Порівняльна таблиця

до проєкту постанови Правління Національного банку України

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

Зміст положення (норми) чинного нормативно-правового акта	Зміст відповідного положення (норми) проєкту нормативно-правового акта
Положення про захист інформації та кіберзахист учасниками платіжного ринку, затверджене постановою Правління Національного банку України від 19 травня 2021 року № 43 (зі змінами)	
I. Загальні положення	I. Загальні положення
1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про платіжні послуги", "Про основні засади забезпечення кібербезпеки України", ~~"Про електронні довірчі послуги"~~.	1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про платіжні послуги", "Про основні засади забезпечення кібербезпеки України", **“Про електронну ідентифікацію та електронні довірчі послуги”.**
3. Терміни, що використовуються в цьому Положенні, вживаються в такому значенні: 10) ключовий суб’єкт інформаційного захисту – суб’єкт інформаційного захисту, який належить до однієї категорії або більше: оператор важливої платіжної системи, якщо він виконує функції технологічного оператора платіжних послуг у цій платіжній системі; важливий технологічний оператор платіжних послуг; технологічний оператор платіжних послуг, який надає послуги платіжній системі, створеній нерезидентом, та який	3. Терміни, що використовуються в цьому Положенні, вживаються в такому значенні: …. 10) ключовий суб’єкт інформаційного захисту – суб’єкт інформаційного захисту, який належить до однієї категорії або більше: оператор **системно важливої /** важливої платіжної системи, якщо він виконує функції технологічного оператора платіжних послуг у цій платіжній системі; важливий технологічний оператор платіжних послуг; технологічний оператор платіжних послуг, який надає послуги платіжній системі, створеній

отримав дозвіл Національного банку України (далі – Національний банк) надавати свої послуги в Україні; технологічний оператор платіжних послуг, що надає послуги більше ніж одній платіжній системі; ….. 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 ~~у разі надання інших видів послуг, крім оброблення платіжних операцій в міжнародних карткових платіжних системах~~.	нерезидентом, та який отримав дозвіл Національного банку України (далі – Національний банк) надавати свої послуги в Україні; технологічний оператор платіжних послуг, що надає послуги більше ніж одній платіжній системі; …. 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.
XIII. Вимоги щодо фіксації кіберінцидентів та інцидентів інформаційної безпеки і реагування на них	XIII. Вимоги щодо фіксації кіберінцидентів та інцидентів інформаційної безпеки і реагування на них
45. Суб'єкт інформаційного захисту зобов'язаний невідкладно повідомити Національний банк, якщо виявлено: 1) події, що містять ознаки злочинів, передбачених у розділі XVI Кримінального кодексу України;	45. Суб'єкт інформаційного захисту зобов'язаний невідкладно повідомити Національний банк, якщо виявлено: 1) події, що містять ознаки злочинів, передбачених у розділі XVI Кримінального кодексу України;
~~2) події, які класифікуються згідно із Законом України "Про основні засади забезпечення кібербезпеки України" як кіберінциденти;~~	**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 (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);
3) події, що призвели до витоку чи незаконного розголошення інформації з обмеженим доступом, яка обробляється в ІС~~.~~	3) події, що призвели до витоку чи незаконного розголошення інформації з обмеженим доступом, яка обробляється в ІС**;**
відсутній	**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);**
46. Повідомлення про події, зазначені ~~в пункті~~ 45 розділу XIII цього Положення, слід надавати одним із таких способів: 1) електронним листом засобами системи електронної пошти Національного банку; 2) електронним листом на офіційну електронну поштову скриньку Національного банку; 3) засобами поштового зв'язку на паперовому носії (у разі неможливості використання вищезазначених засобів електронного зв'язку).	46. Повідомлення про події, зазначені в **підпунктах 1, 3, 4 пункту** 45 розділу XIII цього Положення, слід надавати одним із таких способів: 1) електронним листом засобами системи електронної пошти Національного банку; 2) електронним листом на офіційну електронну поштову скриньку Національного банку; 3) засобами поштового зв'язку на паперовому носії (у разі неможливості використання вищезазначених засобів електронного зв'язку).

