ПРАВЛІННЯ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

ПОСТАНОВА

26.11.2015 № 829

Про затвердження нормативно-правових актів з питань інформаційної безпеки

{Із змінами, внесеними згідно з Постановами Національного банку
№ 79 від 17.08.2017
№ 106 від 05.10.2018
№ 38 від 13.02.2019}

Відповідно до статей 7, 56 Закону України "Про Національний банк України", з метою врегулювання взаємовідносин між Національним банком України і банками України, їх філіями, державними, небанківськими установами, які використовують засоби захисту інформації Національного банку України, у зв'язку з унормуванням централізованого порядку укладання та ведення договорів щодо забезпечення засобами захисту інформації Національного банку України Правління Національного банку України **ПОСТАНОВЛЯЄ:**

1. Затвердити:

1) Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, що додається;

2) Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, що додаються;

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

2. Визнати такими, що втратили чинність:

постанову Правління Національного банку України від 02 квітня 2007 року № 112 "Про затвердження Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України", зареєстровану в Міністерстві юстиції України 24 квітня 2007 року за № 419/13686;

підпункт 2 пункту 1 постанови Правління Національного банку України від 07 липня 2015 року № 439 "Про внесення змін до деяких нормативно-правових актів Національного банку України".

3. Департаменту інформаційної безпеки (Лук'янов Д.О.) довести зміст цієї постанови до відома Центральної розрахункової палати Національного банку України, банків України, їх філій, органів Державної казначейської служби України, інших органів державної влади, небанківських установ, які

використовують засоби захисту інформації Національного банку України, для використання в роботі.

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

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

В.о. Голови **О.В. Писарук**

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку
України
26.11.2015 № 829

ПОЛОЖЕННЯ
про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України

{У тексті Положення слова "через територіальне управління" виключено; у тексті Положення та додатках до нього слова "Департамент інформаційної безпеки" у всіх відмінках замінено словами "Департамент безпеки" у відповідних відмінках згідно з Постановою Національного банку № 79 від 17.08.2017}

I. Загальні положення

1. Це Положення розроблено 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 (далі - Національний банк) у сфері інформаційної безпеки.

{Пункт 1 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

2. У тексті Положення терміни та скорочення вживаються в такому значенні:

1) адміністратор інформаційної безпеки - фахівець з питань інформаційної безпеки, призначений внутрішнім документом організації для забезпечення впровадження та підтримки роботи засобів захисту інформації Національного банку в цій організації;

{Підпункт 1 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

2) АКЗІ - апаратура криптографічного захисту інформації, яка є власністю Національного банку;

{Підпункт 2 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

3) АРМ бухгалтера САБ - автоматизоване робоче місце системи автоматизації банку, на якому здійснюється формування файлів/онлайнових пакетів, які містять початкові платежі системи електронних платежів Національного банку;

{Підпункт 3 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

4) АРМ-НБУ-інф - програмне забезпечення "Автоматизоване робоче місце обміну неплатіжною інформацією" Національного банку, призначене для обміну інформацією між системою автоматизації банку та інформаційними задачами;

{Підпункт 4 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

5) ВК - відкритий ключ;

6) ЕЦП - електронний цифровий підпис;

7) ЗЗІ - засоби захисту інформації Національного банку, які використовуються в системі електронних платежів Національного банку та інформаційних задачах;

{Підпункт 7 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

8) інформаційні задачі - програмно-технічні комплекси автоматизації банківської діяльності, які забезпечують оброблення та передавання інформації, що не належить до платіжної та технологічної інформації системи електронних платежів Національного банку, з використанням засобів захисту інформації Національного банку між банківськими та іншими установами і Національним банком;

{Підпункт 8 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

9) криптобібліотеки - бібліотеки криптографічних функцій - накладання та перевірки електронного цифрового підпису, шифрування та дешифрування інформації;

10) організація - банківська або інша установа, яка є безпосереднім учасником системи електронних платежів Національного банку та/або інформаційних задач і використовує засоби захисту інформації Національного банку;

