Офіційно опубліковано 19.08.2022

Правління Національного банку України

П О С Т А Н О В А

12 серпня 2022 року Київ № 178

Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об’єктів критичної інфраструктури в банківській системі України

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, Закону України “Про основні засади забезпечення кібербезпеки України”, з метою нормативного врегулювання питань забезпечення кіберзахисту в банківській системі України Правління Національного банку України **постановляє:**

1. Затвердити Положення про організацію кіберзахисту в банківській системі України (далі – Положення), що додається.

2. Унести до Положення про визначення об’єктів критичної інфраструктури в банківській системі України, затвердженого постановою Правління Національного банку України від 30 листопада 2020 року № 151, такі зміни:

1) пункт 2 викласти в такій редакції:
“2. Це Положення встановлює критерії та порядок віднесення банків України до об’єктів критичної інфраструктури в банківській системі України.”;

2) підпункти 2, 4 пункту 3, пункти 8–12 та додаток виключити.

3. Департаменту безпеки (Ігор Коновалов) після офіційного опублікування довести до відома банків України інформацію про прийняття цієї постанови.

4. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Кирила Шевченка.

5. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування, крім абзацу другого пункту 12, абзаців третього, п’ятого, шостого підпункту 3 пункту 13 розділу II, підпунктів 1, 3 пункту 24 розділу III, пункту 35 розділу IV Положення, які набирають чинності з 01 січня 2023 року.

Голова Кирило ШЕВЧЕНКО

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
від 12 серпня 2022 року № 178

Положення про організацію кіберзахисту в банківській системі України

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).

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

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 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);

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 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);

9) реєстр об’єктів критичної інформаційної інфраструктури – відомості про інформаційні системи, які відповідно до вимог цього Положення віднесено до об’єктів критичної інформаційної інфраструктури;

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;

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 "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 "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).

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;

4) вимоги щодо проведення незалежного 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.

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.

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).

II. Основні засади організації кіберзахисту в банківській системі України

7. Національний банк забезпечує функціонування системи кіберзахисту в банківській системі України (далі – система кіберзахисту) шляхом:

1) нормативно-правового регулювання питань кіберзахисту в банківській системі України з урахуванням кращої європейської та світової практики, міжнародних та національних стандартів з питань кіберзахисту та інформаційної безпеки;

2) організації інформаційного обміну інформацією про кіберзагрози, кібератаки та кіберінциденти з банками України (далі – інформаційний обмін);

3) забезпечення розвитку комунікацій, координації та партнерства між суб'єктами системи кіберзахисту в банківській системі України (далі – суб'єкти кіберзахисту);

4) визначення особливостей кіберзахисту об'єктів критичної інформаційної інфраструктури банківської системи України;

5) сприяння розвитку та вдосконалення систем, комплексів та засобів забезпечення кіберзахисту в банківській системі України;

6) періодичного проведення оцінювання стану кіберзахисту в банківській системі України.

8. Суб’єктами кіберзахисту є:

1) Національний банк;

2) банки України.

9. Об’єктами кіберзахисту в банківській системі (далі – об’єкти кіберзахисту) є:

1) інформаційні системи банку;

2) критична інформаційна інфраструктура банку ОКІ.

10. Функціонування системи кіберзахисту ґрунтується на принципах:

1) пропорційності та адекватності заходів кіберзахисту, що впроваджуються, реальним та потенційним кіберзагрозам;

2) пріоритетності запобіжних заходів;

3) мінімізації кіберризиків у діяльності банку;

4) дотримання вимог нормативно-правових актів Національного банку з питань інформаційної безпеки та кіберзахисту, рекомендацій Національного банку, уключаючи такі, що можуть бути надані Національним банком за результатами контролю відповідно до Положення про контроль № 4;

5) постійної підтримки з боку органів управління банку кіберстійкості банку шляхом організації ефективного управління кіберризиками.

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.

12. Основними технічними інструментами Центру кіберзахисту є MISP-NBU і портал Центру кіберзахисту.

Банк зобов’язаний забезпечити авторизоване підключення до порталу Центру кіберзахисту та забезпечити роботу й обмін інформацією в обсязі

відповідно до розділу ІІІ цього Положення, порядку інформаційного обміну та інструкцій користувача порталу Центру кіберзахисту.

Банк ОКІ зобов'язаний забезпечити підключення до MISP-NBU.

Інші банки потребу в підключенні до MISP-NBU визначають самостійно.

Підключення до MISP-NBU здійснюється шляхом приєднання банку до ЄДБО.

