Офіційно опубліковано 12.10.2018

Правління Національного банку України

П О С Т А Н О В А

05 жовтня 2018 року м. Київ № 106

Про внесення змін
до Правил організації захисту електронних
банківських документів з використанням засобів
захисту інформації Національного банку України

Відповідно до статей 7, 15 та 56 Закону України “Про Національний банк України”, з метою вдосконалення процесів використання засобів захисту інформації Національного банку України Правління Національного банку України **постановляє:**

1. Унести зміни до Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджених постановою Правління Національного банку України від 26 листопада 2015 року № 829 (далі – Правила), виклавши їх у 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

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
26 листопада 2015 року № 829
(у редакції постанови Правління
Національного банку України
від 05 жовтня 2018 року № 106)

Правила
організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України

І. Загальні положення

1. Ці Правила розроблені відповідно до статей 7, 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. У цих Правилах терміни та скорочення вживаються в такому значенні:

1) АРМ ПМГК – автоматизоване робоче місце організації, на якому виконується управління ключовими даними засобами ПМГК;

2) електронний журнал ПМГК (далі – журнал ПМГК) – захищений від модифікації протокол роботи АРМ ПМГК, у якому фіксуються із зазначенням дати та часу всі події управління ключовими даними організації;

3) захищений носій ТК – пристрій, призначений для зберігання ТК, який має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу та від безпосереднього ознайомлення із значенням параметрів ТК.

Інші терміни та скорочення, що вживаються в цих Правилах, використовуються 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), 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) (далі – Інструкція про міжбанківський переказ коштів).

3. Ці Правила регламентують порядок зберігання, використання та обліку ЗЗІ організаціями, які отримали ці ЗЗІ відповідно до Положення про захист. Національний банк України (далі – Національний банк) має право здійснювати перевірку виконання організаціями вимог цих Правил.

ІІ. Призначення відповідальних осіб за роботу із ЗЗІ

4. Організація зобов'язана призначити внутрішнім документом відповідальних осіб за зберігання та використання ЗЗІ (далі – відповідальна особа) з урахуванням особливостей діяльності організації:

1) адміністратора інформаційної безпеки;

2) адміністратора АРМ-СЕП;

3) адміністратора АРМ-НБУ-інф;

4) оператора АРМ бухгалтера САБ;

5) технолога САБ;

6) операціоніста САБ;

7) операторів робочих і технологічних місць САБ та інформаційних задач.

Організація має право призначати осіб, які виконуватимуть обов'язки відповідальних осіб у разі їх відсутності.

Призначення відповідальних осіб в АРМ-СЕП та САБ стосується тільки безпосередніх учасників СЕП.

5. Внутрішній документ організації про призначення відповідальних осіб має містити посаду, ініціали, прізвище працівника, назву ЗЗІ, тип ТК з ідентифікатором ключа.

Організація зобов'язана забезпечувати актуальність внутрішніх документів про призначення відповідальних осіб.

6. Керівник організації зобов'язаний забезпечити подання до Національного банку копії документа або виписки з нього в електронній або

паперовій формі про покладання/звільнення від виконання відповідних обов'язків адміністраторів інформаційної безпеки, адміністраторів АРМ-СЕП, адміністраторів АРМ-НБУ-інф, операторів АРМ бухгалтера САБ протягом трьох робочих днів із дня, наступного за днем їх покладання/звільнення від виконання.

7. Відповідальні особи зобов'язані підписати зобов'язання, яке є додатком до цих Правил (далі – Зобов'язання).

8. Адміністратор інформаційної безпеки зобов'язаний забезпечити генерацію ключової пари (ТК та ВК) відповідальній особі за наявності:

1) внутрішнього документа організації про призначення відповідальної особи;

2) підписаного працівником Зобов'язання.

9. Відповідальною особою заборонено призначати:

1) адміністратора інформаційної безпеки – за зберігання та використання будь-якого ТК;

2) адміністратора АРМ-СЕП – за зберігання та використання ТК оператора АРМ бухгалтера САБ;

3) операціоніста САБ – за зберігання та використання ТК оператора АРМ бухгалтера САБ та/або ТК технолога САБ.

Адміністратор інформаційної безпеки та адміністратор АРМ-СЕП не можуть бути уповноваженими за розроблення або супроводження (адміністрування) САБ.