{Підпункт 10 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

11) організація-замовник - банківська або інша установа, яка приєднується до Єдиного договору банківського обслуговування та надання інших послуг Національним банком України (далі - Єдиний договір) для отримання послуг Національного банку України із надання в користування засобів захисту інформації Національного банку;

{Підпункт 11 пункту 2 розділу I в редакції Постанови Національного банку № 79 від 17.08.2017}

12) ПМГК - програмний або програмно-апаратний модуль генерації ключів криптографічного захисту інформації, який є власністю Національного банку;

{Підпункт 12 пункту 2 розділу I в редакції Постанови Національного банку № 79 від 17.08.2017}

13) САБ - система автоматизації банку;

14) система захисту інформації - сукупність методів і засобів, що включає апаратно-програмні, програмні засоби захисту інформації Національного банку, ключову інформацію та систему розподілу ключової інформації, технологічні засоби контролю та організаційні заходи, які забезпечують захист електронних банківських документів;

{Підпункт 14 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

15) СЕП - система електронних платежів Національного банку;

{Підпункт 15 пункту 2 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

16) СК - смарт-картка;

17) сувора автентифікація - ідентифікація кожного користувача за ознакою володіння своїм секретним ключем;

18) ТВК - таблиця відкритих ключів;

19) ТК - таємний ключ.

Інші терміни та скорочення, що вживаються в цьому Положенні, використовуються в значеннях, визначених Законом України "Про електронні документи та електронний документообіг", стандартами з управління інформаційною безпекою в банківській системі України, затвердженими постановою Правління Національного банку України від 28 жовтня 2010 року № 474, 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 визначає принципи побудови системи захисту

інформації та порядок отримання і повернення ЗЗІ організаціями.

4. Безпосередні учасники СЕП отримують ЗЗІ для використання в СЕП та інформаційних задачах незалежно від моделі обслуговування консолідованого кореспондентського рахунку банку в СЕП. Опосередковані учасники СЕП та організації, які не є учасниками СЕП, отримують ЗЗІ для використання їх в інформаційних задачах Національного банку.

{Абзац перший пункту 4 розділу I із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

Організації взаємодіють за всіма поточними питаннями роботи із ЗЗІ з Департаментом безпеки Національного банку (далі - Департамент безпеки).

{Абзац другий пункту 4 розділу I в редакції Постанови Національного банку № 79 від 17.08.2017}

5. Організації, які використовують ЗЗІ, зобов'язані виконувати організаційні заходи інформаційної безпеки щодо використання, зберігання, обліку ЗЗІ згідно з Правилами організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженими постановою Правління Національного банку від 26 листопада 2015 року № 829 (далі - Правила).

6. Департамент безпеки здійснює перевірку дотримання вимог Правил в організаціях відповідно 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 від 26 листопада 2015 року № 829 (далі - Положення про порядок перевірки).

7. Організація зобов'язана узгоджувати з Департаментом безпеки питання, які можуть виникати під час роботи із ЗЗІ і які не передбачені Правилами.

8. Керівник організації забезпечує дотримання вимог щодо інформаційної безпеки в ній, визначених цим Положенням.

II. Принципи побудови системи захисту інформації

9. Система захисту інформації створена для забезпечення конфіденційності та цілісності інформації в електронній формі на будь-якому етапі її оброблення, а також суворої автентифікації учасників СЕП, учасників інформаційних задач і фахівців організацій, які беруть участь у підготовці й обробленні електронних документів.

10. Для забезпечення цілісності інформації, суворої автентифікації та безперервного захисту електронних банківських документів з часу їх формування система захисту інформації використовує механізми формування (перевірки) ЕЦП на базі асиметричних алгоритмів RSA та Національного стандарту України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих", затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002).

{Пункт 10 розділу II в редакції Постанови Національного банку № 79 від 17.08.2017}

11. Організація для забезпечення захисту інформації зобов'язана мати трибайтний унікальний ідентифікатор (далі - унікальний ідентифікатор).