відсутній	**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.**
Положення про організацію кіберзахисту в банківській системі України, затверджене постановою Правління Національного банку України від 12 серпня 2022 року № 178 (зі змінами)	
I. Загальні положення	I. Загальні положення
2. Терміни та скорочення в цьому Положенні вживаються в такому значенні: …	2. Терміни та скорочення в цьому Положенні вживаються в такому значенні: …
відсутній	**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~~) довірені внутрішні джерела інформації - Центр кіберзахисту Національного банку України (далі - Центр кіберзахисту), команда реагування на кіберінциденти в банківській системі України (CSIRT-NBU, англійською мовою Computer Security Incident Response Team of the National Bank of Ukraine), що входить до складу Центру кіберзахисту, банки України;	**1[1]**) довірені внутрішні джерела інформації - Центр кіберзахисту Національного банку України (далі - Центр кіберзахисту), команда реагування на кіберінциденти в банківській системі України (CSIRT-NBU, англійською мовою Computer Security Incident Response Team of the National Bank of Ukraine), що входить до складу Центру кіберзахисту, банки України;
2) довірені зовнішні джерела інформації – вітчизняні, іноземні та міжнародні команди (центри, групи) реагування на кіберінциденти, ключові постачальники послуг, взаємодія	2) довірені зовнішні джерела інформації – вітчизняні, іноземні та міжнародні команди (центри, групи) реагування на кіберінциденти, ключові постачальники

з якими здійснюється на підставі укладених угод (меморандумів) та асоціацій, участь у роботі яких здійснюється на правах офіційного членства;	послуг, взаємодія з якими здійснюється на підставі укладених угод (меморандумів) та асоціацій, участь у роботі яких здійснюється на правах офіційного членства;
3) ЄДБО – Єдиний договір банківського обслуговування та надання інших послуг Національним банком України (далі – Національний банк);	3) ЄДБО – Єдиний договір банківського обслуговування та надання інших послуг Національним банком України (далі – Національний банк);
3^1) значний кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої (потенційної) кібератаки, рівень критичності яких суттєво загрожує штатному функціонуванню інформаційних систем банку, що безпосередньо забезпечують автоматизацію банківської діяльності, та мають значний негативний вплив на надання банківських послуг, який може призвести до зміни функціональних можливостей таких послуг або робить їх недоступними;	3^1) значний кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої (потенційної) кібератаки, рівень критичності яких суттєво загрожує штатному функціонуванню інформаційних систем банку, що безпосередньо забезпечують автоматизацію банківської діяльності, та мають значний негативний вплив на надання банківських послуг, який може призвести до зміни функціональних можливостей таких послуг або робить їх недоступними;
4) інформація загальноорганізаційного характеру – інформація, що поширюється під час інформаційного обміну, містить описи національних та міжнародних стандартів, інноваційних методик та практики з питань кіберзахисту, світового та вітчизняного досвіду у сфері кібербезпеки та кіберзахисту, посилання на джерела такої інформації;	4) інформація загальноорганізаційного характеру – інформація, що поширюється під час інформаційного обміну, містить описи національних та міжнародних стандартів, інноваційних методик та практики з питань кіберзахисту, світового та вітчизняного досвіду у сфері кібербезпеки та кіберзахисту, посилання на джерела такої інформації;
5) інформація технічного характеру – інформація, що поширюється під час інформаційного обміну та містить відомості про зразки програмного забезпечення, його вразливості та профілі безпечного налаштування, відомості	5) інформація технічного характеру – інформація, що поширюється під час інформаційного обміну та містить відомості про зразки програмного забезпечення, його вразливості та профілі безпечного налаштування,

