Офіційно опубліковано 01.12.2015

Правління Національного банку України

ПОСТАНОВА

26 листопада 20 15 року м. Київ № 829

Про затвердження нормативно-правових актів з питань інформаційної безпеки

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

Інд. 51

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
26 листопада 2015 року № 829

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

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 у сфері інформаційної безпеки.

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 України в цій організації;

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

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 України;

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

5) ВК – відкритий ключ;

6) ЕЦП – електронний цифровий підпис;

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

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 України, з використанням засобів захисту інформації Національного банку України між банківськими та іншими установами і Національним банком України;

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 України та/або інформаційних задач і використовує засоби захисту інформації Національного банку України;

11) організація-замовник – банківська або інша установа, яка укладає договір про використання засобів захисту інформації Національного банку України з Національним банком України, у тому числі за свої філії;

12) ПМГК – програмний модуль генерації ключів, який є власністю Національного банку України;

13) САБ – система автоматизації банку;

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

15) СЕП – система електронних платежів Національного банку України;

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 України (далі – Національний банк).

Організації взаємодіють за всіма поточними питаннями роботи із ЗЗІ з Департаментом інформаційної безпеки Національного банку України (далі – Департамент інформаційної безпеки) та отримують ЗЗІ в територіальних управліннях Національного банку України (далі – територіальні управління) за місцем їх розташування. Організації міста Києва і Київської області отримують ЗЗІ в Департаменті інформаційної безпеки.

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 інформаційної 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 інформаційної 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 несиметричних алгоритмів RSA та ДСТУ 4145-2002.

11. Організація для забезпечення захисту інформації зобов’язана мати трибайтний унікальний ідентифікатор (далі – унікальний ідентифікатор), перший символ якого є літерою на позначення відповідної території, на якій вона розташована, другий і третій символи утворюють унікальний ідентифікатор організації в межах цієї території.

Унікальний ідентифікатор має бути узгоджений з адресою організації в системі електронної пошти Національного банку. Унікальний ідентифікатор записується в ПМГК та АКЗІ, які надаються організації, та не може бути нею змінений, що забезпечує захист від підроблення ключової інформації від імені іншої організації.

Ідентифікатори ключів криптографічного захисту, що використовуються організацією, складаються з шести символів, з яких перші три є унікальним ідентифікатором організації, четвертий символ визначає тип робочого місця учасника СЕП (операціоніст, бухгалтер тощо) або тип інформаційної задачі, п’ятий і шостий – ідентифікатор робочого місця або відповідальної особи.

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 несиметричного алгоритму RSA для всіх робочих місць, де працюють з електронними банківськими документами. Кожен ТК робочого місця захищений особистим паролем відповідальної особи, яка працює з цим ключем.

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

Департамент інформаційної 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 інформаційної 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	ТК АРМ-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:

лист-звернення від організації-замовника до Департаменту інформаційної безпеки про укладення договору із зазначенням для цієї організації-замовника та її філій, якщо такі існують, унікального ідентифікатора, коду банку, назв інформаційних задач, з якими планують працювати, а також орієнтовної дати початку роботи в цих задачах;

укладення договору про використання засобів захисту інформації Національного банку України між організацією-замовником та Національним банком;

забезпечення відповідності приміщень, у яких будуть оброблятися електронні банківські документи, використовуються та зберігаються ЗЗІ, вимогам, що визначені Правилами;

призначення посадових осіб, відповідальних за зберігання та використання ЗЗІ;

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

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

21. Департамент інформаційної безпеки від імені Національного банку та організація-замовник укладають між собою договір відповідно до зразка, викладеного в додатку 1 до цього Положення.

Організація-замовник здійснює оплату Національному банку всіх послуг, наданих Національним банком за цим договором як організації-замовнику, так і її філіям.

Організація-замовник зобов’язана внести зміни до договору в разі:

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

2) зміни місцезнаходження філії з однієї області України на іншу;

3) появи нових філій або закриття наявних.

Організація-замовник зобов’язана переукласти договір у разі зміни свого місцезнаходження з однієї області України на іншу і отримати ЗЗІ з новим ідентифікатором, який відповідає новому місцезнаходженню.

22. Департамент інформаційної безпеки в разі відсутності недоліків за результатами перевірки готовності включення організації в СЕП та/або інформаційні задачі:

1) виготовляє ЗЗІ для цієї організації;

2) надає ЗЗІ організації через територіальне управління за місцезнаходженням організації або безпосередньо для міста Києва та Київської області.

23. Відповідальна за отримання ЗЗІ особа організації зобов’язана прибути до територіального управління за місцем розташування організації 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).

24. Департамент інформаційної безпеки разом з документом на отримання/заміну ЗЗІ зберігає один примірник, а організація – другий примірник акта про приймання-передавання апаратних засобів захисту інформації Національного банку України, за яким АКЗІ та смарт-картки передаються в організацію, а також зберігає копію супровідного листа, а організація – супровідний лист, згідно з яким ПМГК передається в організацію.

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 інформаційної 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 договорі;

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

27. Організація зобов’язана повернути ЗЗІ до Департаменту інформаційної безпеки через територіальне управління в разі:

1) ліквідації;

2) припинення роботи із ЗЗІ, а саме:
виключення з учасників СЕП;
переходу на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку банку на іншу;
зміни місцезнаходження з однієї області України на іншу;

3) виходу з ладу ЗЗІ;

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

28. Організація зобов'язана повернути АКЗІ разом із СК до Департаменту інформаційної безпеки через територіальне управління в разі виходу АКЗІ з ладу або отримання від Департаменту інформаційної безпеки листа з вимогою повернення ЗЗІ протягом трьох робочих днів з укладенням акта про приймання-передавання апаратних засобів захисту інформації Національного банку України, один примірник якого зберігає Департамент інформаційної безпеки, другий – організація.

