ПРОЄКТ

Правління Національного банку України

П О С Т А Н О В А

Київ

Про затвердження Положення про критичну
інформаційну інфраструктуру фінансового сектору
та Змін до деяких нормативно-правових актів
Національного банку України з питань кіберзахисту

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статей 4, 8 Закону України “Про основні засади забезпечення кібербезпеки України”, з метою нормативного врегулювання питань організації та забезпечення кіберзахисту об’єктів критичної інформаційної інфраструктури фінансового сектору Правління Національного банку України **постановляє:**

1. Затвердити Положення про критичну інформаційну інфраструктуру фінансового сектору (далі – Положення про КІІ), що додається.

2. Затвердити Зміни до:

1) Положення про захист інформації та кіберзахист учасниками платіжного ринку, затвердженого постановою Правління Національного банку України від 19 травня 2021 року № 43 (зі змінами), що додаються.

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

3. 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, що є операторами критичної інфраструктури фінансового сектору відповідно до Положення про критичну інфраструктуру фінансового сектору, затвердженого постановою Правління Національного банку України від 27 червня 2025 року № 69, визначити об’єкти критичної інформаційної інфраструктури та надати Національному банку України інформацію про об’єкти критичної інформаційної інфраструктури протягом двох місяців із дня набрання чинності цією постановою.

Інформація про об’єкти критичної інформаційної інфраструктури надається у спосіб, встановлений підпунктами 1, 2 пункту 14 розділу ІІ і пунктом 17 розділу ІІ Положення про КІІ.

4. Департаменту безпеки (Олександр Паламарчук) після офіційного опублікування довести до відома банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем, технологічних операторів платіжних послуг, інформацію про прийняття цієї постанови.

5. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Андрія Пишного.

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

Голова Андрій ПИШНИЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Положення
про критичну інформаційну інфраструктуру фінансового сектору

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України “Про основні засади забезпечення кібербезпеки України”, “Про захист інформації в інформаційно-комунікаційних системах” та “Про Національний банк України”.

2. Терміни та скорочення в цьому Положенні вживаються в такому значенні:

1) банк - Оператор – банк, що є оператором критичної інфраструктури фінансового сектору відповідно до Положення про критичну інфраструктуру фінансового сектору, затвердженого постановою Правління Національного банку України від 27 червня 2025 року № 69 (далі – Положення № 69);

2) важливий об’єкт оверсайта, що є оператором критичної інфраструктури фінансового сектору – оператор платіжної системи, яку Національний банк України (далі – Національний банк) визначив системно важливою платіжною або важливою платіжною системою, технологічний оператор платіжних послуг, якого Національний банк визначив важливим технологічним оператором платіжних послуг;

3) ОКІІ – об’єкт критичної інформаційної інфраструктури фінансового сектору;

4) Оператор – оператор критичної інфраструктури фінансового сектору відповідно до Положення № 69;

5) реєстр об’єктів критичної інформаційної інфраструктури фінансового сектору (далі – реєстр ОКІІ) – відомості про інформаційно-комунікаційні системи Операторів, які відповідно до вимог цього Положення віднесені до об’єктів критичної інформаційної інфраструктури фінансового сектору;

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;

7) штатний режим функціонування інформаційно-комунікаційної системи – режим, у якому функціонування інформаційно-комунікаційної системи здійснюється в повному обсязі за передбаченими для цієї системи регламентом та технологією виконання операцій.

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

Термін “кризова ситуація” уживається в цьому Положенні в значенні, наведеному у Законі України “Про критичну інфраструктуру”.

Термін “інформаційно-комунікаційна система” уживається в цьому Положенні в значенні, наведеному у Законі України “Про захист інформації в інформаційно-комунікаційних системах”.

Термін “критичні операції / послуги” уживаються в цьому Положенні в значеннях, наведених у Положенні про порядок здійснення оверсайту платіжної інфраструктури в Україні, затвердженому постановою Правління Національного банку України від 24 серпня 2022 року № 187 (зі змінами) (далі – Положення № 187).