про зразки апаратних, програмних та апаратно-програмних комплексів і систем кіберзахисту, профілі їх налаштування, описи зразків шкідливого програмного забезпечення та наслідків їх роботи, рекомендації щодо заходів реагування, протидії та нейтралізації наслідків роботи останніх, індикатори кіберзагроз, повідомлення про кібератаки та/або кіберінциденти, рекомендації про необхідність або застереження (заборону) вжиття відповідних заходів;	відомості про зразки апаратних, програмних та апаратно-програмних комплексів і систем кіберзахисту, профілі їх налаштування, описи зразків шкідливого програмного забезпечення та наслідків їх роботи, рекомендації щодо заходів реагування, протидії та нейтралізації наслідків роботи останніх, індикатори кіберзагроз, повідомлення про кібератаки та/або кіберінциденти, рекомендації про необхідність або застереження (заборону) вжиття відповідних заходів;
~~6) критична інформаційна інфраструктура - сукупність об'єктів критичної інформаційної інфраструктури банку, визначена об'єктом критичної інфраструктури в банківській системі України;~~	
~~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;~~	
8) портал Центру кіберзахисту Національного банку – спеціалізований сайт Національного банку, створений для організації роботи та надання сервісів Центром кіберзахисту, що доступний за посиланням https://cyber.bank.gov.ua/ (далі – портал Центру кіберзахисту);	8) портал Центру кіберзахисту Національного банку – спеціалізований сайт Національного банку, створений для організації роботи та надання сервісів Центром кіберзахисту, що доступний за посиланням https://cyber.bank.gov.ua/ (далі – портал Центру кіберзахисту);
~~9) реєстр об'єктів критичної інформаційної інфраструктури - відомості про інформаційні системи, які~~	

~~відповідно до вимог цього Положення віднесено до об'єктів критичної інформаційної інфраструктури;~~	
9[1]) рівень критичності кіберінциденту – ступень негативного впливу на банк та/або суб'єктів системи кіберзахисту в банківській системі України, що може відбутися в результаті реалізації кіберзагроз;	9[1]) рівень критичності кіберінциденту – ступень негативного впливу на банк та/або суб'єктів системи кіберзахисту в банківській системі України, що може відбутися в результаті реалізації кіберзагроз;
10) система кіберзахисту в банківській системі України – сукупність суб'єктів, упроваджених систем, комплексів та засобів забезпечення кіберзахисту, взаємопов'язаних заходів організаційного, технічного, інформаційного характеру щодо забезпечення належного рівня кібербезпеки та кіберстійкості банківської системи України;	10) система кіберзахисту в банківській системі України – сукупність суб'єктів, упроваджених систем, комплексів та засобів забезпечення кіберзахисту, взаємопов'язаних заходів організаційного, технічного, інформаційного характеру щодо забезпечення належного рівня кібербезпеки та кіберстійкості банківської системи України;
10[1]) системний кіберризик – ризик порушення стабільності банківської системи внаслідок реалізації кіберзагроз щодо окремого банку через відповідні недоліки в його кіберстійкості;	10[1]) системний кіберризик – ризик порушення стабільності банківської системи внаслідок реалізації кіберзагроз щодо окремого банку через відповідні недоліки в його кіберстійкості;
11) MISP-NBU Центру кіберзахисту (англійською мовою Malware Information Sharing Platform of the National Bank of Ukraine) – спеціалізований сайт Національного банку, що побудований на базі платформи з відкритим програмним кодом MISP і доступний за посиланням https://misp.bank.gov.ua/, призначений для організації доступу банків до системи збору, обробки, зберігання і обміну інформацією загальноорганізаційного та технічного характеру в режимі реального часу з урахуванням вимог конфіденційності (далі – MISP-NBU).	11) MISP-NBU Центру кіберзахисту (англійською мовою Malware Information Sharing Platform of the National Bank of Ukraine) – спеціалізований сайт Національного банку, що побудований на базі платформи з відкритим програмним кодом MISP і доступний за посиланням https://misp.bank.gov.ua/, призначений для організації доступу банків до системи збору, обробки, зберігання і обміну інформацією загальноорганізаційного та технічного характеру в режимі реального часу з