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

1) повідомити Департамент інформаційної 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 інформаційної безпеки;

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

3) повернути до Департаменту інформаційної безпеки через територіальне управління ЗЗІ з актом, зазначеним у підпункті 2 цього пункту, один примірник якого зберігає Департамент інформаційної 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 інформаційної 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 інформаційної 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 інформаційної 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 інформаційної 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 інформаційної безпеки надає учасникам СЕП письмові відповіді щодо порушених питань.

V. Внутрішній контроль за станом інформаційної безпеки в організації

36. Організація зобов’язана інформувати Департамент інформаційної безпеки впродовж одного робочого дня телефоном та протягом трьох робочих днів листом засобами системи електронної пошти Національного банку в таких випадках:

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 інформаційної безпеки.

Директор Департаменту інформаційної безпеки Д. О. Лук’янов

ПОГОДЖЕНО
Заступник Голови
Національного банку України
_______________ Я. В. Смолій
(підпис)
“_26_” ____11_____ 2015 року
(дата)

Додаток 1
до Положення
(пункт 21 розділу ІІІ)

ДОГОВІР № ___
про використання засобів захисту інформації Національного банку України
(Зразок)

м. ___________ ____________________
(дата)

Національний банк України (далі – Виконавець) в особі ______________________________________ ___________________________,
(посада) (прізвище, ім'я, по батькові)
який діє на підставі__________________ від _____________ № ______, та
(назва документа)
____ (далі – Замовник) в особі
(найменування організації)
____, який діє на підставі
(посада, прізвище, ім'я, по батькові)
___________________________ від ___________ № ____ (далі – Сторони),
(назва документа)
уклали цей договір про таке.

1. Предмет договору

1.1. Виконавець зобов'язується надати Замовнику та його установам, визначеним у додатку 1 до цього договору, такі послуги:

надати у користування засоби захисту інформації Національного банку України (далі – засоби захисту інформації) для використання їх у системі електронних платежів Національного банку України (далі – СЕП) та у програмно-технічних комплексах автоматизації банківської діяльності, які забезпечують оброблення та передавання інформації, що не належить до платіжної і технологічної інформації СЕП, між банківськими та іншими установами і Національним банком України (далі – інформаційні задачі):

апаратуру криптографічного захисту інформації (далі – АКЗІ) згідно з актом приймання-передавання засобів захисту інформації Національного банку України;

програмне забезпечення "Автоматизоване робоче місце обміну неплатіжною інформацією" (далі – АРМ-НБУ-інф) із вбудованою системою захисту інформації (системою електронної пошти Національного банку України), а також послуги з його супроводження;

програмні модулі генерації ключів криптографічного захисту інформації (далі – ПМГК) згідно з описом у супровідному листі.

1.2. Використання, зберігання та приймання-передавання засобів захисту інформації здійснюються відповідно до нормативно-правових актів Національного банку України з питань інформаційної безпеки.

2. Строки виконання зобов’язань за договором

2.1. Виконавець зобов’язується протягом дії цього договору надавати послуги Замовнику.

2.2. Замовник має здійснити оплату до _______ числа наступного місяця.

3. Загальна вартість за договором

3.1. Вартість послуг за цим договором, враховуючи всі витрати Виконавця, визначається згідно з тарифами на операції (послуги), установленими нормативно-правовими актами Національного банку України.

3.2. У разі внесення Національним банком України змін до тарифів розмір оплати змінюється від часу набрання чинності цими змінами (без додаткового внесення змін до договору).

4. Права та обов’язки Сторін

4.1. Виконавець має право:

перевіряти Замовника та його установи, які отримали засоби захисту інформації згідно з додатком 1 до договору, щодо дотримання ними вимог захисту інформації та правил організації захисту електронних банківських документів із використанням засобів захисту інформації Національного банку України, установлених Національним банком України;

зупиняти обслуговування Замовника та/або його установ у разі порушень ним правил роботи із засобами захисту інформації або передавання (навіть тимчасово) отриманих Замовником та його установами засобів захисту інформації третім особам, установам чи організаціям, у тому числі іншим установам Замовника (установи Замовника отримують призначені їм засоби захисту інформації у Національному банку України самостійно);

запроваджувати нові програмно-технічні та технологічні засоби, розроблені для поліпшення послуг, що надаються Замовнику;

без додаткового погодження здійснювати договірне списання коштів із кореспондентського рахунку Замовника, відкритого у Виконавця, у разі ненадходження від Замовника оплати за надані Виконавцем послуги в сумі та в строк, що обумовлені в розділі 5 цього договору.

4.2. Замовник та його установи, визначені в додатку 1 до цього договору, мають право:

користуватися наданими засобами захисту інформації в СЕП та інформаційних задачах;

отримувати від Виконавця консультації з питань, пов'язаних з експлуатацією та зберіганням засобів захисту інформації;

використовувати надані ПМГК для робочих місць системи автоматизації банку, СЕП та інформаційних задач згідно з діючою технологією.

