Офіційно опубліковано 20.01.2021

Правління Національного банку України

П О С Т А Н О В А

16 січня 2021 року м. Київ № 4

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

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 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 Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг (далі − Положення), що додається.

2. Департаменту безпеки (Ігор Коновалов) 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 Кирила Шевченка.

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

Голова Кирило ШЕВЧЕНКО

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
16 січня 2021 року № 4

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

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про банки і банківську діяльність", "Про основні засади забезпечення кібербезпеки України", "Про електронні документи та електронний документообіг", "Про електронні довірчі послуги", з урахуванням Директиви Європейського парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95 (далі – Положення № 95), Положення про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116 (далі – Положення № 116).

2. Це Положення встановлює:

1) порядок організації та здійснення Національним банком України (далі – Національний банк) заходів контролю за дотриманням банками вимог законодавства, яке регулює відносини у сферах кіберзахисту, інформаційної безпеки та електронних довірчих послуг, а також нормативно-правових актів Національного банку, що здійснюється на виконання покладених на Національний банк наглядових функцій (далі – контроль);

2) вимоги щодо проведення банком самооцінки стану інформаційної безпеки/кіберзахисту.

3. У цьому Положенні терміни вживаються в таких значеннях:

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 ІІІ цього Положення, без виходу за місцезнаходженням банку;

2) дата перевірки – календарна дата, станом на яку здійснюється перевірка, за результатами якої інформація відображається в довідці про перевірку;

3) довгостроковий кваліфікований електронний підпис (далі – КЕП) – кваліфікований електронний підпис, що відповідає формату з повним набором даних для перевірки кваліфікованого електронного підпису в довгостроковому періоді (понад два роки);

4) інспекційна група – група працівників структурного підрозділу центрального апарату Національного банку, яка здійснює контроль за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та надання кваліфікованих електронних довірчих послуг (далі – Департамент), уповноважених на здійснення перевірки банку;

5) кіберризик – ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз;

6) кіберстійкість – властивість інформаційної інфраструктури банку, забезпечувати функціонування бізнес-процесів банку, продуктом яких є банківські та фінансові послуги, під час кібератак і кіберінцидентів, яка має постійно підтримуватися органами управління банку шляхом організації управління кіберризиками та впровадження заходів кіберзахисту;

7) куратор перевірки – працівник Департаменту, визначений у розпорядчому акті Національного банку про проведення перевірки, який здійснює загальне керівництво процесом перевірки, координує вирішення питань, що виникають під час перевірки;

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

9) перевірка – планова перевірка банку з питань інформаційної безпеки, кіберзахисту, надання кваліфікованих електронних довірчих послуг, що проводиться інспекційною групою безпосередньо за його місцезнаходженням;

10) позапланова перевірка – перевірка банку з питань інформаційної безпеки, кіберзахисту, надання електронних довірчих послуг, що проводиться за наявності обґрунтованих підстав відповідно до розпорядчого акта Національного банку інспекційною групою безпосередньо за його місцезнаходженням;

11) програма перевірки – узагальнений перелік питань, що підлягають перевірці.

Інші терміни в цьому Положенні вживаються в значеннях, визначених у Законах України "Про електронні довірчі послуги", "Про основні засади забезпечення кібербезпеки України", "Про банки і банківську діяльність" та нормативно-правових актах Національного банку.

4. Національний банк здійснює контроль з метою:

1) оцінювання ефективності функціонування системи управління інформаційною безпекою (далі – СУІБ) банку;

2) оцінювання повноти виконання банком вимог нормативно-правових актів Національного банку з питань інформаційної безпеки, кіберзахисту;

3) оцінювання рівня управління ризиками інформаційної безпеки/кіберризиками банком і системи внутрішнього контролю, яка функціонує на всіх організаційних рівнях, за напрямами діяльності, що перевіряються;

4) прийняття засвідчувальним центром рішення про внесення відомостей про кваліфікованого надавача електронних довірчих послуг до Довірчого списку;

5) перевірки виконання вимог нормативно-правових актів з питань надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг, відомості про якого внесені до Довірчого списку за поданням засвідчувального центру.

5. Національний банк здійснює контроль шляхом проведення:

1) виїзних заходів контролю у формі перевірок;

2) безвиїзних заходів контролю.

6. Виїзні заходи контролю у формі перевірок здійснюються інспекційною групою згідно з календарним планом, що складається відповідно до розділу ІІ цього Положення.

7. Вимоги цього Положення поширюються на банки.