Термін “удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису” уживається в цьому Положенні в значенні, наведеному у Положенні про використання електронного підпису та електронної печатки, затвердженому постановою Правління Національного банку України від 20 грудня 2023 року № 172.

Терміни “секторальний орган”, “фінансовий сектор” уживається в цьому Положенні в значенні, наведеному у Положенні № 69.

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 кіберзахисту ОКІІ і визначає:

1) критерії та порядок віднесення інформаційно-комунікаційних систем Оператора до ОКІІ;

2) вимоги стосовно заходів із забезпечення кіберзахисту ОКІІ.

4. Віднесення об’єктів інформаційної інфраструктури Національного банку до ОКІІ, формування та ведення реєстру ОКІІ здійснюються в порядку, визначеному Національним банком.

5. Оператор має право використовувати хмарні послуги для забезпечення функціонування ОКІІ за умови дотримання вимог статті 10 Закону України “Про хмарні послуги”.

6. Використання Оператором програмних, апаратних, програмно-апаратних засобів у складі ОКІІ здійснюється з урахуванням вимог Законів України “Про санкції”, “Про основні засади забезпечення кібербезпеки України”, “Про захист інформації в інформаційно-комунікаційних системах”, інших законів України.

7. Оператору заборонено:

1) використовувати програмні, апаратні, програмно-апаратні засоби у складі ОКІІ, що включені до відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання, ведення якого передбачено статтєю 4 Закону України “Про основні засади забезпечення кібербезпеки України”;

2) обирати в якості постачальника ОКІІ та/або розробника ОКІІ юридичну особу, 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 України, та/або належать суб’єктам, діяльність яких підпадає під дію Закону України “Про санкції” (далі – Закон про санкції) та стосовно яких прийнято рішення про застосування санкцій в Україні.

8. Національний банк має право здійснювати контроль стану впровадження заходів, встановлених цим Положенням:

1) для банків - Операторів під час здійснення заходів контролю, передбачених Положенням про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затвердженого постановою Правління Національного банку України від 16 січня 2021 року № 4 (зі змінами);

2) для важливих об’єктів оверсайта, що є операторами критичної інфраструктури фінансового сектору, під час здійснення виїзного моніторингу відповідно до Положення про проведення виїзного та безвиїзного моніторингу об’єктів оверсайта платіжної інфраструктури, затвердженого постановою Правління Національного банку України від 31 грудня 2022 року № 257 (зі змінами);

3) для установи, яка є власником, держателем та адміністратором єдиної централізованої бази даних щодо обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів (далі – Єдина централізована база даних), під час здійснення нагляду та контролю за дотриманням вимог Положення про функціонування Єдиної централізованої бази даних щодо обов’язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів, затвердженого постановою Правління Національного банку України від 26 грудня 2024 року № 165 (далі – Положення № 165).

9. Вимоги цього Положення поширюються на Операторів, які відповідно до пункту 21 розділу ІІ Положення № 69 забезпечують виконання завдань, реалізацію прав та обов’язків Оператора, дотримання вимог, визначених Законом України “Про критичну інфраструктуру” та законодавством у сфері захисту критичної інфраструктури.

ІІ. Критерії та порядок віднесення об’єктів інформаційної інфраструктури Операторів до ОКІІ

10. Оператор зобов’язаний віднести до ОКІІ інформаційно-комунікаційні системи, власником або розпорядником яких він є, та які одночасно відповідають двом критеріям:

1) порушення штатного режиму функціонування таких інформаційно-комукаційних систем безпосередньо призведе до виникнення кризової ситуації на об’єкті критичної інфраструктури Оператора;

2) у Оператора немає альтернативних за функціональними можливостями інформаційно-комунікаційних систем для забезпечення штатного режиму функціонування об’єкта критичної інфраструктури Оператора.