4.3. Виконавець бере на себе зобов'язання:

належним чином та своєчасно надавати Замовнику та його установам, визначеним у додатку 1 до цього договору, засоби захисту інформації, в тому числі оновлені, з потрібною документацією до них та консультації з питань захисту інформації і правил користування засобами захисту інформації;

своєчасно інформувати Замовника про зміни, які планується вносити до системи захисту інформації Національного банку України;

здійснювати заміну АКЗІ в разі виходу її з ладу та безкоштовний ремонт, крім випадків, зазначених у пункті 6.2 цього договору;

забезпечувати своєчасну заміну ПМГК в разі його пошкодження або виходу з ладу, крім випадків, зазначених у пункті 6.2 цього договору.

4.4. Замовник бере на себе зобов'язання:

не передавати (навіть тимчасово) отримані ним засоби захисту інформації, які використовуються в СЕП та інформаційних задачах, третім особам, установам чи організаціям, не допускати обміну наданих засобів захисту інформації між установами Замовника;

дотримуватися технологічної дисципліни в роботі із засобами захисту інформації, забезпечувати їх використання і зберігання згідно з вимогами Виконавця. Негайно інформувати Виконавця про виникнення порушень умов зберігання та використання засобів захисту інформації і вживати заходів для їх усунення;

утримувати засоби захисту інформації в належному стані;

забезпечувати цілісність голографічної наклейки на АКЗІ;

не використовувати надані засоби захисту інформації для завдань, які не обумовлені наявними інструкціями;

забезпечувати наявність потрібних технічних засобів для підключення АКЗІ згідно з вимогами Виконавця;

забезпечувати транспортування засобів захисту інформації до місця їх встановлення в Замовника та до місця їх заміни у Виконавця;

своєчасно здійснювати оплату Виконавцю за виконані роботи і надані послуги;

передати (повернути) Виконавцю АКЗІ протягом трьох робочих днів після припинення дії цього договору;

оплачувати Виконавцю послуги з проведення фахівцями Національного банку України аналізу в разі:

повторно виявлених у Замовника порушень вимог захисту інформації та правил організації захисту електронних банківських документів із використанням та зберіганням засобів захисту інформації, установлених Національним банком України;

втрати або пошкодження АКЗІ;

пошкодження голографічної наклейки на АКЗІ;

втрати або пошкодження смарт-картки для АКЗІ;

втрати або пошкодження ПМГК та його повторного надання на заміну втраченого або пошкодженого ПМГК.

5. Порядок розрахунків

5.1. Період, за який Виконавець розраховує суму оплати за надані послуги, є: з ___ числа попереднього місяця до ___ числа розрахункового місяця включно.

5.2. Виконавець щомісяця до ___ числа розрахункового місяця надсилає Замовнику засобами системи електронної пошти Національного банку України акт наданих послуг із розрахунком їх вартості згідно з тарифами на операції (послуги), установленими нормативно-правовими актами Національного банку України. Замовник має здійснити оплату за розрахунком, зазначеним в акті наданих послуг (у тому числі пені) до _______ числа наступного місяця.

Здійснення оплати послуг Замовником підтверджує, що такі послуги надані Виконавцем у повному обсязі без будь-яких зауважень.

У разі незгоди Замовник у строк до трьох робочих днів направляє Виконавцю вмотивовану відмову від оплати.

У разі порушення строку проведення розрахунків і нарахування пені її розмір включається до акта наданих послуг за наступний розрахунковий місяць.

Акт наданих послуг із підписами та відбитком печатки Виконавець надсилає Замовнику за потребою (запитом) засобами поштового зв’язку.

5.3. Розрахунок за виконані роботи, надані послуги за неповний робочий місяць (у разі укладення, розірвання договору) здійснюється за фактичний час.

5.4. У разі ненадходження оплати від Замовника у строк, обумовлений у цьому договорі, та відсутності письмового заперечення від Замовника до акта наданих послуг Виконавець має право без додаткового погодження здійснювати договірне списання суми з кореспондентського рахунку Замовника, відкритого у Виконавця, згідно з розрахунком. Для заповнення реквізиту “Призначення платежу” Виконавець зазначає номер і дату договору, за якими має здійснюватися договірне списання.

6. Відповідальність Сторін

6.1. Виконавець несе відповідальність перед Замовником за правильне та своєчасне надання засобів захисту інформації Замовнику та його установам, визначеним у додатку 1 до цього договору, для забезпечення можливості роботи в СЕП та в інформаційних задачах Національного банку України.

6.2. Замовник відшкодовує Виконавцю збитки, завдані ним у зв’язку з порушенням умов зберігання і використання засобів захисту інформації.

6.3. У разі прострочення оплати за виконані роботи та надані послуги Замовник сплачує Виконавцю суму боргу з урахуванням установленого індексу інфляції за весь час прострочення і ___ проценти річних із простроченої суми.

6.4. За порушення строків оплати Замовником послуг Виконавця, передбачених цим договором, Замовник сплачує Виконавцю на його вимогу пеню в розмірі 0,1 відсотка від суми простроченого платежу за кожний день прострочення.

7. Форс-мажор

7.1. Сторони договору звільняються від відповідальності за часткове або повне невиконання будь-якого з положень цього договору, якщо це невиконання стало наслідком причин, що перебувають поза сферою контролю Сторони, яка його не виконала. Такі причини включають стихійне лихо, надзвичайні погодні умови, пожежі, війни, страйки, військові дії, громадські заворушення, але не обмежуються ними (далі – форс-мажор). Період звільнення від відповідальності починається з часу оголошення однією зі Сторін форс-мажору і закінчується (чи закінчився б), якщо ця Сторона вжила заходів, яких вона і справді могла б ужити, для виходу з форс-мажору. Форс-мажор автоматично продовжує строк виконання зобов’язань на весь період його дії та ліквідації наслідків. Про настання форс-мажорних обставин Сторони мають інформувати одна одну невідкладно.

