудит надавача фінансових платіжних послуг переглядається відповідальним органом.

120. Положення про внутрішній аудит надавача фінансових платіжних послуг документально закріплює процес здійснення функції внутрішнього аудиту та враховує вимоги цього Положення.

22. Оформлення результатів внутрішнього аудиту

121. Підрозділ внутрішнього аудиту за результатами проведеної роботи готує та подає відповідальному органу два рази на рік протягом 15 днів місяця, наступного за звітним періодом (пів року):

1) звіт про діяльність підрозділу внутрішнього аудиту;

2) аудиторський звіт за результатами внутрішнього аудиту;

3) інші документи за результатами внутрішнього аудиту і пропозиції щодо усунення виявлених порушень та підвищення ефективності процесів управління та контролю надавача фінансових платіжних послуг.

122. В аудиторському звіті за результатами внутрішнього аудиту викладаються виявлені недоліки в діяльності надавача фінансових платіжних послуг, порушення надавачем фінансових платіжних послуг вимог законодавства України, причини, що зумовили такі недоліки та/або порушення, пропозиції щодо їх усунення.

123. Аудиторський звіт про результати проведення внутрішньої аудиторської перевірки надавача фінансових платіжних послуг складається з урахуванням вимог стандартів внутрішнього аудиту, підписується (власноруч або електронним підписом) внутрішнім аудитором (працівником підрозділу внутрішнього аудиту), який безпосередньо виконував перевірку, та головним внутрішнім аудитором надавача фінансових платіжних послуг.

124. Аудиторський звіт за результатами внутрішнього аудиту надається керівникам структурних підрозділів, які підлягали аудиту, виконавчому органу та раді для вжиття своєчасних і належних організаційних (коригувальних) заходів.

125. Процес моніторингу (відстеження) підрозділом внутрішнього аудиту надавача фінансових платіжних послуг результатів внутрішніх аудиторських перевірок починається після підписання / затвердження аудиторського звіту та закінчується після виконання усіх наданих рекомендацій (пропозицій).

126. Відсутність подальшого моніторингу (відстеження) результатів внутрішніх аудиторських перевірок встановлюється шляхом підтвердження керівником підрозділу внутрішнього аудиту надавача фінансових платіжних послуг виконання об'єктом аудиту всіх та повною мірою рекомендацій (пропозицій), що надавалися за результатами аудиту.

VI. Система управління ризиками

23. Загальні засади побудови системи управління ризиками

127. Система управління ризиками надавача фінансових платіжних послуг повинна забезпечувати виявлення, вимірювання, моніторинг, контроль, звітування та мінімізацію (зниження до контрольованого рівня) таких суттєвих ризиків, на які наражається надавач фінансових платіжних послуг, як наявні (реалізовані, поточні), так і потенційні (нереалізовані):

1) операційного ризику, включаючи такі складові, як кіберризики та ризики безпеки;

2) комплаєнс-ризику.

128. Надавач фінансових платіжних послуг має право розширювати перелік суттєвих видів ризиків, визначений у пункті 127 глави 23 розділу VI цього Положення, самостійно встановлювати критерії, за якими визначатиметься суттєвість інших видів ризиків діяльності надавача фінансових платіжних послуг, з урахуванням складності, обсягів, видів, характеру здійснюваних надавачем фінансових платіжних послуг операцій, організаційної структури та профілю ризику надавача фінансових платіжних послуг і визначати порядок виявлення таких ризиків. До таких ризиків можуть належати: кредитний ризик, ризик ліквідності, ринковий ризик, ризик контрагента.

129. Надавач фінансових платіжних послуг створює комплексну, адекватну та ефективну систему управління ризиками, яка повинна відповідати таким принципам:

1) ефективність – забезпечення об'єктивної оцінки розміру ризиків надавача фінансових платіжних послуг та повноти заходів щодо управління ризиками з

оптимальним використанням фінансових ресурсів, персоналу та інформаційних систем щодо управління ризиками надавача фінансових 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 підрозділами і працівниками надавача фінансових платіжних послуг та їх відповідальності згідно з таким розподілом;

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

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

6) пропорційність – відповідність системи управління ризиками розміру надавача фінансових платіжних послуг, складності, обсягам, видам, характеру здійснюваних надавачем фінансових платіжних послуг операцій за видами платіжних послуг, включених до ліцензії на надання платіжних послуг, організаційній структурі та профілю ризику надавача фінансових платіжних послуг;

7) незалежність – свобода від обставин, що становлять загрозу для неупередженого виконання підрозділом з управління ризиками та підрозділом контролю за дотриманням норм (комплаєнс) своїх функцій;

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, включаючи бек-тестування.

130. Ефективна, комплексна та адекватна система управління ризиками надавача фінансових платіжних послуг повинна містити:

1) організацію системи управління ризиками, яка ґрунтується на застосуванні моделі трьох ліній захисту, забезпечує чіткий розподіл функцій, обов’язків і повноважень з управління ризиками між усіма суб’єктами системи управління ризиками, а також між працівниками надавача фінансових платіжних послуг і передбачає їх відповідальність згідно з таким розподілом;

2) культуру управління ризиками та кодекс поведінки (етики);

3) внутрішні документи з питань управління ризиками;

4) інформаційну систему щодо управління ризиками та звітування;

5) інструменти для ефективного управління ризиками.

131. Суб’єктами системи управління ризиками надавача фінансових платіжних послуг є:

1) відповідальний орган;

2) комітети ради;

3) виконавчий орган;

4) бізнес-підрозділи, підрозділи підтримки або особи, на яких покладено виконання функцій відповідних підрозділів;

5) підрозділ з управління ризиками / головний ризик-менеджер та підрозділ контролю за дотриманням норм (комплаєнс) / головний комплаєнс-менеджер;

6) підрозділ внутрішнього аудиту / головний внутрішній аудитор;

7) керівники та працівники надавача фінансових платіжних послуг, які здійснюють внутрішній контроль відповідно до повноважень, визначених внутрішніми документами, та не входять до складу органів і підрозділів надавача фінансових платіжних послуг, зазначених у підпунктах 1–6 пункту 131 глави 23 розділу VI цього Положення.

132. Надавач фінансових платіжних послуг зобов’язаний здійснювати вимірювання (оцінку) ризиків відповідно до вимог глави 27 розділу VI цього Положення та з урахуванням взаємозв’язку ризиків і впливу окремого ризику на інші ризики, що притаманні діяльності надавача фінансових платіжних послуг.

Вимірювання ризиків, проведене надавачем фінансових платіжних послуг, повинно бути задокументовано, включаючи детальний опис та пояснення ризиків, що охоплюються вимірюванням, використані підходи, а також ключові судження та припущення, зроблені під час такого вимірювання.

133. Система управління ризиками надавача фінансових платіжних послуг може передбачати вимірювання ризиків за новими платіжними продуктами та значними змінами в діяльності надавача фінансових платіжних послуг до початку їх упровадження, включаючи зміни в реалізації платіжних продуктів, зміни в системі управління надавача фінансових платіжних послуг.

134. Надавач фінансових платіжних послуг у своїй системі управління ризиками зобов'язаний передбачити процеси та інструменти для моніторингу ризиків, що дають змогу своєчасно виявляти ризики та адекватно управляти ними.

135. Надавач фінансових платіжних послуг у своїй системі управління ризиками зобов'язаний передбачити методи (інструменти) управління виявленими ризиками в межах підходів до управління ризиками. Такими методами управління ризиками можуть бути:

1) прийняття ризику;

2) передавання ризику;

3) пом'якшення або зниження ризику;

4) уникнення ризику;

5) інші методи, доступні для застосування надавачем фінансових платіжних послуг.

