ПРОЄКТ

Правління Національного банку України

П О С Т А Н О В А

Київ

Про критичну інфраструктуру фінансового сектору

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статей 8, 9, 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. Визнати такими, що втратили чинність:

1) постанова 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” (зі змінами).

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

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

Голова Андрій ПИШНИЙ

Інд. 58

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Положення
про критичну інфраструктуру фінансового сектору

І. 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), в якій розміщуються керівництво установи, працівники підрозділів установи, які забезпечують надання основних послуг, здійснюють управління об’єктами критичної інфраструктури та забезпечують їх функціонування;

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

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

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 фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем, технологічних операторів платіжних послуг;

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

6) 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 у цьому Положенні у значенні, наведеному у Положенні про передавання запасів готівки на зберігання до уповноважених банків та проведення операцій з ними, затвердженому постановою Правління Національного банку від 17 вересня 2021 року № 95 (зі змінами).

Інші терміни у цьому Положенні вживаються у 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 об’єктів критичної інфраструктури фінансового сектору і визначає:

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

2) методику визначення механізмів та критерії віднесення ідентифікованих об’єктів критичної інфраструктури фінансового сектору до однієї з категорій критичності;

3) порядок розроблення паспортів безпеки на об’єкти критичної інфраструктури фінансового сектору.

4. Порядок віднесення об’єктів інфраструктури Національного банку до об’єктів критичної інфраструктури та їх категорізація здійснюється у порядку, визначеному Національним банком.

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

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

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, важливою платіжною системою;

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

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 фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, визначені Оператором окремим рішенням 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 об'єктів критичної інфраструктури.

До об`єктів критичної інфраструктури Оператора обов'язково відносяться 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 провести категоризацію ОКІ відповідно до методики категоризації об'єктів критичної інфраструктури фінансового сектору, передбаченої в розділі ІІІ цього Положення.

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

Заступник керівника Оператора очолює Комісію, до складу якої включаються 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 необхідністю, також можуть включатися представники інших підрозділів Оператора та представники секторального органу (за згодою).

9. Результати роботи Комісії оформлюється Актом категоризації об'єкта критичної інфраструктури фінансового сектору (далі - Акт), який складається у двох примірниках за формою наведеною у додатку 1.

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

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

12. Оператор, у разі розміщення декількох 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 Акту на такий об'єкт.

13. Відомості, що містяться в Акті, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом, а додатки (за наявності) до Акту є невід'ємною його частиною.

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

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

15. Секторальний орган, у разі наявності зауважень до Акту, не пізніше ніж протягом двох робочих днів після завершення строку, передбаченого у пункті 14

розділу ІІ цього Положення, повертає Акт на доопрацювання Оператору у порядку відправлення/надсилання, визначеному Національним банком.

Оператор зобов'язаний протягом 10 робочих днів врахувати 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 Акту секторальний орган направляє Оператору. Секторальний орган та Оператор забезпечують збереження Акту увесь строк існування ОКІ та упродовж одного року після втрати об'єктом статусу об'єкта критичної інфраструктури.

18. Секторальний орган, на підставі затвердженого та погодженого Акту, 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 повідомляє листом Оператора 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 об'єкта критичної інфраструктури та/або його цільового призначення;

2) місця розташування ОКІ;

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

23. Оператор, при виникненні умов, передбачених у пункті 22 розділу ІІ 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 об’єкта критичної інфраструктури або його частини, інформує секторальний орган про наміри змінити цільове призначення, режим функціонування чи намір передати права на об’єкт критичної інфраструктури.

25. Секторальний орган має право ініціювати здійснення Оператором повторної категоризації ОКІ у разі змін законодавства у сфері захисту критичної інфраструктури та/або за результатами перевірки та/або оцінки стану захищеності ОКІ та/або виникнення умов, передбачених у цьому пункті.

