**Порівняльна таблиця**

до проекту постанови Правління Національного банку України

“Про затвердження Змін до деяких нормативно-правових актів Національного банку України **з питань інформаційної безпеки та кіберзахисту**”

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

| 1 | 2 |
| --- | --- |
| Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг |
| І. Загальні положення | І. Загальні положення |
| 1. Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про банки і банківську діяльність”, “Про основні засади забезпечення кібербезпеки України”, “Про електронні документи та електронний документообіг”, “Про електронні довірчі послуги”, з урахуванням ~~Директиви Європейського парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу~~, Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95 (далі – Положення № 95), Положення про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116 (далі – Положення № 116). | 1. Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про банки і банківську діяльність”, “Про основні засади забезпечення кібербезпеки України”, “Про електронні документи та електронний документообіг”, “Про **електронну ідентифікацію та** електронні довірчі послуги”, з урахуванням **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**, Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95 (далі – Положення № 95), Положення про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116 **(зі змінами, далі – Положення № 116), Положення про використання засобів криптографічного захисту інформації Національного банку України, затвердженого постановою Правління Національного банку України від 14 квітня 2023 року № 49 (далі – Положення 49).** |
| 3. У цьому Положенні терміни вживаються в таких значеннях: | 3. У цьому Положенні терміни вживаються в таких значеннях: |
| …~~8~~) ~~незалежний~~ аудит інформаційної безпеки (далі – зовнішній аудит інформаційної безпеки) – процес одержання банком оцінки інформаційної безпеки за результатом проведення процедури аудиту інформаційної безпеки; | ….**1)** аудит інформаційної безпеки (далі – зовнішній аудит інформаційної безпеки) – процес одержання банком оцінки інформаційної безпеки за результатом проведення процедури аудиту інформаційної безпеки; |
| ~~1~~) безвиїзні заходи контролю - аналіз інформації, документів щодо діяльності банку з питань інформаційної безпеки, кіберзахисту, надання кваліфікованих електронних довірчих послуг, який проводиться Національним банком у порядку, установленому в розділі III цього Положення, без виходу за місцезнаходженням банку; | **11**) безвиїзні заходи контролю - аналіз інформації, документів щодо діяльності банку з питань інформаційної безпеки, кіберзахисту, надання кваліфікованих електронних довірчих послуг, який проводиться Національним банком у порядку, установленому в розділі III цього Положення, без виходу за місцезнаходженням банку; |
| 9) перевірка – планова перевірка банку з питань інформаційної безпеки, кіберзахисту, надання кваліфікованих електронних довірчих послуг, що проводиться інспекційною групою безпосередньо за його місцезнаходженням; | 9) перевірка – планова перевірка банку з питань інформаційної безпеки, кіберзахисту, надання кваліфікованих електронних довірчих послуг, що проводиться інспекційною групою безпосередньо за його місцезнаходженням **та/або за його межами шляхом віддаленого доступу до документів, інформації та систем автоматизації з використанням інформаційно-комунікаційних технологій;** |
| 10) позапланова перевірка – перевірка банку з питань інформаційної безпеки, кіберзахисту, надання електронних довірчих послуг, що проводиться за наявності обґрунтованих підстав відповідно до розпорядчого акта Національного банку інспекційною групою безпосередньо за його місцезнаходженням; | 10) позапланова перевірка – перевірка банку з питань інформаційної безпеки, кіберзахисту, надання електронних довірчих послуг, що проводиться за наявності обґрунтованих підстав відповідно до розпорядчого акта Національного банку інспекційною групою безпосередньо за його місцезнаходженням **та/або за його межами шляхом віддаленого доступу до документів, інформації та систем автоматизації з використанням інформаційно-комунікаційних технологій**; |
