



Правління Національного банку України
ПОСТАНОВА

27 червня 2025 року

Київ

№ 69

Про критичну інфраструктуру фінансового сектору

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статей 8–10, 12, 14, 19 Закону України “Про критичну інфраструктуру”, з метою нормативного врегулювання питань організації та забезпечення захисту об’єктів критичної інфраструктури Правління Національного банку України **постановляє**:

1. Затвердити:

1) Положення про критичну інфраструктуру фінансового сектору, що додається;

2) Зміни до Положення про організацію кіберзахисту в банківській системі України, затвердженого постановою Правління Національного банку України від 12 серпня 2022 року № 178 (зі змінами), що додаються.

2. Банкам, іншим особам, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторам платіжних систем, технологічним операторам платіжних послуг здійснити категоризацію об’єктів критичної інфраструктури протягом шести місяців із дня набрання чинності цією постановою.

3. Визнати такими, що втратили чинність:

1) постанову Правління Національного банку України від 30 листопада 2020 року № 151 “Про затвердження Положення про визначення об’єктів критичної інфраструктури в банківській системі України”;

2) пункт 2 постанови Правління Національного банку України від 12 серпня 2022 року № 178 “Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об’єктів критичної інфраструктури в банківській системі України”.

4. Контроль за виконанням цієї постанови покласти на заступника Голови Національного банку України Олексія Шабана.

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

Голова

Андрій ПИШНИЙ

Інд. 58

Положення
про критичну інфраструктуру фінансового сектору

I. Загальні положення

1. Це Положення розроблено відповідно до Законів України “Про критичну інфраструктуру” та “Про Національний банк України”.

2. Терміни в цьому Положенні вживаються в такому значенні:

1) адміністративна будівля – будівля головного офісу установи (частина будівлі), у якій розміщуються керівники установи, працівники підрозділів установи, які забезпечують надання основних послуг, здійснюють управління об’єктами критичної інфраструктури та забезпечують їх функціонування;

2) основна послуга – послуга, яка надається оператором критичної інфраструктури та віднесена законодавством у сфері захисту критичної інфраструктури до життєво важливих (основних) послуг та/або виконання життєво важливих функцій;

3) секторальний орган у сфері захисту критичної інфраструктури (далі – секторальний орган) – Національний банк України (далі – Національний банк), який визначений законодавством України відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у фінансовому секторі;

4) секторальний перелік об’єктів критичної інфраструктури фінансового сектору (далі – Секторальний перелік) – зведені відомості про ідентифіковані та категоризовані об’єкти критичної інфраструктури (далі – ОКІ) Національного банку, банків, інших осіб, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем, технологічних операторів платіжних послуг;

5) фінансовий сектор – Національний банк, банки, інші особи, що здійснюють діяльність на ринках небанківських фінансових послуг, державне

регулювання та нагляд за діяльністю яких здійснює Національний банк, оператори платіжних систем, технологічні оператори платіжних послуг.

Термін “уповноважений банк” вживається в цьому Положенні в значенні, наведеному в Положенні про передавання запасів готівки на зберігання до уповноважених банків та проведення операцій з ними, затвердженому постановою Правління Національного банку України від 17 вересня 2021 року № 95 (зі змінами).

Інші терміни в цьому Положенні вживаються в значеннях, наведених у Законах України “Про критичну інфраструктуру”, “Про банки і банківську діяльність”, “Про електронну ідентифікацію та електронні довірчі послуги”, “Про платіжні послуги”, “Про хмарні послуги”, “Про обов’язкове страхування цивільно-правової відповідальності власників наземних транспортних засобів” та нормативно-правових актах Національного банку.

3. Це Положення розроблено з метою унормування організації та забезпечення захисту ОКІ фінансового сектору і визначає:

1) порядок віднесення об’єктів банків, інших осіб, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем, технологічних операторів платіжних послуг (далі – установи) до ОКІ;

2) методику визначення механізмів та критерії віднесення ідентифікованих ОКІ фінансового сектору до однієї з категорій критичності;

3) порядок розроблення паспортів безпеки на ОКІ фінансового сектору.

4. Віднесення об’єктів інфраструктури Національного банку до ОКІ та їх категоризація здійснюються в порядку, визначеному Національним банком.

II. Порядок віднесення об’єктів фінансового сектору до критичної інфраструктури

5. До операторів критичної інфраструктури фінансового сектору (далі – Оператор) належать:

1) Національний банк;

2) банк, який визначений Національним банком як системно важливий;

3) уповноважений банк;

4) банк, який має статус кваліфікованого надавача електронних довірчих послуг, відомості про якого внесені до Довірчого списку за поданням засвідчувального центру;

5) оператор платіжної системи, яку Національний банк визначив системно важливою платіжною системою або важливою платіжною системою;

б) технологічний оператор платіжних послуг, якого Національний банк визначив важливим технологічним оператором платіжних послуг;

7) установа, яка є власником, держателем та адміністратором єдиної централізованої бази даних щодо обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів;

8) інші установи, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, визначені Операторами окремими рішеннями Національного банку, негативний вплив від знищення, пошкодження або порушення функціонування інфраструктури яких може суттєво вплинути на стале надання основних послуг у фінансовому секторі.

6. Оператор зобов'язаний ідентифікувати об'єкти інфраструктури, від яких залежить надання основних послуг Оператором, та віднести такі об'єкти до ОКІ.

До ОКІ Оператора обов'язково мають бути віднесені об'єкти, якими Оператор володіє на праві власності, оренди або на інших законних підставах, а саме:

1) адміністративні будівлі;

2) центри обробки даних;

3) сховища Національного банку (у тому числі приміщення касових вузлів), де зберігається готівка;

4) сховища уповноважених банків для зберігання запасів готівки Національного банку.

7. Оператор зобов'язаний здійснити категоризацію ОКІ відповідно до методики категоризації ОКІ фінансового сектору, визначеної в розділі III цього Положення.

8. Оператор своїм внутрішнім документом за підписом керівника Оператора створює комісію з ідентифікації та категоризації ОКІ Оператора (далі – Комісія).

Заступник керівника Оператора очолює Комісію, до складу якої входять представники підрозділів Оператора, які забезпечують виконання функцій з надання основних послуг, функціонування об'єктів, цивільного захисту, безпеки, фізичної охорони, інформаційної безпеки, кіберзахисту, безперервної діяльності, управління ризиками, а також фінансового підрозділу.

До складу Комісії за потреби також можуть залучатися представники інших підрозділів Оператора та представники секторального органу (за згодою).