{Пункт 11 розділу II в редакції Постанови Національного банку № 79 від 17.08.2017}

12. Організація забезпечує захист електронних банківських документів, шифрування/дешифрування і накладання/перевірку ЕЦП за допомогою таких криптографічних ЗЗІ:

1) апаратно-програмних ЗЗІ, до складу яких входять АКЗІ, СК, програмне забезпечення керування АКЗІ, що вбудоване в АРМ-СЕП і не може бути вилучене або використане окремо, з відповідними ТВК та криптобібліотеками;

2) програмних ЗЗІ, до складу яких входять програмний модуль для шифрування, вбудований в АРМ-СЕП, ПМГК з незаповненими ТВК, носіїв ТК, відповідними ТВК та криптобібліотеками.

13. Національний банк забезпечує побудову ключової системи криптографічного захисту для СЕП та інформаційних задач. Ця система складається з ключів програмних ЗЗІ, що генеруються в організаціях за допомогою наданих ПМГК, і ключів апаратних ЗЗІ, які генеруються

безпосередньо АРМ-СЕП за допомогою АКЗІ.

14. Основними ЗЗІ в АРМ-СЕП є АКЗІ.

Адміністратор АРМ-СЕП здійснює генерацію ключової пари (ТК та ВК) для АКЗІ на комп'ютері, де розміщується АРМ-СЕП, за допомогою програмного забезпечення керування АКЗІ, що вбудоване в АРМ-СЕП. Генерація здійснюється відповідно до алгоритму, визначеного в національному стандарті України ДСТУ 4145-2002. Для забезпечення безперебійної роботи АРМ-СЕП з апаратурою захисту адміністратор АРМ-СЕП повинен записувати ТК на дві СК (основну та резервну). Ключова інформація під час роботи АКЗІ використовується виключно на рівні АКЗІ, що унеможливлює підроблення та перехоплення ключової інформації.

У разі виходу з ладу АКЗІ адміністратор АРМ-СЕП здійснює перехід до роботи з програмними ЗЗІ.

15. За допомогою ПМГК організація має право генерувати ключову пару (ТК та ВК) відповідно до асиметричних алгоритмів RSA та ДСТУ 4145-2002 для всіх робочих місць, де працюють з електронними банківськими документами. Кожен ТК робочого місця захищений особистим паролем відповідальної особи, яка працює з цим ключем.

{Абзац перший пункту 15 розділу II із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

Для забезпечення захисту ключової інформації від несанкціонованої модифікації адміністратор інформаційної безпеки надсилає ВК до Департаменту безпеки для сертифікації (крім ВК для робочих місць операціоністів, що використовуються лише в САБ).

Департамент безпеки здійснює сертифікацію ВК та надсилає засобами системи електронної пошти Національного банку на адресу організації відповідні сертифікати ВК. Організація вживає заходів щодо своєчасного оновлення ТВК відповідно до експлуатаційної документації для АРМ-СЕП, АРМ-НБУ-інф, САБ та інформаційних задач.

16. Департамент безпеки надає криптобібліотеки безкоштовно всім організаціям, які використовують ЗЗІ, для вбудовування в програмне забезпечення САБ або інше відповідне програмне забезпечення.

17. В організації використовуються такі ЗЗІ:

№ з/п	Назва ЗЗІ	Кількість
1	АКЗІ (для безпосереднього учасника СЕП)	1
2	СК (для безпосереднього учасника СЕП)	2
3	ПМГК	1
4	Копія ПМГК	1
5	ТКАРМ-СЕП (для безпосереднього учасника СЕП)	1 + копія
6	ТК АРМ-НБУ-інф	1 + копія
7	ТК АРМ бухгалтера САБ (для безпосереднього учасника СЕП)	За кількістю відповідальних осіб, але не більше 5
8	ТК технолога (для безпосереднього учасника СЕП)	За кількістю відповідальних осіб, але не більше 5
9	ТК операціоністів (для безпосереднього учасника СЕП)	За кількістю відповідальних осіб
10	ТК інших робочих та технологічних місць для інформаційних задач	За вказівками Національного банку

18. Центральна розрахункова палата Національного банку надає консультації щодо супроводження АРМ-СЕП/АРМ-НБУ-інф, а також технологічного процесу проходження електронних платежів у СЕП та електронних документів в інформаційних задачах.