ІІІ. Методика категоризації об’єктів критичної інфраструктури фінансового сектору

26. Установа здійснює ідентифікацію об’єктів критичної інфраструктури у порядку, визначеному у розділі ІІ цього Положення.

27. Категорія критичності ОКІ визначається на основі 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 у 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 у 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 у додатку 2 до цього Положення та проставленням у графі “Оцінка $КС_j$” відповідного балу;

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 у додатку 3 до цього Положення та проставленням у графі "Оцінка КМі" відповідного балу;

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

$$РК_{ОКІ} = \frac{КС_{max}+\sum КМ_i}{68}$$

де $РК_{ОКІ}$ – узагальнена нормована оцінка рівня критичності об'єкта критичної інфраструктури;

$КС_{max}$ – максимальний бал з усіх оцінок $КС_j$, які отримав об'єкт критичної інфраструктури за секторальними критеріями, однією із n послуг, що надається ОКІ (додаток 2), де j є {1, n}, які надає ОКІ;

$\Sigma КМ_i$ – сума балів, які отримав об'єкт критичної інфраструктури за всіма міжсекторальними критеріями (додаток 3), де і є {1, 16};

4) віднесення до певної категорії критичності здійснюється шляхом порівняння розрахованої узагальненої нормованої оцінки рівня критичності ОКІ ($РК_{ОКІ}$) з діапазонами значень оцінки рівня ОКІ, зазначених у колонці 4 таблиці наведеної в підпункті 4 пункту 28 розділу III цього Положення. При цьому, якщо оцінка потрапляє у відповідний діапазон значень, 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	$РК_{ОКІ}$	від 0,9 до 1,0
2	II категорія критичності	$РК_{ОКІ}$	від 0,75 до 0,9
3	III категорія критичності	$РК_{ОКІ}$	від 0,53 до 0,75
4	IV категорія критичності	$РК_{ОКІ}$	від 0,2 до 0,53
5	Не критично	$РК_{ОКІ}$	від 0 до 0,2

5) результати розрахунків та визначення категорії ОКІ з відповідним обґрунтуванням оформлюються Актом, форма та процедура оформлення якого визначається 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 підтверджуючим 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 у додатку 4 (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 ОКІ.

31. Відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.

32. Паспорт безпеки ОКІ оформлюється згідно форми, наведеної у додатку 4 до цього Положення, і містить інформацію щодо:

1) загальної характеристики Оператора;

2) загальної характеристики об’єкта критичної інфраструктури;

3) переліку послуг та їх надавачів (постачальників), які забезпечують функціонування об’єкта критичної інфраструктури;

4) загроз та ризиків об’єкту критичної інфраструктури;

5) заходів щодо забезпечення безпеки та стійкості об’єкта критичної інфраструктури;

6) плану заходів із захисту критичної інфраструктури.

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

Факсимильне відтворення підпису за допомогою засобів механічного або іншого копіювання на паспорті безпекі ОКІ не допускається.

34. Паспорт безпеки ОКІ надсилається в 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 та у разі відсутності зауважень (пропозицій) погоджує паспорт безпеки ОКІ та повертає один примірник Оператору.

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

37. Оператор зобов'язаний протягом 10 робочих днів здійснити доопрацювання паспорту безпеки ОКІ з урахуванням отриманих від секторального органу зауважень та/або пропозицій, та за результатами доопрацювання направити на погодження до секторального органу, у порядку, передбаченому пунктом 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 об'єктів критичної інфраструктури, із дотриманням положень, передбачених пунктами 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 змін вимог до захисту обєктів критичної інфраструктури;

3) за результатами повторної ідентифікації та категоризації ОКІ.

40. Секторальний орган та Оператор забезпечують збереження паспортів безпеки ОКІ увесь строк існування ОКІ та упродовж одного року після втрати об'єктом статусу об'єкта критичної інфраструктури.