13. Центр кіберзахисту забезпечує:

1) реалізацію інформаційного обміну відповідно до розділу ІІІ цього Положення;

2) функціонування CSIRT-NBU;

3) координацію дій з питань кіберзахисту в банківській системі шляхом:

інформування банків України про наявні (відомі та/або виявлені) кіберзагрози або зафіксовані спроби вчинення кібератак;

підключення банків до порталу Центру кіберзахисту;

підключення банків до MISP-NBU;

розроблення класифікації кіберінцидентів у банківській системі України та публікацію такої класифікації на порталі Центру кіберзахисту;

розроблення базових рекомендацій з питань забезпечення кіберзахисту для банків України, базових сценаріїв реагування на кіберінциденти та публікацію таких рекомендацій/сценаріїв на порталі Центру кіберзахисту;

надання консультативної допомоги з питань організації кіберзахисту;

4) організацію виконання заходів щодо об'єктів критичної інформаційної інфраструктури відповідно до розділу IV цього Положення;

5) організацію проведення навчально-методичних заходів, навчань з питань кіберзахисту в банківській системі України.

14. Центр кіберзахисту має право отримувати від банків інформацію, документи і матеріали, потрібні для реалізації функцій, зазначених у пункті 13 розділу ІІ цього Положення.

15. CSIRT-NBU забезпечує:

1) реагування на кібератаки або кіберінциденти шляхом:

моніторингу кіберзагроз, збору, накопичення та аналізу даних про кіберінциденти в банківській системі України;

поширення інформації про кіберзагрози, кібератаки, кіберінциденти відповідно до розділу ІІІ цього Положення;

аналізу кіберзагроз, вивчення зразків шкідливого програмного забезпечення, формування та поширення інформації про індикатори кіберзагроз відповідно до розділу ІІІ цього Положення, розроблення та надання рекомендацій з протидії кіберзагрозам;

надання консультативної допомоги з питань виявлення кіберінцидентів та усунення їх наслідків, реагування та протидії кіберзагрозам;

2) адміністрування (уключаючи розроблення інструкцій користувачів) та інформаційне наповнення порталу Центру кіберзахисту, MISP-NBU;

3) взаємодію з підрозділами кіберзахисту (кібербезпеки) основних суб'єктів національної системи кібербезпеки України, урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA (англійською мовою Computer Emergency Response Team of Ukraine, CERT-UA), довіреними зовнішніми джерелами інформації;

4) надання сервісів щодо виявлення та реагування на кіберінциденти, кібератаки в банківській системі України відповідно до умов ЄДБО.

16. CSIRT-NBU має право:

1) отримувати від банків інформацію, потрібну для здійснення реагування на кібератаки, кіберінциденти в банківській системі України;

2) здійснювати моніторинг інформаційного простору та мережі Інтернет щодо виявлення вразливостей та/або можливої компрометації об'єктів кіберзахисту, витоків електронних даних із банків.

17. Банк зобов'язаний покласти функції із забезпечення кіберзахисту на підрозділ інформаційної безпеки або створити окремий підрозділ з питань кіберзахисту (далі – підрозділ з питань кіберзахисту), що має безпосередньо підпорядковуватися відповідальній особі за інформаційну безпеку банку [англійською мовою Chief Information Security Officer (далі – CISO)].

Банк зобов'язаний визначити права та обов'язки, функції, відповідальність, потрібні професійні знання, досвід і кваліфікацію в посадових інструкціях працівників підрозділу з питань кіберзахисту.

18. Банк як суб'єкт системи кіберзахисту зобов'язаний ужити заходів щодо протидії кіберзагрозам, визначених за результатами аналізу вразливостей об'єктів кіберзахисту та пов'язаних із:

1) наданням, використанням, скасуванням та контролем доступу (уключаючи віддалений доступ) до об'єктів кіберзахисту, контролем використання облікових записів користувачів (уключаючи привілейованих);

2) забезпеченням реєстрації кожним компонентом об'єкта кіберзахисту подій для виявлення кіберінцидентів або ознак кібератак;

3) упровадженням процесу управління кіберінцидентами як складової процесу управління інцидентами безпеки інформації банку;

4) розробленням плану реагування на кіберзагрози, кібератаки та кіберінциденти на об'єктах кіберзахисту (далі – План реагування), узгодженого з політикою інформаційної безпеки, планом забезпечення безперервної діяльності банку та базовими сценаріями реагування на кіберінциденти;

5) здійсненням оперативного реагування на кібератаки та кіберінциденти відповідно до Плану реагування, інформуванням Центру кіберзахисту відповідно до базових сценаріїв реагування на кіберінциденти; наданням на запит CSIRT-NBU інформації, потрібної для здійснення реагування на кібератаки, кіберінциденти в банківській системі України в термін та обсязі, що зазначені в запиті;

6) створенням, зберіганням резервних копій даних, відновленням даних із резервних копій та заміною компонентів об'єктів кіберзахисту в разі виходу їх із ладу відповідно до нормативно-правових актів Національного банку з питань забезпечення безперервності діяльності;

