**Порівняльна таблиця**

до проєкту постанови Правління Національного банку України

“Про критичну інфраструктуру фінансового сектору”

|  |  |
| --- | --- |
| Зміст положення (норми) чинного нормативно-правового акта | Зміст відповідного положення (норми) проєкту нормативно-правового акта |

|  |  |
| --- | --- |
| Положення про організацію кіберзахисту в банківській системі України  *У тексті Положення слово та літери “банк ОКІ” у всіх відмінках замінити словом та літерами “банк – оператор критичної інфраструктури” у відповідних відмінках.* | |
| І. Загальні положення | І. Загальні положення |
| 1. Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про основні засади забезпечення кібербезпеки України”, з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, ~~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 27010:2018 “Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій” (ISO/IEC 27010:2015, IDT), прийнятого наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 10 грудня 2018 року № 470 (далі - Національний стандарт України ДСТУ ISO/IEC 27010:2018), регламенту Європейського парламенту і Ради (ЄС) від 14 грудня 2022 року № 2022/2554 щодо цифрової операційної стійкості фінансового сектору та внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909/2014 та (ЄС) 2016/1011. | 1. Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про основні засади забезпечення кібербезпеки України”, з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, Національного стандарту України ДСТУ ISO/IEC 27010:2018 “Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій” (ISO/IEC 27010:2015, IDT), прийнятого наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 10 грудня 2018 року № 470 (далі - Національний стандарт України ДСТУ ISO/IEC 27010:2018), регламенту Європейського парламенту і Ради (ЄС) від 14 грудня 2022 року № 2022/2554 щодо цифрової операційної стійкості фінансового сектору та внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС)  № 648/2012, (ЄС) № 600/2014, (ЄС) № 909/2014 та (ЄС) 2016/1011. |
| 2. Терміни та скорочення в цьому Положенні вживаються в такому значенні:  … | 2. Терміни та скорочення в цьому Положенні вживаються в такому значенні:  … |
| ~~7) об'єкт критичної інформаційної інфраструктури - інформаційна система об'єкта критичної інфраструктури в банківській системі України, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;~~ |  |
| ~~Термін “об'єкт критичної інфраструктури в банківській системі України” вживається в значенні, визначеному Положенням про визначення об'єктів критичної інфраструктури в банківській системі України, затвердженим постановою Правління Національного банку України від 30 листопада 2020 року № 151 (далі - Положення про ОКІ № 151)~~. | **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. Це Положення розроблено з метою унормування питань організації та забезпечення кіберзахисту і визначає:  … | 3. Це Положення розроблено з метою унормування питань організації та забезпечення кіберзахисту і визначає:  … |
| 3) вимоги стосовно заходів щодо забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури в банківській системі України; | 3) вимоги стосовно заходів щодо забезпечення кіберзахисту об'єктів критичної ~~інформаційної~~ інфраструктури в банківській системі України; |
| 6. Вимоги цього Положення поширюються на банки України.  Вимоги розділу IV цього Положення поширюються лише на банки України, що ~~визначені об'єктами критичної інфраструктури в банківській системі України відповідно до Положення про ОКІ № 151 (далі - банки ОКІ)~~. | 6. Вимоги цього Положення поширюються на банки України.  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).** |
| **IV. Заходи щодо забезпечення кіберзахисту критичної ~~інформаційної~~ інфраструктури банків ~~ОКІ~~** | **IV. Заходи щодо забезпечення кіберзахисту критичної інфраструктури банків** |
