ПРОЄКТ

Правління Національного банку України

П О С Т А Н О В А

Київ

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

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, Законів України “Про банки і банківську діяльність”, “Про основні засади забезпечення кібербезпеки України”, “Про електронну ідентифікацію та електронні довірчі послуги”, з метою нормативного врегулювання функції контролю за забезпеченням кіберзахисту, інформаційної безпеки, наданням електронних довірчих послуг у банківській системі України Правління Національного банку України **постановляє:**

1. Затвердити Зміни до:

1) Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затвердженого постановою Правління Національного банку України від 16 січня 2021 року № 4, що додаються;

2) Положення про організацію кіберзахисту в банківській системі України, затвердженого постановою Правління Національного банку України від 12 серпня 2022 року № 178, що додаються.

2. Департаменту безпеки (Олександр Паламарчук) після офіційного опублікування довести до відома банків України інформацію про прийняття цієї постанови.

3. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Андрія Пишного.

4. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування.

Голова Андрій ПИШНИЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Зміни до Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг

1. У розділі I:

1) пункт 1 викласти в такій редакції:

“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).”;

2) у пункті 3:

підпункт 1 замінити двома новими підпунктами такого змісту:

“1) аудит інформаційної безпеки (далі – зовнішній аудит інформаційної безпеки) – процес одержання банком оцінки інформаційної безпеки за результатом проведення процедури аудиту інформаційної безпеки;

1^1) 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;”;

підпункт 8 виключити;

підпункти 9 та 10 доповнити словами “та/або за його межами шляхом віддаленого доступу до документів, інформації та систем автоматизації з використанням інформаційно-комунікаційних технологій;”;

в абзаці тринадцятому слова “Про електронні довірчі послуги” замінити словами “Про електронну ідентифікацію та електронні довірчі послуги”;

3) підпункт 5 пункту 4 викласти в такій редакції:

“5) перевірки виконання вимог Положення № 116 та Положення № 49.”;

4) пункт 6 виключити.

2. У розділі II:

1) у пункті 8:

підпункт 3 викласти в такій редакції:

“3) аналізу інформації, документів, звітів, отриманих від банків на виконання цього Положення, Положення № 116, Положення № 49;”;

у підпункті 6 слово “висновків” замінити словом “інформації”;

абзац восьмий викласти в такій редакції:

“План перевірок затверджується Національним банком. Інформація щодо переліку банків, перевірки яких включено до затвердженого плану, оприлюднюється на сторінці офіційного Інтернет-представництва Національного банку.”;

2) підпункт 3 пункту 10 викласти в такій редакції:

“3) порушення вимог Положення № 116.”;

3) в абзаці першому пункту 11 цифри “20” замінити цифрами “10”;

4) у пункті 15:

у підпунктах 1 та 6 слово “телекомунікаційної” замінити словом “комунікаційної”;

пункт доповнити двома новими підпунктами 7 та 8 такого змісту:

“7) здійснювати із використанням техніки Національного банку фото- / відеофіксацію під час проведення процедури демонстрації, що передбачена підпунктом 6 пункту 15 розділу II цього Положення;

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.”;

пункт доповнити двома новими абзацами такого змісту:

“Демонстрація, яка передбачена у підпункті 6 пункту 15 розділу ІІ цього Положення, 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 цього Положення, проводиться за погодженням із куратором перевірки та попереднім повідомленням контактної особи від банку безпосередньо за місцезнаходженням банку або з використанням засобів відеозв`язку.”;

5) розділ після пункту 15 доповнити новим пунктом 15^1 такого змісту:

“15^1. Матеріали (дані) фото- / відеофіксації, які отримані відповідно до підпункту 7 пункту 15 розділу ІІ цього Положення, долучаються до справи перевірки.”;

6) у підпункті 6 пункту 17 слово “телекомунікаційної” замінити словом “комунікаційної”;

7) у пункті 25 слова “нагляду (оверсайту) платіжних систем” замінити словами “оверсайту платіжної інфраструктури”;

8) пункт 26 викласти в такій редакції:

“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.”.