	урахуванням вимог конфіденційності (далі – MISP-NBU).
Термін “аудит інформаційної безпеки” вживається в значенні, визначеному Положенням про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затвердженим постановою Правління Національного банку України від 16 січня 2021 року № 4 (далі – Положення про контроль № 4).	Термін “аудит інформаційної безпеки” вживається в значенні, визначеному Положенням про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затвердженим постановою Правління Національного банку України від 16 січня 2021 року № 4 **(зі змінами)** (далі – Положення про контроль № 4).
~~Терміни “об’єкт критичної інфраструктури”, “оператор критичної інфраструктури”, “реєстр об’єктів критичної інфраструктури” уживаються в значеннях, визначених у Законі України “Про критичну інфраструктуру”.~~ Терміни “об’єкт критичної інформаційної інфраструктури”, “критична інформаційна інфраструктура” уживаються в значеннях, визначених у Законі України “Про основні засади забезпечення кібербезпеки України”. ~~Термін “АРМ-НБУ-інформаційний” уживається в значенні, визначеному в Положенні про використання засобів криптографічного захисту інформації Національного банку України, затвердженому постановою Правління Національного банку України від 14 квітня 2023 року № 49.~~ Інші терміни в цьому Положенні вживаються в значеннях, визначених у Законі України “Про основні засади забезпечення кібербезпеки України” та нормативно-правових актах Національного банку.	Терміни “об’єкт критичної інформаційної інфраструктури”, “критична інформаційна інфраструктура” уживаються в значеннях, визначених у Законі України “Про основні засади забезпечення кібербезпеки України”. Інші терміни в цьому Положенні вживаються в значеннях, визначених у Законі України “Про основні засади забезпечення кібербезпеки України” та нормативно-правових актах Національного банку.

3. Це Положення розроблено з метою унормування питань організації та забезпечення кіберзахисту і визначає: 1) основні засади функціонування системи кіберзахисту в банківській системі України; 2) принципи забезпечення інформаційного обміну між Центром кіберзахисту і банками України; ~~3) вимоги стосовно заходів щодо забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури в банківській системі України;~~	3. Це Положення розроблено з метою унормування питань організації та забезпечення кіберзахисту і визначає: 1) основні засади функціонування системи кіберзахисту в банківській системі України; 2) принципи забезпечення інформаційного обміну між Центром кіберзахисту і банками України;
5. Національний банк має право здійснювати перевірку стану впровадження заходів щодо забезпечення кіберзахисту, встановлених ~~у розділах II, IV цього Положення~~, під час здійснення заходів контролю, передбачених Положенням про контроль № 4.	5. Національний банк має право здійснювати перевірку стану впровадження заходів щодо забезпечення кіберзахисту, встановлених **цим Положенням**, під час здійснення заходів контролю, передбачених Положенням про контроль № 4.
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).~~	6. Вимоги цього Положення поширюються на банки України.
II. Основні засади організації кіберзахисту в банківській системі України	II. Основні засади організації кіберзахисту в банківській системі України

13. Центр кіберзахисту забезпечує:	13. Центр кіберзахисту забезпечує:
4) організацію виконання заходів щодо об'єктів критичної інформаційної інфраструктури ~~відповідно до розділу IV цього Положення~~;	4) організацію виконання заходів щодо об'єктів критичної інформаційної інфраструктури;
III. Організація інформаційного обміну	III. Організація інформаційного обміну
20. Учасниками інформаційного обміну є суб'єкти кіберзахисту, визначені в пункті 8 розділу II цього Положення.	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.**
~~IV. Заходи щодо забезпечення кіберзахисту критичної інфраструктури банків - операторів критичної інфраструктури~~	
~~30. Банк - оператор критичної інфраструктури зобов'язаний віднести до об'єктів критичної інформаційної інфраструктури (далі - ОКІІ) інформаційні системи об'єкта критичної інфраструктури, які відповідають двом критеріям:~~ ~~1) порушення функціонування інформаційних систем внаслідок кіберінциденту, кібератаки безпосередньо вплине на стале функціонування об'єкта критичної інфраструктури банку - оператора критичної інфраструктури;~~ ~~2) у банку - оператора критичної інфраструктури немає альтернативних за функціональними можливостями інформаційних систем для забезпечення сталого функціонування об'єкта критичної інфраструктури банку - оператора критичної інфраструктури.~~	