ІІ. Організація та порядок проведення виїзних заходів контролю

8. Департамент здійснює планування виїзних заходів контролю на підставі ризик-орієнтованого підходу, що ґрунтується на результатах:

1) здійснення безвиїзних і виїзних заходів контролю;

2) аналізу інформації з офіційних джерел щодо діяльності банків;

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

4) опрацювання інформації про віднесення банку до об’єкта критичної інфраструктури;

5) опрацювання інформації про внесення відомостей про банк як кваліфікованого надавача електронних довірчих послуг до Довірчого списку;

6) опрацювання висновків щодо поточного рівня ризиків інформаційної безпеки/кіберризиків і його впливу на кіберстійкість банку з урахуванням наявної інформації про факти, події та обставини в його діяльності.

План перевірок затверджується розпорядчим актом Національного банку і оприлюднюється на сторінці офіційного Інтернет-представництва Національного банку.

9. Перевірка банку проводиться на підставі розпорядчого акта Національного банку про проведення планової перевірки, у якому зазначаються найменування банку, що перевіряється, підстава для проведення перевірки, дата перевірки, терміни проведення перевірки (дати початку і закінчення), склад інспекційної групи та куратор перевірки (із зазначенням прізвищ, імен, по батькові, посад та номерів службових посвідчень).

Перевірка банку здійснюється відповідно до програми перевірки, яка оформляється як додаток до розпорядчого акта Національного банку про планову перевірку.

Національний банк має право включати в програму перевірки питання з перевірки банку як кваліфікованого надавача електронних довірчих послуг не

раніше ніж через шість місяців з дня внесення відомостей про нього до Довірчого списку.

10. Національний банк має право проводити позапланову перевірку з метою термінового встановлення причин, обставин, масштабу негативного впливу на життєдіяльність банку та/або банківську систему в разі отримання документально підтвердженої інформації про:

1) інциденти інформаційної безпеки/кіберінциденти, наслідком яких є реалізована загроза для безпеки інформації банку та його клієнтів;

2) інциденти інформаційної безпеки/кіберінциденти, наслідки яких можуть спричинити системний ризик у банківській системі;

3) порушення вимог законодавства у сфері електронних довірчих послуг.

Позапланова перевірка призначається за окремим дорученням Голови Національного банку та оформляється наказом Національного банку за його підписом (далі − наказ про позапланову перевірку).

У наказі про позапланову перевірку зазначаються найменування банку, що перевіряється, підстава/підстави для проведення перевірки, дата і терміни проведення перевірки (дати початку і закінчення), склад інспекційної групи та куратор перевірки (із зазначенням прізвищ, імен, по батькові, посад та номерів службових посвідчень), питання, які підлягають перевірці.

Під час проведення позапланової перевірки з'ясовуються лише ті питання, потреба перевірки яких стала підставою для здійснення цієї перевірки.

11. Національний банк повідомляє банк про проведення планової перевірки не пізніше ніж за 20 календарних днів до її початку.

Повідомлення про проведення планової перевірки оформляється листом в електронній формі Національного банку, який підписується керівником/заступником керівника Департаменту, надсилається до банку засобами електронної пошти Національного банку і містить інформацію про підстави для проведення перевірки, дату і терміни проведення перевірки (дати початку і закінчення), склад інспекційної групи та куратора перевірки (із зазначенням прізвищ, імен, по батькові, посад та номерів службових посвідчень), програму перевірки і може містити додатки (запити про надання документів, інформації, форми для заповнення).

Банк зобов'язаний своєчасно та в повному обсязі надати інформацію і документи (їх копії та/або витяги з них), зазначені в повідомленні про проведення планової перевірки, у визначеному форматі та в установлені Національним банком строки.

Національний банк здійснює позапланову перевірку із повідомленням керівника банку, що надсилається не пізніше дня початку такої перевірки.

12. Куратор перевірки або члени інспекційної групи під час проведення перевірки (планової або позапланової) у разі виникнення потреби в отриманні додаткової/додаткових інформації/документів, що стосується/стосуються перевірки, мають право запитувати в банку інформацію (в електронному або паперовому вигляді у визначених обсягах, форматі, структурі, порядку, термінах і носіях інформації), документи (їх копії та/або витяги з них) та письмові пояснення шляхом надання запиту у формі електронного документа (далі – запит) до вручення (надсилання) банку довідки про перевірку.

