Правління Національного банку України

П О С Т А Н О В А

м. Київ

Про затвердження Положення про організацію
кіберзахисту 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.

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 пункту 32 розділу IV Положення, який набирає чинності з 01 вересня 2022 року.

Голова Кирило ШЕВЧЕНКО

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку
України

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, національних стандартів України ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" (ISO/IEC 27001:2013, 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), 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. У цьому Положенні терміни та скорочення вживаються в таких значеннях:

1) довірені внутрішні джерела інформації – Центр кіберзахисту, команда реагування на кіберінциденти в банківській системі України, 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 загально-організаційного характеру – інформація, що циркулює під час інформаційного обміну та містить описи національних та міжнародних стандартів, інноваційних методик та практик з питань кіберзахисту, світового та вітчизняного досвіду в сфері кібербезпеки та кіберзахисту, посилання на джерела такої інформації;

5) інформація технічного характеру – інформація, що циркулює 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 та 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, що визначений об’єктом критичної інфраструктури в банківській системі України;

7) 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) система кіберзахисту в банківській системі України – сукупність суб’єктів, впроваджених систем, комплексів та засобів забезпечення кіберзахисту, взаємопов’язаних заходів організаційного, технічного, інформаційного характеру щодо забезпечення належного рівня кібербезпеки та кіберстійкості банківської системи України;

9) CSIRT-NBU (англійською мовою Computer Security Incident Response Team of the National Bank of Ukraine) - команда реагування на кіберінциденти в банківській системі України, що входить до складу Центру кіберзахисту;

10) 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 загально-організаційного 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).

Терміни "об'єкт критичної інфраструктури в банківській системі України", "об'єкт критичної інформаційної інфраструктури" вживаються в значеннях, визначених 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 та визначає:

1) основні засади функціонування системи кіберзахисту в банківській системі України;

2) принципи забезпечення інформаційного обміну між Центром кіберзахисту Національного банку (далі – Центр кіберзахисту) і банками України;

3) вимоги щодо заходів із 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 посилених заходів із забезпечення кіберзахисту, що встановлені розділом IV цього Положення, під час здійснення заходів контролю відповідно до Положення про контроль № 4.

6. Вимоги цього Положення поширюються на банки України. Вимоги розділу IV цього Положення поширюються 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 у банківській системі України (далі – система кіберзахисту) шляхом:

1) нормативно-правового регулювання питань кіберзахисту у банківській системі України з урахуванням кращих європейських та світових практик, 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 комунікації, координації та партнерства між суб’єктами системи кіберзахисту у 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 у банківській системі України.

8. Суб’єктами кіберзахисту є:

1) Національний банк;

2) банки ОКІ;

3) інші банки України, що не включені до підпункту 2 пункту 8 розділу II цього Положення.

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

1) інформаційні системи банку, які безпосередньо забезпечують автоматизацію банківської діяльності, у тому числі в яких обробляється інформація, що становить банківську таємницю;

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.

Положення про Центр кіберзахисту, регламент роботи Центру кіберзахисту, порядок інформаційного обміну, керівний та персональний склад Центру кіберзахисту затверджуються розпорядчими документами Національного банку. Регламент роботи Центру кіберзахисту, порядок інформаційного обміну 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, а банк ОКІ також і до MISP-NBU, та забезпечити роботу й

обмін інформацією в обсязі відповідно до розділу ІІІ цього Положення, порядку інформаційного обміну та інструкцій користувача порталу Центру кіберзахисту. Інші банки необхідність підключення 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 у банківській системі шляхом:

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

підключення банків до порталу Центру кіберзахисту, MISP-NBU;

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

розроблення базових рекомендації 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 Положення про ОКІ № 151;

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

Центр кіберзахисту має право отримувати від банків інформацію, документи і матеріали, необхідні для реалізації функцій, вказаних у цьому пункті.

14. CSIRT-NBU забезпечує:

1) реагування на кібератаки або кіберінциденти шляхом:

здійснення 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;

здійснення 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 у банківській системі України відповідно до умов ЄДБО.

15. CSIRT-NBU має право:

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

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

16. 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, необхідні професійні знання, досвід і кваліфікацію у посадових інструкціях працівників підрозділу з питань кіберзахисту.