III. Обов'язки відповідальних осіб

10. Адміністратор інформаційної безпеки зобов'язаний:

1) вести облік ЗЗІ під час отримання, заміни та повернення ЗЗІ до Національного банку в журналі обліку ЗЗІ, який повинен містити відомості про назву ЗЗІ та його заводський номер, дату отримання/повернення ЗЗІ, прізвище, ініціали особи, яка отримала ЗЗІ (дата, підпис), відмітку про повернення ЗЗІ (дата, підпис);

2) забезпечувати зберігання ЗЗІ та журналу обліку ЗЗІ;

3) здійснювати тестування ПМГК;

4) забезпечувати технологічну дисципліну під час роботи АРМ ПМГК;

5) забезпечувати налаштування комп'ютера з АРМ ПМГК відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку;

6) забезпечувати умови генерації ключових пар (ТК та ВК) на АРМ ПМГК для відповідальних осіб;

7) забезпечувати відправлення на сертифікацію до Національного банку ВК, що потребують сертифікації;

8) здійснювати резервне копіювання електронного журналу ПМГК у встановленому порядку;

9) здійснювати передавання ВК операціоністів САБ до архіву організації в установленому порядку;

10) здійснювати контроль за налаштуванням АРМ-СЕП, АРМ-НБУ-інф відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку;

11) здійснювати контроль за дотриманням відповідальними особами цих Правил, внутрішнього порядку зберігання ТК;

12) здійснювати підтримку актуальності ключових даних організації;

13) інформувати керівника організації про загрози і випадки компрометації ЗЗІ та про вихід ЗЗІ з ладу.

11. Адміністратор АРМ-СЕП, адміністратор АРМ-НБУ-інф, оператор АРМ бухгалтера САБ, операціоніст САБ, технолог САБ, оператор робочого, технологічного місця САБ, оператор інформаційної задачі, зобов'язані:

1) забезпечувати технологічну дисципліну в роботі з програмним забезпеченням робочого місця;

2) особисто здійснювати генерацію ключової пари (ТК та ВК) (з урахуванням часу на сертифікацію) і знищення ТК (копій – за наявністю);

3) здійснювати контроль за строком дії власного ТК;

4) виконувати правила використання і зберігання ЗЗІ;

5) зберігати ТК у неробочий час і в робочий час, якщо вони не використовуються в роботі, у спосіб, який виключає можливість несанкціонованого доступу до ТК;

6) інформувати адміністратора інформаційної безпеки про загрози і випадки компрометації ЗЗІ та про вихід ЗЗІ з ладу.

12. Адміністратор АРМ-СЕП, адміністратор АРМ-НБУ-інф зобов’язані:

1) забезпечувати налаштування комп’ютера з АРМ-СЕП, комп’ютера з АРМ-НБУ-інф відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку;

2) у разі передавання ЗЗІ між собою вести журнали приймання-передавання ЗЗІ адміністраторів відповідних АРМів (далі – журнал приймання-передавання ЗЗІ), що повинен містити відомості про назву ЗЗІ та його заводський номер, дату отримання/повернення ЗЗІ, прізвище, ініціали особи, що отримала ЗЗІ (дата, підпис), відмітку про повернення ЗЗІ (дата, підпис).

13. Організація зобов’язана дотримуватися такого порядку допуску відповідальних осіб до ЗЗІ:

1) допуск до роботи з ПМГК має адміністратор інформаційної безпеки;

2) допуск до роботи з АКЗІ, СК, ТК АРМ-СЕП має адміністратор АРМ-СЕП;

3) допуск до роботи з ТК АРМ-НБУ-інф має адміністратор АРМ-НБУ-інф;

4) допуск до роботи з ТК робочих і технологічних місць САБ та інформаційних задач має відповідальна особа і тільки до власного ТК;

5) відповідальні особи виконують генерацію ключової пари (ТК та ВК) за допомогою ПМГК в присутності адміністратора інформаційної безпеки;

6) адміністратор інформаційної безпеки виконує функції контролю на АРМ-СЕП, АРМ-НБУ-інф у присутності адміністратора АРМ-СЕП, адміністратора АРМ-НБУ-інф.

IV. Порядок роботи з АКЗІ

14. Вимоги цього розділу поширюються тільки на організації, які є безпосередніми учасниками СЕП.

15. Адміністратор інформаційної безпеки зобов’язаний після отримання АКЗІ та СК зробити відповідний запис у журналі обліку ЗЗІ.