Достатнім доказом дії форс-мажорних обставин є документ, виданий уповноваженим органом.

7.2. Якщо зазначені обставини триватимуть більше ніж 6 місяців, то кожна зі Сторін матиме право відмовитися від подальшого виконання зобов’язань за цим договором і в такому разі жодна зі Сторін не матиме права на відшкодування іншою Стороною можливих збитків.

8. Порядок зміни та розірвання договору

8.1. Зміни до цього договору вносяться у письмовій формі шляхом укладення додаткових договорів, крім випадку зміни будь-яких реквізитів, що зазначені в розділі 12 цього договору. У цьому випадку зміни до положень розділу 12 вносяться шляхом обміну листами, підписаними уповноваженими особами Сторін, та скріпленими печатками.

8.2. Додатковий договір стає невід’ємною частиною цього договору і набирає чинності з дня підписання обома Сторонами.

8.3. Сторона, яка вважає за потрібне змінити чи розірвати договір, надсилає пропозиції про це другій Стороні.

8.4. Сторона, яка одержала пропозицію про зміну чи розірвання договору, у двадцятиденний строк після одержання пропозиції повідомляє другу Сторону про результати її розгляду.

8.5. Якщо Сторони не досягли згоди щодо зміни (розірвання) договору або в разі неодержання відповіді у встановлений строк з урахуванням часу поштового обігу, зацікавлена Сторона має право передати вирішення спору до суду.

8.6. У разі зміни однією зі Сторін будь-яких реквізитів, зазначених у розділі 12 цього договору, Сторона, яка змінила реквізити, у строк до _____ днів після їх зміни письмово повідомляє про це другу Сторону. Сторона, яка одержала це повідомлення, має письмово повідомити другу Сторону про його одержання.

9. Порядок розгляду спорів

9.1. Спори, що виникають протягом дії договору, вирішуються шляхом переговорів.

9.2. У разі недосягнення згоди шляхом переговорів спори вирішуються в судовому порядку.

10. Строк дії договору

10.1. Договір, укладений на строк _________, набирає чинності з дня його підписання.

10.2. Дія договору припиняється у випадках, передбачених законодавством України.

10.3. Цей договір вважається продовженим на один рік, якщо за 30 (тридцять) календарних днів до закінчення його дії одна зі Сторін письмово не повідомить іншу про намір щодо його розірвання. Кількість продовжень необмежена.

11. Інші умови договору

11.1. Цей договір складено в двох примірниках українською мовою по одному для кожної зі Сторін, причому обидва примірники мають однакову юридичну силу.

11.2. Відносини Сторін, що виникають під час дії цього договору і які не врегульовані ним, регулюються законодавством України.

12. Місцезнаходження (поштові адреси), платіжні реквізити і підписи Сторін

12.1. Місцезнаходження обслуговування Замовника за цим Договором:

____

12.2. Місцезнаходження, платіжні реквізити, ідентифікаційний код Виконавця:

____
____

12.3. Місцезнаходження, платіжні реквізити, ідентифікаційний код Замовника:

____
____

Продовження додатка 1

12.4. Для вирішення всіх питань, пов’язаних із виконанням цього договору, відповідальними представниками є:

від Виконавця ________________ від Замовника _______________________
______________________________ __________________________________

Виконавець __________________ Замовник _________________________
(підпис) (підпис)
М. П. М. П.

Примітки.

1. При укладенні договору сторони використовують зазначений зразок договору, проте мають право вносити до нього зміни, зумовлені особливостями конкретної ситуації та засобів захисту інформації, про передачу яких ідеться в договорі.

2. Організації, які є учасниками інформаційних задач (отримують тільки програмні засоби захисту інформації), укладають договір за цим зразком із виключенням із нього підпунктів та слів, що стосуються апаратних засобів захисту інформації і СЕП та абзацу п’ятого пункту 4.1 глави 4 і пункту 5.4 глави 5 цього договору.

3. Організації, які не мають підпорядкованих установ або територіальних органів, укладають договір за цим зразком, виключивши з нього підпункти і слова, що стосуються установ Замовника, та додаток до договору.

Продовження додатка 1

Додаток 1
до договору про використання засобів захисту інформації Національного банку України від
___________ № ___________
(дата) (номер)

Перелік установ Замовника,
які отримують засоби захисту інформації Національного банку України

№ з/п	Назва установи та адреса розташування засобів захисту інформації установи	Трибайтний ідентифікатор установи в системі захисту інформації	АКЗІ	ПМГК	Програмне забезпечення АРМ-СЕП	Програмне забезпечення АРМ-НБУ-інф
1	2	3	4	5	6	7
1	ПАТ “…”		так	так	так	так
2	Філія ПАТ “…” м…., вул.…		ні	так	ні	так
…						

“Виконавець___________
(підпис)
М. П.”

“Замовник___________
(підпис)
М. П.”

Додаток 2
до Положення
(пункт 23 розділу III)

ПОГОДЖЕНО Керівник (заступник керівника) організації	ЗАТВЕРДЖЕНО Директор (заступник директора) Департаменту інформаційної безпеки Національного банку України
_____________________________ (підпис, ініціали, прізвище) “___” ___________ 20__ р.	_____________________________ (підпис, ініціали, прізвище) “___” ______________ 20__ р.
М. П.	М. П.