17. Банк, як суб'єкт системи кіберзахисту, зобов'язаний вжити заходів з протидії кіберзагрозам, визначених за результатами аналізу вразливостей об'єктів кіберзахисту, та пов'язаних з:

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’єкту кіберзахисту подій, необхідних 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, інформування Центру кіберзахисту відповідно до базових сценаріїв реагування на кіберінциденти;

6) створенням, зберіганням резервних копій даних, відновленням даних з резервних копій та заміни компонентів об’єктів кіберзахисту у випадку виходу їх з ладу відповідно до нормативно-правових актів Національного банку з питань забезпечення безперервності діяльності;

7) забезпечення 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 персоналу банка з питань кіберзахисту;

10) забезпеченням мережевого захисту (уключаючи сегментацію мереж банку, встановлення та налаштування засобів мережевого захисту, контроль мережевих протоколів і служб);

11) захистом від зловмисного коду;

12) забезпеченням аналізу вразливостей, отриманням, тестуванням, впровадженням 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.

Реалізація заходів кіберзахисту здійснюється з урахуванням обов'язкових мінімальних вимог, встановлених Положенням про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженим постановою Правління Національного банку України від 28 вересня 2017 року № 95.

18. Банк має право передавати на аутсорсинг функції щодо забезпечення кіберзахисту інформаційної інфраструктури банку (далі – аутсорсинг функції кіберзахисту) за умови виконання заходів та вимог, передбачених главою 47 розділу VI Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженим постановою Правління Національного банку від 11 червня 2018 року № 64 (зі змінами).

III. Організація інформаційного обміну

19. Учасниками інформаційного обміну є суб'єкти кіберзахисту, визначені у пункті 8 розділу II цього Положення.

20. Інформаційний обмін здійснюється з метою:

1) вжиття 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 персоналу учасників інформаційного обміну.

21. Інформаційний обмін ґрунтується на таких загальних принципах:

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

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

3) обов'язковість знеособлення інформації, що надана банком, при її подальшому розповсюдженні;

4) відповідність інформації, що розповсюджується, цілям інформаційного обміну відповідно до пункту 20 розділу ІІІ цього Положення.

22. Банк зобов'язаний покласти функції щодо здійснення інформаційного обміну на підрозділ з питань кіберзахисту, створити поштову скриньку CYBER у поштовому домені банку для обміну повідомленнями та надати доступ до неї визначеним відповідальним особам за взаємодію з Центром кіберзахисту, CSIRT-NBU під час здійснення інформаційного обміну.

23. Інформаційний обмін відбувається відповідно до порядку, встановленого Центром кіберзахисту, у формі:

1) поширення інформації загально-організаційного характеру, технічного характеру шляхом розміщення Центром кіберзахисту на своєму порталі та/або розсилання засобами електронної пошти з поштової скриньки csirt-nbu@bank.gov.ua на поштову скриньку CYBER підрозділів з питань кіберзахисту;

2) інформування банків України про наявні кіберзагрози або зафіксовані спроби вчинення кібератак шляхом розміщення Центром кіберзахисту оперативних повідомлень на своєму порталі та/або офіційного листування;

3) 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 з питань кіберзахисту;

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

24. Учасник інформаційного обміну повинен маркувати електронні повідомлення, що циркулюють під час інформаційного обміну, спеціальними мітками з урахуванням протоколу “Світлофор”, визначеному додатком 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 розповсюджується серед всіх учасників інформаційного обміну. Банк – учасник інформаційного обміну при отриманні такої інформації має право поширювати її тільки працівникам банку та/або за необхідністю в межах банківської групи, контрагентам - ключовим постачальникам послуг;

3) мітка TLP amber – для маркування інформації, що розповсюджується 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 необхідністю, в межах банківської групи;

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

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

26. Центр кіберзахисту має право:

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

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

27. Під час інформаційного обміну у формах, встановлених пунктом 24 розділу ІІІ цього Положення, заборонено пересилати інформацію, що становить банківську таємницю та службову інформацію. Передавання такої інформації здійснюється відповідно до законодавства України.

28. Банку не дозволяється:

1) редагувати (модифікувати) інформацію, що отримана з довірених джерел інформації, при наданні її іншим учасникам інформаційного обміну;

2) використовувати інформацію, що була отримана у ході інформаційного обміну з іншою метою, ніж вказаною в пункті 20 розділу III цього Положення, якщо інше не передбачено законодавством України.