III. Порядок отримання і повернення ЗЗІ

19. Умовами для отримання ЗЗІ є:

1) приєднання організації-замовника до Єдиного договору для отримання таких видів послуг Національного банку:

розрахунково-інформаційного обслуговування в системі електронних платежів Національного банку (для учасників СЕП);

системою електронної пошти Національного банку (далі - система ЕП);

із надання в користування засобів захисту інформації Національного банку, крім випадків, якщо організацією-замовником є установи Державної казначейської служби України, Державна служба фінансового моніторингу України, Державна фіскальна служба України, Національне антикорупційне бюро України, Державна установа "Офіс адміністрування проектів міжнародного фінансового співробітництва", Державна іпотечна установа, Фонд гарантування вкладів фізичних осіб, Центральна виборча комісія (далі - державні установи). Для державних установ - укладення договору про використання засобів захисту інформації Національного банку між організацією-замовником та Національним банком та підключення до системи ЕП;

2) забезпечення відповідності приміщень, у яких будуть оброблятися електронні банківські документи, використовуються та зберігаються ЗЗІ, вимогам, визначеним Правилами;

3) призначення посадових осіб, відповідальних за зберігання та використання ЗЗІ;

4) лист-доручення (довіреність) про отримання конкретних ЗЗІ особі, відповідальній за отримання ЗЗІ для організації.

{Пункт 19 розділу III в редакції Постанови Національного банку № 79 від 17.08.2017}

19[1]. Організація подає до Департаменту безпеки лист про готовність до включення в СЕП та/або інформаційні задачі Національного банку та наказ про призначення посадових осіб, відповідальних за зберігання та використання ЗЗІ.

{Розділ III доповнено новим пунктом 19[1] згідно з Постановою Національного банку № 79 від 17.08.2017}

20. Департамент безпеки проводить перевірку готовності організації-замовника, її філій до включення в СЕП та інформаційні задачі відповідно до розділу III Положення про порядок перевірки.

21. Приєднання організації-замовника, крім державних установ, до Єдиного договору здійснюється відповідно до Публічної пропозиції Національного банку України на укладення Єдиного договору банківського обслуговування та надання інших послуг Національним банком України, розміщеної на сторінці офіційного Інтернет-представництва Національного банку. Державні установи та Національний банк укладають між собою договір про використання засобів захисту інформації Національного банку України відповідно до зразка, наведеного в додатку 1 до цього Положення.

Організація зобов'язана внести зміни до додатка 1 до Заяви про приєднання до Єдиного договору/договору в разі зміни адреси розташування ЗЗІ.

{Пункт 21 розділу III в редакції Постанови Національного банку № 79 від 17.08.2017}

22. Департамент безпеки в разі відсутності недоліків за результатами перевірки готовності включення організації в СЕП та/або інформаційні задачі виготовляє та надає ЗЗІ організації.";

{Пункт 22 розділу III в редакції Постанови Національного банку № 79 від 17.08.2017}

23. Відповідальна за отримання ЗЗІ особа організації зобов'язана прибути до Національного банку з документом, який засвідчує особу, та листом-дорученням або довіреністю, які надають право на отримання/заміну ЗЗІ, для отримання ЗЗІ з оформленням акта про приймання-передавання апаратних засобів захисту інформації Національного банку України (додаток

2).