11. Банк - Оператор додатково до вимог, визначених пунктом 10 розділу ІІ цього Положення має право віднести до ОКІІ:

1) інформаційно-комунікаційні системи, власником або розпорядником яких він є, та які безпосередньо забезпечують автоматизацію здійснення банком - Оператором критичних функцій, визначених банком - Оператором відповідно до

розділу IV Положення про плани відновлення діяльності банків України та банківських груп, затвердженого постановою Правління Національного банку України від 18 липня 2019 року № 95 (зі змінами) (далі – Положення № 95);

2) інформаційно-комунікаційну систему, яка використовується під час надання електронних довірчих послуг, якщо банк - Оператор має статус кваліфікованого надавача електронних довірчих послуг, відомості про якого внесені до Довірчого списку за поданням засвідчувального центру.

12. Важливий об'єкт оверсайта, що є оператором критичної інфраструктури фінансового сектору, додатково до вимог, визначених пунктом 10 розділу II цього Положення, має право віднести до ОКІІ:

1) інформаційно-комунікаційні системи, що безпосередньо забезпечують автоматизацію надання ним критичних операцій / послуг;

2) інформаційно-комунікаційну систему, яка використовується під час надання електронних довірчих послуг, якщо важливий об'єкт оверсайта, що є оператором критичної інфраструктури фінансового сектору, має статус кваліфікованого надавача електронних довірчих послуг, відомості про якого внесені до Довірчого списку за поданням засвідчувального центру.

13. Установа, яка є власником, держателем та адміністратором Єдиної централізованої бази даних, додатково до вимог, визначених пунктом 10 розділу II цього Положення, має право віднести до ОКІІ інформаційно-комунікаційні системи, що забезпечують функціонування Єдиної централізованої бази даних та/або можливість постійного цілодобового доступу користувачів до відкритої інформації, що міститься в Єдиній централізованій базі даних у мережі Інтернет.

14. Оператор зобов'язаний протягом місяця з дня отримання листа від секторального органу відповідно до пункту 20 розділу II Положення № 69 з повідомленням про внесення відомостей про його об'єкти критичної інфраструктури до Реєстру об'єктів критичної інфраструктури:

1) сформувати та затвердити керівником Оператора перелік інформаційно-комунікаційних систем Оператора, віднесених до ОКІІ (далі – перелік ОКІІ) відповідно до пунктів 10-13 розділу II цього Положення;

2) надіслати затверджений перелік ОКІІ Національному банку з урахуванням вимог законодавства України з питань захисту інформації з обмеженим доступом.

15. Оператор зобов'язаний підтримувати в актуальному стані перелік ОКІІ та надсилати Національному банку з урахуванням вимог законодавства України

з питань захисту інформації з обмеженим доступом, оновлений перелік ОКІІ протягом місяця з дня його затвердження.

16. Оператор:

1) щороку станом на 01 листопада переглядає перелік ОКІІ;

2) про результати перегляду інформує Національний банк щороку до 01 грудня та надсилає актуалізований перелік ОКІІ (у разі його оновлення) з урахуванням вимог законодавства України з питань захисту інформації з обмеженим доступом.

17. Оператор зобов'язаний протягом місяця після затвердження переліку ОКІІ або його оновлення:

1) сформувати відомості про ОКІІ у вигляді електронного документа у форматі xlsx згідно з формою, наведеною у додатку до цього Положення;

2) підписати сформовані відомості за допомогою кваліфікованого електронного підпису або удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті електронного підпису, керівника Оператора;

3) надіслати Національному банку відомості про ОКІІ для внесення до реєстру ОКІІ з урахуванням вимог законодавства України з питань захисту інформації з обмеженим доступом.

18. Національний банк упродовж 20 робочих днів із дня отримання від Оператора відомостей про ОКІІ розглядає отримані матеріали та приймає рішення (за відсутності зауважень) щодо внесення цих відомостей до реєстру ОКІІ.

19. Національний банк за наявності зауважень до відомостей про ОКІІ не пізніше ніж протягом двох робочих днів після завершення строку, зазначеного в пункті 18 розділу II цього Положення, повертає відомості про ОКІІ на доопрацювання Оператору в порядку, визначеному Національним банком.

