ПРОЕКТ

Правління Національного банку України

П О С Т А Н О В А

_____ м. Київ № _____

Про затвердження Змін
до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України

Відповідно до статей 7, 15, 55 та 56 Закону України "Про Національний банк України", статей 66, 71 Закону України "Про банки і банківську діяльність", підпункту 6 частини 2 статті 8 Закону України "Про основні засади забезпечення кібербезпеки України" та з метою приведення у відповідність до нормативно-правових актів Національного банку України з питань інформаційної безпеки процесу проведення планових та позапланових перевірок стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України, стану впровадження/функціонування систем управління інформаційною безпекою та повноти виконання банками в Україні заходів безпеки інформації, установлених нормативно-правовими актами Національного банку України, Правління Національного банку України **постановляє:**

1. Затвердити Зміни до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України, затвердженого постановою Правління Національного банку України від 26 листопада 2015 року № 829, що додаються.

2. Департаменту безпеки (Скомаровський О. А.) після офіційного опублікування довести до відома банків в Україні інформацію про прийняття цієї постанови для використання в роботі.

3. Контроль за виконанням цієї постанови покласти на першого заступника Голови Національного банку України Смолія Я. В.

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

В. о. Голови
Національного банку України Я. В. Смолій

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України

Зміни до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України

1. У розділі І:

1) пункт 1 після слова “системах” доповнити словами “, “Про основні засади забезпечення кібербезпеки України”;

2) пункти 2 − 5 викласти в такій редакції:

“2. У цьому Положенні терміни та скорочення вживаються в значеннях, визначених Положенням про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженим постановою Правління Національного банку від 26 листопада 2015 року № 829 (зі змінами) (далі – Положення № 829), Положенням про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженим постановою Правління Національного банку України від 28 вересня 2017 року № 95 (далі – Положення № 95), Інструкцією про міжбанківський переказ коштів в Україні в національній валюті, затвердженою постановою Правління Національного банку України від 16 серпня 2006 року № 320, зареєстрованою в Міністерстві юстиції України 06 вересня 2006 року за № 1035/12909 (зі змінами), Положенням про організацію внутрішнього контролю в банках України, затвердженим постановою Правління Національного банку України від 29 грудня 2014 року № 867.

3. Це Положення регламентує здійснення контролю:

1) стану інформаційної безпеки в організаціях, які отримали ЗЗІ відповідно до Положення № 829;

2) стану впровадження/функціонування системи управління інформаційною безпекою (далі − СУІБ) у банках;

3) повноти виконання банками заходів безпеки інформації, установлених Положенням № 95.

4. Національний банк здійснює контроль за дотриманням організаціями вимог інформаційної безпеки, установлених Правилами організації захисту електронних банківських документів з використанням засобів захисту

інформації Національного банку України, затвердженими постановою Правління Національного банку України від 26 листопада 2015 року № 829 (далі – Правила), Положенням № 829 та Положенням № 95.

5. Національний банк здійснює контроль за станом інформаційної безпеки в організаціях шляхом:

1) аналізу результатів внутрішнього/зовнішнього аудиту, внутрішніх документів, результатів інспекційних перевірок чи безвиїзного нагляду або інших документів про діяльність об’єкта перевірки;

2) здійснення виїзних перевірок (далі – перевірки).”;

3) пункт 6 після слів “надання інформації та” доповнити словом “внутрішніх”;

4) пункт 7 викласти в такій редакції:

“7. Організація зобов’язана надавати Національному банку повну та достовірну інформацію, внутрішні документи та їх копії належної якості у встановлені строки у визначених у відповідному запиті порядку та форматі.”.

2. У розділі ІІ:

1) у назві розділу ІІ слова “Контроль за станом” замінити словами “Перевірка стану”;

2) пункт 9 викласти в такій редакції:

“9. Працівники Національного банку, які здійснюють перевірку, зобов’язані мати документи, що підтверджують їх особу, і розпорядчий акт Національного банку про проведення перевірки.”;

3) пункт 10 виключити;

4) пункти 11, 12 викласти в такій редакції:

“11. Працівники Національного банку, які здійснюють перевірку, мають право:

1) запитувати та отримувати для перевірки внутрішні документи організації (уключаючи результати внутрішнього/зовнішнього аудиту), що дають змогу проконтролювати виконання вимог щодо інформаційної безпеки;

2) відвідувати приміщення організації, уключаючи приміщення з обмеженим доступом;

3) відвідувати робочі місця працівників організації;

4) здійснювати перевірку повноти впровадження заходів безпеки інформації, визначених у Положенні № 95, методами опитування, вивчення та тестування.

12. Національний банк проводить планові і позапланові перевірки.

До плану включаються перевірки організацій, перелік яких визначається Національним банком на підставі ризик-орієнтованого підходу до забезпечення інформаційної безпеки.

Підставами для проведення позапланових перевірок є:

1) включення організації в СЕП та/або інформаційні задачі;

2) перехід банку на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку на іншу;

3) зміна місцезнаходження організації;

4) усунення недоліків, виявлених під час попередньої перевірки;

5) ненадання організацією інформації, внутрішніх документів або їх копій за письмовим запитом Національного банку в установлені строки або надання організацією недостовірної інформації, внутрішніх документів або їх копій за письмовим запитом Національного банку;

6) наявність відомостей, що можуть свідчити про невиконання організацією вимог нормативно-правових актів Національного банку у сфері інформаційної безпеки.”.

3. У розділі ІІІ:

1) пункт 15 викласти в такій редакції:

“15. Національний банк перевіряє готовність організації до включення в СЕП та інформаційні задачі після упровадження організацією заходів щодо організації захисту електронної банківської інформації відповідно до вимог Правил та заходів безпеки інформації відповідно до вимог Положення № 95 (для банків).”;

2) пункти 17, 18 викласти в такій редакції:

“17. Під час перевірки визначається повнота дотримання організацією вимог Правил та Положення № 95 (для банків), які є актуальними на момент проведення перевірки.

18. За результатами перевірки складається довідка про стан інформаційної безпеки в організації.”.

4. У тексті Положення слова “Департамент інформаційної безпеки” у всіх відмінках замінити словами “Національний банк” у відповідних відмінках.

Директор
Департаменту безпеки О. А. Скомаровський

ПОГОДЖЕНО
Перший заступник Голови
Національного банку України
_____ Я. В. Смолій
(підпис)

“____” _____ 2017 року
(дата)