IV. Заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури банків ОКІ

29.Банк ОКІ зобов'язаний:

1) визначити критичними щодо інформаційної безпеки бізнес-процеси діяльності банку, автоматизацію яких забезпечують інформаційні системи, що віднесені до об'єктів критичної інформаційної інфраструктури, з обов'язковим включенням їх до сфери застосування системи управління інформаційною безпекою (далі – СУІБ);

2) здійснити опис критичних бізнес-процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об'єкта критичної інформаційної інфраструктури, які задіяні в цьому процесі;

3) упровадити для критичних бізнес-процесів заходи безпеки, використовуючи ризик-орієнтований підхід, визначені додатком А до національного стандарту України ДСТУ ISO/IEC 27001:2015;

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

5) не рідше одного разу на рік проводити тренування щодо відпрацювання заходів Плану реагування, здійснювати тестування плану забезпечення безперервної діяльності та дій банку ОКІ у разі виникнення надзвичайних ситуацій в частині, що стосується критичної інформаційної інфраструктури банку з обов'язковим документуванням результатів такого тестування.

30.CISO банку ОКІ забезпечує організацію:

1) виконання заходів, передбачених Положенням про ОКІ № 151, щодо визначення та підтримання в актуальному стані переліку інформаційних систем банку, віднесених до об'єктів критичної інформаційної інфраструктури, подання відомостей про ці об'єкти шляхом заповнення та підтримки в актуальному стані відповідних форм, розміщених на порталі Центру кіберзахисту;

2) участі банку ОКІ в інформаційному обміні, у порядку визначеному розділом ІІІ цього Положення;

3) пріоритетної реалізації заходів кіберзахисту критичної інформаційної інфраструктури банку відповідно до розробленого Плану реагування у разі кібератаки (спроби реалізації кіберзагрози) на об'єкти кіберзахисту банку ОКІ;

4) надання інформації про аутсорсинг функції кіберзахисту ОКІ на запит Національного банку в обсязі та у термін, що встановлені у такому запиті;

5) створення умов для підвищення кваліфікації працівників підрозділу з питань кіберзахисту.

31. Зв'язок технологічної платформи критичної інформаційної інфраструктури банку ОКІ з мережею Інтернет має здійснюватися з використанням двох або більше каналів передачі даних, що надаються різними операторами, провайдерами телекомунікацій через захищені вузли доступу із мережі Інтернет.

32. Банку ОКІ не дозволяється використовувати у складі об'єкта критичної інформаційної інфраструктури програмні, апаратні, програмно-апаратні засоби, що мають походження з держави-агресора або розроблені/виготовлені юридичною особою – резидентом такої держави чи юридичною особою, яка перебуває під контролем юридичної особи такої держави.

33. 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

34. Банк самостійно встановлює періодичність проведення незалежного аудиту інформаційної безпеки (далі – зовнішній аудит). Зовнішній аудит проводиться згідно з нормами законодавства, національних стандартів та з урахуванням міжнародних стандартів аудиту. Програма аудиту формується виходячи з особливостей діяльності банку, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

В банках ОКІ зовнішній аудит критичної інформаційної інфраструктури здійснюється відповідно до вимог та порядку, встановленими нормативно-правовими актами Національного банку.

35. Зовнішній аудит проводиться з метою незалежної оцінки:

1) стану захищеності об’єктів кіберзахисту;

2) рівня відповідності системи управління інформаційної безпеки 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.

36.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 (кращих практик) з питань інформаційної безпеки і кіберзахисту, відповідно до яких буде проводитися такий аудит;
визначення процедур і методики проведення зовнішнього аудиту (у тому числі методів аналізу захищеності, включаючи тестування на проникнення penetration testing);
укладання 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 (уключаючи номер реєстрації в Реєстрі аудиторів та суб'єктів аудиторської діяльності) та обрані напрями, що передбачені пунктом 35 розділу V цього Положення;

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

4) збір необхідних відомостей та їх аналіз;

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

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

37.Банк самостійно обирає:

1) аудиторську фірму для проведення зовнішнього аудиту серед юридичних осіб-резидентів України;

2) міжнародні стандарти (кращі практики) з питань інформаційної безпеки і кіберзахисту, відповідно до яких буде проводитися зовнішній аудит згідно з підпунктом 1 пункту 35 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.

Допускається проведення зовнішнього аудиту у рамках аудиту щорічної перевірки фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності аудиторською фірмою.

38. За результатами зовнішнього аудиту банк надає Національному банку відомості про результати зовнішнього аудиту (узагальнені результати оцінок за напрямами, передбаченими пунктом 35 розділу V цього Положення), та затверджений План заходів.