| …Інші терміни в цьому Положенні вживаються в значеннях, визначених у Законах України “Про електронні довірчі послуги”, “Про основні засади забезпечення кібербезпеки України”, “Про банки і банківську діяльність” та нормативно-правових актах Національного банку.  | …Інші терміни в цьому Положенні вживаються в значеннях, визначених у Законах України “Про **електронну ідентифікацію та** електронні довірчі послуги”, “Про основні засади забезпечення кібербезпеки України”, “Про банки і банківську діяльність” та нормативно-правових актах Національного банку.  |
| 4. Національний банк здійснює контроль з метою: | 4. Національний банк здійснює контроль з метою: |
|  …5) перевірки виконання вимог ~~нормативно-правових актів з питань надання кваліфікованих електронних довірчих~~ ~~послуг кваліфікованим надавачем електронних довірчих послуг, відомості про якого внесені до Довірчого списку за поданням засвідчувального центру.~~ | …5) перевірки виконання вимог **Положення № 116 та Положення № 49.** |
|  |  |
| ~~6. Виїзні заходи контролю у формі перевірок здійснюються інспекційною групою згідно з календарним планом, що складається відповідно до розділу ІІ цього Положення.~~ |  |
| II. Організація та порядок проведення виїзних заходів контролю | II. Організація та порядок проведення виїзних заходів контролю |
| 8. Департамент здійснює планування виїзних заходів контролю на підставі ризик-орієнтованого підходу, що ґрунтується на результатах: | 8. Департамент здійснює планування виїзних заходів контролю на підставі ризик-орієнтованого підходу, що ґрунтується на результатах: |
| ...3) аналізу інформації, документів, звітів, отриманих від банків на виконання Положення № 116; | ….3) аналізу інформації, документів, звітів, отриманих від банків на виконання **цього Положення,** Положення № 116**, Положення № 49**; |
|  …6) опрацювання ~~висновків~~ щодо поточного рівня ризиків інформаційної безпеки/кіберризиків і його впливу на кіберстійкість банку з урахуванням наявної інформації про факти, події та обставини в його діяльності. | …6) опрацювання **інформації** щодо поточного рівня ризиків інформаційної безпеки/кіберризиків і його впливу на кіберстійкість банку з урахуванням наявної інформації про факти, події та обставини в його діяльності. |
| План перевірок затверджується ~~розпорядчим актом~~ ~~Національного банку і оприлюднюється на сторінці офіційного Інтернет-представництва Національного банку.~~ | План перевірок затверджується **Національним банком.** **Інформація щодо переліку банків, перевірки яких включено до затвердженого плану,** оприлюднюється на сторінці офіційного Інтернет-представництва Національного банку. |
| 10. Національний банк має право проводити позапланову перевірку з метою термінового встановлення причин, обставин, масштабу негативного впливу на життєдіяльність банку та/або банківську систему в разі отримання документально підтвердженої інформації про:…3) порушення вимог ~~законодавства у сфері електронних довірчих послуг.~~ | 10. Національний банк має право проводити позапланову перевірку з метою термінового встановлення причин, обставин, масштабу негативного впливу на життєдіяльність банку та/або банківську систему в разі отримання документально підтвердженої інформації про:.. 3) порушення вимог **Положення № 116**. |
| 11. Національний банк повідомляє банк про проведення планової перевірки не пізніше ніж за ~~20~~ календарних днів до її початку | 11. Національний банк повідомляє банк про проведення планової перевірки не пізніше ніж за **10** календарних днів до її початку |
| 15. Куратор перевірки і члени інспекційної групи під час проведення перевірки (планової або позапланової) банку мають право:* + 1. безперешкодного доступу до всіх оригіналів документів, матеріалів та інформації, також до тих, що становлять інформацію з грифами обмеження доступу, потрібних для перевірки, до системи автоматизації банку (уключаючи персоналізований доступ у режимі перегляду), інформаційно-~~теле~~комунікаційної системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів банку;