Запит складається на ім’я керівника банку, підписується за допомогою КЕП куратора перевірки та передається банку в електронній формі. Такий запит підлягає обов’язковій реєстрації банком у день отримання та поверненню з накладеними в день отримання (якщо такої можливості немає, то не пізніше наступного робочого дня) КЕП керівника банку та позначкою часу.

Банк у відповідь на запит зобов’язаний своєчасно та в повному обсязі надати достовірну інформацію, матеріали, документи (їх копії та/або витяги з них, засвідчені в порядку, установленому законодавством України) у визначених порядку, форматі, структурі, вигляді та збережені на визначених носіях. Інформація та документи мають надаватися у форматі та якості, які забезпечують безперешкодне та однозначне тлумачення даних, зазначених у них.

Інформація, документи (їх копії та/або витяги з них) у паперовій та/або електронній формі на визначених носіях інформації, письмові пояснення, підготовлені банком на запит, надаються за підписом керівника банку із супровідним листом. Такий супровідний лист підлягає обов’язковій реєстрації в банку.

13. Куратор перевірки та/або члени інспекційної групи фіксують факти ненадання банком інформації і документів (їх копій та/або витягів з них, засвідчених у порядку, установленому законодавством України), зазначених у повідомленні про проведення планової перевірки відповідно до пункту 11 розділу ІІ цього Положення та/або зазначених у запиті відповідно до пункту 12 розділу ІІ цього Положення, шляхом складання акта про ненадання інформації/документів. Такі факти відображаються в довідці про перевірку.

14. Зустріч куратора перевірки, членів інспекційної групи з керівником банку, відповідальною особою за інформаційну безпеку банку (Chief information security officer, CISO) проводиться в перший день планової/позапланової перевірки. Керівнику банку вручається копія наказу про планову/позапланову перевірку, засвідчена в порядку, установленому законодавством України,

узгоджуються питання комунікації (уключаючи визначення контактної особи від банку), можливості обміну інформацією, а також інші організаційні питання.

15. Куратор перевірки і члени інспекційної групи під час проведення перевірки (планової або позапланової) банку мають право:

1) безперешкодного доступу до всіх оригіналів документів, матеріалів та інформації, також до тих, що становлять інформацію з грифами обмеження доступу, потрібних для перевірки, до системи автоматизації банку (уключаючи персоналізований доступ у режимі перегляду), інформаційно-телекомунікаційної системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів банку;

2) вільного доступу до всіх приміщень банку (уключаючи приміщення юридичних або фізичних осіб, із якими в банку є договірні відносини для виконання його функцій на умовах аутсорсингу, якщо такі приміщення використовуються для розміщення обладнання, що забезпечує функціонування інформаційних систем банку або роботу в системі електронних платежів Національного банку) у робочий час та неробочий час за потреби;

3) збирати та вимагати від банку надання будь-якої інформації, матеріалів, документів (їх копій та/або витягів з них, засвідчених у порядку, установленому законодавством України), письмових пояснень, потрібних для здійснення перевірки;

4) одержувати від банку та виносити за межі його приміщень матеріали перевірки, уключаючи копії документів, засвідчені в порядку, установленому законодавством України, що свідчать/можуть свідчити про порушення законодавства з питань інформаційної безпеки, кіберзахисту, надання електронних довірчих послуг, для здійснення наглядових дій у межах, передбачених цим Положенням заходів контролю;

5) користуватися потрібними для проведення перевірки та організації діяльності інспекційної групи технічними засобами, уключаючи комп’ютери, змінні носії інформації, програмні засоби, копіювальні апарати, сканери, телефони, заносити в приміщення та виносити з приміщення банку технічні та програмні засоби, що належать Національному банку;

6) вимагати від банку демонстрації та ознайомлення з функціональними можливостями і налаштуваннями системи автоматизації банку, інформаційно-телекомунікаційної системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів банка.

16. Куратор перевірки і члени інспекційної групи під час проведення перевірки (планової або позапланової) банку зобов'язані:

1) дотримуватися вимог законодавства України;

2) не розголошувати та не використовувати в інший спосіб інформацію з обмеженим доступом, що стала їм відома у зв'язку з виконанням обов'язків, крім випадків, передбачених законодавством України;

3) дотримуватися норм етичної поведінки.

