Офіційно опубліковано 20.02.2019

Правління Національного банку України

П О С Т А Н О В А

13 лютого 2019 року м. Київ № 38

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, 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 (Олександр Скомаровський) 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 Якова Смолія.

4. Постанова набирає чинності з 31 березня 2019 року.

Голова Яків СМОЛІЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
26 листопада 2015 року № 829
(у редакції постанови Правління
Національного банку України
від 13 лютого 2019 року №38)

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

I. 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 у сфері інформаційної безпеки.

2. Терміни та скорочення в цьому Положенні вживаються в значеннях, визначених Законом України "Про електронні довірчі послуги", 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) (далі – Положення про захист), 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 (у редакції постанови Правління Національного банку України від 05 жовтня 2018 року № 106) (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 України (далі – 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 достовірної інформації у вигляді письмових пояснень, документів в електронній (уключаючи електронний журнал ПМГК) та/або паперовій формі у строк, в обсязі, за форматом та за структурою, що визначені в такому запиті.

6. Керівник організації зобов'язаний забезпечити подання звіту щодо використання ЗЗІ (далі – Звіт) згідно з додатком до цього Положення.

Звіт подається організаціями до Національного банку один раз на рік протягом одного місяця, наступного за звітним періодом (рік), у паперовій або електронній формі. У разі подання Звіту в паперовій формі такий Звіт засвідчується власноручним підписом керівника організації. Подання Звіту в електронній формі здійснюється у форматі pdf із кваліфікованим електронним підписом керівника організації і такий Звіт надсилається засобами електронної пошти Національного банку.

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 інформаційні задачі Національного банку;

2) зміна місцезнаходження організації або зміна адреси розташування ЗЗІ, які організація отримала відповідно до Положення про захист;

3) ненадання організацією інформації або надання недостовірної та/або неповної інформації у Звіті 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. Перевірка повинна здійснюватися у строк, що не перевищує трьох робочих днів.

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

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

12. 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 їх використання і зберігання;

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

4) перевіряти налаштування АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК на відповідність експлуатаційній документації, вимогам і рекомендаціям Національного банку.

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

14. Довідка 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.

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

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

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

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

18. Працівники Національного банку, уповноважені на здійснення перевірки готовності організації до включення в СЕП та/або інформаційні задачі Національного банку, 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 Олександр СКОМАРОВСЬКИЙ

Додаток
до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України
(пункт 6 розділу I)

Звіт
щодо використання ЗЗІ

_____
(найменування організації)

за 20 ___ рік

№ з/п	Зміст запитання	Відповідь на запитання
1	2	3
1	Чи призначені відповідальні особи відповідно до пункту 4 розділу II Правил № 829 (так чи ні)? Якщо ні, зазначити причину	
2	Назва, дата (число, місяць, рік) та номер діючого внутрішнього документа (документів) про покладання/звільнення від виконання обов'язків адміністраторів інформаційної безпеки, адміністраторів АРМ-СЕП, адміністраторів АРМ-НБУ-інф, операторів АРМ бухгалтера САБ	
3	Інформація про місцезнаходження ПМГК, АРМ ПМГК (адреса розташування, номер приміщення)	
4	Чи є робочі місця відповідальних осіб, які розташовані за іншою адресою, ніж зазначена в колонці 2 рядка 3 Звіту (так чи ні)? Якщо так, додати до Звіту опис процедури генерації ключових пар (ТК та ВК) такими відповідальними особами	
5	Чи взяті та оформлені всіма відповідальними особами зобов'язання відповідно до пункту 7 розділу II та додатка до Правил № 829 (так чи ні)? Якщо ні, зазначити причину	
6	Чи є призначення або повноваження відповідальних осіб, заборонені пунктом 9 розділу II Правил № 829	

1	2	3
	(так чи ні)? Якщо так, зазначити, які саме є призначення або повноваження та причину їх наявності	
7	Чи виконує адміністратор інформаційної безпеки в повному обсязі обов'язки, визначені в пункті 10 розділу III, пунктах 25, 36, 40 розділу V Правил № 829 (так чи ні)? Якщо ні, зазначити перелік обов'язків, що не виконує адміністратор інформаційної безпеки, та причини їх невиконання	
8	Чи здійснюють відповідальні особи особисто генерацію ключових пар (ТК та ВК) (так чи ні)? Якщо ні, зазначити причину	
9	Чи здійснюють відповідальні особи контроль за строком дії власних ТК (так чи ні)? Якщо ні, зазначити причину	
10	Чи є внутрішній порядок зберігання ТК відповідно до пункту 33 розділу V Правил № 829 (так чи ні)? Якщо так, зазначити назву та реквізити такого документа. Якщо ні, зазначити причину	
11	Чи ознайомлені відповідальні особи з внутрішнім порядком зберігання ТК (так чи ні)? Якщо ні, зазначити причину	
12	Чи забезпечено налаштування комп'ютера з АРМ-СЕП відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку[1] (так чи ні)? Якщо ні, зазначити причину	
13	Чи забезпечено налаштування комп'ютера з АРМ-НБУ-інф відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку (так чи ні)? Якщо ні, зазначити причину	
14	Чи забезпечено дотримання порядку доступу відповідальних осіб до ЗІ відповідно до пункту 13 розділу III Правил № 829 (так чи ні). Якщо ні, зазначити причину	
15	Кількість випадків заміни АКЗІ та/або СК за звітний період[1], зазначити причину заміни	
16	Кількість випадків заміни ПМГК за звітний період, зазначити причину заміни	
17	Кількість випадків компрометації ТК за звітний період	
18	Кількість сеансів генерацій ключових пар (ТК та ВК) за звітний період (за кожним ПМГК окремо)	
19	Кількість ТК (на останній робочий день звітного періоду), що використовуються в організації:	

1	2	3
20	усього	
21	оператора АРМ Бухгалтера[1]	
22	технолога САБ[1]	
23	операціоніста САБ[1]	
24	Інформація про САБ організації[1] (назва, версія, розробник)	
25	Чи є в організації архів ВК операціоністів САБ[1] (так чи ні)? Якщо ні, зазначити причину	
26	Чи є в організації архів журналу ПМГК (так чи ні)? Якщо ні, зазначити причину	
27	Чи забезпечено розміщення АРМ ПМГК, АРМ-СЕП, АРМ-НБУ-інф та АРМ бухгалтера САБ відповідно до пунктів 43, 45 розділу VII Правил № 829 (так чи ні)? Якщо ні, зазначити причину	
28	Чи є внутрішній документ про призначення працівників, які мають доступ до приміщень з АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК відповідно до пункту 48 розділу VII Правил № 829 (так чи ні)? Якщо так, зазначити назву та реквізити такого документа. Якщо ні, зазначити причину	
29	Інформація про місцезнаходження АРМ-СЕП, АКЗІ, АРМ-НБУ-інф (адреса розташування, номер приміщення)	

“___” _____ 20__ року Керівник організації _____ _____
(підпис) (ініціали, прізвище)

[1]Заповнює лише учасник СЕП.