Оператор зобов'язаний протягом 10 робочих днів урахувати зауваження, забезпечити усунення недоліків та повторно направити відомості про ОКІІ з урахуванням вимог законодавства України з питань захисту інформації з обмеженим доступом до Національного банку.

20. Національний банк на підставі отриманих від Оператора відомостей про ОКІІ та за відсутності зауважень до них:

1) вносить ці відомості до реєстру ОКІІ;

2) надсилає листа до Оператора з повідомленням про внесення відомостей про його ОКІІ до реєстру ОКІІ.

21. Оператор зобов’язаний підтримувати в актуальному стані відомості про ОКІІ та надсилати Національному банку ці відомості протягом місяця з дня їх актуалізації з урахуванням вимог законодавства України з питань захисту інформації з обмеженим доступом.

Національний банк має право вимагати від Оператора надання додаткової інформації для уточнення відомостей про ОКІІ шляхом направлення запиту.

Оператор у відповідь на запит Національного банку зобов’язаний у строк, визначений у цьому запиті, та в повному обсязі надати інформацію про ОКІІ.

ІІІ. Заходи щодо забезпечення кіберзахисту ОКІІ банку - Оператора

22. Банк - Оператор зобов’язаний:

1) під час проведення процедури аналізу впливу негативних чинників на процеси діяльності відносити такі бізнес-процеси до вищого рівня критичності та передбачати пріоритетність їх відновлення під час складання плану забезпечення безперервної діяльності;

2) не рідше одного разу на рік проводити тренування щодо відпрацювання заходів Плану реагування на кіберзагрози, кібератаки та кіберінциденти на об’єктах кіберзахисту, передбачений пунктом 18 розділу ІІ Положення про організацію кіберзахисту в банківській системі України, затвердженого постановою Правління Національного банку України від 12 серпня 2022 року № 178 (зі змінами) (далі – Положення № 178), здійснювати тестування плану забезпечення безперервної діяльності та дій банку - Оператора в разі виникнення надзвичайних ситуацій у частині, що стосується функціонування ОКІІ, з обов’язковим документуванням результатів такого тестування;

3) забезпечити участь банку - Оператора в інформаційному обміні в порядку, визначеному в розділі ІІІ Положення № 178;

4) створити умови для підвищення кваліфікації працівників підрозділу з питань кіберзахисту, навчання працівників банку - Оператора стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм.

23. Банк - Оператор зобовязаний призначити відповідальну особу за ОКІІ або покласти виконання цієї функції на працівника підрозділу з інформаційної безпеки, сформованого відповідно до пункту 26 розділу ІV Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі

України, затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95.

24. Відповідальна особа за ОКІІ банку - Оператора здійснює:

1) виконання заходів щодо перегляду та підтримання в актуальному стані переліку ОКІІ, надання актуального переліку ОКІІ до Національного банку відповідно до пунктів 14 – 16 розділу ІІ цього Положення;

2) виконання заходів щодо перегляду та підтримання в актуальному стані відомостей про ОКІІ, надання актуальних відомостей до Національного банку відповідно до пунктів 17, 21 розділу ІІ цього Положення.

IV. Заходи щодо забезпечення кіберзахисту ОКІІ важливого об’єкта оверсайта, що є оператором критичної інфраструктури фінансового сектору

25. Важливий об’єкт оверсайта, що є оператором критичної інфраструктури фінансового сектору зобовязаний призначити відповідальну особу за ОКІІ або покласти виконання цієї функції на відповідальних осіб за забезпечення захисту інформації, кіберзахисту та інформаційної безпеки, визначених відповідно до пунктів 9-10 розділу ІІ Положення про захист інформації та кіберзахист учасниками платіжного ринку, затвердженого постановою Правління Національного банку України від 19 травня 2021 року № 43 (зі змінами) (далі – Положення № 43).

