



Правління Національного банку України
ПОСТАНОВА

м. Київ

№ _____

Про внесення 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 та 56 Закону України “Про Національний банк України”, статті 66 Закону України “Про банки і банківську діяльність”, з метою оптимізації процесу здійснення контролю за використанням засобів захисту інформації Національного банку України й удосконалення нормативно-правових актів Національного банку України Правління Національного банку України **постановляє:**

1. Унести 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, виклавши його в новій редакції, що додається.

2. Департаменту безпеки (Скомаровський О. А.) після офіційного опублікування довести до відома банків України та інших установ, які використовують засоби захисту інформації Національного банку України, інформацію про прийняття цієї постанови.

3. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Смолія Я. В.

4. Постанова набирає чинності з 31 березня 2019 року.

Голова

Я. В. Смолій

ЗАТВЕРДЖЕНО

Постанова Правління

Національного банку України

26 листопада 2015 року № 829

(у редакції постанови Правління

Національного банку України

)

Положення

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

І. Загальні положення

1. Це Положення розроблено відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статті 66 Закону України “Про банки і банківську діяльність”, Законів України “Про платіжні системи та переказ коштів в Україні”, “Про захист інформації в інформаційно-телекомунікаційних системах” і нормативно-правових актів Національного банку України (далі – Національний банк) у сфері інформаційної безпеки.

2. Терміни та скорочення в цьому Положенні вживаються в значеннях, визначених Положенням про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженим постановою Правління Національного банку України від 26 листопада 2015 року № 829 (зі змінами), 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 № 829), 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).

3. Це Положення регламентує порядок здійснення контролю за виконанням організаціями вимог щодо використання ЗЗІ, установлених Правилами № 829.

4. Національний банк здійснює контроль за використанням організаціями ЗЗІ (далі – контроль) шляхом:

- 1) аналізу інформації, документів, звітів, отриманих від організацій;
- 2) здійснення виїзних перевірок.

5. Національний банк має право вимагати від організації надання інформації для здійснення контролю шляхом направлення запиту.

Керівник організації зобов'язаний забезпечити надання на запит Національного банку письмових пояснень, достовірної інформації, документів у визначених у запиті форматі, структурі, обсягах та в установленій у запиті строк.

6. Керівник організації зобов'язаний забезпечити періодичне (не рідше ніж один раз на рік) подання звіту щодо використання в організації ЗЗІ в установлені Національним банком строки та у визначених Національним банком порядку й форматі.

7. Національний банк забезпечує нерозголошення інформації, отриманої ним під час здійснення контролю, третім особам, за винятком випадків, передбачених законодавством України.

II. Порядок здійснення виїзних перевірок

8. Національний банк має право здійснювати виїзні перевірки виконання організаціями вимог, установлених Правилами № 829 (далі – перевірки).

Підставами для проведення перевірок є:

- 1) уключення організації в СЕП та/або інформаційних задач Національного банку;
- 2) зміна місцезнаходження організації або зміна адреси розташування ЗЗІ;
- 3) ненадання організацією інформації або надання недостовірної та/або неповної інформації у звітах щодо використання ЗЗІ та/або за запитом Національного банку. Під час проведення перевірки з'ясовуються лише ті питання, необхідність у перевірці яких стала підставою для її здійснення;
- 4) ненадання організацією інформації або надання недостовірної та/або неповної інформації про вжиття заходів щодо усунення недоліків, порушень, виявлених під час здійснення перевірки.

9. Працівники Національного банку, уповноважені на здійснення перевірки, зобов'язані мати документи, що підтверджують їх особу, та документ, на підставі якого здійснюється перевірка.

10. Перевірка здійснюється в присутності адміністратора інформаційної безпеки та/або посадової особи, призначеної керівником організації.

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

1) ознайомлюватися з журналами (ПМГК, обліку ЗЗІ, приймання-передавання ЗЗІ) та внутрішніми документами організації, що підтверджують виконання вимог Правил № 829;

2) відвідувати приміщення організації, де використовуються та зберігаються ЗЗІ, вивчати умови використання і зберігання ЗЗІ;

3) відвідувати робочі місця працівників організації, які використовують ЗЗІ;

4) перевіряти налаштування АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку.

12. Працівники Національного банку, уповноважені на здійснення перевірки, за результатами перевірки складають довідку про перевірку. Така довідка має містити описову частину, висновки, виявлені порушення, недоліки та строки їх усунення. Довідка також може містити іншу інформацію та рекомендації для організації.

13. Довідка про перевірку складається у двох примірниках за підписом працівників Національного банку, уповноважених на здійснення перевірки, та керівника організації. Один примірник довідки зберігається в Національному банку, другий – в організації.

14. Керівник організації в разі наявності заперечень щодо висновків, викладених у довідці про перевірку, має право надати обґрунтовані письмові заперечення (пояснення) із документальним підтвердженням (у разі їх наявності), які є невід'ємною частиною довідки про перевірку. У такому випадку довідка про перевірку доповнюється відміткою "із запереченнями (поясненнями)".

15. Організація в установлені у довідці про перевірку строки надає до Національного банку інформацію про вжиття заходів щодо усунення недоліків, порушень, виявлених під час здійснення перевірки.

Ш. Виїзна перевірка готовності організації до включення в СЕП та/або інформаційні задачі Національного банку

16. Національний банк перевіряє готовність організації до включення в СЕП та/або інформаційні задачі після впровадження організацією заходів відповідно до вимог Правил № 829.

17. Працівники Національного банку, уповноважені на здійснення перевірки готовності організації до включення в СЕП та/або інформаційні задачі, перевіряють:

1) наявність технічних можливостей для організації робочих місць відповідальних осіб згідно з вимогами Правил № 829;

2) наявність відповідальних осіб за зберігання та використання засобів захисту інформації Національного банку, внутрішніх документів організації про їх призначення та підписаних ними зобов'язань відповідно до вимог Правил № 829.

Директор Департаменту безпеки

О. А. Скомаровський