3. Розділ ІІІ після пункту 28 доповнити новим пунктом 28^1 такого змісту:

“28[1]. 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.”.

4. У розділі IV:

1) у пункті 30 слова “ризиків інформаційної безпеки / кіберризиків” замінити словами “процесів організації та забезпечення інформаційної безпеки / кіберзахисту”;

2) пункт 31 викласти в такій редакції:

“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 Звіту до Національного банку.”;

3) Розділ після пункту 31 доповнити двома новими пунктами 31[1] та 31[2] такого змісту:

“31[1]. 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.

31^2. Звіт складається щорічно станом на 31 березня та подається до Національного банку протягом одного місяця, наступного за звітним періодом (рік).”.

5. Додаток до Положення виключити.

6. Положення доповнити двома новими додатками, виклавши їх в такій редакції:

“Додаток 1
до Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг
(пункт 28^1 розділу III)

Повідомлення про істотні зміни в організації інформаційної безпеки та кіберзахисту

_____
(найменування банку)

№ з/п	Підстава подання повідомлення згідно п. 28^1 розділу III цього Положення	Розгорнутий опис зміни	Причина зміни та очікуваний банком вплив зміни на кіберстійкість банку
1	2	3	4
1			
2			
…			

Додаток 2
до Положення про здійснення контролю
за дотриманням банками вимог
законодавства з питань інформаційної
безпеки, кіберзахисту та електронних
довірчих послуг
(пункт 31 розділу IV)

Оцінювання процесів організації та забезпечення інформаційної безпеки / кіберзахисту

I. Звіт
з питань оцінювання процесів організації та забезпечення інформаційної безпеки / кіберзахисту
станом на 31 березня 20__ року

Таблиця 1

№ з/п	Твердження	Самооцінка відповідності твердженню	Дайте розгорнутий коментар щодо питання та за потреби обґрунтуйте самооцінку	Розгорнутий коментар банку
1	2	3	4	5
1	Управління			
2	Затверджена стратегія розвитку інформаційної безпеки / кіберзахисту охоплює звітний період	ТАК / ЧАСТКОВО / НІ	Зазначте реквізити актуальної стратегії та період який вона охоплює. Чи вносилися зміни до стратегії розвитку інформаційної безпеки (кіберзахисту) протягом звітного періоду? Якщо так, зазначте причини та коротко зміст змін	

Продовження додатка 2

Продовження таблиці 1

1	2	3	4	5
3	Затверджено розподіл відповідальностей за інформаційну безпеку / кіберзахист	ТАК / ЧАСТКОВО / НІ	Зазначте яким чином формалізовано розподіл відповідальностей за забезпечення інформаційної безпеки/кіберзахисту	
4	Призначена відповідальна особа за інформаційну безпеку банку (CISO) є Головою Правління / Заступником Голови Правління	ТАК / ЧАСТКОВО / НІ	Зазначити ПІБ, посаду CISO відповідно до штатного розкладу, назву та реквізити документа про призначення, а також актуальні контакти (включно з номером службового мобільного телефону)	
5	В структурі банку наявний та укомплектований підрозділ з інформаційної безпеки, що безпосередньо підпорядкований CISO	ТАК / ЧАСТКОВО / НІ	Зазначте якій посадовій особі підпорядковується такий підрозділ, його фактичну чисельність, основні завдання та функції. Зазначте на який підрозділ банку покладені функції із забезпечення кіберзахисту (повне найменування підрозділу, дату покладання зазначених функцій та якій посадовій особі підпорядковується такий підрозділ)	
6	Колективний керівний орган із питань упровадження та	ТАК / ЧАСТКОВО /	Вкажіть актуальний склад колективного керівного органу з	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
	функціонування СУІБ відповідає вимогам щодо складу та виконує покладені на нього обв'язки	НІ	питань упровадження та функціонування СУІБ із зазначенням посад його членів і реквізитів документів щодо їх призначення. Зазначте періодичність або кількість засідань колективного керівного органу з питань упровадження та функціонування СУІБ за звітний період	
7	Банком здійснено оцінювання ефективності СУІБ протягом звітного періоду	ТАК / ЧАСТКОВО / НІ	Вкажіть період за який здійснено останнє оцінювання, результати оцінювання та органи управління банку, що їх розглядали. Зазначте назву та реквізити документів щодо розгляду результатів оцінювання	
8	Затверджений перелік бізнес-процесів, критичних щодо інформаційної безпеки, є актуальним	ТАК / ЧАСТКОВО / НІ	Зазначте перелік таких процесів, а також щодо кожного з процесів структурні підрозділи банку, що є їх власниками. Вкажіть критерії, за якими визначалася їх критичність, назву та реквізити документу щодо останнього перегляду переліку	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
9	Контроль			
10	Рада банку здійснює контроль за забезпеченням інформаційної безпеки / кіберзахисту в банку та має достатні для цього компетенції	ТАК / ЧАСТКОВО / НІ	У який спосіб Рада банку здійснює контроль за забезпеченням інформаційної безпеки / кіберзахисту в банку. Зазначте, чи здійснений розподіл повноважень між членами Ради банку, що передбачає персональне закріплення членів ради за напрямом питань щодо інформаційної безпеки / кіберзахисту [зазначте хто саме з членів ради здійснює контроль в частині забезпечення інформаційної безпеки / кіберзахисту, та які компетенції (знання, навички, досвід, кваліфікацію) вони мають для здійснення такого контролю]	
11	Відповідальна особа за інформаційну безпеку банку (CISO) здійснює контроль за впровадженням заходів безпеки інформації в банку	ТАК / ЧАСТКОВО / НІ	У який спосіб відповідальна особа за інформаційну безпеку банку (CISO) здійснює контроль за впровадженням заходів безпеки інформації. Зазначте, чи	