| 30. Банк ~~ОКІ~~ зобов'язаний віднести до об'єктів критичної інформаційної інфраструктури інформаційні системи~~, що~~ ~~безпосередньо забезпечують автоматизацію банківської діяльності (надання банківських послуг) банку ОКІ та~~ відповідають двом критеріям:  1) порушення функціонування ~~інформаційної системи~~ внаслідок кіберінциденту, кібератаки ~~може вплинути на~~ ~~стале функціонування банку ОКІ та безперервність надання банком ОКІ відповідних послуг~~;  2) якщо немає в банку ОКІ альтернативних за функціональними можливостями інформаційних систем для надання аналогічних відповідних послуг. | 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 ~~ОКІ~~ має право віднести до ~~об'єктів критичної інформаційної інфраструктури (далі -~~ ОКІІ~~)~~ інші інформаційні системи, що безпосередньо забезпечують автоматизацію процесів надання банком ОКІ фінансових послуг та інших видів його діяльності відповідно до [статті 47](https://zakon.rada.gov.ua/laws/show/2121-14#n819) Закону України “Про банки і банківську діяльність”, надання кваліфікованих електронних довірчих послуг за умови відповідності критеріям, викладеним у [пункті 30](https://zakon.rada.gov.ua/laws/show/v0178500-22#n148) розділу IV цього Положення. | 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](https://zakon.rada.gov.ua/laws/show/2121-14#n819) Закону України “Про банки і банківську діяльність”, надання кваліфікованих електронних довірчих послуг за умови відповідності критеріям, викладеним у **підпункті 2** [**пункту** 30](https://zakon.rada.gov.ua/laws/show/v0178500-22#n148) розділу IV цього Положення. |
| 32. Банк ~~ОКІ~~ зобов'язаний протягом місяця з дня отримання повідомлення ~~про включення його до переліку об'єктів критичної інфраструктури в банківській системі України~~:  1) сформувати перелік інформаційних систем банку, віднесених до ОКІІ (далі - перелік ОКІІ), відповідно до пункту 30 розділу IV цього Положення ~~та затвердити його~~;  2) надати затверджений перелік ОКІІ Національному банку. | 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.** |
| 33. Банк ~~ОКІ~~ зобов'язаний підтримувати в актуальному стані перелік ОКІІ та надавати Національному банку оновлений перелік ОКІІ протягом місяця з дня його затвердження. | 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. |
| 34. Банк ~~ОКІ~~:  1) щороку переглядає перелік ОКІІ;  2) про результати перегляду інформує Національний банк щороку до ~~20~~ грудня. | 34. Банк – **оператор критичної інфраструктури**:  1) щороку **станом на 01 листопада** переглядає перелік ОКІІ;  2) про результати перегляду інформує Національний банк щороку до **01** грудня **та надає актуалізований перелік ОКІІ (у разі його оновлення) у спосіб, встановлений пунктом 41 розділу IV цього Положення**. |
| 35. Банк ~~ОКІ~~ зобов'язаний протягом місяця після затвердження ~~власного~~ переліку ОКІІ:  1) сформувати відомості про ОКІІ згідно з додатком до цього Положення;  2) підписати сформовані відомості за допомогою кваліфікованого електронного підпису CISO банку ~~ОКІ~~;  3) надати Національному банку відомості про ОКІІ для внесення до реєстру об'єктів критичної інформаційної інфраструктури ~~в банківській системі України шляхом завантаження через портал Центру кіберзахисту~~. | 35. Банк – **оператор критичної інфраструктури** зобов'язаний протягом місяця після затвердження переліку ОКІІ або **його оновлення**:  1) сформувати відомості про ОКІІ згідно з додатком до цього Положення;  2) підписати сформовані відомості за допомогою кваліфікованого електронного підпису CISO банку - **оператора критичної інфраструктури**;  3) надати Національному банку відомості про ОКІІ для внесення до реєстру об'єктів критичної інформаційної інфраструктури **в спосіб, встановлений пунктом 41 розділу IV цього Положення.** |
| 36. Банк ~~ОКІ~~ зобов'язаний підтримувати в актуальному стані відомості про ОКІІ.  Національний банк має право вимагати від банку ~~ОКІ~~ надання додаткової інформації для уточнення відомостей про ОКІІ шляхом направлення запиту.  Банк ~~ОКІ~~ у відповідь на запит зобов'язаний у термін, визначений у запиті, та в повному обсязі надати уточнювальну інформацію про ОКІІ. | 36. Банк – **оператор критичної інфраструктури** зобов'язаний підтримувати в актуальному стані відомості про ОКІІ **та надавати Національному банку ці відомості протягом місяця з дня їх актуалізації у спосіб, встановлений пунктом 41 розділу IV цього Положення.**  Національний банк має право вимагати від банку – **оператора критичної інфраструктури** надання додаткової інформації для уточнення відомостей про ОКІІ шляхом направлення запиту.  Банк – **оператор критичної інфраструктури** у відповідь на запит зобов'язаний у термін, визначений у запиті, та в повному обсязі надати уточнювальну інформацію про ОКІІ. |