136. Надавач фінансових платіжних послуг у своїй системі управління ризиками зобов'язаний передбачити порядок звітування про ризики, загальну оцінку ризиків та пов'язані з ними плани дій раді та керівникам надавача фінансових платіжних послуг залежно від обставин. Процедура ескалації ризиків надавача фінансових платіжних послуг, зазначена в підпункті 7 пункту 147 глави 24 розділу VI цього Положення, повинна давати змогу звітувати про проблеми, пов'язані з ризиками, у межах періодичної звітності, а також поза періодичною звітністю для термінових питань. Діяльність надавача фінансових платіжних послуг, що виходить за межі затвердженого ризик-апетиту, лімітів ризиків,

повинна бути предметом відповідного аналізу та вимагати відповідного схвалення радою або іншим визначеним радою органом.

24. Внутрішні документи надавача фінансових платіжних послуг з питань системи управління ризиками

137. Надавач фінансових платіжних послуг у межах системи управління ризиками розробляє і впроваджує внутрішні документи з питань управління ризиками з урахуванням вимог Закону про платіжні послуги та цього Положення.

138. Надавач фінансових платіжних послуг розробляє внутрішні документи у формі стратегій, політики, положень, процедур, які документально закріплюють процес управління ризиками та враховують вимоги цього Положення.

139. Надавач фінансових платіжних послуг зобов'язаний мати затверджені відповідальним органом такі внутрішні документи в межах системи управління ризиками:

1) стратегію управління ризиками;

2) декларацію схильності до ризиків;

3) політику управління ризиками, включаючи ліміти ризиків, розподіл повноважень щодо прийняття ризиків, та політику управління окремими видами ризиків у випадках, визначених цим Положенням;

4) порядки та процедури управління ризиками у випадках, визначених цим Положенням.

140. Надавач фінансових платіжних послуг має право використовувати у своїй діяльності внутрішні положення / процедури фінансової групи щодо управління ризиками, якщо такий надавач фінансових платіжних послуг входить до визнаної Національним банком фінансової групи, за умови відповідності таких документів вимогам цього Положення.

141. Відповідальний орган здійснює контроль за дотриманням внутрішніх документів, визначених у пункті 139 глави 24 розділу VI цього Положення, з урахуванням вимог цього Положення.

142. Надавач фінансових платіжних послуг має право об’єднувати окремі внутрішні документи в один або кілька документів, не порушуючи вимог цього Положення щодо їх розроблення, наповнення, затвердження, перегляду та інших вимог.

143. Внутрішні документи з питань управління ризиками повинні визначати також порядок взаємодії між усіма організаційними рівнями надавача фінансових платіжних послуг, включаючи керівників надавача фінансових платіжних послуг.

144. Надавач фінансових платіжних послуг своєчасно та періодично переглядає (не рідше одного разу на рік) та оновлює (актуалізує) внутрішні документи з питань управління ризиками з урахуванням змін у законодавстві України, дія яких поширюється на надавача фінансових платіжних послуг, змін у профілі ризиків надавача фінансових платіжних послуг, а також з урахуванням інших внутрішніх чи зовнішніх подій та/або обставин.

Зміни в системі управління ризиками надавача фінансових платіжних послуг, а також причини таких змін повинні бути задокументовані і підлягають затвердженню відповідальним органом. Внутрішні документи з питань управління ризиками надавача фінансових платіжних послуг повинні бути доступними для внутрішнього аудиту, зовнішнього аудиту та Національного банку для проведення ними відповідних оцінок ефективності системи управління ризиками.

145. Стратегія управління ризиками надавача фінансових платіжних послуг обов’язково повинна містити:

1) основні цілі управління ризиками;

2) перелік суттєвих ризиків із зазначенням видів операцій, які генерують ці ризики;

3) принципи та підходи щодо визначення прийнятного співвідношення дохідності та ризиків;

4) загальні принципи управління ризиками.

146. Декларація схильності до ризиків визначає:

1) рівень ризик-апетиту, який повинен узгоджуватись із загальною стратегією (стратегією розвитку) надавача фінансових платіжних послуг та впроваджуватися в його діяльність;

2) види ризиків, щодо яких надавач фінансових платіжних послуг прийняв рішення про доцільність / необхідність їх утримання з метою досягнення його стратегічних цілей та виконання плану діяльності надавача фінансових платіжних послуг;

3) види ризиків, яких надавач фінансових платіжних послуг повинен уникати.

147. Політика управління ризиками (крім комплаєнс-ризику) надавача фінансових платіжних послуг повинна містити:

1) визначення та класифікацію ризиків, включаючи інші визначені надавачем фінансових платіжних послуг суттєві ризики, притаманні діяльності надавача фінансових платіжних послуг, за видами ризиків;

2) перелік видів ризиків;

3) процеси та інструменти щодо виявлення, вимірювання (оцінки), моніторингу, контролю та звітування щодо ризиків, включаючи критерії суттєвості, що застосовуються надавачем фінансових платіжних послуг до нових ризиків, порядок їх виявлення та пом’якшення;

4) ліміти ризиків за визначеними надавачем фінансових платіжних послуг видами ризиків відповідно до ризик-апетиту надавача фінансових платіжних послуг та порядок контролю за їх дотриманням;

5) методи, інструменти, положення, методичні вказівки, ключові припущення та обмеження в управлінні ризиками;

6) зміст та форму звітності щодо ризиків, порядок і періодичність / терміни її надання користувачам;

7) процедуру ескалації ризиків, що встановлює порядок інформування ради, комітету з управління ризиками, виконавчого органу про порушення лімітів ризиків, ризик-апетиту;

8) процес погодження з радою змін до стратегії управління ризиками, декларації схильності до ризику, лімітів ризиків;

9) положення, що регламентують діяльність підрозділу з управління ризиками, з урахуванням вимог, установлених у главі 25 розділу VI цього Положення:

організаційну структуру підрозділу з управління ризиками (у разі його створення);

розподіл обов'язків, повноважень учасників системи управління ризиками та їх відповідальності щодо управління ризиками, що є добре інтегрованим в організаційну структуру надавача фінансових платіжних послуг та в процеси прийняття рішень;

порядок звітування перед радою;

10) підходи щодо здійснення стрес-тестування у випадках, визначених цим Положенням.

148. Надавач фінансових платіжних послуг має право включити до політики управління ризиками інші положення щодо управління ризиками додатково до встановлених у пункті 147 глави 24 розділу VI цього Положення, які не суперечать вимогам цього Положення.

149. Політика управління ризиками надавача фінансових платіжних послуг повинна відображати зв'язок системи управління ризиками із загальною системою корпоративного управління надавача фінансових платіжних послуг та його корпоративною культурою.

150. Надавач фінансових платіжних послуг зобов'язаний запровадити культуру управління ризиками з метою просування обізнаності членів ради та членів колегіального виконавчого органу, а також інших працівників надавача фінансових платіжних послуг (включаючи осіб, які виконують функції або окремі завдання та процеси в межах функцій на аутсорсингу) щодо ризиків, ризик-апетиту, стратегії управління ризиками на всіх організаційних рівнях, що сприяє:

1) усвідомленню ризик-апетиту та пов'язаних із ним лімітів ризиків (включаючи ліміти ризиків, установлені для окремих підрозділів надавача фінансових платіжних послуг та в межах таких підрозділів);

2) послідовному впровадженню системи управління ризиками в усіх підрозділах / функціях надавача фінансових платіжних послуг;

3) підтриманню своєчасного (своєчасної) вимірювання (оцінки) та інформуванню про нові ризики, які можуть бути суттєвими для надавача фінансових платіжних послуг.

151. Надавач фінансових платіжних послуг зобов’язаний дотримуватися положень та вимог внутрішніх документів, що регулюють діяльність з управління ризиками.

25. Функція управління ризиками надавача фінансових платіжних послуг

152. Надавач фінансових платіжних послуг з метою впровадження системи управління ризиками зобов’язаний забезпечити створення та ефективне виконання функції управління ризиками. Підрозділ з управління ризиками забезпечує виконання функції з управління ризиками відповідно до вимог Закону про платіжні послуги та цього Положення.

153. Підрозділ з управління ризиками діє на підставі положення, що затверджується відповідальним органом, і підпорядковується головному ризик-менеджеру (у разі створення окремого підрозділу з управління ризиками). Головний ризик-менеджер підпорядковується відповідальному органу та звітує перед ним.