7) забезпеченням доступності та відмовостійкості об'єктів кіберзахисту;

8) забезпеченням участі в інформаційному обміні, сприянням Центру кіберзахисту, CSIRT-NBU у реагуванні на кібератаки або кіберінциденти, встановленні причин і умов їх виникнення та/або реалізації;

9) забезпеченням обізнаності працівників банку з питань кіберзахисту;

10) забезпеченням мережевого захисту (уключаючи сегментацію мереж банку, встановлення та налаштування засобів мережевого захисту, контроль за мережевими протоколами і службами);

11) захистом від зловмисного коду;

12) забезпеченням аналізу вразливостей, отриманням, тестуванням, упровадженням оновлень програмного забезпечення, спрямованих на усунення його вразливостей;

13) забезпеченням кіберзахисту під час взаємодії з ключовими постачальниками послуг;

14) порядком використання змінних носіїв інформації, електронної пошти банку для запобігання реалізації кіберзагроз.

19. Банк зобов'язаний здійснювати реалізацію заходів кіберзахисту з урахуванням обов'язкових мінімальних вимог, установлених Положенням про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженим постановою Правління Національного банку України від 28 вересня 2017 року № 95.

ІІІ. Організація інформаційного обміну

20. Учасниками інформаційного обміну є суб'єкти кіберзахисту, визначені в пункті 8 розділу ІІ цього Положення.

21. Інформаційний обмін здійснюється з метою:

1) ужиття спільних заходів щодо своєчасного виявлення, запобігання, нейтралізації кіберзагроз та попередження про можливі кібератаки, забезпечення кіберстійкості банківської системи;

2) мінімізації ризиків реалізації кібератак, наслідків реалізованих кібератак на об'єкти кіберзахисту;

3) підвищення обізнаності працівників учасників інформаційного обміну.

22. Інформаційний обмін ґрунтується на таких загальних принципах:

1) поширення інформації, отриманої виключно з довірених внутрішніх та зовнішніх джерел інформації;

2) своєчасність, об'єктивність, дієвість та доречність для учасників інформаційного обміну інформації, що поширюється;

3) обов'язковість знеособлення інформації, що надана банком, під час її подальшого поширення;

4) відповідність інформації, що поширюється, цілям інформаційного обміну відповідно до пункту 21 розділу ІІІ цього Положення.

23. Банк зобов'язаний:

1) покласти функції щодо здійснення інформаційного обміну на підрозділ з питань кіберзахисту;

2) створити поштову скриньку CYBER у поштовому домені банку для обміну повідомленнями;

3) надати доступ до скриньки CYBER відповідальним особам за взаємодію з Центром кіберзахисту, CSIRT-NBU під час здійснення інформаційного обміну.

24. Інформаційний обмін здійснюється відповідно до порядку, установленого Національним банком, у формі:

1) поширення інформації загальноорганізаційного характеру, технічного характеру шляхом розміщення Центром кіберзахисту на своєму порталі;

2) розсилання засобами електронної пошти з поштової скриньки csirt-nbu@bank.gov.ua на поштову скриньку CYBER підрозділів з питань кіберзахисту;

3) інформування банків України про наявні кіберзагрози або зафіксовані спроби вчинення кібератак шляхом розміщення Центром кіберзахисту оперативних повідомлень на своєму порталі;

4) інформування банків України про наявні кіберзагрози або зафіксовані спроби вчинення кібератак шляхом офіційного листування;

5) поширення інформації про кіберзагрози, індикаторів кіберзагроз шляхом розміщення CSIRT-NBU відповідних оперативних повідомлень на MISP-NBU та/або розсилання електронних повідомлень засобами електронної пошти з поштової скриньки csirt-nbu@bank.gov.ua на поштову скриньку CYBER підрозділів із питань кіберзахисту;

6) проведення спільних нарад, конференцій, семінарів, консультацій, засідань робочих груп, заходів щодо обміну набутим досвідом роботи у сфері кіберзахисту.

25. Учасник інформаційного обміну повинен маркувати електронні повідомлення, що поширюються під час інформаційного обміну, спеціальними мітками з урахуванням протоколу “Світлофор”, визначеного в додатку С до Національного стандарту України ДСТУ ISO/IEC 27010:2018 (англійською мовою Traffic Light Protocol) (далі – мітка TLP), у таких значеннях:

1) мітка TLP white – для маркування інформації, що поширюється без обмежень;

2) мітка TLP green – для маркування інформації, що поширюється серед усіх учасників інформаційного обміну. Банк – учасник інформаційного обміну під час отримання такої інформації має право поширювати її лише працівникам банку та/або за потреби в межах банківської групи контрагентам – ключовим постачальникам послуг;

3) мітка TLP amber – для маркування інформації, що поширюється серед обмеженого кола учасників інформаційного обміну, що визначається відправником – учасником інформаційного обміну. Банк – учасник інформаційного обміну має право поширювати таку інформацію виключно в межах банку та/або за потреби в межах банківської групи;

4) мітка TLP red – для маркування інформації, що поширюється виключно для обмеженого кола учасників інформаційного обміну та їх працівників, що визначається відправником – учасником інформаційного обміну.