| 37. Банк ~~ОКІ~~ зобов'язаний:  1) визначити критичними щодо інформаційної безпеки бізнес-процеси діяльності банку, автоматизацію яких забезпечують ОКІІ, з обов'язковим уключенням їх до сфери застосування системи управління інформаційною безпекою (далі - СУІБ) та упровадженням для них заходів безпеки, використовуючи ризик-орієнтований підхід~~, що визначені в додатку А до Національного стандарту України ДСТУ ISO/IEC 27001:2015;~~….. | 37. Банк **– оператор критичної інфраструктури** зобов'язаний:  1) визначити критичними щодо інформаційної безпеки бізнес-процеси діяльності банку, автоматизацію яких забезпечують ОКІІ, з обов'язковим уключенням їх до сфери застосування системи управління інформаційною безпекою (далі - СУІБ) та упровадженням для них заходів безпеки, використовуючи ризик-орієнтований підхід; |
| 38. CISO банку ~~ОКІ~~ забезпечує організацію:  3) участі банку ~~ОКІ~~ в інформаційному обміні в порядку, визначеному в розділі III цього Положення;  4) пріоритетної реалізації заходів кіберзахисту критичної інформаційної інфраструктури банку відповідно до розробленого Плану реагування в разі кібератаки (спроби реалізації кіберзагрози) на об'єкти кіберзахисту банку ~~ОКІ~~;  ……………….  6) створення умов для підвищення кваліфікації працівників підрозділу з питань кіберзахисту, навчання працівників банку ~~ОКІ~~ стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм. | 38. CISO банку **– оператора критичної інфраструктури** забезпечує організацію:  3) участі банку **– оператора критичної інфраструктури** в інформаційному обміні в порядку, визначеному в розділі III цього Положення;  4) пріоритетної реалізації заходів кіберзахисту критичної інформаційної інфраструктури банку відповідно до розробленого Плану реагування в разі кібератаки (спроби реалізації кіберзагрози) на об'єкти кіберзахисту банку **– оператора критичної інфраструктури**;  ………………….  6) створення умов для підвищення кваліфікації працівників підрозділу з питань кіберзахисту, навчання працівників банку **– оператора критичної інфраструктури** стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм. |
| 39. Зв'язок технологічної платформи критичної інформаційної інфраструктури банку ~~ОКІ~~ з мережею Інтернет повинен здійснюватися з використанням двох або більше каналів передавання даних, що надаються різними операторами, провайдерами телекомунікацій через захищені вузли доступу з мережі Інтернет. | 39. Зв'язок технологічної платформи критичної інформаційної інфраструктури банку **– оператора критичної інфраструктури** з мережею Інтернет повинен здійснюватися з використанням двох або більше каналів передавання даних, що надаються різними операторами, провайдерами телекомунікацій через захищені вузли доступу з мережі Інтернет. |
| 40. Використання банком ~~ОКІ~~ програмних, апаратних, програмно-апаратних засобів у складі об'єкта критичної інформаційної інфраструктури здійснюється з урахуванням вимог Законів України [“Про санкції”](https://zakon.rada.gov.ua/laws/show/1644-18), [“Про основні засади забезпечення кібербезпеки України”](https://zakon.rada.gov.ua/laws/show/2163-19), інших законів України. | 40. Використання банком **– оператором критичної інфраструктури** програмних, апаратних, програмно-апаратних засобів у складі об'єкта критичної інформаційної інфраструктури здійснюється з урахуванням вимог Законів України [“Про санкції”](https://zakon.rada.gov.ua/laws/show/1644-18), [“Про основні засади забезпечення кібербезпеки України”](https://zakon.rada.gov.ua/laws/show/2163-19), інших законів України. |
| 41. Відомості про ~~об'єкти критичної інформаційної інфраструктури~~ ~~банків ОКІ~~ є інформацією з обмеженим доступом. | 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.** |