Продовження додатка 2

Продовження таблиці 1

1	2	3	4	5
			вважаються достатніми наявні знання, навички, досвід, кваліфікація CISO для здійснення такого контролю	
12	Протягом звітного періоду здійснювався контроль за рівнем обізнаності працівників банку з питань інформаційної безпеки / кіберзахисту	ТАК / ЧАСТКОВО / НІ	Якщо так, коротко опишіть процедуру такого контролю, а також зазначте період здійснення, результати та спосіб їх використання	
13	Протягом звітного періоду завершені внутрішні аудити, об’єктом яких були процеси управління ризиками інформаційної безпеки / кіберзахисту банку та/або СУІБ банку	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначте перелік таких аудитів (тема, дата, період, об’єкт аудиту)	
14	Протягом звітного періоду завершені зовнішні аудити, об’єктом яких були процеси управління ризиками інформаційної безпеки / кіберзахисту банку та/або СУІБ банку	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначте перелік таких аудитів (тема, дата, період, об’єкт аудиту) та назву організацій, що їх проводили	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
15	Станом на дату заповнення цього Звіту рекомендації, надані за результатами здійснених внутрішніх / зовнішніх аудитів, об'єктом яких були процеси управління ризиками інформаційної безпеки / кіберзахисту банку та/або СУІБ банку, виконані	ТАК / ЧАСТКОВО / НІ	Якщо частково або ні, зазначте перелік таких рекомендацій	
16	Контрольна діяльність, що здійснюється банком у межах функціонування системи внутрішнього контролю, охоплює питання контролю за інформаційною безпекою та обміном інформацією	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначте заходи та процедури контролю, упроваджені банком для надання впевненості керівникам банку щодо досягнення банком операційних, інформаційних та комплаєнс-цілей діяльності банку, визначених у його стратегії, уключаючи інформацію про результати останнього оцінювання ефективності контролю за інформаційною безпекою та обміном інформацією як елементом системи внутрішнього контролю	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
17	Упродовж звітного періоду банком здійснювалась періодична перевірка відповідності наданих прав доступу до інформаційних систем, які забезпечують функціонування критичних бізнес-процесів	ТАК / ЧАСТКОВО / НІ	Зазначте до яких інформаційних систем та якими засобами / методами здійснювався контроль, які були виявлені невідповідності, їх причини, статус усунення виявлених невідповідностей та вжиті запобіжні заходи (за наявності, у розрізі систем)	
18	Упродовж звітного періоду банком здійснювалась періодична перевірка наданих / змінених / скасованих прав доступу до інформаційних систем, які забезпечують функціонування критичних бізнес-процесів, для працівників третіх сторін	ТАК / ЧАСТКОВО / НІ	Зазначте до яких інформаційних систем та якими засобами/методами здійснювався контроль, які були виявлені невідповідності, їх причини, статус усунення виявлених невідповідностей та вжиті запобіжні заходи (за наявності, у розрізі систем)	
19	Управління ризиками			
20	Банком розроблені документи щодо управління (визначення, оцінювання, оброблення, моніторингу тощо) ризиком	ТАК / ЧАСТКОВО / НІ	Якщо так, вкажіть вичерпний перелік таких документів (із зазначенням їх реквізитів)	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
	інформаційної безпеки / кіберризиком			