17. Керівник банку зобов'язаний виконувати вимоги куратора перевірки та членів інспекційної групи, зазначені в пункті 15 розділу ІІ цього Положення, сприяти та не створювати перешкод проведенню перевірки (планової або позапланової), а також:

1) забезпечувати надання інформації і документів (їх копій та/або витягів з них, засвідчених у порядку, установленому законодавством України), зазначених у повідомленні про проведення планової перевірки відповідно до пункту 11 розділу ІІ цього Положення та запиті відповідно до пункту 12 розділу ІІ цього Положення;

2) забезпечити оперативний зв'язок куратора перевірки, членів інспекційної групи з контактною особою банку;

3) після отримання копії наказу про планову/позапланову перевірку цього банку, засвідченої в порядку, установленому законодавством України, забезпечити на період її проведення кураторові перевірки та кожному члену інспекційної групи вільний (на першу вимогу) вхід/вихід до/із службових приміщень банку протягом усього робочого дня, а за потреби в неробочий час;

4) забезпечити кураторові перевірки та членам інспекційної групи вільний доступ до всіх документів, інформації та матеріалів з питань, визначених у програмі перевірки банку;

5) виділити кураторові перевірки та членам інспекційної групи на період проведення перевірки окремі робочі місця в ізольованому від працівників банку та сторонніх осіб службовому приміщенні, що обладнане необхідними меблями, сейфом для зберігання документів, комп'ютерами і відповідає санітарно-гігієнічним умовам, установленим нормативно-правовими актами в цій сфері; забезпечити можливість користуватися телефоном, засобами копіювально-

розмножувальної техніки. Доступ до зазначеного службового приміщення керівника та інших працівників банку, осіб, у яких таке приміщення перебуває у власності, оренді чи іншому праві користування, під час проведення перевірки здійснюється тільки в присутності членів інспекційної групи;

6) забезпечувати кураторові перевірки, членам інспекційної групи демонстрацію та ознайомлення з функціональними можливостями, налаштуваннями системи автоматизації банку, інформаційно-телекомунікаційної системи кваліфікованого надавача електронних довірчих послуг, інших систем та інформаційних ресурсів;

7) забезпечувати членам інспекційної групи за запитом та наявністю технічної можливості персоналізований доступ у режимі перегляду до системи автоматизації банку та інформаційних систем, що використовуються для забезпечення безпеки інформації з процедурою ідентифікації, на підставі службового посвідчення працівника Національного банку;

8) забезпечувати коректну поведінку працівників банку під час проведення перевірки.

18. Члени інспекційної групи в разі створення представниками банку перешкод для проведення перевірки та/або незабезпечення керівником банку умов відповідно до пункту 16 розділу II цього Положення повідомляють про це куратора перевірки і складають акт про здійснення перешкод.

19. За результатами проведення планової або позапланової перевірки складається довідка про перевірку у двох примірниках, підписується членами інспекційної групи, куратором перевірки, керівником банку. Довідка про перевірку може складатися у формі електронного документа та підписуватися шляхом накладення КЕП.

Довідка про перевірку містить описову частину, висновки, що формуються на підставі отриманих результатів перевірки та з урахуванням професійного судження членів інспекційної групи, інформацію про виявлені порушення (факти, що можуть свідчити про здійснення банком ризикової діяльності), недоліки, які мають вплив на діяльність банку, може містити іншу інформацію щодо результатів перевірки, вимоги про усунення встановлених порушень та рекомендації банку.

Матеріали, які надані банком у відповідь на запит відповідно до пункту 12 розділу II цього Положення та підтверджують факти (дії, події, випадки, обставини), долучаються як матеріали перевірки до справи перевірки.

Члени інспекційної групи здійснюють перевірку відповідно до методичних рекомендацій щодо здійснення перевірок, схвалених розпорядчим актом

Національного банку, надають висновки за результатом перевірки із застосуванням професійного судження та несуть відповідальність за достовірність відомостей і обґрунтованість висновків, викладених у довідці про перевірку.

20. Два примірники довідки про перевірку передаються керівникові банку для ознайомлення та підписання із зазначенням дати передавання та підпису про отримання на копії першого (титульного) листа довідки про перевірку, який залишається в одного з членів інспекційної групи.

Керівник банку зобов'язаний не пізніше ніж на третій робочий день з дати отримання довідки про перевірку ознайомитися з інформацією, викладеною в довідці, підписати обидва примірника довідки власноручно, зазначивши дату й позначку "ознайомлений", повернути перший примірник довідки інспекційній групі.

Довідка про перевірку, яка складається в електронній формі, після підписання членами інспекційної групи (шляхом накладання КЕП) передається банку засобами системи електронної пошти Національного банку з обов'язковою реєстрацією банком у день отримання.