16. Адміністратор інформаційної безпеки зобов’язаний передати АКЗІ адміністратору АРМ-СЕП і зробити запис у журналі обліку ЗЗІ.

Адміністратор АРМ-СЕП зобов’язаний отримати АКЗІ.

Адміністратор АРМ-СЕП зобов’язаний установити АКЗІ та забезпечити постійне її підключення до комп’ютера, на якому функціонує програмно-апаратний комплекс АРМ-СЕП.

17. Адміністратор АРМ-СЕП зобов’язаний перед уведенням АКЗІ в роботу забезпечити виконання всіх вимог до технічних умов експлуатації АКЗІ, які наведені в документації на неї.

18. Адміністратор АРМ-СЕП зобов’язаний згенерувати ключову пару (ТК та ВК) для АКЗІ за допомогою програмно-технічного комплексу АРМ-СЕП для введення АКЗІ в експлуатацію і записати копію ТК АКЗІ на другу (резервну) СК під час генерації ключових пар (ТК та ВК).

Адміністратор АРМ-СЕП надсилає ВК АКЗІ на сертифікацію до Національного банку та уводить АКЗІ в експлуатацію після отримання сертифіката ВК та здійснення відповідних налаштувань АРМ-СЕП.

Адміністратор АРМ-СЕП зобов’язаний здійснювати своєчасну генерацію ключової пари (ТК та ВК) для АКЗІ у зв’язку із закінченням строку дії ТК.

19. Адміністратори АРМ-СЕП зобов’язані передавати АКЗІ і СК між собою із унесенням запису до журналу приймання-передавання ЗЗІ. Адміністратори АРМ-СЕП під час передавання ЗЗІ та після закінчення роботи мають право не відключати АКЗІ від комп’ютера.

Адміністратор АРМ-СЕП зобов’язаний зберігати СК у неробочий час і в робочий час, якщо вони не використовуються в роботі, у спосіб, який виключає можливість несанкціонованого доступу до СК.

20. Адміністратор АРМ-СЕП зобов’язаний здійснити заміну АКЗІ разом із СК у разі виходу з ладу АКЗІ під час експлуатації, пошкодження АКЗІ або голографічної наклейки, втрати АКЗІ, на вимогу Національного банку.

Адміністратор АРМ-СЕП організації зобов’язаний:

1) повідомити адміністратора інформаційної безпеки про причину виходу з ладу АКЗІ та/або СК і узгодити заходи для заміни АКЗІ та/або СК;

2) діяти відповідно до Інструкції про міжбанківський переказ коштів.

21. Адміністратор інформаційної безпеки для заміни АКЗІ та/або СК зобов'язаний:

1) повідомити Національний банк протягом трьох робочих днів про перехід на використання програмних ЗЗІ АРМ-СЕП;

2) забезпечити доставку ЗЗІ (за винятком втрачених) до Національного банку;

3) зробити відмітку про повернення АКЗІ та/або СК, що виведені з експлуатації, у журналі обліку ЗЗІ;

4) провести відповідне службове розслідування в разі пошкодження АКЗІ, СК, голографічної наклейки, втрати АКЗІ або СК, висновки за результатами якого подати до Національного банку;

5) отримати ЗЗІ на заміну та зробити відповідний запис у журналі обліку ЗЗІ;

6) видати адміністратору АРМ-СЕП отримані ЗЗІ відповідно до пункту 16 розділу IV цих Правил;

7) повідомити Національний банк протягом трьох робочих днів про перехід на роботу з АКЗІ.

22. Адміністратор АРМ-СЕП зобов'язаний перейти на роботу з резервною СК у разі виходу з ладу СК.

V. Порядок роботи з ПМГК і ТК

23. Адміністратор інформаційної безпеки після отримання ПМГК зобов'язаний:

1) зробити відповідний запис у журналі обліку ЗЗІ;

2) здійснити заміну початкового пароля ПМГК;

3) здійснити перевірку функціонування ПМГК шляхом пробної генерації ключової пари (ТК та ВК).

24. Адміністратор інформаційної безпеки, якщо ПМГК не працює, зобов'язаний повідомити про це Національний банк.

25. Адміністратор інформаційної безпеки зобов’язаний зберігати ПМГК у неробочий час і в робочий час, якщо він не використовується в роботі, у спосіб, який виключає можливість несанкціонованого доступу до ПМГК.