21	Протягом звітного періоду здійснено оцінювання ризиків інформаційної безпеки / кіберризиків відповідно до сфери застосування СУІБ	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначите період оцінювання та стисло опишіть його результати. Вкажіть якими органами управління банку здійснювався розгляд та затвердження результатів оцінювання (із зазначенням реквізитів протоколів засідання органів)	
22	План оброблення ризиків інформаційної безпеки / кіберризиків, або інший документ який передбачає оброблення відповідних ризиків (далі – План) є актуальним та виконується відповідно до передбачених у ньому строків	ТАК / ЧАСТКОВО / НІ	Зазначте реквізити Плану та інформацію щодо органів управління банку, якими він затверджувався. Чи мали місце протягом звітного періоду випадки порушення / перенесення строків виконання чи відміни заходів, передбачених Планом? У випадку наявності, вкажіть перелік таких заходів із зазначенням відповідних причин	
23	Призначений ризик-координатор, відповідальний за	ТАК / ЧАСТКОВО /	Зазначте посаду (відповідно до штатного розкладу), назву та	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
	управління ризиком інформаційної безпеки, зі складу підрозділу першої лінії захисту, функції якого полягають в управлінні інформаційною безпекою	НІ	реквізити внутрішньобанківського розпорядчого документу щодо призначення ризик-координатора, відповідального за управління ризиком інформаційної безпеки	
24	Під час управління ризиком інформаційної безпеки / кіберризиком банком використовуються задокументовані ключові індикатори ризиків	ТАК / ЧАСТКОВО / НІ	При використанні індикаторів, зазначте їх перелік. За наявності протягом звітного періоду випадків перевищення рівнів ключових індикаторів ризику, вкажіть відповідні індикатори та причини їх перевищення	
25	Стрес-тестування операційного ризику містило сценарії, які включали тестування ризику інформаційної безпеки / кіберризику в періоді звітування	ТАК / ЧАСТКОВО / НІ	За наявності, вкажіть перелік (короткий опис) сценаріїв, які включали тестування ризику інформаційної безпеки / кіберризику	
26	В банку наявні ІТ-залежні бізнес-процеси, зокрема щодо розробки та підтримки програмного забезпечення, функціонування яких частково або цілком	ТАК / НІ	Якщо так, зазначте найменування та короткий опис бізнес-процесів, постачальників технологічних послуг. Надайте стислий опис процедури оцінювання ризиків	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
	забезпечується за рахунок постачальників технологічних послуг		інформаційної безпеки / кіберризиків, пов'язаних з передаванням окремих процесів / функцій постачальникам технологічних послуг	
27	Процес управління ризиком інформаційної безпеки / кіберризиком автоматизовано шляхом впровадження інформаційної системи, яка забезпечує агрегування даних щодо ризиків банку, оперативне та достовірне вимірювання ризиків як на рівні окремого банку, так і на рівні банківської групи як в звичайних, так і в стресових ситуаціях	ТАК / ЧАСТКОВО / НІ	Зазначте якими засобами здійснено автоматизацію. Опишіть яким чином забезпечено реєстрацію та аналіз внутрішніх подій ризику інформаційної безпеки	
28	Заходи інформаційної безпеки/кіберзахисту			
29	Заходи безпеки інформації відповідно до Положення № 95 впроваджено	ТАК / ЧАСТКОВО / НІ	Якщо частково або ні, зазначте номери пунктів Положення № 95, упровадження яких станом на дату заповнення цього Звіту не завершено чи впроваджені заходи	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
			переглядаються. Для кожного з пунктів вкажіть причини не впровадження / перегляду та визначені строки та заходи, що планується здійснити	