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

[Обрати значення грифу]
Прим. №__

ПОГОДЖЕНО	ЗАТВЕРДЖЕНО
_____	_____
(найменування посади відповідальної особи секторального органу)	(найменування посади керівника Оператора)
_____ _____	_____ _____
(підпис) (власне ім’я, прізвище)	(підпис) (власне ім’я, прізвище)
___ _____ 20___ р.	___ _____ 20___ р.

АКТ
категоризації об’єкта критичної інфраструктури фінансового сектору
_____
назва об’єкта

Відповідно до методики категоризації об’єктів критичної інфраструктури фінансового сектору, визначеної Національним банком, Комісією створеною відповідно до _____(внутрішній документ Оператора) здійснено ідентифікацію об’єкта критичної інфраструктури _____ (назва 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 Єдиного державного реєстру підприємств та організацій України (далі - ЄДРПОУ)	

Продовження додатка 1
Продовження таблиці 1

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

2. Загальний опис об’єкту передбачає загальний опис ОКІ (його складових), основні послуги та функції, що надаються (виконуються)_____
_____

3. Оцінка критичності ОКІ:

1) опис та обґрунтування рівня негативного впливу у разі знищення, пошкодження або порушення функціонування ОКІ за секторальними критеріями згідно додатку 2 до цього 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 та/або припинення операцій з запасами готівки Національного банку унаслідок 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	$КС_4$

Продовження додатка 1
Продовження таблиці 2

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 у разі знищення, пошкодження або порушення функціонування ОКІ за міжсекторальними критеріями згідно додатку 3 до цього 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: час	$КМ_5$
6	Припинення або порушення функціонування державних органів	$КМ_6$
7	Негативний вплив на довіру людей до державних інституцій	$КМ_7$
8	Шкода інтересам інших держав - партнерів України	$КМ_8$
9	Заподіяння збитків оператору критичної інфраструктури (у відсотках прогнозованого обсягу річного доходу за всіма видами діяльності)	$КМ_9$
10	Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	$КМ_{10}$
11	Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету)	$КМ_{11}$

Продовження додатка 1
Продовження таблиці 3

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 в 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) в заданий 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 (відсотків встановленого часу на виготовлення продукції)	$КМ_{16}$
17	Сума балів за міжсекторальними критеріями	$\Sigma КМ_i$

4. Зазначається розрахунок узагальненої нормованої оцінки рівня критичності (РКокі), який здійснюється відповідно до підпункту 3 пункту 28 розділу ІІІ цього Положеня.

5. Висновок.

Висновок про віднесення “Найменування ОКІ” до “___” категорії

критичності на основі узагальненої нормованої оцінки рівня критичності об’єкта критичної інфраструктури відповідно до правила, наведеного у підпункті 4 пункту 28 розділу ІІІ цього Положення.

Голова Комісії:

Члени Комісії:

Пояснення до додатку 1

1. У пункті 2, загальний опис надається для кожного з виду ОКІ, і має 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: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бали)	Рівень негативного впливу: незначні наслідки (1 бал)	Оцінка $КС_i$
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 важливим банком 3 категорії	Системно важливим банком 2 або 1 категорії	Іншим системно важливим банком	Не застосовується	$КС_1$

Продовження додатка 2
Продовження таблиці

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	Оператором системно важливої платіжної системи	Оператором важливої платіжної системи або важливим технологічним оператором 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 з запасами готівки Національного банку	Повне припинення здійснення операцій з запасами готівки Національного банку	Обмеження щодо здійснення операцій з запасами готівки Національного банку	Здійснюються лише операції зі зменшення запасів готівки Національного банку	Не застосовується	$КС_3$

Продовження додатка 2
Продовження таблиці

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 послуг фінансових послуг	Не застосовується	Оператором єдиної централізованої бази даних щодо обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів	Не застосовується	Не застосовується	$КС_5$

Продовження додатка 2

II. Пояснення щодо застосування критеріїв

1. Оцінка проводиться шляхом вибору варіанта рівня негативного впливу за кожним критерієм та обґрунтування вибору.