9. Результати роботи Комісії оформляються актом категоризації об'єкта критичної інфраструктури фінансового сектору (далі – Акт), який складається у двох примірниках за формою, наведеною в додатку 1 до цього Положення.

10. Акт обов'язково повинен містити обґрунтування оцінки рівнів негативного впливу в разі знищення, пошкодження ОКІ або порушення його функціонування, що розраховуються згідно із секторальними й міжсекторальними критеріями, наведеними в додатках 2 і 3 до цього Положення.

11. Акт оформляється на кожний ідентифікований ОКІ, підписується головою, членами Комісії та затверджується керівником Оператора.

12. Оператор у разі розміщення кількох ОКІ Оператора в одній будівлі або в різних будівлях на одній території, які мають єдиний периметр безпеки та систему охорони, має право розглядати їх як один ОКІ зі складанням загального Акта на такий об'єкт.

13. Відомості, що містяться в Акті, є інформацією з обмеженим доступом, вимоги щодо захисту якої встановлені законодавством України, а додатки (за наявності) до Акта є невід'ємною його частиною.

14. Оператор надсилає Акт, затверджений його керівником, на погодження до секторального органу з урахуванням вимог законодавства з питань захисту інформації з обмеженим доступом.

Секторальний орган упродовж 20 робочих днів із дня отримання Акта розглядає отримані матеріали з урахуванням критеріїв віднесення об'єктів Оператора до ОКІ фінансового сектору, обґрунтування їх категорій критичності та приймає рішення про його погодження в порядку, визначеному цим Положенням.

15. Секторальний орган за наявності зауважень до Акта не пізніше ніж протягом двох робочих днів після завершення строку, зазначеного в пункті 14 розділу II цього Положення, повертає Акт на доопрацювання Оператору в порядку, визначеному Національним банком.

Оператор зобов'язаний протягом 10 робочих днів урахувати зауваження, забезпечити усунення недоліків та повторно направити Акт на погодження до секторального органу.

16. Секторальний орган має право додатково витребувати від Оператора необхідні документи, а Оператор зобов'язаний надати такі документи для підтвердження, обґрунтування та визначення категорії критичності ОКІ.

17. Один примірник погодженого Акта секторальний орган направляє Оператору. Секторальний орган та Оператор забезпечують збереження Акта протягом усього строку функціонування ОКІ та впродовж одного року після втрати об'єктом статусу ОКІ.

18. Секторальний орган на підставі затвердженого та погодженого Акта забезпечує внесення відомостей про ОКІ Оператора до Секторального переліку.

19. Секторальний орган після внесення відомостей про ОКІ до Секторального переліку подає повідомлення до уповноваженого органу у сфері захисту критичної інфраструктури України про внесення відомостей про ОКІ до Реєстру об'єктів критичної інфраструктури (далі – Реєстр).

20. Секторальний орган надсилає листа до Оператора з повідомленням про внесення відомостей про його ОКІ до Реєстру.

21. Оператор на підставі отриманого повідомлення від секторального (уповноваженого) органу зобов'язаний забезпечити виконання завдань, реалізацію прав та обов'язків Оператора, дотримання вимог, визначених Законом України “Про критичну інфраструктуру” та законодавством у сфері захисту критичної інфраструктури.

22. Оператор зобов'язаний упродовж десяти робочих днів письмово повідомити секторальний орган про зміну:

1) юридичної особи (власника) Оператора та/або ОКІ та/або його цільового призначення;

2) місця розташування ОКІ;

3) умов надання та виконання основної послуги Оператора та/або інших умов функціонування ОКІ, що можуть вплинути на категорію критичності ОКІ.

23. Оператор у разі виникнення умов, передбачених у пункті 22 розділу II цього Положення, зобов'язаний упродовж 10 робочих днів забезпечити повторну ідентифікацію та категоризацію ОКІ.

24. Оператор завчасно, але не менше ніж за 30 календарних днів до дати зміни стану ОКІ або його частини, інформує секторальний орган про наміри змінити цільове призначення, режим функціонування чи намір передати права на ОКІ.

25. Секторальний орган має право ініціювати здійснення Оператором повторної категоризації ОКІ в разі зміни законодавства у сфері захисту критичної інфраструктури та/або за результатами перевірки та/або оцінки стану захищеності ОКІ, та/або виникнення умов, передбачених у пункті 22 розділу II цього Положення.

III. Методика категоризації об'єктів критичної інфраструктури фінансового сектору

26. Установа здійснює ідентифікацію ОКІ в порядку, визначеному в розділі II цього Положення.

27. Категорія критичності ОКІ визначається на підставі аналізу та оцінки рівня негативного впливу внаслідок порушення або припинення функціонування об'єкта інфраструктури за сукупністю критеріїв, що визначають його соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, реалізації життєво важливих функцій та надання життєво важливих послуг, відповідно до:

1) секторальних критеріїв визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ, які наведено в додатку 2 до цього Положення (далі – секторальні критерії);

2) міжсекторальних критеріїв визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ, які наведено в додатку 3 до цього Положення (далі – міжсекторальні критерії).

28. Категорія ОКІ установи визначається за такою процедурою:

1) визначається рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ з використанням секторальних критеріїв, що здійснюється шляхом заповнення форми, наведеної в додатку 2 до цього Положення, та проставленням у графі “Оцінка КС_j” відповідного бала;

2) визначається рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ з використанням міжсекторальних критеріїв, що здійснюється шляхом заповнення форми, наведеної в додатку 3 до цього Положення, та проставленням у графі “Оцінка КМі” відповідного бала;

3) здійснюється розрахунок узагальненої нормованої оцінки рівня критичності ОКІ за формулою:

$$PK_{OKI} = \frac{KC_{max} + \sum KM_i}{68},$$

де PK_{OKI} – узагальнена нормована оцінка рівня критичності ОКІ;

KC_{max} – максимальний бал з усіх оцінок KC_j , які отримав ОКІ за секторальними критеріями стосовно однієї з n послуг, що надається ОКІ (додаток 2), де $j \in \{1, n\}$, які надає ОКІ;

$\sum KM_i$ – сума балів, які отримав ОКІ за всіма міжсекторальними критеріями (додаток 3), де $i \in \{1, 16\}$;

4) віднесення до певної категорії критичності здійснюється шляхом порівняння розрахованої узагальненої нормованої оцінки рівня критичності ОКІ (PK_{OKI}) з діапазонами значень оцінки рівня ОКІ, зазначених у колонці 4 таблиці підпункту 4 пункту 28 розділу III цього Положення, та якщо оцінка потрапляє у відповідний діапазон значень, то об’єкту присвоюється відповідна категорія критичності ОКІ:

Таблиця

№	Категорія критичності ОКІ	Оцінка рівня критичності ОКІ	Діапазон значень оцінки рівня ОКІ
1	2	3	4
1	I категорія критичності	PK_{OKI}	від 0,9 до 1,0
2	II категорія критичності	PK_{OKI}	від 0,75 до 0,9
3	III категорія критичності	PK_{OKI}	від 0,53 до 0,75
4	IV категорія критичності	PK_{OKI}	від 0,2 до 0,53
5	Не критично	PK_{OKI}	від 0 до 0,2

;

5) результати розрахунків та визначення категорії ОКІ з відповідним обґрунтуванням оформляються Актом, форма та процедура оформлення якого визначені цим Положенням.