30	Під час надання віддаленого доступу до інформаційних систем банку (включно з доступом представників третіх сторін) впроваджені заходи інформаційної безпеки	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначте перелік упроваджених заходів безпеки та їх стислий опис	
31	Банком забезпечена безперервність функціонування всіх впроваджених заходів інформаційної безпеки в межах процесу управління безперервністю діяльності	ТАК / ЧАСТКОВО / НІ	Вкажіть які дії протягом звітного періоду банк вживав для гарантування безперервності функціонування заходів інформаційної безпеки. Зазначте назви та реквізити документів, якими передбачені такі дії	
32	Банком розроблений та підтримується в актуальному стані план реагування на кіберзагрози, кібератаки та кіберінциденти на об’єктах кіберзахисту	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначити дату останнього перегляду документа та реквізити документа, яким підтверджується такий перегляд	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
33	Банк протягом звітного періоду здійснив тестування плану реагування на кіберзагрози, кібератаки та кіберінциденти на об'єктах кіберзахисту	ТАК / НІ	Якщо так, надайте опис дій, виконаних під час тестування та інформацію про об'єкти, яких воно стосувалось	
34	Протягом звітного періоду здійснена перевірка ефективності заходів щодо захисту периметра мережі банку шляхом виконання тесту на проникнення	ТАК / НІ	Якщо так, вкажіть коли та опишіть процедуру здійснення такого тесту (методика, об'єкти, технічні засоби). Зазначте назву зовнішньої організації, у випадку її залучення до виконання тесту на проникнення	
35	Банком здійснено заходи щодо виправлення вразливостей критичного та високого рівня, виявлених в результаті перевірки ефективності заходів щодо захисту периметра мережі банку	ТАК / ЧАСТКОВО / НІ	Якщо частково або ні, зазначте перелік невиправлених вразливостей, із вказанням їх рівня та коротким описом	
36	Упроваджено програму підвищення обізнаності/навчання працівників банку, що розглядає питання інформаційної безпеки / кіберзахисту	ТАК / ЧАСТКОВО / НІ	Якщо так, зазначте перелік заходів, які здійснювалися в межах такої програми упродовж звітного періоду, окремо вкажіть заходи, що стосувалися підвищення кваліфікації працівників, відповідальних за забезпечення	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
			інформаційної безпеки/кіберзахисту (з зазначенням тематики, організатора, кількості працівників, які взяли у них участь)	
37	Ресурси та засоби для забезпечення інформаційної безпеки та кіберзахисту			
38	Процеси забезпечення інформаційної безпеки та кіберзахисту банку наділені фінансовими ресурсами. Такі ресурси є доступними і достатніми для вирішення задач в межах операційної діяльності, а також досягнення цілей стратегії розвитку інформаційної безпеки / кіберзахисту банку	ТАК / ЧАСТКОВО / НІ	Зазначте основні принципи формування бюджету для потреб інформаційної безпеки / кіберзахисту банку. Вкажіть співвідношення (у відсотках) затверджених бюджетів для потреб забезпечення інформаційної безпеки / кіберзахисту банку та на потреби розвитку / підтримки інформаційних технологій (загальної цифровізації банку).	
39	Процеси забезпечення інформаційної безпеки та кіберзахисту банку підтримуються достатньою кількістю працівників, що	ТАК / ЧАСТКОВО / НІ	Зазначте кількість штатних працівників банку, функції яких безпосередньо пов`язані із забезпеченням інформаційної	