~~31. Банк – оператор критичної інфраструктури має право віднести до ОКІІ інші інформаційні системи, що безпосередньо забезпечують автоматизацію процесів надання банком – оператором критичної інфраструктури банківських, фінансових послуг та здійснення інших видів його діяльності відповідно до статті 47 Закону України "Про банки і банківську діяльність", надання кваліфікованих електронних довірчих послуг за умови відповідності критеріям, викладеним у підпункті 2 пункту 30 розділу IV цього Положення.~~	
~~32. Банк – оператор критичної інфраструктури зобов'язаний протягом місяця з дня отримання повідомлення від Національного банку про внесення відомостей про його об'єкти критичної інфраструктури до реєстру об'єктів критичної інфраструктури:~~ ~~1) сформувати та затвердити перелік інформаційних систем банку – оператора критичної інфраструктури, віднесених до ОКІІ (далі – перелік ОКІІ), відповідно до пунктів 30, 31 розділу IV цього Положення;~~ ~~2) надати затверджений перелік ОКІІ Національному банку в спосіб, установлений у пункті 41 розділу IV цього Положення.~~	
~~33. Банк – оператор критичної інфраструктури зобов'язаний підтримувати в актуальному стані перелік ОКІІ та надавати Національному банку в спосіб, установлений у пункті 41 розділу IV цього Положення, оновлений перелік ОКІІ протягом місяця з дня його затвердження.~~	

~~34. Банк – оператор критичної інфраструктури:~~ ~~1) щороку станом на 01 листопада переглядає перелік ОКІ;~~ ~~2) про результати перегляду інформує Національний банк щороку до 01 грудня та надає актуалізований перелік ОКІ (у разі його оновлення) у спосіб, установлений у пункті 41 розділу IV цього Положення.~~	
~~35. Банк – оператор критичної інфраструктури зобов'язаний протягом місяця після затвердження переліку ОКІ або його оновлення:~~ ~~1) сформувати відомості про ОКІ 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 ОКІ для внесення до реєстру об'єктів критичної інформаційної інфраструктури в спосіб, установлений у пункті 41 розділу IV цього Положення.~~	
~~36. Банк – оператор критичної інфраструктури зобов'язаний підтримувати в актуальному стані відомості про ОКІ та надавати Національному банку ці відомості протягом місяця з дня їх актуалізації у спосіб, установлений у пункті 41 розділу IV цього Положення.~~ ~~Національний банк має право вимагати від банку – оператора критичної інфраструктури надання додаткової~~	

~~інформації для уточнення відомостей про ОКІ шляхом направлення запиту.~~ ~~Банк - оператор критичної інфраструктури у відповідь на запит зобов'язаний у строк, визначений у запиті, та в повному обсязі надати уточнювальну інформацію про ОКІ.~~	
~~37. Банк - оператор критичної інфраструктури зобов'язаний:~~ ~~1) визначити критичними щодо інформаційної безпеки бізнес-процеси діяльності банку, автоматизацію яких забезпечують ОКІ, з обов'язковим уключенням їх до сфери застосування системи управління інформаційною безпекою (далі - СУІБ) та упровадженням для них заходів безпеки, використовуючи ризик-орієнтований підхід;~~ ~~2) 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;~~ ~~3) не рідше одного разу на рік проводити тренування щодо відпрацювання заходів Плану реагування, здійснювати тестування плану забезпечення безперервної діяльності та дій банку - оператора критичної інфраструктури в разі виникнення надзвичайних ситуацій у частині, що стосується критичної інформаційної інфраструктури банку, з обов'язковим документуванням результатів такого тестування.~~	