2. Належність банку до системно важливого банку, його категорія визначається 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 оператора системно важливої платіжної системи, оператора важливої платіжної системи, важливого технологічного оператора 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.

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: катастрофічні наслідки (4 бали)	Рівень негативного впливу: критичні наслідки (3 бали)	Рівень негативного впливу: значні наслідки (2 бал)	Рівень негативного впливу: незначні наслідки (1 бал)	Рівень негативного впливу: надто малий (0 балів)	Оцінка $КМ_і$
1	2	3	4	5	6	7	8	9
1	Соціальна	Заподіяння шкоди життю та здоров'ю людей: кількість населення,	Небезпека для життя або здоров'я більш як 75 000 людей	Небезпека для життя та здоров'я більш як 5000 людей	Небезпека для життя або здоров'я більш як 50 людей	Небезпека для життя або здоров'я менш як 50 людей	Не критично	$КМ_1$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		що може постраждати						
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 для 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	Нанесені збитки більш як 30 млн. гривень	Нанесені збитки більш як 18 млн. гривень	Нанесені збитки більш як 2 млн. гривень	Нанесені збитки менш як на 2 млн. гривень	Не критично	$КМ_3$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
4	Екологічна	Заподіяння шкоди навколишньому природному середовищу: географічний масштаб	Шкідливий вплив розповсюджуєтьс я на територію більш як однієї області або на території не менш як трьох міст обласного значення	Шкідливий вплив розповсюджуєтьс я на територію однієї області або на територію більш як одного міста обласного значення	Шкідливий вплив розповсюджуєт ься на територію одного міста обласного значення	Шкідливий вплив розповсюджуєт ься на територію об’єкта інфраструктури	Не критич но	$КМ_4$
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 середо-вище та безпечні умови життя зберігається протягом від півроку до одного року	Шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від одного місяця до півроку	Шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом одного місяця	Не критич но	$КМ_5$

Продовження додатка 3
Продовження таблиці

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 та 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	$КМ_7$

Продовження додатка 3
Продовження таблиці

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 не має місце 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	Більш як 15 відсотків	Від 10 до 15 відсотків	Від 5 до 10 відсотків	Менш як 5 відсотків	Не критично	$КМ_9$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		прогнозованого обсягу річного доходу за всіма видами діяльності)						
10	Економічна	Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках прог-нозованого 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	$КМ_{10}$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
11	Економічна	Заподіяння збитків місцевим бюджетам (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	$КМ_{11}$
12	Безперервного функціонування критичної інфраструктури	Негативний вплив на безперервне та стійке функціонування іншого об’єкта інфраструктури, що забезпечує надання таких самих	Матиме негативний вплив (якщо так, вкажіть який)				Не критично	$КМ_{12}$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		основних послуг						
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, вкажіть який)				Не критично	$КМ_{13}$
14	Безпеки та оборони	Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що	Припинення або порушення функціонування пунктів управління Верховного Головнокомандувача Збройних Сил, Головнокомандувача Збройних Сил, Начальника	Припинення або порушення функціонування пунктів управління або ситуаційного центру центральних органів виконавчої влади, інших державних органів, органів	Припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів	Припинення або порушення функціонування територіальних органів центральних органів виконавчої влади	Не критично	$КМ_{14}$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		оцінюється в рівні (значущості) пункту управління або ситуаційного центру	Генерального штабу Збройних Сил або ситуаційного центру Офісу Президента України, Кабінету Міністрів України, Ради національної безпеки та оборони України	державного управління, юрисдикція яких поширюється на всю територію України, пунктів управління Сухопутних військ, Повітряних Сил, Військово-Морських Сил, десантно-штурмових військ, сил спеціальних операцій, Національної гвардії, Державної прикордонної служби України				
15	Безпеки та оборони	Припинення або порушення	Більш як 15 відсотків	Від 10 до 15 відсотків	Від 5 до 10 відсотків	Менше як 5 відсотків	Не критично	$КМ_{15}$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		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						