….6) вимагати від банку демонстрації та ознайомлення з функціональними можливостями і налаштуваннями системи автоматизації банку, інформаційно-~~теле~~комунікаційної системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів банк~~а~~. | 15. Куратор перевірки і члени інспекційної групи під час проведення перевірки (планової або позапланової) банку мають право:1) безперешкодного доступу до всіх оригіналів документів, матеріалів та інформації, також до тих, що становлять інформацію з грифами обмеження доступу, потрібних для перевірки, до системи автоматизації банку (уключаючи персоналізований доступ у режимі перегляду), інформаційно-**комунікаційної** системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів банку;….6) вимагати від банку демонстрації та ознайомлення з функціональними можливостями і налаштуваннями системи автоматизації банку, інформаційно-**комунікаційної** системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів банк**у**; |
|  *відсутній* | **7**) **здійснювати із використанням техніки Національного банку фото- / відеофіксацію під час проведення процедури демонстрації, що передбачена підпунктом 6 пункту 15 розділу ІІ цього Положення;** |
| *відсутній* | **8) призначати і проводити інтерв’ю з керівниками банку та працівниками структурних підрозділів банку, до сфери відповідальності яких належать питання інформаційної безпеки та кіберзахисту, управління інформаційно-комунікаційними технологіями, управління операційними ризиками банку.**  |
| *відсутній* | **Демонстрація, яка передбачена у підпункті 6 пункту 15 розділу ІІ, проводиться за місцезнаходженням банку (в приміщеннях підрозділів банку, що здійснюють супроводження / адміністрування програмних, апаратних, програмно-апаратних засобів забезпечення інформаційної безпеки і кіберзахисту банку, та приміщеннях, пов’язаних з наданням електронних довірчих послуг) та/або за допомогою засобів відеозв'язку, і може супроводжуватись фото- / відеофіксацією фактів, які мають ознаки недотримання банком вимог законодавства з питань інформаційної безпеки, кіберзахисту, надання електронних довірчих послуг.****Інтерв’ю, яке передбачене у підпункті 8 пункту 15 розділу ІІ, проводиться за погодженням із куратором перевірки та попереднім повідомленням контактної особи від банку безпосередньо за місцезнаходженням банку або з використанням засобів відеозв`язку.** |
| *відсутній* | **151. Матеріали (дані) фото- / відеофіксації, які отримані відповідно до підпункту 7 пункту 15 розділу ІІ цього Положення, долучаються до справи перевірки.** |
| 17. Керівник банку зобов'язаний виконувати вимоги куратора перевірки та членів інспекційної групи, зазначені в [пункті 15](https://zakon.rada.gov.ua/laws/show/v0004500-21#n79) розділу II цього Положення, сприяти та не створювати перешкод проведенню перевірки (планової або позапланової), а також:…6) забезпечувати кураторові перевірки, членам інспекційної групи демонстрацію та ознайомлення з функціональними можливостями, налаштуваннями системи автоматизації банку, інформаційно-~~теле~~комунікаційної системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів; | 17. Керівник банку зобов'язаний виконувати вимоги куратора перевірки та членів інспекційної групи, зазначені в [пункті 15](https://zakon.rada.gov.ua/laws/show/v0004500-21#n79) розділу II цього Положення, сприяти та не створювати перешкод проведенню перевірки (планової або позапланової), а також:…6) забезпечувати кураторові перевірки, членам інспекційної групи демонстрацію та ознайомлення з функціональними можливостями, налаштуваннями системи автоматизації банку, інформаційно-**комунікаційної** системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів; |
| 25. Департамент має право вносити на засідання Комітету з питань нагляду та регулювання діяльності банків, ~~нагляду (оверсайту) платіжних систем~~ інформацію про результати проведеної перевірки банку і пропозиції щодо застосування/незастосування до банку адекватних заходів впливу для прийняття цим Комітетом відповідного рішення. | 25. Департамент має право вносити на засідання Комітету з питань нагляду та регулювання діяльності банків, **оверсайту платіжної інфраструктури** інформацію про результати проведеної перевірки банку і пропозиції щодо застосування/незастосування до банку адекватних заходів впливу для прийняття цим Комітетом відповідного рішення. |