{Пункт 23 розділу III із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

24. Департамент безпеки разом з документом на отримання/заміну ЗЗІ зберігає один примірник, а організація - другий примірник акта про приймання-передавання засобів захисту інформації Національного банку, за яким АКЗІ, смарт-картки та програмно-апаратний модуль генерації ключів криптографічного захисту інформації передаються в організацію. У разі використання ПМГК на гнучкому магнітному диску Департамент безпеки зберігає копію супровідного листа, а організація - супровідний лист, згідно з яким цей ПМГК передається в організацію.

{Абзац перший пункту 24 розділу III в редакції Постанови Національного банку № 79 від 17.08.2017}

Департамент інформаційних технологій Національного банку постачає криптобібліотеки, необхідні для роботи АРМ-СЕП і АРМ-НБУ-інф, разом з цими АРМ, у тому числі в разі їх оновлень - разом з оновленнями програмного забезпечення цих АРМ. Криптобібліотеки та програмний модуль криптографічного захисту інформації, вбудований в АРМ-СЕП, обліку і поверненню не підлягають.

Криптобібліотеки, призначені для вбудування в САБ або інше програмне забезпечення, постачаються за окремим листом Департаменту безпеки або за запитом від організації.

25. Для завершення підготовки до включення в СЕП організація зобов'язана виконати генерацію ключів для АРМ-СЕП та отримати їх сертифікати за один робочий день до включення до Довідника учасників СЕП.

26. Організація, яка отримала ЗЗІ, не має права:

передавати їх третім особам, установам чи організаціям, а також іншим установам однієї юридичної особи;

використовувати їх за іншим місцезнаходженням, ніж це зазначено в додатку 1 до Заяви про приєднання до Єдиного договору/договорі;

{Абзац третій пункту 26 розділу III із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

використовувати їх в інших платіжних системах банків, у територіально відокремлених відділеннях (філіях) банків.

27. Організація зобов'язана повернути ЗЗІ до Департаменту безпеки в разі:

1) ліквідації;

2) припинення роботи із ЗЗІ, а саме:

виключення з учасників СЕП та/або інформаційних задач Національного банку;

{Абзац другий підпункту 2 пункту 27 розділу III із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

переходу на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку банку на іншу;

{Абзац четвертий підпункту 2 пункту 27 розділу III виключено на підставі Постанови Національного банку № 79 від 17.08.2017}

3) виходу з ладу ЗЗІ;

4) на вимогу Департаменту безпеки в разі виявлення суттєвих порушень в організації захисту електронних банківських документів.

28. Організація зобов'язана повернути АКЗІ разом із СК та/або програмно-апаратний модуль генерації ключів до Департаменту безпеки в разі виходу АКЗІ та/або програмно-апаратного модуля генерації ключів з ладу або отримання від Департаменту безпеки листа з вимогою повернення ЗЗІ протягом трьох робочих днів з укладенням акта про приймання-передавання засобів захисту інформації Національного банку, один примірник якого зберігає Департамент безпеки, другий - організація.

{Пункт 28 розділу III в редакції Постанови Національного банку № 79 від 17.08.2017}

29. Організація у випадках, передбачених підпунктами 1 і 2 пункту 27, зобов'язана:

1) повідомити Департамент безпеки про передбачувані строки і порядок

виключення з учасників СЕП, переходу на іншу модель обслуговування консолідованого кореспондентського рахунку банку або зміни місцезнаходження, погодити перелік ЗЗІ, що підлягають поверненню до Департаменту безпеки;

2) ужити заходів щодо повернення до Департаменту безпеки, знищення на місці і передавання до архіву організації ЗЗІ, справ, журналів обліку зі складанням відповідного акта (додаток 3);

3) повернути до Департаменту безпеки ЗЗІ з актом, зазначеним у підпункті 2 цього пункту, один примірник якого зберігає Департамент безпеки, другий - організація.

30. Організація, яка використовує ЗЗІ, зобов'язана виконувати організаційні вимоги щодо їх отримання, використання та зберігання і своєчасної заміни відповідних ключів до них.

Департамент безпеки має право вилучати з організації ЗЗІ в разі невиконання вимог щодо використання та зберігання ЗЗІ і вимог до приміщень.