154. Головний ризик-менеджер несе відповідальність за виконання функцій підрозділом з управління ризиками.

155. Головний ризик-менеджер повинен відповідати вимогам щодо професійної придатності та ділової репутації, визначеним Положенням про авторизацію надавачів фінансових платіжних послуг.

156. Функція з управління ризиками передбачає:

1) забезпечення практичних заходів з ефективного функціонування системи управління ризиками, просування та підтримання культури управління ризиками;

2) сприяння впровадженню системи управління ризиками, надання допомоги керівникам надавача фінансових платіжних послуг та іншим підрозділам надавача фінансових платіжних послуг з метою ефективного функціонування системи управління ризиками в надавачі фінансових платіжних послуг;

3) здійснення моніторингу системи управління ризиками;

4) забезпечення своєчасного виявлення, вимірювання (оцінки), моніторингу, контролю та звітування щодо ризиків, визначених у політиці управління ризиками надавача фінансових платіжних послуг, та нових ризиків (потенційних, поки не виявлених), включаючи ризики, що виникають у зв'язку з політикою винагороди та іншими заохоченнями;

5) розроблення та підтримання в актуальному стані методик, інструментів та моделей, що використовуються надавачем фінансових платіжних послуг для вимірювання (оцінки) ризиків;

6) забезпечення моніторингу, контролю за наближенням величини ризиків до лімітів ризиків, надання рекомендацій раді та виконавчому органу та/або ініціювання рішень уповноважених органів щодо вжиття заходів для попередження їх порушень, пом'якшення ризиків та/або їх уникнення;

7) підготовку та подання звітів щодо ризиків раді, комітетам ради, виконавчому органу та іншим користувачам, які приймають рішення відповідно до внутрішніх документів з питань системи управління ризиками, та консультування керівників надавача фінансових платіжних послуг з питань управління ризиками, включаючи стратегічні питання;

8) складання профілю ризиків надавача фінансових платіжних послуг та здійснення його моніторингу;

9) забезпечення координації роботи з питань управління ризиками між структурними підрозділами / працівниками надавача фінансових платіжних послуг;

10) розроблення, участь у розробленні внутрішніх документів з питань управління ризиками;

11) інформування ради, комітету з управління ризиками та виконавчого органу щодо порушень лімітів ризиків, ризик-апетиту надавача фінансових платіжних послуг;

12) виконання завдань, визначених у внутрішніх документах надавача фінансових платіжних послуг (включаючи стратегію управління ризиками, політику управління ризиками);

13) забезпечення безперервності роботи підрозділу з управління ризиками надавача фінансових платіжних послуг.

157. Функція управління ризиками може передбачати виконання інших завдань і процедур, які не суперечать вимогам цього Положення.

158. Підрозділ з управління ризиками виконує покладену на нього функцію шляхом розроблення та контролю за впровадженням і виконанням вимог законодавства України, внутрішніх положень і процедур управління ризиками відповідно до стратегії та політики управління ризиками (включаючи ліміти ризиків), декларації схильності до ризиків.

26. Ліміти ризиків

159. Рада в межах системи управління ризиками має право делегувати комітету з управління ризиками, іншому визначеному радою органу повноваження щодо погодження на здійснення операцій, що призводять до перевищення лімітів ризиків. Система управління ризиками в разі такого делегування повинна передбачати затвердження радою процедури контролю за використанням таких делегованих повноважень. Така процедура повинна обов’язково містити:

1) види ризиків, щодо яких дозволяються допустимі перевищення;

2) максимальний обсяг допустимих перевищень;

3) вимоги до документування рішення щодо допустимого перевищення;

4) порядок інформування ради щодо допустимих перевищень.

160. Надавач фінансових платіжних послуг має право встановлювати значення лімітів ризиків щодо окремих операцій або ризиків, включаючи значення лімітів ризиків в абсолютних значеннях та/або у відсотках до інших його показників (загального розміру активів, загальної суми зобов’язань, інших показників).

161. Надавач фінансових платіжних послуг накопичує інформацію щодо перевищення лімітів ризиків, на які отримано дозвіл у визначеному у внутрішніх документах надавача фінансових платіжних послуг (далі – допустимі перевищення), та порушень лімітів ризиків.

162. Відповідальний орган або орган, визначений статутом надавача фінансових платіжних послуг, проводить позачерговий перегляд значень лімітів ризиків, якщо допустимі перевищення або порушення лімітів ризиків є частими

або постійними відповідно до внутрішніх документів. Результатом такого перегляду можуть бути:

1) перегляд значень діючих лімітів ризиків;

2) перегляд делегованих повноважень щодо допустимих перевищень;

3) залишення значень лімітів ризиків без змін і затвердження плану заходів щодо запобігання їх подальшому перевищенню / порушенню.

27. Вимірювання ризиків

163. Надавач фінансових платіжних послуг для вимірювання (оцінки) ризиків зобов'язаний використовувати дані, що є достовірними, повними та точними.

164. Надавач фінансових платіжних послуг зобов'язаний оцінювати якісні і кількісні показники ризиків.

165. Надавач фінансових платіжних послуг зобов'язаний використовувати ефективні моделі та інструменти для вимірювання (оцінки) ризиків.

Надавач фінансових платіжних послуг під час обрання моделей та інструментів вимірювання (оцінки) ризиків ураховує:

1) особливості своєї діяльності, характер, обсяг операцій, профіль ризику;

2) потреби надавача фінансових платіжних послуг для здійснення своєї діяльності.

Обрання моделей та інструментів вимірювання (оцінки) ризиків здійснюється особами, які мають відповідний досвід та кваліфікацію.

166. Структура та модель даних щодо ризиків повинна бути деталізованою, а саме: надавати можливість здійснення ідентифікації та вимірювання ризиків, а також оцінки якості роботи моделей, інструментів з урахуванням особливостей діяльності надавача фінансових платіжних послуг, рівня складності, обсягу операцій, профілю ризику.

167. Надавач фінансових платіжних послуг забезпечує своєчасну актуалізацію даних, що використовуються для розрахунку величини ризиків, та здійснює перевірку їх достовірності, повноти, точності та відповідності, а також здійснює перегляд (не рідше ніж один раз на рік) ефективності застосовуваних ним моделей та інструментів оцінки ризиків.

168. Надавач фінансових платіжних послуг з метою вимірювання (оцінки) ризиків та визначення своєї спроможності протистояти факторам ризиків, на які такий надавач фінансових платіжних послуг наражається під час своєї діяльності або які можуть виникнути надалі, зобов'язаний здійснювати стрес-тестування та самостійно встановлювати їх наповнення, перелік ризиків, за якими здійснює стрес-тестування, методи, порядок та частоту їх проведення.

169. Надавач фінансових платіжних послуг регулярно (не рідше ніж один раз на рік) проводить бек-тестування моделей та/або інструментів оцінки ризиків шляхом порівняння фактичних даних з результатами, отриманими за допомогою моделі та/або інструменту. Надавач фінансових платіжних послуг має право не здійснювати бек-тестування моделей та/або інструментів оцінки ризиків за умови формування судження щодо недостатності історичних даних щодо таких моделей та інструментів.

28. Інформування та звітування з питань управління ризиками

170. Надавач фінансових платіжних послуг з метою виявлення, вимірювання (оцінки) ризиків, інформування про ризики, на які наражається надавач фінансових платіжних послуг, моніторингу та аналізу ефективності системи управління ризиками:

1) забезпечує агрегування даних щодо ризиків надавача фінансових платіжних послуг, оперативне та коректне вимірювання (оцінку) ризиків;

2) розробляє процедури обробки та агрегування даних щодо ризиків, формування звітності, політику конфіденційності та збереження такої інформації, а також доступу до неї.