| 26. ~~Куратор перевірки за результатами перевірки за наявності виявлених недоліків, порушень вимог Закону України “Про електронні довірчі послуги”, Положення № 116, регламенту роботи засвідчувального центру і нормативно-правових актів Національного банку в сфері електронних довірчих послуг подає керівнику засвідчувального центру витяг з довідки про перевірку~~ для прийняття рішення щодо: *відсутній*  ~~1~~) інформування спеціального уповноваженого центрального органу виконавчої влади з питань організації спеціального зв’язку та захисту інформації у сферах електронних довірчих послуг та електронної ідентифікації про виявлені порушення вимог ~~законодавства у сфері електронних довірчих послуг~~ для здійснення заходів відповідно до вимог законодавства у сфері електронних довірчих послуг;~~2) скасування/блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача;~~~~3) направлення подання про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку відповідно до Закону України “Про електронні довірчі послуги”.~~ | 26. **Результати перевірки питань, передбачених підпунктом 5 пункту 4 розділу І цього Положення, надаються засвідчувальному центру** для прийняття рішення щодо:  1) **направлення** **кваліфікованому надавачу електронних довірчих послуг листа про усунення встановлених перевіркою порушень / недоліків.** **2)** інформування спеціального уповноваженого центрального органу виконавчої влади з питань організації спеціального зв’язку та захисту інформації у сферах електронних довірчих послуг та електронної ідентифікації про виявлені порушення вимог **Положення № 116** для здійснення заходів відповідно до вимог законодавства у сфері електронних довірчих послуг.   |
| III. Організація проведення безвиїзних заходів контролю | III. Організація проведення безвиїзних заходів контролю |
| *відсутній* | **281. Банк зобов'язаний інформувати Національний банк про істотні зміни в організації інформаційної безпеки та кіберзахисту банку, що пов’язані з:****1) звільненням або переміщенням на іншу посаду / призначенням CISO;****2) змінами в розподілі функцій, обов'язків і повноважень органів управління та контролю банку в частині питань інформаційної безпеки та кіберзахисту;****3) змінами в організаційній структурі банку в частині підрозділів, до функцій яких належить забезпечення інформаційної безпеки та кіберзахисту банку;****4) ухваленням рішення щодо запровадження нового продукту або значних змін у діяльності банку, що матимуть вплив на організацію інформаційної безпеки та кіберзахисту банку;****5) ухваленням рішення щодо передачі на аутсорсинг функцій із забезпечення інформаційної безпеки / кіберзахисту банку, або зміну постачальника таких послуг.****Банк здійснює таке інформування шляхом подання повідомлення засобами системи електронної пошти Національного банку за формою згідно з Додатком 1 до цього Положення протягом п’яти робочих днів з дня запровадження таких змін.**  |
| IV. Вимоги щодо проведення банком самооцінки стану інформаційної безпеки/кіберзахисту | IV. Вимоги щодо проведення банком самооцінки стану інформаційної безпеки/кіберзахисту |
| 30. Банк зобов'язаний проводити щорічну самооцінку стану інформаційної безпеки/кіберзахисту шляхом складання щорічного Звіту з питань оцінювання ~~ризиків інформаційної безпеки/кіберризиків~~ (далі - Звіт) із урахуванням відомостей за результатами періодичного проведення: … | 30. Банк зобов'язаний проводити щорічну самооцінку стану інформаційної безпеки/кіберзахисту шляхом складання щорічного Звіту з питань оцінювання **процесів організації та забезпечення інформаційної безпеки / кіберзахисту** (далі - Звіт) із урахуванням відомостей за результатами періодичного проведення:…. |
| 31. Керівник банку зобов'язаний забезпечити ~~своєчасне подання до Національного банку Звіту, надання повної та достовірної інформації у Звіті, складеному за формою згідно з додатком до цього Положення, у формі електронного документа з накладеним КЕП керівника банку, засобами електронної пошти Національного банку з урахуванням вимог, установлених Національним банком щодо пересилання документів із грифом обмеження доступу. Звіт складається щорічно станом на 31 березня та подається до Національного банку протягом одного місяця, наступного за звітним періодом (рік).~~ | 31. **Керівник банку зобов'язаний забезпечити надання повної та достовірної інформації у Звіті, складеному за формою згідно з Додатком 2 до цього Положення та своєчасне подання такого Звіту до Національного банку.** |
|  *відсутній* | **311. Звіт подається до Національного банку в формі електронного документа у форматі xlsx з накладеним КЕП керівника банку засобами системи електронної пошти Національного банку з урахуванням вимог, установлених Національним банком щодо пересилання документів із грифом обмеження доступу.**  |