Керівник банку зобов'язаний не пізніше ніж на третій робочий день з дати отримання довідки про перевірку в електронній формі:

1) розглянути і підписати довідку шляхом накладання КЕП;

2) повернути інспекційній групі довідку в електронній формі з накладеним КЕП керівника банку;

3) надіслати лист із накладеним КЕП до Національного банку на ім'я куратора перевірки з інформацією про ознайомлення з довідкою про перевірку засобами системи електронної пошти Національного банку.

21. Керівник банку в разі наявності заперечень щодо відомостей і висновків, викладених у довідці про перевірку, має право одночасно із поверненням підписаного ним першого примірника довідки надати обґрунтовані письмові заперечення (пояснення) із документальним підтвердженням (у разі їх наявності), які є невід'ємною частиною довідки про перевірку. Довідка про перевірку в такому випадку доповнюється відміткою "із запереченнями (поясненнями)".

Керівник банку в разі подання довідки про перевірку в електронній формі за наявності заперечень щодо фактів і висновків, викладених у довідці про перевірку, має право не пізніше ніж на третій робочий день надіслати лист із накладеним КЕП кураторові перевірки з обґрунтованими запереченнями

(поясненнями) із документальним підтвердженням (за їх наявності) засобами системи електронної пошти Національного банку.

Надання банком заперечень до довідки про перевірку не звільняє банк від визначених законодавством України, а також нормативно-правовими актами Національного банку обов'язків, виконання яких пов'язане з фактом отримання банком довідки про перевірку.

22. Власником довідки про перевірку, додатків до неї та інших матеріалів перевірки з моменту їх отримання уповноваженими на перевірку працівниками Національного банку є виключно Національний банк. Довідка про перевірку разом із додатками та інші матеріали перевірки становлять інформацію з обмеженим доступом. Усі документи, складені Національним банком із використанням та/або на підставі інформації, що міститься в довідці про перевірку банку, додатках до неї, інших матеріалах перевірки, становлять інформацію з обмеженим доступом, яка відповідно до законодавства України не має доводитися до відома осіб, яких вона стосується, та поширюються Національним банком у порядку, визначеному законодавством України.

23. Банк за результатами перевірки протягом 30 робочих днів з дня підписання керівником банку довідки про перевірку зобов'язаний подати до Національного банку на погодження план заходів, що має містити інформацію про дієві заходи, що будуть здійснені банком для усунення встановлених порушень, недоліків, урахування наданих рекомендацій із визначенням відповідальних осіб банку та строків їх виконання (далі – План заходів).

24. Банк зобов'язаний подавати до Національного банку звіт про стан виконання погодженого Національним банком Плану заходів, що містить перелік ужитих банком заходів щодо усунення порушень, недоліків, урахування наданих рекомендацій, у строк (період), обсязі, за форматом та структурою, визначеними Національним банком за результатом погодження Плану заходів.

25. Департамент має право вносити на засідання Комітету з питань нагляду та регулювання діяльності банків, нагляду (оверсайту) платіжних систем інформацію про результати проведеної перевірки банку і пропозиції щодо застосування/незастосування до банку адекватних заходів впливу для прийняття цим Комітетом відповідного рішення.

26. Куратор перевірки за результатами перевірки за наявності виявлених недоліків, порушень вимог Закону України "Про електронні довірчі послуги", Положення № 116, регламенту роботи засвідчувального центру і нормативно-правових актів Національного банку в сфері електронних довірчих послуг подає

керівнику засвідчувального центру витяг з довідки про перевірку для прийняття рішення щодо:

1) інформування спеціального уповноваженого центрального органу виконавчої влади з питань організації спеціального зв’язку та захисту інформації у сферах електронних довірчих послуг та електронної ідентифікації про виявлені порушення вимог законодавства у сфері електронних довірчих послуг для здійснення заходів відповідно до вимог законодавства у сфері електронних довірчих послуг;

2) скасування/блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача;

3) направлення подання про виключення кваліфікованого надавача електронних довірчих послуг з Довірчого списку відповідно до Закону України “Про електронні довірчі послуги”.