171. Звітність про ризики надавача фінансових платіжних послуг повинна містити актуальну інформацію про ризики, своєчасно надаватися комітетам ради, відповідальному органу, виконавчому органу та іншим користувачам, які приймають рішення, та забезпечувати повне розуміння ними ситуації щодо рівня ризиків надавача фінансових платіжних послуг для прийняття своєчасних та адекватних управлінських рішень.

172. Уповноважені підрозділи / працівники надавача фінансових платіжних послуг складають звітність про ризики, яка повинна бути:

1) точною, вивіреною та достовірно відображати рівень прийнятого надавачем фінансових платіжних послуг ризику;

2) комплексною – охоплювати всі види ризиків надавача фінансових платіжних послуг, визначені політикою управління ризиками надавача фінансових платіжних послуг;

3) чіткою та інформативною – надавати чітку та однозначну інформацію, бути достатньо вичерпною для прийняття своєчасних та адекватних управлінських рішень;

4) періодичною та поширеною серед користувачів звітності про ризики із забезпеченням конфіденційності.

173. Відповідальний орган або орган, визначений статутом надавача фінансових платіжних послуг, комітети ради, виконавчий орган встановлюють періодичність складання та подання звітності про ризики як у звичайних умовах, так і в стресових ситуаціях. Періодичність подання звітності про ризики повинна бути не меншою ніж:

1) один раз на квартал для узагальнених звітів про ризики;

2) один раз на рік для детальних звітів про ризики.

174. Надавач фінансових платіжних послуг в узагальненому звіті про ризики зобов’язаний розкривати інформацію в розрізі кожного виду ризику (крім комплаєнс-ризику), визначеного відповідно до пунктів 127, 128 глави 23 розділу VI цього Положення, та обов’язково містити інформацію про:

1) узагальнені дані подій за видами ризиків, аналізу їх динаміки;

2) зміни до профілю ризиків надавача фінансових платіжних послуг, що відбулися;

3) дотримання встановленого ризик-апетиту та значень лімітів ризику;

4) виявлені нові ризики та результати їх вимірювання (оцінки);

5) результати вимірювання (оцінки) ризиків за новими продуктами, значними змінами в діяльності надавача фінансових платіжних послуг;

6) результати здійснення стрес-тестування (для операційного ризику);

7) пропозиції щодо застосування інструментів та методів для управління ризиками;

8) дотримання вимог внутрішніх документів з управління ризиками, включаючи інформацію щодо допустимих перевищень і порушень лімітів ризиків.

175. Надавач фінансових платіжних послуг у детальному(их) звіті (звітах) про ризики зобов'язаний розкривати інформацію в розрізі кожного виду ризику (крім комплаєнс-ризику), визначеного відповідно до пунктів 127, 128 глави 23 розділу VI цього Положення, та, крім інформації, зазначеної в пункті 174 глави 28 розділу VI цього Положення, повинен обов'язково містити таку інформацію:

1) результати оцінки профілю ризиків, які повинні містити опис видів ризиків, на які наражався надавач фінансових платіжних послуг протягом звітного періоду, та видів ризиків, що очікуються протягом періоду бізнес-планування надавача фінансових платіжних послуг, спосіб управління ризиками та якісну і кількісну інформацію за результатами вимірювання (оцінки) ризиків за кожним видом ризику;

2) результати здійснення стрес-тестування, методів і припущень, що були використані для стрес-тестування, аналізу чутливості до ризиків, якщо такий аналіз здійснювався;

3) опис заходів, що використовуються для вимірювання (оцінки) ризиків, включаючи будь-які суттєві зміни протягом звітного періоду;

4) опис методів та інструментів, що використовуються для управління ризиками, процесів моніторингу ефективності таких методів та інструментів, а також інформацію про методи та інструменти, що надавач фінансових платіжних послуг розглядає для використання з метою управління ризиками протягом періоду бізнес-планування надавача фінансових платіжних послуг, а також обґрунтування і вплив таких методів та інструментів зниження ризиків;

5) огляд значних подій за видами ризиків, результатів дослідження їх причин і заходів щодо запобігання таким подіям надалі;

6) про суттєву концентрацію ризиків протягом звітного періоду та суттєву концентрацію ризиків, що очікуються протягом періоду бізнес-планування надавача фінансових платіжних послуг;

7) висновки та пропозиції щодо внесення змін до системи управління ризиками надавача фінансових платіжних послуг з метою вдосконалення процедур управління ризиками;

8) результати бек-тестування моделей та інструментів оцінки ризиків.

176. Надавач фінансових платіжних послуг зобов'язаний мати технічні можливості для формування іншої звітності про ризики, крім регулярної звітності, визначеної в пункті 173 глави 28 розділу VI цього Положення:

1) під час стресових ситуацій;

2) у разі зміни потреб щодо необхідної управлінської інформації;

3) у разі отримання запитів Національного банку або інших регуляторних чи контролюючих органів.

177. Підрозділ з управління ризиками в разі значного підвищення ризику (наближення фактичних показників ризику до встановлених значень лімітів ризику, ризик-апетиту або потенційного їх порушення, або суттєвої зміни профілю ризиків надавача фінансових платіжних послуг) не пізніше наступного робочого дня інформує про це комітет з управління ризиками, відповідальний орган, виконавчий орган з метою прийняття своєчасних та адекватних управлінських рішень у межах процедури ескалації ризиків.

29. Особливості управління окремими видами ризиків надавача фінансових платіжних послуг

178. Управління ризиками надавача фінансових платіжних послуг за напрямом управління комплаєнс-ризиком надавача фінансових платіжних послуг додатково до положень, визначених у главах 23, 24 розділу VI цього Положення, повинно передбачати:

1) заходи, яких зобов'язаний вживати надавач фінансових платіжних послуг для розподілу чітких обов'язків щодо регулярного виявлення, документування та моніторингу відповідних ризиків, пов'язаних із комплаєнс-ризиком;

2) ідентифікацію комплаєнс-ризику, якому піддається надавач фінансових платіжних послуг або може піддаватися, його аналіз та оцінку використовуваних інструментів, методів управління комплаєнс-ризиком;

3) процедури збору та моніторингу подій, пов'язаних із комплаєнс-ризиком;

4) заходи і внутрішні процеси управління комплаєнс-ризиком;

5) ліміти ризику щодо основних сфер комплаєнс-ризику надавача фінансових платіжних послуг.

179. Управління комплаєнс-ризиком надавача фінансових платіжних послуг може передбачати інші заходи, крім визначених у пункті 178 глави 29 розділу VI цього Положення, які не суперечать вимогам цього Положення.

180. Управління ризиками надавача фінансових платіжних послуг за напрямом управління іншими суттєвими ризиками, визначеними відповідно до пункту 128 глави 23 розділу VI цього Положення, повинно здійснюватися відповідно до вимог, визначених у пунктах 178, 179 глави 29 розділу VI цього Положення, що застосовуються до управління комплаєнс-ризиком надавача фінансових платіжних послуг.

181. Особливості управління операційним ризиком та його складовими визначено в розділі VII цього Положення.

VII. Управління операційним ризиком

30. Загальні підходи до управління операційним ризиком

182. Надавач фінансових платіжних послуг створює ефективну систему управління операційним ризиком, що має повністю інтегруватися в загальну систему управління ризиками надавача фінансових платіжних послуг.

183. Надавач фінансових платіжних послуг оцінює операційний ризик з урахуванням його взаємозв’язку та впливу на інші ризики, що притаманні діяльності надавача фінансових платіжних послуг.

184. Надавач фінансових платіжних послуг самостійно визначає перелік кількісних показників ризик-апетиту до операційного ризику. Перелік повинен обов’язково містити показник максимального обсягу втрат від подій операційного ризику протягом наступних 12 місяців, який обчислюється для кожного окремого календарного року.

31. Політика та процедури управління операційним ризиком

185. Надавач фінансових платіжних послуг розробляє та періодично переглядає (не рідше одного разу на рік) політику, порядок та процедури

управління операційним ризиком та його складових з метою забезпечення їх ефективності та відповідності рівню ризик-апетиту до цього ризику.