|  *відсутній* | **312. Звіт складається щорічно станом на 31 березня та подається до Національного банку протягом одного місяця, наступного за звітним періодом (рік).** |
|  *відсутній* | **Додаток 1****до Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг****(пункт 281 розділу ІІІ)****Повідомлення про істотні зміни в організації інформаційної безпеки та кіберзахисту****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****(найменування банку)**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** **з/п** | **Підстава подання повідомлення згідно п. 281 розділу ІІІ цього Положення**  | **Розгорнутий опис зміни** | **Причина зміни та очікуваний банком вплив зміни на кіберстійкість банку** |
| **1** | **2** | **3** | **4** |
| **1.** |  |  |  |
| **2.** |  |  |  |
| **…** |  |  |  |
|  |  |  |  |

 |
| Додаток до Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг(пункт 31 розділу ІV)~~Звіт~~ ~~з питань оцінювання ризиків інформаційної безпеки / кіберризиків станом на 31 березня 20\_\_ року~~ | Додаток **2**до Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг(пункт 31 розділу ІV)Оцінювання **процесів організації та забезпечення інформаційної безпеки / кіберзахисту** |
|  | *Додаток викладений у новій редакції* |
| Положення про організацію кіберзахисту в банківській системі України |
| 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 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,~~ 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). | 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,**. |
| 2. Терміни та скорочення в цьому Положенні вживаються в такому значенні:… | 2. Терміни та скорочення в цьому Положенні вживаються в такому значенні:… |
| *відсутній* | **31) 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.** |
| *відсутній* | **91) 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.** |
| *відсутній* | **101) системний кіберризик  - ризик порушення стабільності банківської системи внаслідок реалізації кіберзагроз щодо окремого банку через відповідні недоліки в його кіберстійкості.** |
| Термін "~~незалежний~~ 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 (далі - Положення про контроль № 4). |
| 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: … |
| 4) вимоги щодо проведення ~~незалежного~~ аудиту інформаційної безпеки в банківській системі України. | 4) вимоги щодо проведення аудиту інформаційної безпеки в банківській системі України. |
| 4. Це Положення не встановлює додаткових вимог щодо звітування банків про інциденти інформаційної безпеки / кіберінциденти, яке здійснюється під час складання щорічних звітів з питань оцінювання ~~ризиків інформаційної безпеки / кіберризиків~~, у порядку, встановленому Положенням про контроль № 4. | 4. Це Положення не встановлює додаткових вимог щодо звітування банків про інциденти інформаційної безпеки / кіберінциденти, яке здійснюється під час складання щорічних звітів з питань оцінювання **процесів організації та забезпечення інформаційної безпеки / кіберзахисту**, у порядку, встановленому Положенням про контроль № 4. |
| 5. Національний банк має право здійснювати перевірку стану впровадження заходів щодо забезпечення кіберзахисту, встановлених у ~~розділі 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 у **розділах ІІ, IV** цього Положення, під час здійснення заходів контролю, передбачених Положенням про контроль № 4. |
| II. Основні засади організації кіберзахисту в банківській системі України | II. Основні засади організації кіберзахисту в банківській системі України |
| 11. Національний банк з метою поєднання та координації зусиль суб'єктів кіберзахисту забезпечує створення та функціонування Центру кіберзахисту.Національний банк затверджує ~~регламент роботи Центру кіберзахисту та порядок інформаційного обміну, які розміщуються на порталі Центру кіберзахисту~~. | 11. Національний банк з метою поєднання та координації зусиль суб'єктів кіберзахисту забезпечує створення та функціонування Центру кіберзахисту.Національний банк затверджує **та розміщує на порталі Центру кіберзахисту:** **1) регламент роботи Центру кіберзахисту;** **2) порядок інформування банками про значні кіберінциденти;** **3) порядок інформаційного обміну.** |