АКТ
про приймання-передавання апаратних засобів захисту інформації Національного банку України

м. _____________ “___” _________ 20__ р.

Представник Департаменту інформаційної безпеки ___________________
(ініціали, прізвище)
та представник ____
(найменування організації) (ініціали, прізвище)
відповідно до договору від ________________ № ______ здійснили передавання
від Національного банку України до __________________________________/
(найменування організації)
від ___________________________________ до Національного банку України
(найменування організації)
таких засобів захисту інформації Національного банку України:
апаратури криптографічного захисту № _________ у комплекті;
смарт-карток № ___________ .

Примітка. Подається перелік засобів захисту інформації Національного банку України, що передаються з наданням номерів, які візуально доступні для зчитування на засобах захисту інформації.

Здав _____________________________
(підпис, ініціали, прізвище)

Прийняв __________________________
(підпис, ініціали, прізвище)

Додаток 3
до Положення
(пункт 29 розділу ІІІ)

ПОГОДЖЕНО	ЗАТВЕРДЖЕНО
Директор (заступник директора)	Керівник (заступник керівника)
Департаменту інформаційної безпеки	організації
Національного банку України	
______________________________	______________________________
(підпис, ініціали, прізвище)	(підпис, ініціали, прізвище)
“___” ___________ 20__ р.	“___” ______________ 20__ р.
М. П.	М. П.

АКТ

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

м. __________ “___” _________ 20__ р.

У зв’язку з припиненням роботи __________________________________
(найменування організації)
з “______” ___________________ 20__ р. у СЕП/інформаційних задачах Національного банку України і дії договору про використання засобів захисту інформації Національного банку України від “___” __________ 20___ р. № ________

або:

У зв’язку зі зміною моделі обслуговування консолідованого кореспондентського рахунку банку ___________________________________
(найменування організації)
у СЕП з “___” ________ 20__ р. і припиненням договору про використання засобів захисту інформації Національного банку України від “____” _____________ 20__ р. № _________ нами вжито таких заходів:

1. До Департаменту інформаційної безпеки Національного банку України повернуто:

апаратуру криптографічного захисту інформації № ________ у комплекті;

смарт-картки № _________;

2. Знищені на місці:

програмний модуль генерації ключів та його копія (версія __________,

Продовження додатка 3

дата виготовлення __________);

таємний ключ АРМ-СЕП s_*300.*;

копія таємного ключа АРМ-СЕП s_*300.*;

таємні ключі АРМ бухгалтера
s_*.* (перелік усіх ключів) – усього ___ ключів;

копії таємних ключів АРМ бухгалтера
s_*.* (перелік усіх ключів) – усього ___ ключів;

таємні ключі операціоністів – усього ___ ключів;

програмний комплекс АРМ-СЕП;

таємний ключ АРМ-НБУ-інф s_*500.*;

копія таємного ключа АРМ-НБУ-інф s_*500.*;

програмний комплекс АРМ-НБУ-інф;

таємні ключі інформаційних задач – усього ___ ключів;

відкриті ключі АРМ-СЕП/АРМ-НБУ-інф, АРМ бухгалтера САБ, таблиці відкритих ключів АРМ-СЕП/АРМ-НБУ-інф, АРМ бухгалтера та інших робочих місць САБ, файли сертифікатів відкритих ключів для роботи в СЕП.

3. Передані в архів ____:
(найменування організації)

справи і журнали обліку адміністратора інформаційної безпеки;

журнали обліку АРМ-СЕП/АРМ-НБУ-інф;

електронні архіви електронних платежів і відкритих ключів операціоністів.

4. Копій знищених і переданих документів, програм, засобів захисту інформації Національного банку України немає.

Адміністратор інформаційної безпеки ________________________________
(підпис, ініціали, прізвище)

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
26 листопада 2015 року № 829

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) ГМД – гнучкий магнітний диск;

2) захищений носій ТК – носій таємного ключа, обладнаний вбудованими апаратними засобами криптозахисту (Touch Memory, токени тощо);

3) незахищений носій ТК – носій таємного ключа, необладнаний вбудованими засобами криптозахисту (ГМД, флеш-носії тощо);

4) носій ТК – носій таємного ключа (захищений або незахищений).

Інші терміни та скорочення, що вживаються в цих Правилах, використовуються в значеннях, визначених Законом України “Про електронні документи та електронний документообіг”, 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 (далі – Положення про захист), 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 (із змінами).

3. Ці Правила регламентують порядок використання, зберігання, передавання та облік ЗЗІ організаціями, які отримали ці ЗЗІ відповідно до Положення про захист. Департамент інформаційної безпеки Національного банку України (далі – Департамент інформаційної безпеки) перевіряє виконання цих 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 України від 26 листопада 2015 року № 829.

II. Призначення відповідальних осіб за роботу із ЗЗІ

4. Організація зобов’язана призначити відповідальних за роботу із ЗЗІ осіб (далі – відповідальна особа) та осіб, які виконуватимуть обов’язки в разі відсутності відповідальних осіб, а саме:

1) адміністратора інформаційної безпеки;

2) адміністратора АРМ-СЕП/АРМ-НБУ-інф;

3) оператора АРМ бухгалтера САБ;

4) технолога САБ;

5) операціоніста САБ;

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

Адміністратор інформаційної безпеки реєструє відповідальних осіб у розділі І журналу обліку адміністратора інформаційної безпеки (додаток 1).