26. Відповідальна особа за ОКІІ важливого об’єкта оверсайта, що є оператором критичної інфраструктури фінансового сектору зобов’язана:

1) забезпечувати виконання заходів щодо перегляду та підтримання в актуальному стані переліку ОКІІ, надання актуального переліку ОКІІ до Національного банку відповідно до пунктів 14 – 16 розділу ІІ цього Положення;

2) забезпечувати виконання заходів щодо перегляду та підтримання в актуальному стані відомостей про ОКІІ, надання актуальних відомостей до Національного банку відповідно до пунктів 17, 21 розділу ІІ цього Положення.

27. Важливий об’єкт оверсайта, що є оператором критичної інфраструктури фінансового сектору зобов’язаний забезпечити вжиття заходів щодо протидії кіберзагрозам, визначених за результатами аналізу вразливостей ОКІІ та пов'язаних із:

1) наданням, використанням, скасуванням та контролем доступу (уключаючи віддалений доступ) до ОКІІ;

2) забезпеченням реєстрації та ведення журналу регістрації подій (логи) кожним компонентом ОКІІ для виявлення кіберінцидентів або ознак кібератак;

3) розробленням Плану реагування на кіберзагрози, кібератаки та кіберінциденти на ОКІІ, узгодженого з політикою інформаційної безпеки, планом забезпечення безперервної діяльності важливого об’єкту оверсайта, що є оператором критичної інфраструктури фінансового сектору;

4) створенням, зберіганням резервних копій даних, відновленням даних із резервних копій та заміною компонентів ОКІІ в разі виходу їх із ладу відповідно до внутрішніх документів з питань забезпечення безперервності діяльності;

5) забезпеченням доступності та відмовостійкості ОКІІ;

6) забезпеченням участі в інформаційному обміні з Центром кіберзахисту Національного банку відповідно до порядку, установленого у пункті 24 розділу ІІІ Положення № 178;

7) забезпеченням аналізу вразливостей, отриманням, тестуванням, упровадженням оновлень програмного забезпечення, що забезпечує функціонування ОКІІ, спрямованих на усунення його вразливостей;

8) захистом ОКІІ від зловмисного коду.

28. Важливий об’єкт оверсайта, що є оператором критичної інфраструктури фінансового сектору зобов'язаний здійснювати реалізацію заходів кіберзахисту ОКІІ з урахуванням вимог та заходів щодо забезпечення захисту інформації, кіберзахисту та інформаційної безпеки у сфері надання платіжних послуг, установлених Положенням № 43.

V. Заходи щодо забезпечення кіберзахисту ОКІІ установою, яка є власником, держателем та адміністратором Єдиної централізованої бази даних

29. Установа, яка є власником, держателем та адміністратором Єдиної централізованої бази даних, зобовязана призначити відповідальну особу за ОКІІ та визначити її права та функціональні обов'язки, сферу відповідальності, кваліфікаційні вимоги, вимоги щодо наявності досвіду роботи у сфері кіберзахисту та інформаційної безпеки в посадовій інструкції цієї відповідальної особи.

30. Відповідальна особа за ОКІІ установи, яка є власником, держателем та адміністратором Єдиної централізованої бази даних, зобов’язана забезпечувати:

1) виконання заходів щодо перегляду та підтримання в актуальному стані переліку ОКІІ, надання актуального переліку ОКІІ до Національного банку відповідно до пунктів 14 –16 розділу ІІ цього Положення;

2) виконання заходів щодо перегляду та підтримання в актуальному стані відомостей про ОКІІ, надання актуальних відомостей про ОКІІ до Національного банку відповідно до пунктів 17, 21 розділу ІІ цього Положення;

3) участь в інформаційному обміні з Центром кіберзахисту Національного банку відповідно до порядку, установленого у пункті 24 розділу ІІІ Положення № 178.

31. Установа, яка є власником, держателем та адміністратором Єдиної централізованої бази даних, зобов'язана здійснювати реалізацію заходів щодо захисту інформації, що міститься в Єдиній централізованій базі даних, відповідно до вимог законодавства України з питань кібербезпеки, захисту інформації та персональних даних, технічного та криптографічного захисту інформації та розділу VI Положення № 165.