26. Адміністратор інформаційної безпеки, якщо ПМГК не працює або ПМГК пошкоджений з вини персоналу організації, зобов’язаний:

1) повідомити Національний банк протягом трьох робочих днів про це;

2) замовити та отримати новий ПМГК відповідно до Положення про захист;

3) уживати заходів, що передбачені в пунктах 23 – 25 розділу V цих Правил.

27. Адміністратор інформаційної безпеки в разі втрати ПМГК або втрати контролю за місцезнаходженням ПМГК зобов’язаний:

1) повідомити Національний банк протягом одного робочого дня про такий випадок із зазначенням серійного номера втраченого ПМГК;

2) провести службове розслідування, висновки за результатами якого подати до Національного банку;

3) замовити та отримати новий ПМГК відповідно до Положення про захист;

4) уживати заходів, що передбачені в пунктах 23 – 25 розділу V цих Правил.

28. Організація зобов’язана забезпечити зміну паролів до ПМГК у разі звільнення відповідальної особи від обов’язків адміністратора інформаційної безпеки.

29. Відповідальна особа зобов’язана генерувати ключову пару (ТК та ВК) на АРМ ПМГК у присутності адміністратора інформаційної безпеки.

Усі спроби генерації ключової пари (ТК та ВК), у тому числі й невдалі, фіксуються в журналі ПМГК в автоматичному режимі.

ВК після їх генерації (за винятком ВК операціоністів САБ) підлягають обов’язковій сертифікації в Національному банку.

30. Організація зобов’язана використовувати лише захищені носії ТК. Національний банк має право встановлювати вимоги до захищених носіїв ТК, які використовуються організацією.

Національний банк надає відповідні криптобібліотеки підтримки носіїв ТК, рекомендації щодо налаштування доступу до ТК програмної частини системи захисту інформації.

31. Відповідальна особа має право створити копії ТК (за винятком ТК операціоністів САБ) для запобігання зупиненню роботи організації в СЕП та/або в інформаційних задачах у разі псування носія ТК за умови наявності документа організації, який визначає створення копій ТК та відповідальних за їх зберігання осіб.

На копії ТК поширюються всі вимоги щодо зберігання та використання, як і на основні ТК.

32. Відповідальна особа зобов'язана встановити пароль для носія ТК. Відповідальній особі заборонено розголошувати пароль та передавати носій ТК (крім випадків, якщо передбачено передавання ТК робочого місця іншій відповідальній особі).

33. Організація зобов'язана затвердити внутрішній порядок зберігання ТК залежно від конкретних умов її функціонування, забезпечивши дотримання вимог цих Правил.

Організація має право використовувати захищені носії ТК для розв'язання інших завдань організації (обмеження доступу до комп'ютерів, приміщень).

34. Адміністратор АРМ-СЕП, адміністратор АРМ-НБУ-інф зобов'язані передавати ТК відповідних АРМів (АРМ-СЕП, АРМ-НБУ-інф) (і за необхідності їх копії) між собою із здійсненням запису в журналі приймання-передавання ЗЗІ.

35. Організація зобов'язана вести архів ВК операціоністів САБ та архів журналу ПМГК протягом усього строку зберігання архівів електронних банківських документів.

36. Адміністратор інформаційної безпеки зобов'язаний забезпечувати своєчасну генерацію ключової пари (ТК та ВК) відповідальними особами і відправлення ВК на сертифікацію до Національного банку.

37. Відповідальна особа зобов'язана знищувати ТК (та їх копії) після закінчення строку дії.

ТК не вносяться до будь-якого архіву організації.

38. Відповідальна особа в разі компрометації ТК зобов'язана припинити використання такого ТК і повідомити про таку подію адміністратору інформаційної безпеки.

39. Адміністратор інформаційної безпеки в разі компрометації ТК зобов’язаний:

1) повідомити Національний банк системою електронної пошти Національного банку, у разі компрометації ТК АРМ-СЕП або АРМ бухгалтера САБ;

2) забезпечити вилучення відповідного ВК з ключових даних організації;

3) забезпечити генерацію нової ключової пари (ТК та ВК) і надалі вживати заходів щодо введення в дію ТК;

4) провести службове розслідування, висновки за результатами якого подати до Національного банку.