Продовження додатка 2
Продовження таблиці 1

1	2	3	4	5
	володіють знаннями, навичками та досвідом у предметній сфері		безпеки / кіберзахисту Банку, кількість вакантних посад. Надайте інформацію щодо плинності відповідних кадрів упродовж звітного періоду та оцініть рівень плинності (високий та контрольований; високий та неконтрольований; середній та контрольований; середній та неконтрольований; низький).	
40	Банк забезпечений ліцензійними інформаційними системами і програмно-апаратними засобами для ефективного забезпечення інформаційної безпеки та кіберзахисту	ТАК / ЧАСТКОВО / НІ	Вкажіть перелік (із зазначенням найменування та короткого опису призначення) інформаційних систем та програмно-апаратних засобів, що використовуються банком для забезпечення інформаційної безпеки та кіберзахисту	
41	Інформаційний блок (не передбачає подальшого оцінювання)			
42	Банк використовує хмарні послуги / технології для забезпечення захисту інформації / кіберзахисту	ТАК / НІ	Якщо так, щодо кожного випадку використання хмарних послуг / технологій зазначте їх вид, найменування, короткого опису	

Продовження додатка 2

Продовження таблиці 1

1	2	3	4	5
			призначення, постачальника хмарної технології (із зазначенням країни постачальника) та перелік бізнес-процесів, у яких вона використовується	
43	Протягом звітного періоду банком були зареєстровані інциденти інформаційної безпеки / кіберінциденти, що призвели до переривань в роботі критичних бізнес-процесів або мали інший негативний вплив та віднесені банком до інцидентів, що мають високий / критичний / надзвичайний рівень впливу.	ТАК / НІ	Якщо так, щодо кожного з таких інцидентів надайте інформацію про суть інциденту, вкажіть дату та причини його виникнення, величину негативного впливу, зокрема потенційну	
44	Наявний актуальний сертифікат відповідності СУІБ банку міжнародному стандарту ISO/IEC 27001, виданий акредитованою Міжнародним форумом з акредитації (International Accreditation Forum) організацією	ТАК / НІ	Якщо так, вкажіть реквізити сертифіката, його строк дії та організацію, яка проводила сертифікацію	

Продовження додатка 2

Продовження таблиці 1

1	2	3	4	5
45	В штаті банку наявні аудитори, що мають підтверджені кваліфікації у сфері інформаційних технологій або інформаційної безпеки	ТАК / НІ	Якщо так, то зазначте фактичну чисельність таких аудиторів та реквізити документів, що підтверджують їх кваліфікацію	
46	Банк впроваджує заходи відповідно до пункту 23 розділу ІІ цього Положення та рекомендацій, наданих у межах перевірок Національного банку з питань інформаційної безпеки / кіберзахисту	ТАК / НІ	Якщо так, вкажіть перелік заходів, виконання яких триває на дату заповнення цього Звіту	

Продовження додатка2

II. Оцінка загального рівня організації інформаційної безпеки та кіберзахисту в банку

Таблиця 2

№ з/п	Питання	Оцінка	Розгорнутий коментар щодо обраного рівня
1	2	3	4
1	Оцініть загальний рівень організації (зрілості) інформаційної безпеки та кіберзахисту в банку (за шкалою від 1 до 5), обґрунтуйте самооцінку		

III. Пояснення для заповнення додатка

1. Орієнтовний перелік характеристик (критеріїв) для банків щодо визначення рівня у відповідях в колонці 3 таблиці 1

Таблиця 3

Так	Частково	Ні
1	2	3
Фактична ситуація в банку відповідає описаній у твердженні Процес / процедура впроваджена та має системний характер.	Документи затверджені не в повному обсязі або потребують актуалізації. Наявні недоліки щодо запроваджених заходів.	Фактична ситуація в банку не відповідає описаній у твердженні. Процес / процедура не впроваджена або не має системного характеру. Документ не розроблений.