В Акті надається опис та обґрунтування рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування ОКІ за секторальними та міжсекторальними критеріями, що підкріплюється підтвердним документом, який містить відповідні відомості.

IV. Порядок розроблення та погодження паспортів безпеки на об'єкти критичної інфраструктури фінансового сектору

29. Оператор з метою проведення аналізу можливих загроз та мінімізації негативних наслідків для ОКІ, запобігання та попередження виникнення таких загроз розробляє паспорт безпеки на об'єкт критичної інфраструктури за формою, наведеною в додатку 4 до цього Положення (далі – паспорт безпеки ОКІ).

30. Оператор розробляє на кожний ОКІ паспорт безпеки ОКІ протягом трьох місяців з дня отримання від секторального органу повідомлення про внесення відомостей про об'єкт до Реєстру.

31. Відомості, що містяться в паспорті безпеки, є інформацією з обмеженим доступом, вимоги щодо захисту якої встановлені законодавством України.

32. Паспорт безпеки ОКІ повинен містити інформацію щодо:

- 1) загальної характеристики Оператора;
- 2) загальної характеристики ОКІ;
- 3) переліку послуг та їх надавачів (постачальників), які забезпечують функціонування ОКІ;
- 4) загроз та ризиків ОКІ;
- 5) заходів щодо забезпечення безпеки та стійкості ОКІ;
- 6) плану заходів із захисту критичної інфраструктури.

33. Паспорт безпеки ОКІ підписується особою, відповідальною за організацію захисту критичної інфраструктури Оператора, та затверджується керівником Оператора.

Факсимільне відтворення підпису за допомогою засобів механічного або іншого копіювання на паспорті безпеки ОКІ не допускається.

34. Паспорт безпеки ОКІ надсилається у двох примірниках до секторального органу із супровідним листом, підписаним керівником Оператора.

35. Секторальний орган розглядає паспорт безпеки ОКІ протягом 30 робочих днів з дня його отримання від Оператора і, якщо немає зауважень

(пропозицій), погоджує паспорт безпеки ОКІ та повертає один примірник Оператору.

36. Секторальний орган у разі наявності зауважень (пропозицій) до паспорта безпеки ОКІ повертає його Оператору з відповідним обґрунтуванням у порядку, визначеному Національним банком.

37. Оператор зобов'язаний протягом 10 робочих днів здійснити доопрацювання паспорта безпеки ОКІ з урахуванням отриманих від секторального органу зауважень та/або пропозицій та за результатами доопрацювання направити на погодження до секторального органу в порядку, визначеному в пункті 34 розділу IV цього Положення.

38. Секторальний орган після погодження паспорта безпеки ОКІ подає уповноваженому органу у сфері захисту критичної інфраструктури повідомлення про його погодження (перегляд).

Паспорт безпеки ОКІ Національного банку затверджується заступником Голови Національного банку, на якого покладено обов'язки з організації роботи з формування та реалізації Національним банком державної політики у сфері захисту критичної інфраструктури.

39. Паспорт безпеки ОКІ переглядається на виконання вимог до захисту ОКІ з дотриманням положень, визначених у пунктах 29–37 розділу IV цього Положення, один раз на рік (до 31 січня року, наступного за звітним) та:

- 1) у разі перегляду проектних загроз національного, секторального та/або об'єктового (у разі наявності) рівня;
- 2) у разі зміни вимог до захисту ОКІ;
- 3) за результатами повторної ідентифікації та категоризації ОКІ.

40. Секторальний орган та Оператор забезпечують збереження паспортів безпеки ОКІ протягом усього строку функціонування ОКІ та впродовж одного року після втрати об'єктом статусу ОКІ.

Додаток 1
до Положення про критичну
інфраструктуру фінансового сектору
(пункт 9 розділу II)

Форма акта
категоризації об'єкта критичної інфраструктури фінансового сектору

(Обрати значення грифа)
Прим. № __

ПОГОДЖУЮ

ЗАТВЕРДЖУЮ

Найменування посади відповідальної
особи секторального органу

Найменування посади керівника
Оператора

Особистий підпис

Власне ім'я
ПРИЗВИЩЕ

Особистий підпис

Власне ім'я
ПРИЗВИЩЕ

Дата

Дата

АКТ

категоризації об'єкта критичної інфраструктури фінансового сектору

_____ (назва об'єкта)

Відповідно до методики категоризації об'єктів критичної інфраструктури фінансового сектору, визначеної Національним банком України, комісією, створеною відповідно до _____ (реквізити внутрішнього документа Оператора), здійснено ідентифікацію об'єкта критичної інфраструктури _____ (найменування Оператора) та проведено його категоризацію.

1. Загальна інформація про об'єкт критичної інфраструктури (далі – ОКІ):

Таблиця 1

№ з/п	Перелік обов'язкових відомостей щодо ОКІ	Відомості
1	2	3
1	Назва ОКІ (умовна, скорочена)	
2	Адреса фактичного місцезнаходження ОКІ	
3	Власник ОКІ (найменування юридичної особи, код за Єдиним державним реєстром підприємств і організацій України (далі – ЄДРПОУ)	
4	Підсектор критичної інфраструктури	

1	2	3
5	Тип основної послуги, яку надає ОКІ	
6	Життєво важлива послуга / функція	
7	Оператор критичної інфраструктури (повне найменування юридичної особи)	
8	Код за ЄДРПОУ Оператора	
9	Зареєстроване місцезнаходження Оператора	
10	Фактична адреса Оператора	
11	Форма власності Оператора	
12	КВЕД основної діяльності Оператора	

2. Загальний опис ОКІ (його складових), основні послуги та функції, що надаються (виконуються): _____.