IV. Заходи інформаційної безпеки в СЕП

31. Технологічні засоби контролю, вбудовані в програмно-технічні комплекси СЕП, не можуть бути відключені. У разі виявлення нестандартної ситуації, яка може свідчити про підозру щодо несанкціонованого доступу до СЕП від імені певного учасника СЕП, ЦОСЕП автоматично припиняє приймання початкових електронних розрахункових документів та повідомлень від цього учасника.

32. Основним засобом шифрування файлів (пакетів) СЕП є АКЗІ. Робота АКЗІ контролюється вбудованими в ЦОСЕП і АРМ-СЕП програмними ЗЗІ і забезпечує апаратне шифрування (розшифрування) інформації за алгоритмом, визначеним у національному стандарті України ДСТУ ГОСТ 28147:2009.

Як резервний засіб шифрування в СЕП використовується вбудована в ЦОСЕП і АРМ-СЕП функція програмного шифрування.

33. Засоби шифрування ЦОСЕП і АРМ-СЕП (як АКЗІ, так і програмне шифрування) забезпечують сувору автентифікацію відправника та отримувача електронного банківського документа, цілісність кожного документа в результаті неможливості його підроблення або несанкціонованого модифікування в шифрованому вигляді.

АРМ-СЕП і ЦОСЕП у режимі реального часу забезпечують додаткову сувору взаємну автентифікацію під час установлення сеансу зв'язку.

Під час роботи АРМ-СЕП створює журнали програмного та апаратного шифрування і захищений від модифікації протокол роботи АРМ-СЕП, у якому фіксуються всі дії, що ним виконуються, із зазначенням дати та часу оброблення електронних банківських документів. Наприкінці банківського дня журнали програмного та апаратного шифрування і протокол роботи АРМ-СЕП підлягають обов'язковому збереженню в архіві.

34. Департамент безпеки надає банкам (філіям) інформаційні послуги щодо достовірності інформації за електронними банківськими документами в разі виникнення спорів на основі копії архіву роботи АРМ-СЕП за відповідний банківський день.

Департамент безпеки розшифровує копію цього архіву та визначає:

1) ідентифікатор банку - учасника СЕП, який надіслав (зашифрував) електронний банківський документ;

2) ідентифікатор банку - учасника СЕП, якому адресовано електронний банківський документ;

3) дату, годину та хвилину виконання шифрування електронного банківського документа;

4) дату, годину та хвилину розшифрування електронного банківського документа;

5) відповідність усіх електронних цифрових підписів, якими був захищений від модифікації електронний банківський документ.

Під час використання АКЗІ додатково визначаються:

1) номер АКЗІ, на якій виконувалося шифрування або розшифрування електронного банківського документа;

2) номер СК, якою користувалися під час шифрування або розшифрування електронного банківського документа.

35. Департамент безпеки надає послуги щодо розшифрування інформації за електронними банківськими документами, якщо між учасниками СЕП виникли спори з питань, пов'язаних з електронними банківськими документами, у разі:

1) невиконання автентифікації або розшифрування електронного банківського документа;

2) відмови від факту одержання електронного банківського документа;

3) відмови від факту формування та надсилання електронного банківського документа;

4) ствердження, що одержувачу надійшов електронний банківський документ, а насправді він не надсилався;

5) ствердження, що електронний банківський документ був сформований та надісланий, а він не формувався або було надіслане інше повідомлення;

6) виникнення спору щодо змісту одного й того самого електронного банківського документа, сформованого та надісланого відправником і одержаного та правильно автентифікованого одержувачем;

7) роботи з архівом роботи АРМ-СЕП під час проведення ревізій тощо.

Департамент безпеки надає учасникам СЕП письмові відповіді щодо порушених питань.