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

5. Організація зобов’язана подавати до Департаменту інформаційної безпеки копію документа або виписку з нього в електронній або паперовій формі:

1) про призначення відповідальних осіб протягом трьох робочих днів з часу їх призначення;

2) про покладання обов’язків/звільнення від виконання відповідних обов’язків в організації, зокрема покладання інших обов’язків, адміністраторів інформаційної безпеки, адміністраторів АРМ-СЕП/АРМ-НБУ-інф і операторів АРМ бухгалтера САБ протягом трьох робочих днів із часу їх призначення/звільнення.

6. Адміністратор інформаційної безпеки зобов’язаний ознайомитися з нормативно-правовими актами Національного банку України (далі – Національний банк) з питань інформаційної безпеки та підписати зобов’язання адміністратора інформаційної безпеки (додаток 2).

Представник Департаменту інформаційної безпеки зобов’язаний перевірити знання адміністратором інформаційної безпеки своїх функціональних обов’язків та відповідних нормативно-правових актів Національного банку, зробити на зобов’язанні відмітку про проведення цієї перевірки і зберігати копію цього зобов’язання.

7. Адміністратор інформаційної безпеки має право дати дозвіл на роботу на АРМ-СЕП/АРМ-НБУ-інф, робочих і технологічних місцях САБ та інформаційних задач відповідальним особам після їх ознайомлення з нормативно-правовими актами Національного банку, іншими документами з питань інформаційної безпеки.

Адміністратор інформаційної безпеки зобов’язаний ознайомити відповідальних осіб з правилами роботи та зберігання ТК.

Відповідальна особа зобов’язана підписати відповідне зобов’язання (додаток 3).

8. Департамент інформаційної безпеки має право звернутися до керівника організації з пропозицією призначити нового адміністратора інформаційної безпеки в разі неналежного виконання ним своїх обов’язків.

9. Організація зобов’язана забезпечити відповідальних осіб особистими печатками (штампами, пломбіраторами тощо) для опечатування ЗЗІ, сейфів (для зберігання незахищених носіїв ТК) і приміщення з АРМ-СЕП/АРМ-НБУ-інф.

Адміністратор інформаційної безпеки зобов’язаний зареєструвати печатки (штампи, пломбіратори) у розділі VI журналу обліку адміністратора інформаційної безпеки (додаток 1).

Відповідальні особи не мають права передавати один одному печатки (штампи, пломбіратори) для тимчасового користування.

10. Організація забезпечує підбір відповідальних осіб для роботи із ЗЗІ згідно з таблицею суміщення функціональних обов’язків (додаток 4).

III. Функціональні обов’язки відповідальних осіб

11. Адміністратор інформаційної безпеки зобов’язаний:

1) знати нормативно-правові акти Національного банку з питань інформаційної безпеки і використовувати їх у роботі;

2) виконувати вимоги щодо інформаційної безпеки в організації та підписати зобов’язання адміністратора інформаційної безпеки;

3) забезпечувати конфіденційність системи захисту інформації в організації;

4) отримувати ЗЗІ і проводити їх заміну в територіальному управлінні Національного банку;

5) здійснювати тестування ПМГК та брати участь у тестуванні інших ЗЗІ;

6) здійснювати листування з Департаментом інформаційної безпеки з питань інформаційної безпеки;

7) ознайомлювати відповідальних осіб організації з нормативно-правовими актами Національного банку з питань інформаційної безпеки та перевіряти знання правил використання і зберігання ТК й інших ЗЗІ;

8) забезпечувати відповідальних осіб ЗЗІ;

9) вести облік ЗЗІ і здійснювати контроль за їх прийманням-передаванням;

10) вести справу адміністратора інформаційної безпеки і забезпечувати її збереження;

11) надавати допомогу відповідальним особам в генерації ТК;

12) забезпечувати належне зберігання ЗЗІ, їх передавання іншому адміністратору інформаційної безпеки в разі двозмінної роботи або у зв’язку з тимчасовою відсутністю на роботі – відпусткою, навчанням, хворобою тощо;

13) забезпечувати відправлення на сертифікацію ВК, що потребують сертифікації;

14) вести архів ВК операціоністів;

15) здійснювати копіювання ПМГК та знищення копій ПМГК у встановленому порядку;

16) здійснювати контроль за дотриманням відповідальними особами правил інформаційної безпеки під час роботи із ЗЗІ та їх зберігання;

17) здійснювати контроль за своєчасною заміною ТК відповідальними особами;

18) здійснювати контроль за змінами ТВК у разі необхідності;

19) здійснювати контроль за правильним і своєчасним знищенням відповідальними особами ТК та їх копій;

20) забезпечувати вилучення відповідного ВК з ТВК шляхом генерації ТК на видалення в разі звільнення від обов’язків відповідальних осіб або компрометації ТК;

21) виконувати заміну криптобібліотек і ТВК у САБ та інформаційних задачах, якщо Національний банк ініціює їх заміну;

22) здійснювати перевірки відповідності приміщень з АРМ-СЕП/АРМ-НБУ-інф і сейфів, у яких зберігаються ЗЗІ, вимогам інформаційної безпеки;

23) знати експлуатаційну документацію на АРМ-СЕП/АРМ-НБУ-інф з питань роботи системи захисту інформації;