~~38. CISO банку – оператора критичної інфраструктури забезпечує організацію:~~ ~~1) виконання заходів щодо перегляду та підтримання в актуальному стані переліку ОКІІ, надання актуального переліку ОКІІ до Національного банку відповідно до пунктів 32-34 розділу IV цього Положення;~~ ~~2) виконання заходів щодо перегляду та підтримання в актуальному стані відомостей про ОКІІ, надання актуальних відомостей до Національного банку відповідно до пунктів 35, 36 розділу IV цього Положення;~~ ~~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 – оператора критичної інфраструктури відповідно до розробленого Плану реагування в разі кібератаки (спроби реалізації кіберзагрози) на об'єкти кіберзахисту банку – оператора критичної інфраструктури;~~ ~~5) надання інформації про аутсорсинг функції кіберзахисту ОКІ на запит Національного банку в обсязі та в термін, що встановлені в такому запиті;~~ ~~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 - 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 - оператором критичної інфраструктури програмних, апаратних, програмно-апаратних засобів у складі об'єкта критичної інформаційної інфраструктури здійснюється з урахуванням вимог Законів України "Про санкції", "Про основні засади забезпечення кібербезпеки України", інших законів України.~~	
~~41. Відомості про ОКІІ є інформацією з обмеженим доступом. Банки - оператори критичної інфраструктури зобов'язані надавати інформацію (інформування про перегляд переліків ОКІІ, переліки ОКІІ, відомості про ОКІІ) у випадках, визначених у пунктах 32-36 розділу IV цього Положення, в електронній формі через АРМ НБУ-інформаційний.~~	
V. Вимоги до проведення аудиту інформаційної безпеки в банківській системі України	V. Вимоги до проведення аудиту інформаційної безпеки в банківській системі України
42. Банк зобов'язаний проводити незалежний аудит інформаційної безпеки (далі - зовнішній аудит). Банк самостійно встановлює періодичність проведення зовнішнього аудиту. Періодичність проведення зовнішнього	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**

аудиту для банку - ~~оператора критичної інфраструктури~~ залежить від категорії критичності ~~ОКІ~~ та становить: …	залежить від категорії критичності **об'єктів критичної інфраструктури** та становить: …
~~Додаток до Положення про організацію кіберзахисту в банківській системі України (підпункт 1 пункту 35 розділу IV)~~ ~~I. Відомості про ОКІ~~ ~~1. Повне найменування банку – оператора критичної інфраструктури, адреса його місцезнаходження (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 IP-адрес банку – оператора критичної інфраструктури.~~	

~~4. Відомості про ОКІ:~~ ~~1) повне найменування ОКІ відповідно до документа про введення в експлуатацію, дата введення в експлуатацію, повне найменування юридичної особи - виробника та країна його походження, наявність та кінцевий термін технічної підтримки;~~ ~~2) повна назва об'єкта критичної інфраструктури, до складу якого входить ОКІ [у разі віднесення об'єкта до критичної інформаційної інфраструктури відповідно до пункту 30 розділу IV Положення про організацію кіберзахисту в банківській системі України (далі - Положення)], призначення ОКІ, перелік банківських, фінансових та інших видів його діяльності, надання яких він забезпечує (у разі віднесення об'єкта до критичної інформаційної інфраструктури відповідно до пункту 31 розділу IV Положення);~~ ~~3) повне найменування юридичної особи - власника та адреса фактичного розташування (індекс, область, місто, вулиця, номер будинку) технологічної платформи ОКІ;~~ ~~4) вид інформації за порядком доступу, що обробляється на ОКІ;~~ ~~5) наявність інформаційного обміну ОКІ з іншими інформаційними системами, повна назва цих систем, повне найменування юридичної особи - власника;~~	

~~6) уніфіковані ідентифікатори (англійською мовою Uniform Resource Identifier) ОКІ, що опубліковані в мережі Інтернет.~~ ~~II. Пояснення до заповнення додатка~~ ~~5. Під час викладення відомостей про ОКІ потрібно надавати інформацію в розрізі кожного ОКІ (4-1, 4-2, 4-3, ...).~~ ~~6. Під час надання інформації, зазначеної в підпункті 2 пункту 4 розділу I цього додатка, потрібно зазначити послуги відповідно до статті 47 Закону України "Про банки і банківську діяльність".~~	

Директор Департаменту безпеки Олександр ПАЛАМАРЧУК