ІІІ. Організація проведення безвиїзних заходів контролю

27. Департамент здійснює безвиїзні заходи контролю з питань інформаційної безпеки, кіберзахисту та надання кваліфікованих електронних довірчих послуг шляхом проведення аналізу дотримання банком вимог законодавства України на підставі:

1) довідки про перевірку, матеріалів перевірки банку, Плану заходів;

2) інформації, документів (їх копій та/або витягів із них, засвідчених у порядку, установленому законодавством України) у паперовій та/або електронній формі щодо усунення банком порушень/недоліків і виконання рекомендацій, отриманих від банку;

3) інформації, звітів, отриманих від банку, уключаючи відомості за результатами проведення зовнішніх незалежних аудитів інформаційної безпеки;

4) інформації та документів, отриманих від підрозділів Національного банку, суб’єктів забезпечення кібербезпеки, інших державних органів, а також іншої інформації та документів, отриманих Національним банком під час виконання ним своїх функцій;

5) інформації та документів, отриманих від Центру кіберзахисту Національного банку, засвідчувального центру.

28. Національний банк має право вимагати від банку надання інформації для здійснення безвиїзних заходів контролю шляхом направлення запиту. Запит оформляється в електронній формі у вигляді службового листа Національного банку, підписується керівником/заступником керівника Департаменту шляхом накладення КЕП та надсилається засобами системи електронної пошти Національного банку. Керівник банку зобов'язаний забезпечити надання на запит Національного банку достовірної інформації у вигляді письмових пояснень, документів у електронній або паперовій формі, у спосіб, строк, в обсязі, за форматом та структурою, визначеними в такому запиті.

29. Банк, що має намір стати кваліфікованим надавачем довірчих послуг, у заяві про внесення до Довірчого списку зазначає про готовність надавати кваліфіковані довірчі послуги. Засвідчувальний центр за результатами аналізу інформації, наведеної в заяві про внесення до Довірчого списку, приймає рішення про внесення відомостей про банк як кваліфікованого надавача до Довірчого списку (або відмову у внесенні відомостей до Довірчого списку) відповідно до вимог Положення № 116 і регламенту роботи засвідчувального центру. Виконання банком – кваліфікованим надавачем електронних довірчих послуг вимог Положення № 116 перевіряється під час планової перевірки.

IV. Вимоги щодо проведення банком самооцінки стану інформаційної безпеки/кіберзахисту

30. Банк зобов'язаний проводити щорічну самооцінку стану інформаційної безпеки/кіберзахисту шляхом складання щорічного Звіту з питань оцінювання ризиків інформаційної безпеки/кіберризиків (далі – Звіт) із урахуванням відомостей за результатами періодичного проведення:

1) оцінювання ризиків інформаційної безпеки/кіберзахисту;

2) оцінювання результативності інформаційної безпеки та ефективності СУІБ;

3) зовнішнього аудиту інформаційної безпеки;

4) внутрішнього аудиту інформаційної безпеки/кіберзахисту (далі – внутрішній аудит).

31. Керівник банку зобов'язаний забезпечити своєчасне подання до Національного банку Звіту, надання повної та достовірної інформації у Звіті, складеному за формою згідно з додатком до цього Положення, у формі електронного документа з накладеним КЕП керівника банку, засобами

електронної пошти Національного банку з урахуванням вимог, установлених Національним банком щодо пересилання документів із грифом обмеження доступу. Звіт складається щорічно станом на 31 березня та подається до Національного банку протягом одного місяця, наступного за звітним періодом (рік).

32. Керівник банку організовує проведення зовнішнього аудиту (з метою одержання банком оцінки інформаційної безпеки) відповідно до законодавства в сфері захисту інформації та кібербезпеки. Така оцінка використовується банком для забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ банку, визначення можливостей вдосконалення та потреби проведення коригувальних дій та ураховується Національним банком під час планування заходів контролю.

Вимоги до проведення незалежного аудиту інформаційної безпеки встановлюються відповідним нормативно-правовим актом Національного банку.

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

Звіт
з питань оцінювання ризиків інформаційної безпеки/кіберризиків
станом на 31 березня 20__ року

_____
(найменування банку)

№ з/п	Зміст запитання	Відповідь
1	2	3
1	Чи розроблена банком стратегія розвитку інформаційної безпеки (кібербезпеки)? Якщо так, то зазначити назву та реквізити такого документа. Який період охоплює така стратегія? Чи вносилися зміни до стратегії розвитку інформаційної безпеки (кібербезпеки) протягом звітного періоду? Якщо так, то вказати причини	
2	Які структурні підрозділи банку визначені відповідальними за досягнення цілей стратегії інформаційної безпеки (кібербезпеки)?	
3	Яка ступінь досягнення цілей, визначених чинною стратегією розвитку інформаційної безпеки (кібербезпеки), на дату заповнення цього Звіту?	
4	Яким чином здійснюється звітування керівництву банку щодо виконання цілей, передбачених стратегією інформаційної безпеки (кібербезпеки)?	