3. Оцінка критичності ОКІ:

1) опис та обґрунтування рівня негативного впливу в разі знищення, пошкодження або порушення функціонування ОКІ за секторальними критеріями згідно з додатком 2 до Положення про критичну інфраструктуру фінансового сектору (далі – Положення) з подальшим внесенням відповідних показників до таблиці 2:

Таблиця 2

№ з/п	Фактор негативного впливу	Показник рівня негативного впливу ОКІ
1	2	3
1	Припинення або порушення процесу надання банківських послуг унаслідок знищення, пошкодження або порушення функціонування ОКІ	КС ₁
2	Припинення або порушення процесу надання платіжних послуг унаслідок знищення, пошкодження або порушення функціонування ОКІ	КС ₂
3	Втрата запасів готівки Національного банку України та/або припинення операцій із запасами готівки Національного банку України внаслідок знищення, пошкодження або порушення функціонування ОКІ	КС ₃
4	Припинення або порушення процесу надання кваліфікованих електронних довірчих послуг унаслідок знищення, пошкодження або порушення функціонування ОКІ	КС ₄

1	2	3
5	Припинення надання небанківських фінансових послуг унаслідок знищення, пошкодження або порушення функціонування ОКІ	КС ₅
6	Максимальний бал за секторальними критеріями	КС _{max}

2) опис та обґрунтування рівня негативного впливу в разі знищення, пошкодження або порушення функціонування ОКІ за міжсекторальними критеріями згідно з додатком 3 до Положення з подальшим внесенням відповідних показників до таблиці 3:

Таблиця 3

№ з/п	Фактор негативного впливу	Показник рівня негативного впливу ОКІ
1	2	3
1	Заподіяння шкоди життю та здоров'ю людей: кількість населення, що може постраждати	КМ ₁
2	Заподіяння шкоди життю та здоров'ю людей: географічний масштаб	КМ ₂
3	Заподіяння шкоди навколишньому природному середовищу: економічні втрати	КМ ₃
4	Заподіяння шкоди навколишньому природному середовищу: географічний масштаб	КМ ₄
5	Заподіяння шкоди навколишньому природному середовищу: часовий період	КМ ₅
6	Припинення або порушення функціонування державних органів	КМ ₆
7	Негативний вплив на довіру людей до державних інституцій	КМ ₇
8	Заподіяння шкоди інтересам інших держав – партнерів України	КМ ₈
9	Заподіяння збитків оператору критичної інфраструктури (у відсотках від прогнозованого обсягу річного доходу за всіма видами діяльності)	КМ ₉
10	Заподіяння збитків державному бюджету (зниження доходів бюджету у відсотках від прогнозованої річної дохідної частини бюджету)	КМ ₁₀
11	Заподіяння збитків місцевим бюджетам (зниження доходів бюджету у відсотках від прогнозованої річної дохідної частини бюджету)	КМ ₁₁

1	2	3
12	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких самих основних послуг	КМ ₁₂
13	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	КМ ₁₃
14	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється на рівні (значущості) пункту управління або ситуаційного центру	КМ ₁₄
15	Припинення або порушення виробництва товарів, виконання робіт та надання послуг оборонного призначення, які є предметом оборонних закупівель, для забезпечення потреб сектору безпеки і оборони, а також інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони: зниження обсягів продукції (робіт, послуг) у визначений період часу (у відсотках)	КМ ₁₅
16	Припинення або порушення виробництва товарів, виконання робіт та надання послуг оборонного призначення, які є предметом оборонних закупівель, для забезпечення потреб сектору безпеки і оборони, а також інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони: збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (у відсотках від встановленого часу на виготовлення продукції)	КМ ₁₆
17	Сума балів за міжсекторальними критеріями	ΣКМ _i

4. Розрахунок узагальненої нормованої оцінки рівня критичності (РКокі), який здійснюється відповідно до підпункту 3 пункту 28 розділу III Положення.

5. Висновок.

Висновок про віднесення _____ до _____ категорії
(назва ОКІ) (категорія)

критичності на основі узагальненої нормованої оцінки рівня критичності ОКІ

відповідно до правила, наведеного в підпункті 4 пункту 28 розділу III Положення.

Голова комісії	Особистий підпис	Власне ім'я ПРІЗВИЩЕ
Члени комісії:	Особистий підпис	Власне ім'я ПРІЗВИЩЕ
	Особистий підпис	Власне ім'я ПРІЗВИЩЕ
	Особистий підпис	Власне ім'я ПРІЗВИЩЕ

Пояснення щодо заповнення додатка 1

1. У пункті 2 загальний опис надається для кожного виду ОКІ і повинен містити відомості про основні послуги, які надаються об'єктом, інформаційні системи, які забезпечують їх надання, підрозділи та кількість персоналу, який розміщується на об'єкті, середньостатистичну кількість готівки (визначається як середньорічна сума банкнот / монет), яка зберігається.

Додаток 2
до Положення про критичну
інфраструктуру фінансового
сектору
(пункт 10 розділу II)

Секторальні критерії
визначення рівня негативного впливу на надання основних послуг у разі
знищення, пошкодження або порушення функціонування ОКІ

I. Оцінка наслідків негативного впливу на надання основних послуг відповідно до секторальних критеріїв.

Таблиця

№ з/п	Тип основної послуги	Фактор негативного впливу	Рівень негативного впливу				Оцінка КС _i
			катастрофічні наслідки (4 бали)	критичні наслідки (3 бали)	значні наслідки (2 бали)	незначні наслідки (1 бал)	
1	2	3	4	5	6	7	8
1	Надання банківських послуг	Наслідком знищення, пошкодження або порушення функціонування ОКІ є припинення або порушення процесу надання банківських послуг	Системно важливий банк 3 категорії	Системно важливий банк 2 або 1 категорії	Інший системно важливий банк	Не застосовується	КС ₁

1	2	3	4	5	6	7	8
2	Надання платіжних послуг	Наслідком знищення, пошкодження або порушення функціонування ОКІ є припинення або порушення процесу надання платіжних послуг	Оператор системно важливої платіжної системи	Оператор важливої платіжної системи або важливий технологічний оператор платіжних послуг	Не застосовується	Не застосовується	КС ₂
3	Зберігання уповноваженими банками запасів готівки Національного банку та проведення операцій із ними	Наслідком знищення, пошкодження або порушення функціонування ОКІ є втрата запасів готівки Національного банку та/або припинення операцій із запасами готівки Національного банку	Більш як 50% ліміту запасів готівки на зберіганні в уповноваженому банку	Більш як 40% ліміту запасів готівки на зберіганні в уповноваженому банку	Більш як 30% ліміту запасів готівки на зберіганні в уповноваженому банку	Більш як 10% ліміту запасів готівки на зберіганні в уповноваженому банку	КС ₃