186. Політика управління операційним ризиком може бути складовою політики управління ризиком надавача фінансових платіжних послуг або окремим документом і повинна містити:

1) мету, завдання та принципи управління операційним ризиком;

2) організаційну структуру процесу управління операційним ризиком з урахуванням розподілу функціоналу відповідно до трьох ліній захисту учасників процесу, їх повноважень, відповідальності та порядку взаємодії;

3) підходи щодо виявлення, вимірювання, моніторингу, контролю, звітування та пом’якшення операційного ризику;

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

5) політику страхування (якщо стратегія з управління ризиками передбачає такий підхід щодо передавання ризику);

6) підходи щодо здійснення стрес-тестування операційного ризику;

7) перелік та формат (інформаційне наповнення) форм управлінської звітності щодо операційного ризику, порядок і періодичність / терміни їх надання суб’єктам системи управління ризиками;

8) критерії звітування для подій операційного ризику та обґрунтування таких критеріїв;

9) внутрішні правила щодо ефективного зниження та контролю за операційними ризиками, кіберризиками та ризиками безпеки, пов’язаними з наданням платіжних послуг (виконанням платіжних операцій), які повинні також містити процедури забезпечення безпеки виконання платіжних операцій, вжиття заходів з ідентифікації помилкових і неналежних платіжних операцій (суб’єктів таких платіжних операцій) та заходів із запобігання або припинення таких платіжних операцій, реагування на інциденти безпеки, здійснення моніторингу та ведення бази даних операційних інцидентів, кіберінцидентів та інцидентів безпеки, пов’язаних із наданням платіжних послуг (виконанням платіжних операцій).

187. Порядок та процедури управління операційним ризиком повинні обов’язково містити:

1) процедури щодо виявлення, вимірювання, моніторингу, контролю, звітування та пом’якшення операційного ризику, включаючи інструменти / індикатори, що використовуються;

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

3) порядок та критерії класифікації подій операційного ризику за типами подій, бізнес-лініями;

4) критерії ідентифікації, класифікації та методологію розрахунку збитків від подій операційного ризику, пов’язаних із кредитним ризиком (за умови, що кошти для виконання платіжної операції надаються користувачу надавачем фінансових платіжних послуг на умовах кредиту);

5) критерії визначення груп пов’язаних операційних подій;

6) опис основних інструментів, що використовуються під час управління операційним ризиком, та порядок їх використання;

7) порядок управління операційним ризиком, що властивий процесу співпраці з аутсорсерами;

8) чітке розмежування функцій управління операційним ризиком та комплаєнс-ризиком з метою уникнення їх дублювання;

9) порядок обміну інформацією між учасниками процесу управління операційним ризиком, включаючи види, форми і терміни надання інформації;

10) програму проведення стрес-тестування операційного ризику;

11) порядок складання та перевірки достовірності регуляторної звітності щодо операційного ризику, що подається до Національного банку.

188. Надавач фінансових платіжних послуг розробляє та впроваджує процедури контролю за повнотою та якістю даних про події операційного ризику надавача фінансових платіжних послуг, що передбачають:

1) розподіл обов’язків та відповідальності між підрозділами надавача фінансових платіжних послуг щодо контролю за повнотою та якістю даних про події операційного ризику надавача фінансових платіжних послуг під час їх збору, унесення до бази внутрішніх подій операційного ризику та подальшої перевірки;

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

189. Надавач фінансових платіжних послуг забезпечує управління операційним ризиком, дотримуючись моделі трьох ліній захисту.

32. Кіберризики та ризики безпеки

190. Надавач фінансових платіжних послуг створює ефективні механізми управління кіберризиками та ризиками безпеки як складовими операційного ризику під час провадження діяльності з надання платіжних послуг з урахуванням впливу на інші ризики, притаманні діяльності надавача фінансових платіжних послуг.

191. Система управління кіберризиками та ризиками безпеки повинна забезпечувати виявлення, вимірювання, моніторинг, контроль, звітування та мінімізацію (зниження до контрольованого рівня) таких ризиків, на які наражається надавач фінансових платіжних послуг, як наявних (реалізованих, поточних), так і потенційних (нереалізованих).

192. Відповідно до своєї системи управління кіберризиками та ризиками безпеки надавач фінансових 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, а також 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.

193. Політика управління кіберризиками та ризиками безпеки надавача фінансових платіжних послуг може бути складовою політики управління операційним ризиком або окремим документом та повинна обов’язково містити:

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

2) організаційну структуру процесу управління кіберризиками та ризиками безпеки з урахуванням розподілу функціоналу учасників процесу відповідно до трьох ліній захисту, їх повноважень, відповідальності та порядку взаємодії;

3) порядок взаємодії між учасниками процесу управління кіберризиками та ризиками безпеки;

4) підходи надавача фінансових платіжних послуг до управління кіберризиками та ризиками безпеки;

5) механізми для встановлення рівня ризиків, які надавач фінансових платіжних послуг уважає допустимими під час надання платіжної послуги з урахуванням усіх бізнес-процесів, що забезпечують надання цієї послуги (далі – рівень ризиків безпеки);

6) наслідки недотримання політики управління кіберризиками та ризиками безпеки персоналом надавача платіжних послуг аутсорсерами, які мають доступ до інформаційної інфраструктури надавача фінансових платіжних послуг (включаючи постачальників послуг технічного характеру, що залучаються надавачем фінансових платіжних послуг на умовах аутсорсингу);

7) процедури та критерії з виявлення, аналізу та оцінки (вимірювання), моніторингу, контролю, звітування та зниження кіберризиків та ризиків безпеки, а також моніторингу загроз їх виникнення.

194. Політика управління кіберризиками та ризиками безпеки надавача фінансових платіжних послуг визначає:

1) необхідність проведення не рідше одного разу на рік аналізу та оцінки впровадженої політики управління кіберризиками та ризиками безпеки платіжних послуг та можливих порушень;

2) відповідність заходів з управління кіберризиками та ризиками безпеки платіжних послуг цілям заходів інформаційної безпеки та кібербезпеки надавача фінансових платіжних послуг;

3) наявність планів реагування на кіберінциденти та інциденти безпеки платіжних послуг з урахуванням можливих сценаріїв.

195. Надавач фінансових платіжних послуг зобов'язаний розробляти, документувати та впроваджувати порядок і процедури управління кіберризиками та ризиками безпеки надавача фінансових 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 серйозних збоїв і невиправданих затримок.

Надавач фінансових платіжних послуг не рідше одного разу на рік переглядає політику управління кіберризиками та ризиками безпеки щодо можливості оновлення / внесення змін перед упровадженням змін до інформаційної інфраструктури, процесів або процедур, а також оновлює / вносить зміни до політики управління кіберризиками та ризиками безпеки після кожного інциденту безпеки рівнів критичності "високий (помаранчевий)", "критичний (червоний)", "надзвичайний (чорний)", визначених у пункті 201 глави 33 розділу VII цього Положення.

196. Порядки та процедури управління кіберризиками та ризиками безпеки надавача фінансових платіжних послуг повинні обов'язково містити:

1) затверджені рівні допустимого ризику для кіберризиків та ризиків безпеки надавача фінансових платіжних послуг;

2) визначення та опис основних інструментів та індикаторів, що використовуються надавачем фінансових платіжних послуг в управлінні кіберризиками та ризиками безпеки, та порядок їх використання;

3) процедуру та методику оцінки кіберризиків та ризиків безпеки;

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

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

6) опис засобів контролю та порядок моніторингу кіберризиків та ризиків безпеки;

7) порядок обміну інформацією між учасниками процесу управління кіберризиками та ризиками безпеки, включаючи визначення видів, форм і строків подання управлінської звітності щодо кіберризиків та ризиків безпеки.

197. Оцінка кіберризиків та ризиків безпеки здійснюється надавачем фінансових платіжних послуг за допомогою інструментів, визначених для оцінки операційного ризику із зазначеною для цих інструментів періодичністю, інструментів, що застосовуються надавачем фінансових платіжних послуг у межах впровадженої системи управління безпекою, або за допомогою інших інструментів, визначених надавачем фінансових платіжних послуг, не рідше одного разу на рік.