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		забезпе-чення потреб безпеки і оборони: зниження обсягів продукції (робіт, послуг) в заданий період часу (у відсотках)						
16	Безпеки та оборони	Припинення або порушення виробництва товарів, ви-конання робіт та надання послуг обо-ронного призначен-ня, які є предметом	Більш як 40 відсотків	Від 10 до 40 відсотків	Від 5 до 10 відсотків	Менш як 5 відсотків	Не крити чно	$КМ_{16}$

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		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						

Продовження додатка 3
Продовження таблиці

1	2	3	4	5	6	7	8	9
		обсягом (відсотків встановлено го часу на виготовлен- ня продукції)						

Додаток 4
до Положення про порядок розроблення та погодження паспортів безпеки на об’єкти критичної інфраструктури фінансового сектору
(пункт 29 розділу IV)

[Обрати значення грифу]
Прим. №__

ПОГОДЖЕНО	ЗАТВЕРДЖЕНО
_____	_____
(найменування посади відповідальної особи секторального органу)	(найменування посади керівника Оператора)
_____ _____	_____ _____
(підпис) (власне ім’я, прізвище)	(підпис) (власне ім’я, прізвище)
___ _____ 20___ р.	___ _____ 20___ р.

ПАСПОРТ БЕЗПЕКИ
на об’єкт критичної інфраструктури
_____
(назва об’єкта критичної інфраструктури)
_____
(унікальний реєстровий номер об’єкта критичної інфраструктури)
_____
(повне найменування юридичної особи Оператора)

____ _____ 20___ р.
(дата складання паспорту безпеки)

Продовження додатку 4

I. Загальна харктеристика Оператора

1. Скорочена назва юридичної особи Оператора

_____

2. Ідентифікаційний код юридичної особи в ЄДРПОУ

_____

3. Місцезнаходження (повна юридична, фактична адреса)

_____

4. Форма власності

_____

5. Структура власності (документально підтверджена, дата оновлення)

_____

6. Країна реєстрації

_____

7. КВЕД основної діяльності

_____

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

_____

II. Загальна характеристика
об'єкта критичної інфраструктури

9. Назва ОКІ (згідно Акта)

_____

10. Категорія критичності згідно Акта та його реєстраційний номер і дата затвердження

_____

11. Унікальний реєстровий номер, дата реєстрації у Реєстрі об'єктів критичної інфраструктури_____

Продовження додатку 4

12. Місцезнаходження об’єкта критичної інфраструктури (фактична адреса)
_____

13. Власник об’єкта критичної інфраструктури (найменування установи та ЄДРПОУ)
_____

14. Дані про складові (будівлі, споруди, технологічні майданчики тощо, згідно Акту)
_____

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

16. Основна (ні) послуга (ги) яку 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 (П.І.Б, посада, контактні дані)_____

23. Інформація про осіб та/або підрозділ, що відповідають за безпеку, стан

та забезпечення функціонування систем захисту та інших послуг, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури (прізвище, власне ім'я, по батькові (у разі 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) кіберзахисту _____

6) інформаційної безпеки_____

7) цивільного захисту, пожежної та техногенної безпеки,

_____

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 електронно 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/постачальників, що є важливими для безперервного функціонування об’єкту критичної інфраструктури _____

Продовження додатку 4

IV. Загрози та ризики об’єкту 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			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			

Продовження додатку 4

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 удосконалення, оновлення та посилення захисту, безпеки та стійкості об’єкта критичної інфраструктури:

Продовження додатку 4

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) _____ _____
(підпис) (власне ім’я, прізвище)

___ _____ 20___ р.

Пояснення до додатку 4

1. Пункт 13 розділу ІІ заповнюється у випадку 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 ІІІ зазначається повне найменування юридичної особи надавача/ів (постачальника/ів) послуг, код за ЄДРПОУ.