1	2	3	4	5	6	7	8
4	Надання кваліфікованих електронних довірчих послуг у банківській системі	Наслідком знищення, пошкодження або порушення функціонування ОКІ є припинення або порушення процесу надання кваліфікованих електронних довірчих послуг щодо обслуговування	Більш як 1 млн чинних кваліфікованих сертифікатів відкритих ключів клієнтів	Більш як 300 тис., але не більше 1 млн чинних кваліфікованих сертифікатів відкритих ключів клієнтів	Більш як 50 тис., але не більше 300 тис. чинних кваліфікованих сертифікатів відкритих ключів клієнтів	Не більше 50 тис. чинних кваліфікованих сертифікатів відкритих ключів клієнтів	КС ₄
5	Надання небанківських фінансових послуг	Наслідком знищення, пошкодження або порушення функціонування ОКІ є припинення надання небанківських фінансових послуг	Не застосовується	Оператор єдиної централізованої бази даних щодо обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів	Не застосовується	Не застосовується	КС ₅

II. Пояснення щодо застосування критеріїв

1. Оцінювання здійснюється шляхом вибору варіанта рівня негативного впливу за кожним критерієм та обґрунтування вибору.

2. Належність банку до системно важливих, його категорія визначаються згідно з рішенням Правління Національного банку України, яке приймається відповідно до Положення про порядок визначення системно важливих банків, затвердженого постановою Правління Національного банку України від 25 грудня 2014 року № 863 (у редакції постанови Правління Національного банку України від 19 червня 2019 року № 79) (зі змінами).

3. Належність установи до операторів системно важливої платіжної системи, операторів важливої платіжної системи, важливих технологічних операторів платіжних послуг визначається відповідно до Положення про порядок здійснення оверсайту платіжної інфраструктури в Україні, затвердженого постановою Правління Національного банку України від 24 серпня 2022 року № 187 (із змінами).

Додаток 3
до Положення про критичну
інфраструктуру фінансового
сектору
(пункт 10 розділу II)

Міжсекторальні критерії
визначення рівня негативного впливу на надання основних послуг у разі
знищення, пошкодження або порушення функціонування ОКІ

I. Оцінка наслідків негативного впливу на надання основних послуг відповідно до міжсекторальних критеріїв.

Таблиця

№ з/п	Сфера	Фактор негативного впливу	Рівень негативного впливу					Оцінка КМ _i
			катастрофічні наслідки (4 бали)	критичні наслідки (3 бали)	значні наслідки (2 бали)	незначні наслідки (1 бал)	надто малий (0 балів)	
1	2	3	4	5	6	7	8	9
1	Соціальна	Заподіяння шкоди життю та здоров'ю людей: кількість населення, що може постраждати	Небезпека для життя або здоров'я більш як 75 000 людей	Небезпека для життя та здоров'я більш як 5 000 людей	Небезпека для життя або здоров'я більш як 50 людей	Небезпека для життя або здоров'я менш як 50 людей	Не критично	КМ ₁

1	2	3	4	5	6	7	8	9
2	Соціальна	Заподіяння шкоди життю та здоров'ю людей: географічний масштаб	Небезпека для життя та здоров'я мешканців на території однієї або більш як однієї області, або на території трьох та більше міст обласного значення	Небезпека для життя та здоров'я мешканців на території однієї області або міського району міста обласного центру, або на всій території одного міста обласного значення	Небезпека для життя та здоров'я людей на території об'єкта та для мешканців, що проживають у безпосередній близькості до розміщення об'єкта	Небезпека для життя та здоров'я людей на території об'єкта	Не критично	КМ ₂
3	Екологічна	Заподіяння шкоди навколишньому природному середовищу: економічні втрати	Завдані збитки більш як 30 млн гривень	Завдані збитки більш як 18 млн гривень	Завдані збитки більш як 2 млн гривень	Завдані збитки менш як 2 млн гривень	Не критично	КМ ₃

1	2	3	4	5	6	7	8	9
4	Екологічна	Заподіяння шкоди навколишньому природному середовищу: географічний масштаб	Шкідливий вплив поширюється на територію більш як однієї області або на території не менш як трьох міст обласного значення	Шкідливий вплив поширюється на територію однієї області або на територію більш як одного міста обласного значення	Шкідливий вплив поширюється на територію одного міста обласного значення	Шкідливий вплив поширюється на територію об'єкта інфраструктури	Не критично	КМ ₄
5	Суспільна	Заподіяння шкоди навколишньому природному середовищу: час	Шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом більш як одного року	Шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від пів року до одного року	Шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від одного місяця до пів року	Шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом одного місяця	Не критично	КМ ₅

1	2	3	4	5	6	7	8	9
6	Політична	Припинення або порушення функціонування державних органів	Припинення або порушення функціонування Верховної Ради України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду, а також Офісу Президента України, Ради національної безпеки і оборони України	Припинення або порушення функціонування центральних органів виконавчої влади та облдержадміністрацій	Припинення або порушення роботи районних держадміністрацій, територіальних органів центральних органів виконавчої влади	Припинення або порушення роботи органів місцевого самоврядування	Не критично	КМ ₆
7	Політична	Негативний вплив на довіру людей до державних інституцій	Матиме значний вплив				Не критично	КМ ₇

1	2	3	4	5	6	7	8	9
8	Політична	Шкода інтересам інших держав – партнерів України	Так, принаймні двом країнам або порушення умов міжнародного договору, укладеного від імені України	Так, принаймні одній країні або порушення умов міжнародного договору, укладеного від імені Уряду України	Можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним	Держави не постраждають або немає порушення умов міжнародного договору, укладеного від імені міністерства, іншого центрального органу виконавчої влади, державного органу	Не критично	КМ ₈
9	Економічна	Заподіяння збитків оператору критичної інфраструктури (у відсотках від прогнозованого обсягу річного	Більш як 15 відсотків	Від 10 до 15 відсотків	Від 5 до 10 відсотків	Менш як 5 відсотків	Не критично	КМ ₉

1	2	3	4	5	6	7	8	9
		доходу за всіма видами діяльності)						
10	Економічна	Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	Більш як 0,1 відсотка	Від 0,1 до 0,05 відсотка	Від 0,05 до 0,01 відсотка	Менш як 0,01 відсотка	Не критично	КМ ₁₀
11	Економічна	Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках від прогнозовано-	Більш як 0,1 відсотка	Від 0,1 до 0,05 відсотка	Від 0,05 до 0,01 відсотка	Менш як 0,01 відсотка	Не критично	КМ ₁₁

1	2	3	4	5	6	7	8	9
		го річного прибутку бюджету)						
12	Безперервного функціонування критичної інфраструктури	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких самих основних послуг	Матиме негативний вплив (якщо так, зазначте який)				Не критично	КМ ₁₂