V. Внутрішній контроль за станом інформаційної безпеки в організації

36. Організація зобов'язана інформувати Департамент безпеки впродовж одного робочого дня телефоном та протягом трьох робочих днів листом засобами системи ЕП в таких випадках:

{Абзац перший пункту 36 розділу V із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

1) виконання (спроби виконання) фіктивного платіжного документа;

2) компрометація ЗЗІ;

3) пошкодження ЗЗІ;

4) несанкціоноване проникнення в приміщення з АРМ-СЕП/АРМ-НБУ-інф (пошкодження вхідних дверей, ґрат на вікнах, спрацювання сигналізації за нез'ясованих обставин тощо);

5) проведення правоохоронними органами та іншими органами державної влади перевірки діяльності організації, унаслідок якої створюються умови для компрометації ЗЗІ;

6) виникнення інших аварійних або надзвичайних ситуацій, що створюють передумови до розкрадання, втрати, пошкодження тощо ЗЗІ.

37. Внутрішній контроль за станом інформаційної безпеки відповідно до вимог нормативно-правових актів Національного банку в діяльності організації забезпечують:

керівник організації (особа, яка виконує його обов'язки);

заступник керівника організації або особа, яка за своїми службовими обов'язками чи за окремим внутрішнім документом організації призначена відповідальною особою за організацію інформаційної безпеки.

38. Адміністратор інформаційної безпеки забезпечує поточний контроль за дотриманням вимог інформаційної безпеки під час використання та зберігання ЗЗІ в організації.

39. Службові особи організації, які відповідають за інформаційну безпеку, зобов'язані надавати письмові або усні відомості про стан ЗЗІ та їх використання, стан захисту інформації в програмному забезпеченні САБ та інших системах, на які поширюються вимоги Національного банку щодо інформаційної безпеки, технологію оброблення електронних банківських документів в організації та систему захисту інформації під час їх оброблення на вимогу Департаменту безпеки.

Директор Департаменту
інформаційної безпеки **Д.О. Лук'янов**

ПОГОДЖЕНО:

Заступник Голови
Національного банку України Я.В. Смолій

Додаток 1
до Положення
(пункт 21 розділу III)

ДОГОВІР

про використання засобів захисту інформації Національного банку України

{Додаток 1 із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

Додаток 2
до Положення
(пункт 23 розділу III)

АКТ
про приймання-передавання засобів захисту інформації Національного банку України

{Додаток 2 із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

Додаток 3
до Положення
(пункт 29 розділу III)

АКТ

про повернення до Департаменту інформаційної безпеки Національного банку України, знищення, передавання до архіву засобів захисту інформації Національного банку України, справ і журналів обліку

{Додаток 3 із змінами, внесеними згідно з Постановою Національного банку № 79 від 17.08.2017}

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку
України
26.11.2015 № 829
(у редакції постанови
Правління
Національного банку
України
05.10.2018 № 106)

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

I. 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.

II. Призначення відповідальних осіб за роботу із ЗЗІ

II. 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**

{Правила в редакції Постанови Національного банку № 106 від 05.10.2018}

Додаток
до Правил організації захисту
електронних банківських
документів
з використанням засобів захисту
інформації
Національного банку України
(у редакції постанови Правління
Національного банку України
05.10.2018 № 106)
(пункт 7 розділу II)

ЗОБОВ'ЯЗАННЯ

{Додаток в редакції Постанови Національного банку № 106 від 05.10.2018}

ЗАТВЕРДЖЕНО
Постанова Правління Національного банку України
26.11.2015 № 829
(у редакції постанови Правління Національного банку України
13.02.2019 № 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

(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.

{Положення в редакції Постанови Національного банку № 38 від 13.02.2019}

Директор Департаменту інформаційної безпеки **Д.О. Лук'янов**

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 (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 №	

	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 ЗІІ 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:	
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 СЄП

{Додаток в редакції Постанови Національного банку № 38 від 13.02.2019}

ПОГОДЖЕНО:

Заступник Голови
Національного банку України Я.В. Смолій

Програмно-технічна підтримка — Управління комп'ютеризованих систем

Інформаційне наповнення — Відділ баз даних нормативно-правової інформації