198. Надавач фінансових платіжних послуг забезпечує впровадження задокументованих і затверджених процесів та процедур щодо:

1) забезпечення безперервності функціонування інформаційної інфраструктури;

2) управління інцидентами / 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.

199. Процедура забезпечення безпеки надавача фінансових 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 фінансових платіжних послуг;

5) процес безпечного видалення локальних або збережених зовні даних, які надавачу фінансових 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.

33. Операційні інциденти, кіберінциденти та інциденти безпеки

200. Надавач фінансових платіжних послуг зобов’язаний забезпечити розроблення, документування та періодичне оновлення політики управління інцидентами під час надання платіжних послуг відповідно до Положення про захист інформації та кіберзахист учасниками платіжного ринку, затвердженого постановою Правління Національного банку України від 19 травня 2021 року № 43 (зі змінами) (далі – Положення про захист інформації та кіберзахист).

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

1) некритичний (білий);

2) низький (зелений);

3) середній (жовтий);

4) високий (помаранчевий);

5) критичний (червоний);

6) надзвичайний (чорний).

202. Рівні критичності, визначені в пункті 201 глави 33 розділу VII цього Положення, попередньо визначаються надавачем платіжних послуг, який зафіксував інцидент безпеки, та обов'язково підтверджуються (уточнюються за потреби) Національним банком.

203. Надавач фінансових платіжних послуг зобов'язаний у довільній формі повідомляти Національний банк про інциденти, які відповідають рівням критичності:

1) середній (жовтий) – протягом п'яти робочих днів із дня, коли було зафіксовано відповідний інцидент;

2) високий (помаранчевий), критичний (червоний) та надзвичайний (чорний) – негайно.

204. Повідомлення, що стосується кіберінцидентів та інцидентів безпеки, здійснюється в строки та спосіб, визначені Положенням про захист інформації та кіберзахист.

205. Повідомлення, що стосується операційних інцидентів, здійснюється в спосіб, визначений у пункті 230 глави 37 розділу VIII цього Положення.

34. Ліміти операційного ризику

206. Надавач фінансових платіжних послуг установлює ліміти (обмеження) для операційного ризику в межах затвердженого ризик-апетиту.

Надавач фінансових платіжних послуг також установлює ліміти для управління різними джерелами концентрації ризиків.

207. Надавач фінансових платіжних послуг установлює значення лімітів операційного ризику у відсотках до регулятивного капіталу надавача фінансових платіжних послуг на останню звітну дату. Надавач фінансових платіжних послуг має право встановлювати значення лімітів ризиків щодо окремих операцій або ризиків в абсолютних значеннях та/або у відсотках до інших показників надавача фінансових платіжних послуг.

208. Надавач фінансових платіжних послуг:

1) визначає порядок установлення значень лімітів ризиків та контролю за їх дотриманням у своїй політиці управління операційним ризиком;

2) переглядає значення лімітів ризиків у разі змін ринкових умов або плану діяльності надавача фінансових платіжних послуг, але не рідше ніж один раз на рік. Перегляд здійснюється на підставі пропозицій бізнес-підрозділів надавача фінансових платіжних послуг та підрозділу з управління ризиками;

3) розробляє процедуру ескалації порушень лімітів ризиків, яка повинна містити:

форму та порядок інформування про порушення лімітів ризиків ради, комітету з управління ризиками, виконавчого органу;

порядок погодження здійснення операцій надавача фінансових платіжних послуг, що призводять до перевищення лімітів ризиків (допустимих перевищень), із зазначенням видів ризиків, щодо яких дозволяються допустимі перевищення, максимального обсягу допустимого перевищення, вимог до документування рішення щодо допустимого перевищення, порядку інформування ради щодо допустимих перевищень.

209. Підрозділ з управління ризиками в порядку, визначеному внутрішніми документами щодо ескалації порушень лімітів ризиків, якомога швидше після виявлення порушення ліміту ризику інформує раду, комітет з управління ризиками, виконавчий орган щодо такого порушення.

210. Відповідальний орган проводить позачерговий перегляд значень лімітів, якщо допустимі перевищення або порушення лімітів ризиків є частими або постійними відповідно до внутрішніх документів. Результатом такого перегляду можуть бути:

1) перегляд значень діючих лімітів;

2) перегляд делегованих повноважень щодо допустимих перевищень;

3) залишення значень лімітів без змін та затвердження плану заходів щодо запобігання їх подальшому перевищенню / порушенню.

35. Безперервність надання платіжних послуг

211. Надавач фінансових платіжних послуг із метою забезпечення належного управління ризиками розробляє методологію забезпечення безперервності надання платіжних послуг, яка включає:

1) політику заходів із забезпечення безперервності надання платіжних послуг;

2) процедуру аналізу впливу негативних факторів на бізнес-процеси надавача фінансових платіжних послуг;

3) план забезпечення безперервності надання платіжних послуг.

212. Політика заходів із забезпечення безперервності надання платіжних послуг повинна обов’язково містити:

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

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

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

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

213. Процедура аналізу впливу негативних факторів на бізнес-процеси надавача фінансових платіжних послуг (далі – 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 збою / переривання діяльності (англійською мовою – recovery time objective);

2) максимально допустимого проміжку часу, за який можлива втрата критичних даних надавача фінансових платіжних послуг у разі збою / відмови систем та сервісів інформаційно-комунікаційних технологій (англійською мовою – recovery point objective).

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

215. Надавач фінансових платіжних послуг у межах здійснення аналізу впливу забезпечує послідовний та комплексний аналіз вразливості процесів, систем та сервісів інформаційно-комунікаційних технологій надавача фінансових платіжних послуг до різних типів імовірних сценаріїв переривання діяльності, включаючи сценарій кібератаки. Надавач фінансових платіжних послуг здійснює кількісну та якісну оцінку ймовірного фінансового, операційного та репутаційного впливу сценаріїв на діяльність надавача фінансових платіжних послуг, використовуючи внутрішні та зовнішні дані.

216. Надавач фінансових платіжних послуг використовує результати аналізу впливу негативних факторів на процеси надавача фінансових платіжних послуг для встановлення цілей і пріоритетів під час розроблення плану забезпечення безперервності надання платіжних послуг. Залишкові ризики переривання діяльності (після оцінки надавачем фінансових платіжних послуг впливу застосування заходів, передбачених планом забезпечення безперервності надання платіжних послуг) повинні перебувати в межах затвердженого надавачем фінансових платіжних послуг ризик-апетиту.

217. Надавач фінансових платіжних послуг із метою забезпечення належного управління ризиками розробляє план забезпечення безперервності надання платіжних послуг, який уключає:

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

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

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

4) заходи з відновлення діяльності для критичних процесів надавача фінансових платіжних послуг;

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

36. Стрес-тестування операційного ризику

218. Надавач фінансових платіжних послуг здійснює не рідше одного разу на рік стрес-тестування операційного ризику для різних короткострокових і довгострокових стрес-сценаріїв, що можуть реалізуватися як для надавача фінансових платіжних послуг, так і для ринку в цілому, з метою виявлення причин можливих втрат унаслідок реалізації операційного ризику та оцінки відповідності результатів здійснення стрес-тестування встановленому рівню ризик-апетиту до операційного ризику.

219. Результатом здійснення стрес-тестування операційного ризику має бути визначення величини можливих втрат надавача фінансових платіжних послуг.

220. Вимоги глави 36 розділу VII цього Положення не поширюються на надавачів фінансових платіжних послуг, які згідно з критеріями, наведеними в Законі України “Про бухгалтерський облік та фінансову звітність в Україні”, належать до мікропідприємств.

221. Надавач фінансових платіжних послуг під час здійснення стрес-тестування використовує метод сценарного аналізу.