Додаток
до Положення про критичну
інформаційну інфраструктуру
фінансового сектору
(підпункт 1 пункту 17 розділу II)

Форма для заповнення Оператором щодо відомостей про ОКІІ

1. Відомості про Оператора

Таблиця 1

№ з/п	Перелік інформації	Інформація для заповнення (надана Оператором)
1	2	3
1	Повне найменування Оператора, адреса його місцезнаходження (індекс, область, місто, вулиця, номер будинку), форма власності, код за Єдиним державним реєстром підприємств та організацій України (далі – ЄДРПОУ)	
2	Повне найменування надавача (надавачів) послуг із доступу до мережі Інтернет, код за ЄДРПОУ, перелік послуг із кіберзахисту (відповідно до договору отримання Оператором послуг із доступу до мережі Інтернет)	
3	Повне найменування надавача (надавачів) хмарних послуг та/або надавача (надавачів) послуг центру обробки даних, код за ЄДРПОУ (за наявності), перелік послуг (відповідно до договору отримання хмарних послуг та/або послуг центру обробки даних)	
4	Діапазон зовнішніх IP-адрес Оператора	

Продовження додатка

2. Відомості про ОКІІ Оператора

Таблиця 2

№	Повна та скорочена назва ОКІІ відповідно до документа про введення в експлуатацію, дата введення в експлуатацію	Повне найменування юридичної особи – постачальника ОКІІ, код за ЄДРПОУ (за наявності), країна її реєстрації, кінцевий термін технічної підтримки ОКІІ (за наявності)	Повне найменування юридичної особи – розробника ОКІІ, код за ЄДРПОУ (за наявності), країна її реєстрації	Призначення ОКІІ	Перелік критичних функцій або критичних операцій / послуг, надання яких забезпечує Оператор (у разі віднесення інформаційної системи до ОКІІ відповідно до пунктів 10, 11 розділу ІІ Положення)	Вид інформації за порядком доступу, що обробляється на ОКІІ	Уніфіковані ідентифікатори (англійською мовою Uniform Resource Identifier) ОКІІ, що опубліковані в мережі Інтернет
1	2	3	4	5	6	7	8
1							

Пояснення до заповнення додатка

1. У таблиці 2:

1) окремим рядком надається інформація щодо кожної інформаційно-комунікаційної системи Оператора, які визначені ОКІІ. Не потрібно зазначати як ОКІІ окремі компоненти інформаційної інфраструктури Оператора, а саме: програмне та апаратне забезпечення, комп’ютерне устаткування, програмно-технічні комплекси та системи, призначені

для приймання, передавання, керування, оброблення, зберігання та захисту інформації, а також канали зв’язку, що використовуються для забезпечення функціонування ОКІІ;

2) у колонці 6 зазначаються критичні функції у розумінні Положення № 95 або критичні операції / послуги у розумінні Положення № 187;

2. Відомості про ОКІІ, що наведені у таблицях 1, 2 цього додатку, надсилаються до Національного банку України в табличній формі одним файлом у форматі xlsx, що сумісний з Microsoft Excel.

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Зміни до
Положення про захист інформації та кіберзахист учасниками платіжного ринку

1. У розділі I:

1) у пункті 1 слова “Про електронні довірчі послуги” замінити словами “Про електронну ідентифікацію та електронні довірчі послуги”;

2) у пункті 3:
у абзаці другому підпункту 10 слова “важливої платіжної системи” замінити словами “системно важливої / важливої платіжної системи”;
підпункт 16 викласти в такій редакції:
“16) суб'єкт інформаційного захисту – надавач платіжних послуг (крім установ електронних грошей, Національного банку, органів державної влади та органів місцевого самоврядування), оператор платіжної системи-резидент та технологічний оператор платіжних послуг.”.