| 13. Центр кіберзахисту забезпечує:…..3) координацію дій з питань кіберзахисту в банківській системі шляхом:…..розроблення ~~класифікації кіберінцидентів  у банківській системі України~~ та публікацію ~~такої класифікації~~ на порталі Центру кіберзахисту; | 13. Центр кіберзахисту забезпечує:…..3) координацію дій з питань кіберзахисту в банківській системі шляхом:…..розроблення **переліку категорій кіберінцидентів (таксономії) і рівнів їх критичності**  у банківській системі України **(далі – Перелік категорій кіберінцидентів)** та **публікацію такого переліку** на порталі Центру кіберзахисту; |
| *відсутній* | **191. Національний банк установлює вимоги до порядку інформування банками про значні кіберінциденти. Опис цих вимог та шаблони повідомлень наведені у порядку інформування банками про значні кіберінциденти, що розміщений на порталі Центру кіберзахисту в розділі** "**Банки/Документація**"**.**  |
| *відсутній* | **192.  Банк, який зафіксував кіберінцидент / кібератаку, визначає попередній рівень критичності відповідно до Переліку категорій кіберінцидентів, що опублікований на порталі Центру кіберзахисту в розділі** "**Банки/Документація**"**.** **Банк з метою запобігання реалізації системного кіберризику зобов’язаний без необґрунтованої затримки інформувати Центр кіберзахисту про значний кіберінцидент  в такому порядку:**1. **протягом 24 годин після того, як банку стало відомо про значний інцидент, шляхом надання попереднього повідомлення засобами електронної пошти на поштову скриньку** cyber@bank.gov.ua **відповідно до порядку інформування банками про значні кіберінциденти;**
2. **протягом 72 годин після того, як банку стало відомо про значний інцидент, шляхом надання проміжного повідомлення, що містить оновлену інформацію про значний кіберінцидент, через портал Центру кіберзахисту або засобами електронної пошти на поштову скриньку** **csirt-nbu@bank.gov.ua** **відповідно до порядку інформування банками про значні кіберінциденти;**
3. **на запит CSIRT-NBU шляхом надання відповіді, що містить проміжний звіт про відповідне оновлення статусу кіберінциденту;**

**4) не пізніше ніж через місяць після надання повідомлення про значний інцидент відповідно до підпункту 2 пункту 192 розділу ІІ цього Положення шляхом надання остаточного звіту, що містить:****детальний опис кіберінциденту, включаючи його наслідки і вплив на діяльність банку;****тип загрози або першопричини, що ймовірно спровокували кіберінцидент;****заходи, що вжиті банком для запобігання повторення реалізації кіберзагроз.****Звіт подається у формі електронного  документа з накладеним КЕП CISO банку засобами системи електронної пошти Національного банку.** |
| *відсутній* | 193**.  Банк має право інформувати Центр кіберзахисту про кіберінцидент, що не визначений банком як значний, з метою та в спосіб, що встановлені в розділі ІІІ цього Положення.** |
| V. Вимоги до проведення ~~незалежного~~ аудиту інформаційної безпеки в банківській системі України | V. Вимоги до проведення аудиту інформаційної безпеки в банківській системі України |
| 42. Банк самостійно встановлює періодичність проведення ~~незалежного~~ 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. | 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. |
| 45. Основними етапами проведення зовнішнього аудиту є:… | 45. Основними етапами проведення зовнішнього аудиту є:… |
| 2) повідомлення Національного банку про обрану аудиторську фірму в довільній формі, що містить відомості про повне найменування аудиторської фірми, номер реєстрації в Реєстрі аудиторів та суб'єктів аудиторської діяльності (у разі проведення зовнішнього аудиту в межах аудиту щорічної перевірки фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності) та обрані напрями, визначені в пункті ~~38~~ розділу IV цього Положення; | 2) повідомлення Національного банку про обрану аудиторську фірму в довільній формі, що містить відомості про повне найменування аудиторської фірми, номер реєстрації в Реєстрі аудиторів та суб'єктів аудиторської діяльності (у разі проведення зовнішнього аудиту в межах аудиту щорічної перевірки фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності) та обрані напрями, визначені в пункті **44** розділу IV цього Положення; |

Директор Департаменту безпеки Олександр ПАЛАМАРЧУК