3. При заповненні 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 добутку балів ймовірностей 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 добутку балів ймовірності та наслідків, після вжитих Оператором заходів щодо забезпечення безпеки та стійкості об’єкта критичної інфраструктури.

4. При заповненні таблиці 2 пункту 32 розділу IV зазначається порядковий номер загрози, яка зазначена в колонці 2 таблиці 1 пункту 31 цього додатку, у відповідності до здійсненої оцінки ризику, наведеної в колонці 3 таблиці 2.

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

6. У пункті 34 розділу VI зазначаються відомості про заходи, які плануються Оператором щодо удосконалення, 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 аудити систем управління та безпеки; навчання персоналу з пить безпеки; проведення тестувань систем безпеки та планів безперервності/реагування/відновлення, тощо).

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Зміни до
Положення про організацію кіберзахисту в банківській системі України

1. У розділі I:

1) у пункті 1 слова 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), Національного стандарту України ДСТУ ISO/IEC 27032:2016 “Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки” (ISO/IEC 27032:2012, IDT), прийнятого наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 27 грудня 2016 року № 448,” виключити;

2) абзац чотирнадцятий пункту 2 замінити трьома новими абзацами чотирнадцятим, п’ятнадцятим та шістнадцятим такого змісту:

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

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

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

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) в назві розділу слова та літери “критичної інформаційної інфраструктури банків ОКІ” замінити словами “критичної інфраструктури банків”;

2) пункти 30, 31 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’єкту критичної інфраструктури банку – оператора критичної інфраструктури;

2) якщо немає в банку – оператора критичної інфраструктури альтернативних за функціональними можливостями інформаційних систем для забезпечення сталого функціонування об’єкту критичної інфраструктури банку – оператору 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 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.”;

3) абзац перший та другий пункту 32 замінити трьома новими абзацами такого змісту:

“32. Банк 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) сформувати та затвердити перелік інформаційних систем банку, віднесених до ОКІІ (далі - перелік ОКІІ), відповідно до пунктів 30, 31 розділу IV цього Положення;

2) надати затверджений перелік ОКІІ Національному банку в спосіб, встановлений пунктом 41 розділу IV цього Положення.”;

4) пункт 33 викласти в такій редакції:

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

5) 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, встановлений пунктом 41 розділу IV цього Положення.”;

6) у пункті 35:

у 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, встановлений пунктом 41 розділу IV цього Положення”;

7) абзац перший пункту 36 після літер “ОКІІ” доповнити словами “та надавати Національному банку ці відомості протягом місяця з дня їх актуалізації у спосіб, встановлений пунктом 41 розділу IV цього Положення.”;

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

9) 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, передбачених пунктами 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 категорії 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, ураховуючи особливості діяльності банку, характер та обсяг банківських, фінансових послуг та інші види 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 та нормативно-правових актів Національного банку, з урахуванням обмежень щодо заборони залучати до проведення незалежного аудиту:

одну і туж саму аудиторську фірму двічі підряд;

аудиторську фірму - юридичну особу або фізичну особу-підприємця, що є резидентами держави-агресора чи держави, що здійснює/здійснювала збройну агресію проти України, або мають кінцевих бенефіціарних власників, які є резидентами держави-агресора або держави, що здійснює/здійснювала збройну агресію проти України, або здійснюють 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 з стандартизації (ISO, англійською мовою International Organization for Standardization) / Міжнародної електротехнічної комісії (IEC, англійською мовою International Electrotechnical Commission) 27001;".

4. Підпункт 2 пункту 4 розділу I додатка до Положення 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 за пунктом 30 цього Положення), призначення ОКІІ, перелік банківських, фінансових та інших видів його діяльності, надання яких він забезпечує (у разі віднесення об’єкта до критичної інформаційної інфраструктури за пунктом 31 цього Положення);”.

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