2. У розділі XIII:

1) у пункті 45:
підпункт 2 викласти в такій редакції:
“2) події, які класифікуються згідно із Положенням про вимоги до системи управління надавача фінансових платіжних послуг, затвердженим постановою Правління Національного банку України від 10 жовтня 2024 року № 123 (зі змінами) (далі – Положення № 123), як кіберінциденти, пов’язані з наданням платіжних послуг (виконанням платіжних операцій) та які відповідають рівням критичності високий (помаранчевий), критичний (червоний) та надзвичайний (чорний) (далі – значні кіберінциденти);”;
пункт доповнити новим підпунктом такого змісту:
“4) події, які класифікуються згідно із Положенням № 123, як кіберінциденти, пов’язані з наданням платіжних послуг (виконанням платіжних операцій) та які відповідають рівню критичності середній (жовтий);”;

2) абзац перший пункту 46 викласти в такій редакції:
“46. Повідомлення про події, зазначені в підпунктах 1, 3, 4 пункту 45 розділу XIII цього Положення, слід надавати одним із таких способів:”;

3) розділ доповнити новим пунктом такого змісту:

“47. Повідомлення про події, зазначені в підпункті 2 пункту 45 розділу XIII цього Положення, слід надавати електронним листом на електронну поштову скриньку Центру кіберзахисту Національного банку cyber@bank.gov.ua.”.

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Зміни до
Положення про організацію кіберзахисту в банківській системі України

1. У розділі I:

1) у пункті 2:

підпункт 1 замінити двома новими підпунктами 1 та 1^1 такого змісту:

“1) банк - Оператор – банк, що є оператором критичної інфраструктури фінансового сектору відповідно до Положення про критичну інфраструктуру фінансового сектору, затвердженого постановою Правління Національного банку України від 27 червня 2025 року № 69 (далі – Положення № 69);

1^1) довірені внутрішні джерела інформації - Центр кіберзахисту Національного банку України (далі - Центр кіберзахисту), команда реагування на кіберінциденти в банківській системі України (англійською мовою Computer Security Incident Response Team of the National Bank of Ukraine, CSIRT-NBU), що входить до складу Центру кіберзахисту, банки України;”.

У зв’язку з цим абзаци третій – двадцятий уважати відповідно абзацами четвертим – двадцять першим;

підпункти 6, 7 виключити.

У зв’язку з цим абзаци одинадцятий – двадцять перший уважати відповідно абзаціми дев’ятим – дев’ятнадцятим;

підпункт 9 включити.

У зв’язку з цим абзаци абзаци одинадцятий - дев’ятнадцятий уважати відповідно абзацами десятим – вісімнадцятим;

абзац чотирнадцятий після слів та цифр “від 16 січня 2021 року № 4” доповнити словами “(зі змінами)”;

абзац п’ятнадцятий виключити.

У зв’язку з цим абзаци шістнадцятий - вісімнадцятий уважати відповідно абзацами п’ятнадцятим - сімнадцятим;

абзац шістнадцятий виключити.

У зв’язку з цим абзац сімнадцятий уважати абзацом шістнадцятим;

2) підпункт 3 пункту 3 виключити;

3) у пункті 5 слова та цифри “у розділах II, IV цього Положення” замінити словами “цим Положенням”;

4) абзац другий пункту 6 виключити.

2. У підпункті 4 пункту 13 розділу II слова та цифри “відповідно до розділу IV цього Положення” виключити.

3. Пункт 20 розділу III викласти в такій редакції:

“20. Учасниками інформаційного обміну є суб'єкти кіберзахисту, визначені в пункті 8 розділу II цього Положення. Центр кіберзахисту має право залучати до участі в інформаційному обміні установи, що є операторами критичної інфраструктури фінансового сектору відповідно до Положення № 69.”.

4. Розділ IV виключити.

5. Абзац другий пункту 42 розділу V викласти в такій редакції:

“Банк самостійно встановлює періодичність проведення зовнішнього аудиту. Періодичність проведення зовнішнього аудиту для банку - Оператора залежить від категорії критичності об’єктів критичної інфраструктури та становить:”.

6. Додаток до Положення виключити.