40. Адміністратор інформаційної безпеки зобов’язаний забезпечити вилучення з роботи відповідних ВК у встановленому порядку, якщо відповідальна особа, яка має ТК для будь-якого робочого місця, звільняється від виконання відповідних функціональних обов’язків.

VI. Порядок використання і зберігання ЗЗІ в разі виникнення надзвичайних ситуацій

41. Організація зобов’язана вжити заходів для усунення загрози втрати ЗЗІ в разі виникнення надзвичайної ситуації.

42. Організація має право визначити тимчасовий порядок використання та зберігання ЗЗІ (за попереднім узгодженням з Національним банком і дотриманням вимог цих Правил) у разі:

1) виникнення необхідності щодо здійснення діяльності в приміщенні іншої організації у разі виникненні аварійної ситуації (відключення електроживлення, пошкодження ліній зв’язку тощо);

2) переведення АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК в інше приміщення;

3) проведення ремонтних робіт.

У такому разі організація зобов’язана копію тимчасового порядку в паперовій або електронній формі надати Національному банку.

VII. Вимоги до розміщення та налаштування АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК

43. Організація зобов’язана розмістити АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК в окремих приміщеннях.

Організація має право розміщувати АРМ-СЕП та АРМ-НБУ-інф в одному приміщенні в разі суміщення обов’язків адміністратора АРМ-СЕП та адміністратора АРМ-НБУ-інф.

44. Організація зобов’язана виключити можливість несанкціонованого доступу до приміщень з АРМ-СЕП, АРМ-НБУ-інф та АРМ ПМГК.

45. Забороняється розміщувати АРМ-СЕП, АРМ бухгалтера САБ та АРМ ПМГК в одному приміщенні (у будь-яких комбінаціях).

46. Дозволяється розміщувати АРМ-СЕП, АРМ-НБУ-інф у серверному приміщенні, якщо такі програмно-апаратні комплекси працюють в автоматичному режимі.

У разі такого розміщення Адміністратор АРМ-СЕП зобов’язаний реагувати на інформаційні повідомлення, які надсилаються до АРМ-СЕП.

47. Дозволяється розміщувати АРМ-СЕП та АРМ-НБУ-інф на одному комп’ютері.

48. Організація зобов’язана внутрішнім документом призначити працівників, які мають допуск до приміщень з АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК.

49. Організація зобов’язана забезпечити налаштування АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК відповідно до експлуатаційної документації, вимог та рекомендацій Національного банку.

50. Організація зобов’язана повідомляти Національний банк про зміни свого місцезнаходження або зміни місцезнаходження АРМ-СЕП, АРМ-НБУ-інф, АРМ ПМГК протягом трьох робочих днів із наступного дня за датою настання таких змін.

Директор Департаменту безпеки О. А. Скомаровський

Додаток
до Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України
(у редакції постанови Правління Національного банку України
від 05 жовтня 2018 року № 106)
(пункт 7 розділу II)

Зобов’язання

Я, _____, який призначений
(посада, прізвище, ім’я, по батькові)

згідно з внутрішнім документом _____
(найменування організації)

від “___” _____ 20__ р. №___ відповідальною особою за зберігання та використання таких засобів захисту інформації Національного банку України

_____
(назва ЗЗІ, тип ТК з ідентифікатором ключа)

ознайомлений з 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), і зобов’язуюся:

1) виконувати вимоги Правил;

2) не передавати іншим особам носії ТК;

3) здійснювати контроль за строком дії власного ТК;

4) не розголошувати паролі входу до АРМів Національного банку, інших програмно-технічних комплексів, паролі до власних ТК та паролі до носіїв ТК;

5) у разі компрометації засобів захисту інформації Національного банку України або виникнення такої загрози негайно повідомляти про це адміністраторові інформаційної безпеки організації або керівникові організації;

6) у разі звільнення з роботи або звільнення від виконання відповідних обов’язків в організації, не пізніше останнього робочого дня або дня виконання обов’язків повернути адміністраторові інформаційної безпеки організації або

керівникові організації всі отримані засоби захисту інформації Національного банку України та забезпечити знищення власних ТК.

Я, _______,
(прізвище, ім’я, по батькові)

попереджений про те, що я є підписувачем електронних документів, на які накладений електронний підпис[1] з використанням мого ТК.

_____
(дата, підпис)

[1] Застосовується в значенні, наведеному в нормативно-правових актах Національного банку України, які визначають умови застосування електронного підпису в банківській системі України.