222. Надавач фінансових платіжних послуг проводить сценарний аналіз з урахуванням суджень працівників підрозділів першої лінії захисту та працівників підрозділу з управління ризиками щодо:

1) імовірного збільшення частоти (кількості) подій та/або обсягу операційних збитків порівняно зі статистикою, що міститься в базі внутрішніх подій операційного ризику;

2) виникнення нових подій операційного ризику внаслідок упровадження нових або внесення значних змін у діючі процеси;

3) виникнення подій операційного ризику зі значним рівнем втрат та низькою імовірністю настання.

VIII. Порядок контролю Національного банку за дотриманням вимог до системи управління

37. Порядок подання звітів та інших документів до Національного банку щодо виконання окремих ключових функцій надавача фінансових платіжних послуг

223. Надавач фінансових платіжних послуг зобов’язаний регулярно подавати до Національного банку протягом 15 робочих днів місяця, наступного за звітним періодом:

1) звіт про роботу підрозділу внутрішнього аудиту (за перше півріччя та рік) за формою згідно з додатком 2 до цього Положення;

2) звіт щодо комплаєнс-ризику, передбачений главою 18 розділу IV цього Положення;

3) звітність про ризики надавача фінансових платіжних послуг, передбачену главою 28 розділу VI цього Положення.

224. Підрозділ внутрішнього аудиту подає до Національного банку письмове повідомлення, підготовлене відповідно до підпункту 11 пункту 114 глави 20 розділу V цього Положення, та інші документи (за потреби).

225. Надавач фінансових платіжних послуг після настання технічного збою або інших невідворотних обставин, які об’єктивно унеможливили виконання надавачем фінансових платіжних послуг вимог законодавства України (далі – технічний збій або інші невідворотні обставини), зобов’язаний документально зафіксувати інформацію про:

1) дату та час настання технічного збою або інших невідворотних обставин;

2) тривалість технічного збою або інших невідворотних обставин;

3) причини настання технічного збою або інших невідворотних обставин;

4) види послуг, на які вплинуло настання технічного збою або інших невідворотних обставин;

5) оцінку впливу технічного збою або інших невідворотних обставин на безперервність надання платіжних послуг;

6) заходи, ужиті для відновлення діяльності та недопущення надалі настання технічного збою або інших невідворотних обставин.

226. Надавач фінансових платіжних послуг у разі настання істотного технічного збою або істотних інших невідворотних обставин зобов'язаний у порядку, строки та спосіб, визначені цим Положенням, повідомити Національний банк про факт настання істотного технічного збою або істотних інших невідворотних обставин.

227. Надавач фінансових платіжних послуг зобов'язаний протягом трьох робочих днів після настання істотного технічного збою або істотних інших невідворотних обставин надавати Національному банку інформацію, зазначену в пункті 225 глави 37 розділу VIII цього Положення.

228. Інформація про настання істотного технічного збою або істотних інших невідворотних обставин надсилається надавачем фінансових платіжних послуг Національному банку:

1) засобами системи електронної пошти Національного банку (у разі підключення);

2) на офіційну електронну поштову скриньку Національного банку nbu@bank.gov.ua;

3) іншими засобами електронного зв'язку, які використовуються Національним банком для електронного документообігу;

4) засобами поштового зв'язку в паперовій формі (у разі неможливості внаслідок настання істотного технічного збою або істотних інших невідворотних обставин надсилання інформації іншими способами).

229. Головний комплаєнс-менеджер повідомляє Національний банк про підтверджені факти неприйнятної поведінки в надавачі фінансових платіжних послуг / порушення в діяльності надавача фінансових платіжних послуг та конфлікти інтересів, що виникли в надавачі фінансових платіжних послуг, якщо відповідальним органом не були застосовані заходи, що забезпечили їх усунення. Інформація про підтверджені факти неприйнятної поведінки в надавачі фінансових платіжних послуг / порушення в діяльності надавача фінансових платіжних послуг та про конфлікти інтересів, що виникли в надавачі фінансових платіжних послуг, надається структурному підрозділу Національного банку, що здійснює безвиїзний нагляд за надавачем фінансових платіжних послуг.

230. Надавач фінансових платіжних послуг, інші особи подають до Національного банку документи / інформацію, подання яких передбачено цим Положенням, в один із таких способів:

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

2) у формі електронного документа, підписаного шляхом накладання КЕП, або електронної копії документа, засвідченої відповідно керівником надавача фінансових платіжних послуг / головним внутрішнім аудитором КЕП, – 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.

231. Надавач фінансових платіжних послуг несе відповідальність за повноту та достовірність даних, що містяться в поданих до Національного банку документах.

232. Документи, що подаються до Національного банку відповідно до цього Положення, мають викладатися українською мовою, не містити виправлень і неточностей, а також розбіжностей між відомостями, викладеними в них.

233. Паперові копії документів, що подаються до Національного банку відповідно до цього Положення, повинні засвідчуватися в такому порядку:

1) копія документа, виданого уповноваженим державним органом, засвідчується органом, який видав цей документ, або нотаріально;

2) копія документа фізичної особи засвідчується підписом такої особи або її уповноваженого представника;

3) копія документа юридичної особи засвідчується підписом її уповноваженого представника.

234. Пакет документів, що подається до Національного банку відповідно до цього Положення, повинен містити документ, що підтверджує повноваження уповноваженого представника, відповідальної особи (крім керівника юридичної особи).

235. Національний банк у разі наявності розбіжностей між даними, що містяться в документах у паперовій формі і в електронних документах чи електронних копіях документів, надає перевагу даним, наведеним у документах на паперових носіях. Національний банк в особі уповноваженої посадової особи має право вимагати від надавача фінансових платіжних послуг, інших осіб надання пояснень щодо розбіжностей між документами на паперових носіях та електронними документами чи електронними копіями документів, а також усунення цих розбіжностей.

236. Національний банк в особі уповноваженої посадової особи Національного банку має право здійснювати офіційну комунікацію із надавачем фінансових платіжних послуг, іншими особами засобами корпоративної електронної пошти (e-mail) Національного банку (шляхом надсилання повідомлення з офіційної електронної поштової скриньки Національного банку nbu@bank.gov.ua) під час розгляду пакета документів. Така комунікація може містити:

1) запитування додаткової інформації, документів і пояснень, потрібних для прийняття рішення згідно з цим Положенням;

2) отримання інформації, пояснень, додаткових документів, потрібних для прийняття рішення згідно з цим Положенням, у вигляді електронних документів та/або електронних копій документів;

3) надсилання повідомлень про рішення, прийняті Національним банком відповідно до цього Положення.

38. Порядок здійснення Національним банком контролю за дотриманням вимог до системи управління надавача фінансових платіжних послуг

237. Національний банк здійснює контроль відповідно до вимог Закону про платіжні послуги та інших законів 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, Положенням про здійснення безвиїзного нагляду на платіжному ринку, за дотриманням надавачем фінансових платіжних послуг, ключовими особами та/або особами, на яких покладено виконання ключових функцій у надавачі фінансових платіжних послуг, вимог цього Положення, здійснює оцінку організації та належного функціонування системи внутрішнього контролю. Національний банк під час здійснення контролю та оцінки має право використовувати професійне судження.

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

1) аналіз діяльності надавача фінансових платіжних послуг, внутрішніх документів щодо управління ризиками, результатів щорічної самооцінки;

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

3) інтерв’ю з керівниками надавача фінансових платіжних послуг та іншими працівниками надавача фінансових платіжних послуг;

4) оцінку відповідності внутрішніх документів надавача фінансових платіжних послуг вимогам цього Положення;

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

239. Національний банк у межах повноважень має право письмово вимагати від надавача фінансових платіжних послуг, ключових осіб та/або осіб, на яких покладено виконання ключових функцій у надавачі фінансових платіжних послуг, з наведенням обґрунтування такої вимоги копії документів, додаткову інформацію, документи та звіти, визначені цим Положенням, а також письмові пояснення щодо системи управління надавача фінансових платіжних послуг.

240. 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).