| V. Вимоги до проведення аудиту інформаційної безпеки в банківській системі України | V. Вимоги до проведення аудиту інформаційної безпеки в банківській системі України |
| 42. Банк самостійно встановлює періодичність проведення аудиту інформаційної безпеки (далі - зовнішній аудит). 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.  ~~У банках ОКІ зовнішній аудит критичної інформаційної інфраструктури здійснюється відповідно до вимог та порядку, що встановлені нормативно-правовими актами Національного банку.~~  Допускається проведення зовнішнього аудиту в межах аудиту щорічної перевірки фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності аудиторською фірмою. | 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:**  **не рідше ніж один раз на два роки для об’єктів I та II категорії критичності;**  **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. |
| 43. Банк самостійно обирає:  1) аудиторську фірму для проведення зовнішнього аудиту серед юридичних осіб - резидентів України;  2) міжнародні стандарти, кращу практику (англійською мовою best practices) з питань інформаційної безпеки і кіберзахисту, відповідно до яких проводитиметься зовнішній аудит з питань, зазначених у підпункті 1 пункту 44 розділу V цього Положення.  Банк до укладення договору перевіряє наявність чинних сертифікатів/дипломів міжнародного та/або державного зразка в аудиторів, які безпосередньо залучатимуться для проведення зовнішнього аудиту. | 43. Банк самостійно обирає:  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.**  2) міжнародні стандарти, кращу практику (англійською мовою best practices) з питань інформаційної безпеки і кіберзахисту, відповідно до яких проводитиметься зовнішній аудит з питань, зазначених у підпункті 1 пункту 44 розділу V цього Положення.  Банк до укладення договору перевіряє наявність чинних сертифікатів/дипломів міжнародного та/або державного зразка в аудиторів, які безпосередньо залучатимуться для проведення зовнішнього аудиту. |
| 44. Зовнішній аудит проводиться з метою незалежної оцінки:  ….  2) ~~рівня~~ відповідності СУІБ банку ~~Національному стандарту України ДСТУ~~ ISO/IEC 27001~~:2015~~ ~~та/або міжнародному стандарту ISO/IEC 27001:2013 “Information technology - Security techniques - Information security management systems - Requirements”, що був прийнятий міжнародною організацією зі стандартизації~~. | 44. Зовнішній аудит проводиться з метою незалежної оцінки:  ….  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. |
| Додаток  до Положення про організацію кіберзахисту в банківській системі України (підпункт 1 пункту 35 розділу IV)  І. Відомості про ОКІІ  1.Повне найменування банку ~~ОКІ~~, юридична адреса (індекс, область, місто, вулиця, номер будинку), форма власності, код за ЄДРПОУ.  2. Повне найменування за ЄДРПОУ надавача (надавачів) послуг із доступу до мережі Інтернет, код за ЄДРПОУ, перелік послуг із кіберзахисту (відповідно до договору отримання банком ~~ОКІ~~ послуг із доступу до мережі Інтернет).    3. Діапазон зовнішніх IР-адрес банку ~~ОКІ~~.  4. Відомості про ОКІІ:  …..  2) ~~призначення ОКІІ, перелік банківських, фінансових та інших послуг, надання яких він забезпечує;~~ | Додаток  до Положення про організацію кіберзахисту в банківській системі України (підпункт 1 пункту 35 розділу IV)  І. Відомості про ОКІІ  1.Повне найменування банку – **оператора критичної інфраструктури**, юридична адреса (індекс, область, місто, вулиця, номер будинку), форма власності, код за ЄДРПОУ.  2. Повне найменування за ЄДРПОУ надавача (надавачів) послуг із доступу до мережі Інтернет, код за ЄДРПОУ, перелік послуг із кіберзахисту (відповідно до договору отримання банком – **оператором критичної інфраструктури** послуг із доступу до мережі Інтернет).    3. Діапазон зовнішніх IР-адрес банку – **оператора критичної інфраструктури**.  4. Відомості про ОКІІ:  …..  **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);**  … |

Начальник управління

захисту критичної інфраструктури Роман ПРОСКУРОВСЬКИЙ