24) виконувати налаштування операційної системи комп’ютера з АРМ-СЕП/АРМ-НБУ-інф відповідно до вимог та рекомендацій Національного банку щодо усунення вразливостей операційної системи;

25) не рідше одного разу на квартал проводити планові перевірки використання ЗЗІ відповідальними особами організації;

26) під час перевірки звертати увагу на наявність ЗЗІ, ключів від сейфів, у яких зберігаються ЗЗІ, облікових даних, дотримання вимог інформаційної безпеки під час зберігання та використання ЗЗІ, обмеження доступу до приміщення з АРМ-СЕП/АРМ-НБУ-інф, знання відповідальними особами нормативно-правових актів Національного банку з питань інформаційної безпеки, правильне і своєчасне заповнення журналів обліку;

27) після закінчення перевірки зробити відповідні записи в розділі IX журналу обліку адміністратора інформаційної безпеки (додаток 1);

28) інформувати керівника організації і Департамент інформаційної безпеки про виявлені недоліки, що можуть загрожувати безпеці електронної банківської інформації;

29) брати участь (за письмовим або усним розпорядженням керівника організації) у розгляді фактів порушення правил інформаційної безпеки в організації.

12. Адміністратор АРМ-СЕП/АРМ-НБУ-інф організації зобов’язаний:

1) знати нормативно-правові акти Національного банку з питань інформаційної безпеки, що стосуються його функцій, і використовувати їх у роботі;

2) забезпечувати конфіденційність системи захисту інформації в організації;

3) знати експлуатаційну документацію на АРМ-СЕП/АРМ-НБУ-інф і вимоги та рекомендації Національного банку щодо усунення вразливостей операційної системи комп’ютера з АРМ-СЕП/АРМ-НБУ-інф;

4) установлювати АКЗІ та драйвери до нього і забезпечувати постійне її підключення до комп’ютера, на якому функціонує АРМ-СЕП;

5) забезпечувати технологічну дисципліну під час роботи АРМ-СЕП/АРМ-НБУ-інф;

6) здійснювати генерацію ключів АРМ-СЕП/АРМ-НБУ-інф та контроль за строком їх дії;

7) зберігати ТК до АРМ-СЕП/АРМ-НБУ-інф (за необхідності – їх копії), АКЗІ та СК для АРМ-СЕП;

8) уносити необхідні зміни до ТВК АРМ-СЕП/АРМ-НБУ-інф за допомогою АРМ-СЕП/АРМ-НБУ-інф;

9) знищувати в установленому порядку ТК АРМ-СЕП/АРМ-НБУ-інф та їх копії;

10) дотримуватися режиму допуску до приміщення з АРМ-СЕП/АРМ-НБУ-інф;

11) здавати під охорону і знімати з охорони приміщення з АРМ-СЕП/АРМ-НБУ-інф;

12) вести журнал приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф (додаток 5);

13) інформувати адміністратора інформаційної безпеки про виявлення недоліків, що можуть призвести до компрометації ЗЗІ або несанкціонованого їх використання;

14) брати участь (за розпорядженням керівника організації) у розгляді фактів порушення правил інформаційної безпеки під час роботи АРМ-СЕП/АРМ-НБУ-інф.

13. Оператори АРМ бухгалтера САБ, операціоністи та оператори інших робочих і технологічних місць САБ та інформаційних задач, які працюють із ЗЗІ, зобов’язані:

1) знати нормативно-правові акти Національного банку з питань інформаційної безпеки, що стосуються їх функцій, і використовувати їх у роботі;

2) забезпечувати конфіденційність відомостей про систему захисту інформації в організації;

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

4) виконувати правила використання і зберігання ЗЗІ;

5) здійснювати генерацію власних ключів;

6) здійснювати контроль за строком дії ключів і своєчасну генерацію (з урахуванням часу на сертифікацію) нових ключів;

7) зберігати власний ТК (за необхідності – його копію), у разі використання незахищеного носія ТК – в особистому сейфі (за його наявності);

8) у разі використання незахищеного носія ТК передавати в установленому порядку на зберігання (якщо немає особистого сейфа) власний ТК (і його копію) адміністратору інформаційної безпеки;

9) забезпечувати схоронність ЗЗІ під час їх використання;

10) знищувати в установленому порядку власні ТК (і їх копії);

11) вести журнал приймання-передавання таємних ключів робочих і технологічних місць (додаток 6) у разі передавання ТК робочого місця іншій відповідальній особі;

12) інформувати адміністратора інформаційної безпеки про виявлення недоліків, що можуть призвести до компрометації ЗЗІ або несанкціонованого їх використання;

13) брати участь (за письмовим або усним розпорядженням керівника організації) у розгляді фактів порушення правил інформаційної безпеки під час роботи САБ та інформаційних задач.

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

1) допуск до ПМГК для роботи з ним мають лише адміністратори інформаційної безпеки;

2) допуск до роботи з АКЗІ, СК, ТК АРМ-СЕП/АРМ-НБУ-інф мають тільки адміністратори АРМ-СЕП/АРМ-НБУ-інф;

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

4) відповідальні особи виконують генерацію власних ТК за допомогою ПМГК лише в присутності адміністратора інформаційної безпеки;

5) адміністратори інформаційної безпеки виконують свої функціональні обов’язки і функції контролю під час роботи з ТВК на АРМ-СЕП/АРМ-НБУ-інф та інших робочих місцях лише в присутності відповідальних осіб.