Продовження додатка2

Продовження таблиці 3

1	2	3
Можлива невелика кількість незначних невідповідностей вимогам / недоліків у функціонуванні процесу / впровадженому заході. Інші варіанти відповідей	Процеси не завжди носять системний характер, у їх функціонуванні можливі виключення. Заходи з інформаційної безпеки загалом упроваджені, щодо не впроваджених заходів керівництвом банку погоджені плани та строки впровадження, передбачені ресурси, відповідні ризики від невпроваджених заходів враховані та контролюються. Інші варіанти відповідей	Банком не впроваджена суттєва кількість заходів; наявні значні недоліки щодо … (наведеного твердження, зазначеного процесу тощо). Відповідальний підрозділ / колективний орган не визначений. Інші варіанти відповідей

2. В колонці 3 таблиці 2 банк проставляє оцінку (рівень зрілості) від “1” до “5”.
Під час оцінювання, банк має щонайменше врахувати:

1) внутрішню нормативну базу;

2) упроваджені (функціонуючі) засоби та заходи безпеки інформації;

3) діючі процеси виявлення, вимірювання, моніторингу та звітування щодо ризику інформаційної безпеки (кіберризику);

4) результати аудитів з питань інформаційної безпеки.

3. Опис рівнів зрілості:

1) Рівень 1 – низький рівень.

На цьому рівні більшість заходів та засобів забезпечення інформаційної безпеки не впроваджені;

2) Проміжні рівні 2 – 4 із поступовим зростанням зрілості;

3) Рівень 5 – стале вдосконалення.

На 5-му рівні банк зосереджений на системному вдосконаленні заходів та засобів забезпечення інформаційної безпеки для досягнення своїх стратегічних цілей та операційних потреб, має змогу забезпечити ефективну превентивну відповідь на нові загрози і ризики.”

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Зміни до Положення про організацію кіберзахисту в банківській системі України

1. У розділі I:

1) у пункті 1:

слова та цифри “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,” виключити;

пункт доповнити словами та цифрами “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) у пункті 2:

пункт після підпункту 3 доповнити новим підпунктом 3^1 такого змісту:

“3^1) значний кіберінцидент - подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої (потенційної) кібератаки, рівень критичності яких суттєво загрожує штатному функціонуванню інформаційних систем банку, що безпосередньо забезпечують автоматизацію банківської діяльності, та мають значний негативний вплив на надання банківських послуг, який може призвести до зміни функціональних можливостей таких послуг або робить їх недоступними;”;

пункт після підпункту 9 доповнити новим підпунктом 9^1 такого змісту:

“9^1) рівень критичності кіберінциденту - ступень негативного впливу на банк та/або суб'єктів системи кіберзахисту в банківській системі України, що може відбутися в результаті реалізації кіберзагроз;”;

після підпункту 10 доповнити новим підпунктом 10^1 такого змісту:

“10^1) системний кіберризик - ризик порушення стабільності банківської системи внаслідок реалізації кіберзагроз щодо окремого банку через відповідні недоліки в його кіберстійкості;”;

в абзаці шістнадцятому слово “незалежний” виключити;

3) у підпункті 4 пункту 3 слово “незалежного” виключити;

4) у пункті 4 слова “ризиків інформаційної безпеки / кіберризиків” замінити словами “процесів організації та забезпечення інформаційної безпеки / кіберзахисту”;

5) у пункті 5 слова та цифри “у розділі IV” замінити словами та цифрами “у розділах II, IV”.

3. У розділі II:

1) абзац другий пункту 11 замінити чотирма новими абзацами такого змісту:

“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.”;

2) абзац п’ятий підпункту 3 пункту 13 викласти в такій редакції:

“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;”;

3) розділ після пункту 19 доповнити трьома новими пунктами 19^1 - 19^3 такого змісту:

“19^1. Національний банк установлює вимоги до порядку інформування банками про значні кіберінциденти. Опис цих вимог та шаблони повідомлень наведені у порядку інформування про значні кіберінциденти, що розміщений на порталі Центру кіберзахисту в розділі “Банки / Документація”.

19^2. 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 19^2 розділу II 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.

19^3. Банк має право інформувати Центр кіберзахисту про кіберінцидент, що не визначений банком як значний, з метою та в спосіб, що встановлені в розділі III цього Положення.”.

4. У розділіV:

1) у назві розділу слово “незалежного” виключити;

2) у пункті 42 слово “незалежного” виключити ;

3) в підпункті 2 пункту 45 цифри “38” замінити цифрами “44”.