1	2	3
5	Чи призначена відповідальна особа за інформаційну безпеку банку (CISO)? Якщо так, то зазначити прізвище, ім’я, по батькові, посаду призначеної особи відповідно до штатного розкладу, назву та реквізити документа про призначення, а також перелік структурних підрозділів банку, що підпорядковуються CISO або щодо яких CISO має повноваження куратора	
6	Чи наявний у структурі банку окремий підрозділ з інформаційної безпеки? Якщо так, то зазначити, якій посадовій особі підпорядковується такий підрозділ, його фактичну чисельність, основні завдання і функції	
7	Чи розроблена банком методика щодо здійснення оцінювання ефективності СУІБ банку? Якщо так, то зазначити назву та реквізити такого документа	
8	Чи здійснено оцінювання ефективності СУІБ банку? Якщо так, то вказати період, за який здійснено останнє оцінювання, результати оцінювання, та органи управління банку, що розглядали результати такого оцінювання (зазначити назву та реквізити такого документа)	
9	Яка сфера застосування СУІБ? Чи визначено перелік бізнес-процесів, що є критичними щодо інформаційної безпеки? Якщо так, то зазначити перелік таких процесів, а також структурних підрозділів банку, визначених їх власниками із посиланням на внутрішні документи банку (зазначити назви та реквізити таких документів)	
10	Чи використовує банк хмарні технології? Якщо так, то зазначити, які та для яких бізнес-процесів/продуктів/цілей	
11	Чи упроваджено програму підвищення обізнаності/навчання працівників банку, що	

1	2	3
	розглядає питання інформаційної безпеки (кібербезпеки)? Коротко описати перелік заходів, що здійснювалися в межах такої програми упродовж звітного періоду	
12	Чи здійснюється періодичний контроль за рівнем обізнаності працівників банку з питань інформаційної безпеки (кібербезпеки)? Якщо так, то коротко описати процедуру такого контролю, а також використання результатів	
13	Чи розроблена банком політика інформаційної безпеки? Якщо так, то зазначити реквізити такого документа, дату останнього перегляду документа	
14	Чи керується банк (що належить до міжнародної банківської групи) настановами, стандартами, практикою з питань інформаційної безпеки та кіберзахисту, використання яких рекомендовано групою? Якщо так, то зазначити якими саме	
15	Чи розроблена банком методика оцінювання та оброблення ризиків інформаційної безпеки/кіберризиків? Якщо так, то зазначити назву, реквізити документа	
16	Чи впроваджено процес управління ризиками інформаційної безпеки/кіберризиками? Якщо так, то зазначити перелік органів управління та структурних підрозділів банку, до функцій яких належить управління ризиками інформаційної безпеки/кіберризиком	
17	Чи здійснено оцінювання ризиків інформаційної безпеки/кіберризиків щодо критичних бізнес-процесів? Якщо так, то зазначити період, за який здійснено останнє оцінювання, стисло описати результати такого оцінювання	
18	Чи наявні в банку бізнес-процеси, функціонування яких частково або цілком забезпечується за рахунок аутсорсингу?	

1	2	3
	Якщо так, то зазначити назви і стислий опис таких бізнес-процесів, а також надати стислий опис процедури оцінювання ризиків інформаційної безпеки/кіберризиків, пов'язаних з передаванням окремих процесів/функцій на аутсорсинг	
19	Чи розроблені банком внутрішні документи (положення щодо застосовності, план оброблення ризиків інформаційної безпеки/кіберризиків) щодо оброблення ризиків? Якщо так, то зазначити назви, реквізити таких документів	
20	Чи затверджено органами управління банку перелік заходів щодо зменшення ймовірності виникнення виявлених ризиків та/або зменшення їх впливу на функціонування критичних бізнес-процесів банку (назва, реквізити документа)?	
21	Чи здійснено оцінку ефективності упроваджених заходів щодо зменшення ризиків? Якщо так, то зазначити період, за який здійснено останнє оцінювання, та органи управління банку, що розглядали результати такого оцінювання (назва, реквізити документа)	
22	Чи в повному обсязі упроваджені заходи безпеки інформації відповідно до Положення № 95? Якщо ні, то зазначити перелік заходів, упровадження яких станом на дату заповнення цього Звіту не завершені	
23	Чи розроблені банком внутрішні документи, які встановлюють вимоги щодо використання, надання, скасування та контролю щодо доступу до інформаційних систем банку? Якщо так, то зазначити назви, реквізити таких документів, дату останнього перегляду документів	
24	Чи дотримується банк принципу надання мінімального рівня повноважень під час	