26. Подальше поширення інформації між учасниками інформаційного обміну здійснюється виключно на основі міток TLP відповідно до порядку інформаційного обміну. Оприлюднення цієї інформації в засобах масової інформації, поширення в мережі Інтернет, соціальних мережах не допускається.

27. Центр кіберзахисту має право:

1) знижувати рівень значення мітки TLP за умови знеособлення інформації, що отримана;

2) підвищувати рівень значення мітки TLP у разі додавання до інформації, що отримана, уточнювальних та/або додаткових відомостей, що мають суттєвий характер.

28. Учасникам інформаційного обміну заборонено пересилати інформацію, що становить банківську таємницю та службову інформацію під час інформаційного обміну у формах, установлених у пункті 24 розділу ІІІ цього

Положення. Передавання такої інформації здійснюється відповідно до законодавства України.

29. Банку не дозволяється:

1) редагувати (модифікувати) інформацію, що отримана з довірених джерел інформації, під час надання її іншим учасникам інформаційного обміну;

2) використовувати інформацію, отриману під час інформаційного обміну, з іншою метою, ніж зазначена в пункті 21 розділу III цього Положення, якщо інше не передбачено законодавством України.

IV. Заходи щодо забезпечення кіберзахисту критичної інформаційної інфраструктури банків ОКІ

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.

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 Закону України "Про банки і банківську діяльність", надання кваліфікованих електронних довірчих послуг за умови відповідності критеріям, викладеним у пункті 30 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.

33. Банк ОКІ зобов’язаний підтримувати в актуальному стані перелік ОКІІ та надавати Національному банку 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.

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.

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.

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;

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 ОКІ в разі виникнення надзвичайних ситуацій у частині, що стосується критичної інформаційної інфраструктури банку, з обов'язковим документуванням результатів такого тестування.

38. CISO банку ОКІ 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 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;

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 ОКІ 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.

40. Використання банком ОКІ 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 об’єкти критичної інформаційної інфраструктури банків ОКІ є інформацією з обмеженим доступом.

V. Вимоги до проведення незалежного 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.

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.

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.

44. Зовнішній аудит проводиться з метою незалежної оцінки:

1) стану захищеності об’єктів кіберзахисту;

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.

45. Основними етапами проведення зовнішнього аудиту є:

1) організація проведення зовнішнього аудиту, що включає:
вибір аудиторської фірми;
визначення переліку об'єктів аудиту, програми аудиту з урахуванням мети проведення аудиту та настанов національних та/або міжнародних стандартів (кращої практики) з питань інформаційної безпеки і кіберзахисту, відповідно до яких проводитиметься такий аудит;
визначення процедур і методики проведення зовнішнього аудиту, методів аналізу захищеності, уключаючи тестування на проникнення penetration testing;
укладення договору з проведення зовнішнього аудиту (уключаючи договір/угоду про нерозголошення конфіденційної інформації NDA);

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;

3) підготовка та погодження плану (графіка) проведення зовнішнього аудиту;

4) збір потрібних відомостей та їх аналіз;

5) підготовка і погодження звіту за результатами проведення зовнішнього аудиту;

6) складання та затвердження плану заходів щодо забезпечення виконання рекомендацій, наданих за результатами проведення зовнішнього аудиту (далі – План заходів).

46. Банк за результатами зовнішнього аудиту надає Національному банку відомості про результати зовнішнього аудиту (узагальнені результати оцінок за напрямами, визначеними в пункті 44 розділу V цього Положення) та затверджений План заходів.

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 IP-адрес банку ОКІ.

4. Відомості про ОКІІ:

1) повне найменування ОКІІ 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) призначення ОКІІ, перелік банківських, фінансових та інших послуг, надання яких він забезпечує;

3) повне найменування юридичної особи-власника та адреса фактичного розташування (індекс, область, місто, вулиця, номер будинку) технологічної платформи ОКІІ;

4) вид інформації за порядком доступу, що обробляється на ОКІІ;

5) наявність інформаційного обміну ОКІІ з іншими інформаційними системами, повна назва цих систем, повне найменування юридичної особи-власника;

6) уніфіковані ідентифікатори (англійською мовою Uniform Resource Identifier) ОКІІ, що опубліковані в мережі Інтернет.

Продовження додатка

II. Пояснення до заповнення додатка

5. Під час викладення відомостей про ОКІІ потрібно надавати інформацію в розрізі кожного ОКІІ (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”.