1	2	3	4	5	6	7	8	9
13	Безперервного функціонування критичної інфраструктури	Негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що надає інші основні послуги	Матиме негативний вплив (якщо так, зазначте який)				Не критично	КМ ₁₃
14	Безпеки та оборони	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється рівнем (значущості)	Припинення або порушення функціонування пунктів управління Верховного Головнокомандувача Збройних Сил України, Головнокомандувача Збройних Сил України,	Припинення або порушення функціонування пунктів управління або ситуаційного центру центральних органів виконавчої влади, інших державних органів, державного управління, юрисдикція яких	Припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів	Припинення або порушення функціонування територіальних органів центральних органів виконавчої влади	Не критично	КМ ₁₄

1	2	3	4	5	6	7	8	9
		пункту управління або ситуаційного центру	Начальника Генерального штабу Збройних Сил України або ситуаційного центру Офісу Президента України, Кабінету Міністрів України, Ради національної безпеки і оборони України	поширюється на всю територію України, пунктів управління Сухопутних військ, Повітряних Сил, Військово-Морських Сил, Десантно-штурмових військ, Сил спеціальних операцій, Національної гвардії України, Державної прикордонної служби України				
15	Безпеки та оборони	Припинення або порушення виробництва товарів, виконання робіт та	Більш як 15 відсотків	Від 10 до 15 відсотків	Від 5 до 10 відсотків	Менше як 5 відсотків	Не критично	КМ ₁₅

1	2	3	4	5	6	7	8	9
		надання послуг оборонного призначення, які є предметом оборонних закупівель, для забезпечення потреб сектору безпеки і оборони, а також інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони: зниження обсягів продукції						

1	2	3	4	5	6	7	8	9
		(робіт, послуг) у визначений період часу (у відсотках)						
16	Безпеки та оборони	Припинення або порушення виробництва товарів, виконання робіт та надання послуг оборонного призначення, які є предметом оборонних закупівель, для забезпечення потреб сектору безпеки і оборони, а також інших	Більш як 40 відсотків	Від 10 до 40 відсотків	Від 5 до 10 відсотків	Менш як 5 відсотків	Не критично	КМ ₁₆

1	2	3	4	5	6	7	8	9
		товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони: збільшення часу виготовлення продукції (робіт, послуг) із визначеним обсягом (відсотків встановленого часу на виготовлення продукції)						

I. Загальна характеристика оператора критичної інфраструктури

1. Скорочене найменування юридичної особи – оператора критичної інфраструктури (далі – Оператор)

2. Ідентифікаційний код юридичної особи за Єдиним державним реєстром підприємств та організацій України (далі – ЄДРПОУ)

3. Місцезнаходження (повна юридична, фактична адреса)

4. Форма власності

5. Структура власності (документально підтверджена, дата оновлення)

6. Країна реєстрації

7. Основний вид діяльності згідно з Класифікацією видів економічної діяльності

8. Відповідальна особа Оператора за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку із секторальним органом та відповідними суб'єктами національної системи захисту критичної інфраструктури [прізвище, власне ім'я, по батькові (за наявності), найменування посади, контактні дані]

II. Загальна характеристика об'єкта критичної інфраструктури

9. Назва об'єкта критичної інфраструктури (далі – ОКІ) [згідно з актом категоризації об'єкта критичної інфраструктури фінансового сектору (далі – Акт)]

10. Категорія критичності згідно з Актом та його реєстраційний номер і дата

затвердження

11. Унікальний реєстровий номер, дата реєстрації в Реєстрі об'єктів критичної інфраструктури

12. Місцезнаходження об'єкта критичної інфраструктури (фактична адреса)

13. Власник об'єкта критичної інфраструктури (найменування установи та код за ЄДРПОУ)

14. Дані про складові (будівлі, споруди, технологічні майданчики тощо, згідно з Актом)

15. Тип основної послуги, яку надає об'єкт критичної інфраструктури

16. Основна(ні) послуга(ги), яку (які) надає або забезпечує об'єкт критичної інфраструктури:

17. Критичні бізнес-процеси та критична інформаційна інфраструктура оператора, що забезпечуються та/або обробляються на об'єкті критичної інфраструктури

18. Загальна кількість працівників на об'єкті критичної інфраструктури (день / ніч)

19. Прогнозована кількість осіб, які можуть одночасно перебувати на об'єкті критичної інфраструктури

20. Наявність власного укриття або захисних споруд цивільного захисту, що готові до використання за призначенням

21. Загальні відомості про організацію охорони та фізичного захисту ОКІ (вид охорони, ким забезпечується тощо)

22. Особа, відповідальна за організацію захисту об'єкта критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури [прізвище, власне ім'я, по батькові (за наявності), найменування посади, контактні дані]

23. Інформація про осіб та/або підрозділ, що відповідають за безпеку, стан та забезпечення функціонування систем захисту та надання інших послуг, від яких залежить процес функціонування ОКІ, реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури [прізвище, власне ім'я, по батькові (за наявності), номер телефону, адреса електронної пошти]:

1) організацію фізичного захисту

2) систему охоронної та/або тривожної сигналізації

3) систему відеоспостереження _____

4) функціонування електронних комунікаційних мереж / послуг

5) кіберзахист _____

6) інформаційну безпеку _____

7) цивільний захист, пожежну та техногенну безпеку

8) постачання послуг зовнішніх інженерних мереж (електромережі, водопровідні мережі, тепломережі, газопостачання тощо)

9) інші послуги _____

III. Перелік послуг, їх надавачів / постачальників,
які забезпечують функціонування об'єкта критичної інфраструктури

24. Послуги центру обробки даних

25. Хмарні послуги

26. Електронні комунікаційні послуги:

1) доступу до мережі Інтернет

2) мобільного зв'язку

3) голосової електронної комунікації

27. Кваліфіковані електронні довірчі послуги

28. Послуги з постачання:

1) теплопостачання

2) водопостачання

3) гарячого водопостачання

4) водовідведення

5) газопостачання

6) електропостачання (оператор системи передачі)

7) електропостачання (оператор системи розподілу)

8) визначена гранична (мінімальна) величина споживання електричної потужності, кВт _____

29. Послуги кіберзахисту / інформаційної безпеки _____

30. Інші послуги та їх надавачі / постачальники, що є важливими для безперервного функціонування об'єкта критичної інфраструктури

IV. Загрози та ризики об'єкта критичної інфраструктури

31. Перелік загроз ОКІ та оцінки їх ризику відповідно до національних, секторальних та об'єктових загроз:

Таблиця 1

№ з/п	Перелік загроз	Оцінка ризику	Залишковий ризик
1	2	3	4
1	1. Загрози національного рівня		
2			
3			
4			
5			
6			
7			
8	2. Загрози секторального рівня у фінансовому секторі		
9			
10			
11			
12			
13			
14			
15	3. Загрози об'єктового рівня		
16			
17			
18			
19			
20			
21			

1	2	3	4
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			

32. Зведена таблиця оцінки ризиків загроз (національних, секторальних, об'єктових) ОКІ:

Таблиця 2

Наслідки (вплив)	Катастрофічні (5)					
	Істотні (4)					
	Помірні (3)					
	Неістотні (2)					
	Незначні (1)					
		Низька (1)	Помірно низька (2)	Середня (3)	Помірно висока (4)	Висока (5)
		Ймовірність				

V. Заходи щодо забезпечення безпеки та стійкості об'єкта критичної інфраструктури

33. Заходи захисту, безпеки та стійкості об'єкта критичної інфраструктури, що вживаються Оператором щодо мінімізації ризиків / загроз ОКІ:

Таблиця 3

№ з/п	Заходи	Ризик / загроза
1	2	3
1		
2		
3		

VI. Планування заходів із захисту критичної інфраструктури

34. Заходи, які плануються Оператором щодо вдосконалення, оновлення та посилення захисту, безпеки та стійкості об'єкта критичної інфраструктури:

Таблиця 4

№ з/п	Заходи	Строк виконання	Ризик / загроза
1	2	3	4
1			
2			
3			

Особа, яка визначена
Оператором
відповідальною за
організацію захисту
об'єкта критичної
інфраструктури (назва
ОКІ)

Особистий підпис Власне ім'я ПРІЗВИЩЕ

_____ 20__ р.

Пояснення щодо заповнення додатка 4

1. Пункт 13 розділу II заповнюється, коли Оператор володіє та/або здійснює оперативне управління об'єктом критичної інфраструктури на правах оренди або інших законних підставах.

2. У пунктах 24–30 розділу III зазначається повне найменування юридичної особи надавача/ів (постачальника/ів) послуг, код за ЄДРПОУ.

3. Під час заповнення таблиці 1 пункту 31 розділу IV зазначається:

1) у колонці 2 – перелік потенційних і реальних загроз національного, секторального та об'єктового рівня для ОКІ;

2) у колонці 3 – оцінка ризику, яка отримана в результаті добуtku балів імовірностей загрози та наслідку її реалізації, для яких встановлюється така градація у балах:

для ймовірностей: низька – 1, помірно низька – 2, середня – 3, помірно висока – 4, висока – 5;

для оцінки наслідків реалізації загрози: низька – 1, помірно низька – 2, середня – 3, помірно висока – 4, висока – 5;

3) у колонці 4 – залишковий ризик – рівень ризику, що визначається для кожної загрози шляхом добуtku балів імовірності та наслідків після вжитих Оператором заходів щодо забезпечення безпеки та стійкості об'єкта критичної інфраструктури.

4. Під час заповнення таблиці 2 пункту 32 розділу IV зазначається порядковий номер загрози, зазначеної в колонці 2 таблиці 1 пункту 31 цього додатка, відповідно до здійсненої оцінки ризику, наведеної в колонці 3 таблиці 2.

5. У пункті 33 розділу V наводяться відомості про документи (політику, накази, регламенти, інструкції, плани та інше), відповідно до яких упроваджені заходи щодо забезпечення безпеки та стійкості ОКІ, управління ризиками, спрямовані на попередження реалізації та/або мінімізацію негативного впливу загроз, наведених у переліку в пункті 31 розділу IV.

6. У пункті 34 розділу VI зазначаються відомості про заходи, які плануються Оператором щодо вдосконалення, оновлення та посилення захисту, безпеки та стійкості об'єкта критичної інфраструктури (оновлення стратегічних, методичних та інструктивних документів; закупівля засобів та послуг із захисту ОКІ; проведення заходів аудиту систем управління та безпеки; навчання персоналу з пить безпеки; проведення тестувань систем безпеки та планів безперервності / реагування / відновлення тощо).

Зміни до
Положення про організацію кіберзахисту в банківській системі України

1. У розділі I:

1) у пункті 1 слова, літери та цифри “Національного стандарту України ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги” (ISO/IEC 27001:2013, Cor 1:2014, IDT), прийнятого наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 18 грудня 2015 року № 193 (далі – Національний стандарт України ДСТУ ISO/IEC 27001:2015),” виключити;

2) абзац сімнадцятий пункту 2 замінити трьома новими абзацами сімнадцятим – дев’ятнадцятим такого змісту:

“Терміни “об’єкт критичної інфраструктури”, “оператор критичної інфраструктури”, “реєстр об’єктів критичної інфраструктури” уживаються в значеннях, визначених у Законі України “Про критичну інфраструктуру”.

Терміни “об’єкт критичної інформаційної інфраструктури”, “критична інформаційна інфраструктура” уживаються в значеннях, визначених у Законі України “Про основні засади забезпечення кібербезпеки України”.

Термін “АРМ-НБУ-інформаційний” уживається в значенні, визначеному в Положенні про використання засобів криптографічного захисту інформації Національного банку України, затвердженому постановою Правління Національного банку України від 14 квітня 2023 року № 49.”.

У зв’язку з цим абзац вісімнадцятий уважати абзацом двадцятим;

3) у підпункті 3 пункту 3 слово “інформаційної” виключити;

4) абзац другий пункту 6 викласти в такій редакції:

“Вимоги розділу IV цього Положення поширюються лише на банки України, що віднесені до операторів критичної інфраструктури фінансового сектору відповідно до нормативно-правових актів Національного банку з питань захисту критичної інфраструктури (далі – банки – оператори критичної інфраструктури).”.

2. У розділі IV:

1) у назві розділу слова та літери “критичної інформаційної інфраструктури банків ОКІ” замінити словами “критичної інфраструктури банків – операторів критичної інфраструктури”;

2) пункти 30–33 викласти в такій редакції:

“30. Банк – оператор критичної інфраструктури зобов’язаний віднести до об’єктів критичної інформаційної інфраструктури (далі – ОКІІ) інформаційні системи об’єкта критичної інфраструктури, які відповідають двом критеріям:

1) порушення функціонування інформаційних систем внаслідок кіберінциденту, кібератаки безпосередньо вплине на стале функціонування об’єкта критичної інфраструктури банку – оператора критичної інфраструктури;

2) у банку – оператора критичної інфраструктури немає альтернативних за функціональними можливостями інформаційних систем для забезпечення сталого функціонування об’єкта критичної інфраструктури банку – оператора критичної інфраструктури.