Додаток 1
до Положення про вимоги до
системи управління надавача
фінансових платіжних послуг
(пункт 57 глави 10 розділу III)

Перелік питань щодо внутрішнього контролю,
які повинні врегульовуватися у внутрішніх документах
надавача фінансових платіжних послуг

1. Організаційна структура надавача фінансових платіжних послуг, завдання, функції, повноваження органів управління та структурних підрозділів надавача фінансових платіжних послуг, включаючи повноваження щодо здійснення внутрішнього контролю.

2. Порядок розподілу та делегування повноважень у надавачі фінансових платіжних послуг.

3. Перелік та опис ключових процесів, щодо яких здійснюється внутрішній контроль, включаючи заходи та форми такого контролю.

4. Облікова політика надавача фінансових платіжних послуг.

5. Правила здійснення контролю за повнотою і точністю облікової інформації та достовірністю звітності надавача фінансових платіжних послуг, здійснення планування ефективного використання фінансових ресурсів із метою досягнення цілей діяльності надавача фінансових платіжних послуг.

6. Перелік функцій, що не має права виконувати один працівник надавача фінансових платіжних послуг та які потребують додаткового рівня контролю.

7. Регламенти / порядки складання звітності (фінансової, регуляторної, управлінської, податкової).

8. Правила підготовки, погодження та укладання надавачем фінансових платіжних послуг договорів.

9. Порядок здійснення відповідальним органом, виконавчим органом та працівниками надавача фінансових платіжних послуг внутрішніх і зовнішніх комунікацій, включаючи обмін інформацією / документами.

10. Правила / порядок здійснення документообігу, включаючи порядок формування та зберігання документів, що утворюються в діяльності надавача фінансових платіжних послуг.

11. Правила ведення архівів документації надавача фінансових платіжних послуг, включаючи електронні документи.

12. Перелік інформації з обмеженим доступом, порядок використання та розкриття такої інформації, включаючи порядок та процедури захисту персональних даних працівників і користувачів надавача фінансових платіжних послуг.

13. Порядок надання, використання, контролю та скасування доступу працівників надавача фінансових платіжних послуг до інформаційних систем, включаючи віддалений доступ.

14. Порядок проведення резервування (копіювання) та архівування даних в інформаційних системах.

15. Порядок захисту інформації в інформаційних системах.

16. Процес подальшого контролю за якістю даних в інформаційних системах.

17. Правила використання працівниками надавача фінансових платіжних послуг корпоративної електронної пошти.

18. Порядок реєстрації, зберігання інформації про інциденти безпеки, управління інцидентами безпеки.

19. Порядок реєстрації, розгляду та опрацювання звернень до надавача фінансових платіжних послуг громадян, юридичних осіб, органів державної влади України та місцевого самоврядування.

20. Положення про систему внутрішнього контролю.

21. Види, періодичність та порядок здійснення заходів із контролю, структурні підрозділи / працівники, відповідальні за проведення заходів із контролю, види, періодичність та порядок підготовки звітів, періодичність, порядок та особи, уповноважені здійснювати розгляд звітів, процедури здійснення коригувальних заходів.

22. Порядок передавання надавачем фінансових платіжних послуг окремих функцій та/або окремих завдань / процесів у межах цих функцій на аутсорсинг, включаючи перелік та опис способів здійснення моніторингу та контролю за здійсненням таких функцій та/або окремих завдань / процесів.

23. Перелік та опис способів здійснення моніторингу та контролю за діяльністю відокремлених підрозділів.

24. Порядок залучення / призначення / звільнення / припинення повноважень осіб, на яких покладено виконання функцій другої та третьої ліній захисту.

25. Порядок підбору, найму, навчання, оцінки працівників надавача фінансових платіжних послуг.

26. Порядок здійснення моніторингу як компонента системи внутрішнього контролю та визначення осіб, відповідальних за його проведення.

27. Порядок здійснення внутрішнього контролю за дотриманням законодавства України про захист прав споживачів фінансових послуг, внутрішніх документів та процесів надавача фінансових платіжних послуг.

28. Положення про внутрішній аудит надавача фінансових платіжних послуг.

29. Порядок та процедури внутрішнього аудиту надавача фінансових платіжних послуг [складання плану (зміни до плану) проведення внутрішніх аудиторських перевірок надавача фінансових платіжних послуг, оформлення результатів та документування, програми забезпечення та підвищення якості внутрішнього аудиту].

30. Стратегія управління ризиками надавача фінансових платіжних послуг.

31. Декларація схильності до ризиків надавача фінансових платіжних послуг.

32. Політика управління ризиками, включаючи ліміти ризиків надавача фінансових платіжних послуг.

Додаток 2
до Положення про вимоги до системи управління надавача фінансових платіжних послуг (підпункт 1 пункту 223 глави 37 розділу VIII)

Звіт
про роботу підрозділу внутрішнього аудиту надавача фінансових платіжних послуг

_____
(повне найменування надавача фінансових платіжних послуг у родовому відмінку, код за Єдиним державним реєстром підприємств і організацій України, місцезнаходження)
на “_____” _____ 20_____ року

№ з/п	Зміст питання / назва показника	Відповідь на питання / значення показника
1	2	3
1	Наявність внутрішніх положень, які регулюють діяльність підрозділу внутрішнього аудиту надавача фінансових платіжних послуг, у тому числі положення про внутрішній аудит надавача фінансових платіжних послуг (так чи ні). Якщо так, то надати їх назву та зазначити дату (число, місяць, рік) і номер рішення ради про затвердження відповідних документів	
2	Наявність документів, відповідно до яких підтверджено забезпечення організаційної незалежності (у разі внесення до них змін протягом звітного періоду) (зазначити дату їх направлення до Національного банку України)	
3	Інформація про керівника підрозділу внутрішнього аудиту надавача фінансових платіжних послуг: прізвище, власне ім’я та по батькові керівника підрозділу внутрішнього аудиту надавача фінансових платіжних послуг; дата (число, місяць, рік) і номер рішення ради про затвердження його кандидатури на посаду керівника	
4	Штатна та фактична чисельність працівників підрозділу внутрішнього аудиту надавача фінансових платіжних послуг. Перелік посад інших осіб, залучених для виконання функцій внутрішнього аудиту (у разі їх залучення) із наданням підтвердних документів щодо їх	

Продовження додатка 2
Продовження таблиці

1	2	3
	залучення, зокрема тих, у яких зазначено підстави необхідності такого залучення	
5	Кількість проведених аудиторських перевірок надавача фінансових платіжних послуг протягом звітного періоду, у тому числі у відокремлених підрозділах надавача фінансових платіжних послуг	
6	Інформація (висновки) про стан реалізації радою, виконавчим органом та керівниками структурних підрозділів надавача фінансових платіжних послуг рекомендацій (пропозицій) за результатами внутрішнього аудиту у звітному періоді. Така інформація (висновки), зокрема, має включати статистику щодо кількості проведених перевірок та рекомендацій (пропозицій), позитивні зрушення за результатами усунення найбільш вагомих порушень та недоліків у діяльності надавача фінансових платіжних послуг та причини в разі їх невиконання [зазначити, з яких питань рекомендації (пропозиції), що мали / мають найбільш матеріальний вплив та системний характер, виконані та з яких не виконані]	
7	Короткий опис проблем (недоліків) у діяльності надавача фінансових платіжних послуг, виявлених під час проведення аудиторських перевірок	
8	Заходи (рекомендації за результатами перевірки підрозділом внутрішнього аудиту надавача фінансових платіжних послуг), ужиті під час проведення аудиторських перевірок	
9	Інформація щодо розгляду радою звіту про виконання річного плану проведення аудиторських перевірок надавача фінансових платіжних послуг із підтвердженням щодо організаційної незалежності підрозділу внутрішнього аудиту надавача фінансових платіжних послуг (зазначити дату надання відповідного звіту до ради та прийняте нею рішення щодо цього звіту)	

Найменування посади Особистий підпис Власне ім’я ПРІЗВИЩЕ

Дата