1	2	3
	надання доступу працівникам та третім сторонам до інформаційних систем банку? Якщо так, то стисло описати якими процедурами та засобами реалізовано застосування такого принципу, а також зазначити перелік упроваджених заходів контролю щодо доступу до інформаційних систем банку	
25	Чи наявні в банку інформаційні системи, для яких упроваджено можливість віддаленого доступу працівників або третіх сторін? Якщо так, то зазначити перелік таких інформаційних систем і бізнес-процесів, у функціонуванні яких беруть участь такі системи, а також коротко зазначити перелік упроваджених заходів безпеки щодо кожної системи	
26	Чи розроблені банком внутрішні документи, які встановлюють вимоги щодо управління інцидентами інформаційної безпеки (кіберінцидентами)? Якщо так, то зазначити назви, реквізити таких документів, дату останнього перегляду документів	
27	Чи упроваджено процес управління інцидентами інформаційної безпеки (кіберінцидентами)? Якщо так, то коротко описати основні етапи такого процесу та яким чином (засобами) він автоматизований. Який структурний підрозділ банку є відповідальним за процес управління інцидентами інформаційної безпеки (кіберінцидентами)?	
28	Чи здійснюється банком оброблення фактів ураження інформаційних систем банку зловмисним кодом у межах процесу управління інцидентами інформаційної безпеки (кіберінцидентами)? Якщо так, то зазначити перелік критеріїв, визначених банком, для віднесення фактів вірусного	

1	2	3
	ураження до інцидентів інформаційної безпеки (кібербезпеки)	
29	Чи здійснюється банком оброблення подій щодо атак або вторгнень до мережі банку в межах процесу управління інцидентами? Якщо так, то зазначити перелік критеріїв, визначених банком, для віднесення таких атак або вторгнень до інцидентів інформаційної безпеки (кібербезпеки)	
30	Зазначити про кількість інцидентів інформаційної безпеки (кіберінцидентів), оброблення яких здійснено в межах процесу управління інцидентами, упродовж звітного періоду. Яка кількість з таких інцидентів мала безпосередній або опосередкований вплив на функціонування критичних бізнес-процесів банку? Яка кількість стосувалася уражень інформаційних систем банку зловмисним кодом?	
31	Чи здійснював банк оцінювання величини негативного впливу інцидентів інформаційної безпеки (кіберінцидентів) на діяльність банку? Якщо так, то стисло описати процедуру такого оцінювання із посиланням на відповідні внутрішні документи банку (назви, реквізити таких документів)	
32	Чи наявні в штаті банку аудитори, що мають підтверджені кваліфікації у сфері інформаційних технологій або інформаційної безпеки? Якщо так, то зазначити кількість таких працівників та документи, що підтверджують їх кваліфікацію	
33	Чи здійснювалися протягом звітного періоду внутрішні аудити, об’єктом яких були процеси управління ризиками інформаційної безпеки/кібербезпеки банку? Якщо так, то зазначити перелік таких аудитів (тема, дата, період, об’єкт аудиту) і ступінь виконання	

1	2	3
	заходів та/або рекомендацій за результатами здійснених таких аудитів на дату заповнення цього Звіту	
34	Чи здійснювалися протягом звітного періоду зовнішні аудити, об’єктом яких були процеси управління ризиками інформаційної безпеки/кібербезпеки та/або СУІБ банку? Якщо так, то зазначити перелік таких аудитів (тема, дата, період, об’єкт аудиту) і ступінь виконання заходів та/або рекомендацій за результатами здійснених таких аудитів на дату заповнення цього Звіту	
35	Дата останньої перевірки ефективності заходів щодо захисту периметра мережі банку шляхом виконання тесту на проникнення. Коротко описати процедуру здійснення такого тесту (методика, об’єкти, технічні засоби)	
36	Яка ступінь виконання Плану заходів відповідно до пункту 23 розділу ІІ цього Положення (за наявності) на дату заповнення цього Звіту?	
37	Чи охоплює контрольна діяльність, що здійснюється банком у межах функціонування системи внутрішнього контролю, питання контролю за інформаційною безпекою та обміном інформацією? Якщо так, то зазначити 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	