31. Банк – оператор критичної інфраструктури має право віднести до ОКІІ інші інформаційні системи, що безпосередньо забезпечують автоматизацію процесів надання банком – оператором критичної інфраструктури банківських, фінансових послуг та здійснення інших видів його діяльності відповідно до статті 47 Закону України “Про банки і банківську діяльність”, надання кваліфікованих електронних довірчих послуг за умови відповідності критеріям, викладеним у підпункті 2 пункту 30 розділу IV цього Положення.

32. Банк – оператор критичної інфраструктури зобов’язаний протягом місяця з дня отримання повідомлення від Національного банку про внесення відомостей про його об’єкти критичної інфраструктури до реєстру об’єктів критичної інфраструктури:

1) сформулювати та затвердити перелік інформаційних систем банку – оператора критичної інфраструктури, віднесених до ОКІІ (далі – перелік ОКІІ), відповідно до пунктів 30, 31 розділу IV цього Положення;

2) надати затверджений перелік ОКІІ Національному банку в спосіб, установлений у пункті 41 розділу IV цього Положення.

33. Банк – оператор критичної інфраструктури зобов’язаний підтримувати в актуальному стані перелік ОКІІ та надавати Національному банку в спосіб, установлений у пункті 41 розділу IV цього Положення, оновлений перелік ОКІІ протягом місяця з дня його затвердження.”;

3) у пункті 34:

підпункт 1 після слова “щороку” доповнити словами та цифрами “станом на 01 листопада”;

у підпункті 2 слова та цифри “до 20 грудня” замінити словами та цифрами “до 01 грудня та надає актуалізований перелік ОКІІ (у разі його оновлення) у спосіб, установлений у пункті 41 розділу IV цього Положення.”;

4) у пункті 35:

в абзаці першому слова та літери “власного переліку ОКІІ:” замінити словами та літерами “переліку ОКІІ або його оновлення.”;

у підпункті 3 слова “в банківській системі України шляхом завантаження через портал Центру кіберзахисту” замінити словами “в спосіб, установлений у пункті 41 розділу IV цього Положення”;

5) у пункті 36:

абзац перший доповнити словами “та надавати Національному банку ці відомості протягом місяця з дня їх актуалізації у спосіб, установлений у пункті 41 розділу IV цього Положення.”;

в абзаці третьому слово “термін” замінити словом “строк”;

6) у підпункті 1 пункту 37 слова, літери та цифри “, що визначені в додатку А до Національного стандарту України ДСТУ ISO/IEC 27001:2015” виключити;

7) підпункт 4 пункту 38 викласти в такій редакції:

“4) пріоритетної реалізації заходів кіберзахисту критичної інформаційної інфраструктури банку – оператора критичної інфраструктури відповідно до розробленого Плану реагування в разі кібератаки (спроби реалізації кіберзагрози) на об’єкти кіберзахисту банку – оператора критичної інфраструктури;”;

8) пункт 41 викласти в такій редакції:

“41. Відомості про ОКІІ є інформацією з обмеженим доступом. Банки – оператори критичної інфраструктури зобов’язані надавати інформацію (інформування про перегляд переліків ОКІІ, переліки ОКІІ, відомості про ОКІІ) у випадках, визначених у пунктах 32–36 розділу IV цього Положення, в електронній формі через АРМ-НБУ-інформаційний.”.

3. У розділі V:

1) пункт 42 викласти в такій редакції:

“42. Банк зобов’язаний проводити незалежний аудит інформаційної безпеки (далі – зовнішній аудит).

Банк самостійно встановлює періодичність проведення зовнішнього аудиту. Періодичність проведення зовнішнього аудиту для банку – оператора критичної інфраструктури залежить від категорії критичності ОКІ та становить:

1) не рідше ніж один раз на два роки для об’єктів I та II категорій критичності;

2) не рідше ніж один раз на три роки для об’єктів III категорії критичності.

Зовнішній аудит проводиться згідно з нормами законодавства України, національних стандартів та з урахуванням міжнародних стандартів аудиту. Програма аудиту формується, урахуваючи особливості діяльності банку, характер та обсяг банківських, фінансових послуг та інших видів діяльності.

Допускається проведення зовнішнього аудиту в межах аудиту щорічної перевірки фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності аудиторською фірмою.”;

2) підпункт 1 пункту 43 викласти в такій редакції:

“1) аудиторську фірму для проведення зовнішнього аудиту серед юридичних осіб – резидентів України відповідно до законодавства України з урахуванням обмежень щодо заборони залучати до проведення незалежного аудиту:

одну і ту саму аудиторську фірму двічі поспіль;

аудиторську фірму – юридичну особу або фізичну особу-підприємця, що є резидентом держави-агресора чи держави, що здійснює / здійснювала збройну агресію проти України, або має кінцевих бенефіціарних власників, яка є резидентом держави-агресора або держави, що здійснює / здійснювала збройну агресію проти України, або здійснює обробку або зберігання даних за допомогою технології хмарних обчислень та центрів обробки даних, що розміщені на території держави-агресора, держави, що здійснює / здійснювала збройну агресію проти України, тимчасово окупованій території та/або належать суб’єктам, діяльність яких підпадає під дію Закону України “Про санкції” та стосовно яких прийнято рішення про застосування санкцій в Україні;”;

3) підпункт 2 пункту 44 викласти в такій редакції:

“2) відповідності впровадження СУІБ банку за стандартом Міжнародної організації зі стандартизації (ISO, англійською мовою International Organization for Standardization) / Міжнародної електротехнічної комісії (IEC, англійською мовою International Electrotechnical Commission) 27001.”.

4. У розділі I додатка:

1) пункт 1 викласти в такій редакції:

“1. Повне найменування банку – оператора критичної інфраструктури, адреса його місцезнаходження (індекс, область, місто, вулиця, номер будинку), форма власності, код за ЄДРПОУ.”;

2) підпункт 2 пункту 4 викласти в такій редакції:

“2) повна назва об’єкта критичної інфраструктури, до складу якого входить ОКІІ [у разі віднесення об’єкта до критичної інформаційної інфраструктури відповідно до пункту 30 розділу IV Положення про організацію кіберзахисту в банківській системі України (далі – Положення)], призначення ОКІІ, перелік банківських, фінансових та інших видів його діяльності, надання яких він забезпечує (у разі віднесення об’єкта до критичної інформаційної інфраструктури відповідно до пункту 31 розділу IV Положення);”.

5. У тексті Положення та додатка до нього слово та літери “банк ОКІ” у всіх відмінках замінити словами “банк – оператор критичної інфраструктури” у відповідних відмінках.