IV. Порядок роботи з апаратними ЗЗІ

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

16. Адміністратор інформаційної безпеки зобов’язаний після отримання АКЗІ та СК зробити відповідний запис у розділі ІІ журналу обліку адміністратора інформаційної безпеки (додаток 1).

17. Адміністратор інформаційної безпеки зобов’язаний передати АКЗІ адміністратору АРМ-СЕП і зробити запис у розділі ІІ журналу обліку адміністратора інформаційної безпеки (додаток 1).

Адміністратор АРМ-СЕП зобов’язаний отримати АКЗІ та зробити відповідний запис у журналі приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф (додаток 5).

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

18. 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.

19. Адміністратор АРМ-СЕП зобов’язаний згенерувати ТК АКЗІ за допомогою програмно-технічного комплексу АРМ-СЕП для введення АКЗІ в експлуатацію і записати копію ТК АКЗІ АРМ-СЕП на другу (резервну) СК під час генерації ключів.

Адміністратор інформаційної безпеки надсилає ВК АКЗІ на сертифікацію до Національного банку.

Адміністратор АРМ-СЕП уводить АКЗІ в експлуатацію після отримання сертифіката ВК, автоматичного включення його до ТВК АКЗІ та здійснення відповідних налаштувань АРМ-СЕП.

Адміністратор АРМ-СЕП зобов’язаний здійснювати своєчасну генерацію ключа АКЗІ у зв’язку із закінченням строку його дії.

20. Адміністратори АРМ-СЕП зобов’язані передавати АКЗІ і СК між собою із внесенням запису до журналу приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф (додаток 5), який вони ведуть і зберігають у приміщенні з АРМ-СЕП. 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 для АКЗІ у сейфі в неробочий час і в робочий час, якщо вони не використовуються в роботі.

21. Адміністратор АРМ-СЕП зобов’язаний здійснити заміну АКЗІ разом із СК у разі виходу з ладу АКЗІ під час експлуатації, пошкодження АКЗІ/СК/голографічної наклейки, втрати АКЗІ або СК та на вимогу Департаменту інформаційної безпеки.

Для цього адміністратор АРМ-СЕП організації зобов’язаний:

1) повідомити ЦРП про перехід на резервні програмні ЗЗІ засобами системи електронної пошти Національного банку;

2) забезпечити переведення АРМ-СЕП на роботу з програмними ЗЗІ за допомогою відповідного настроювання АРМ-СЕП за погодженням з ЦРП;

3) забезпечити продовження роботи АРМ-СЕП у звичайному режимі з використанням програмних ЗЗІ;

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

5) узгодити з ЦРП дату переведення на апаратне шифрування після відновлення роботи АКЗІ. Перехід на апаратні ЗЗІ повинен здійснюватися лише на початку банківського дня за погодженням з ЦРП;

6) узгодити подальші дії з ЦРП у разі виникнення збоїв у роботі АКЗІ під час відкривання банківського дня (на стадії переходу на роботу з використанням АКЗІ).

22. Адміністратор інформаційної безпеки для заміни АКЗІ та/або СК зобов’язаний:

1) протягом трьох робочих днів повідомити Департамент інформаційної безпеки про перехід на використання програмних ЗЗІ АРМ-СЕП;

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

3) зробити відмітку про повернення АКЗІ та/або СК, що виведені з експлуатації, у розділі ІІ журналу обліку адміністратора інформаційної безпеки (додаток 1);

4) провести відповідне службове розслідування в разі пошкодження АКЗІ/СК/голографічної наклейки, втрати АКЗІ або СК, копію матеріалів якого подати до Департаменту інформаційної безпеки;

5) отримати ЗЗІ на заміну та зробити відповідний запис у розділі ІІ журналу обліку адміністратора інформаційної безпеки (додаток 1);

6) видати адміністратору АРМ-СЕП отримані ЗЗІ відповідно до пунктів 17 – 19 розділу IV цих Правил;

7) протягом трьох робочих днів повідомити Департаменту інформаційної безпеки про перехід на роботу з АКЗІ.

23. Адміністратор АРМ-СЕП зобов’язаний перейти на роботу з резервною СК у разі виходу з ладу СК. Адміністратор інформаційної безпеки, зобов’язаний звернутися до Департаменту інформаційної безпеки для заміни СК, що вийшла з ладу, у тому самому порядку, за яким ця СК була отримана відповідно до розділу ІІІ Положення про захист.

V. Порядок роботи з програмними ЗЗІ

24. Адміністратор інформаційної безпеки після отримання ПМГК зобов’язаний:

1) зробити відповідний запис у розділах ІІ і VІІ журналу обліку адміністратора інформаційної безпеки (додаток 1);

2) зняти копію ПМГК за допомогою засобів, які є на ПМГК;

3) зареєструвати копію ПМГК у розділах ІІ і VІІ журналу обліку адміністратора інформаційної безпеки (додаток 1);

4) здійснити перевірку ПМГК шляхом пробної генерації ключів;

5) забезпечити генерацію ключів для всіх робочих місць (діючі ТК мають право використовуватися до закінчення строку їх дії).

25. Адміністратор інформаційної безпеки в разі неможливості зняти копію ПМГК або в разі невдалої генерації ключа зобов’язаний повідомити про це Департамент інформаційної безпеки системою електронної пошти Національного банку протягом одного робочого дня і діяти відповідно до його рекомендацій.

26. Адміністратори інформаційної безпеки зобов’язані під час обміну ПМГК і його копіями між собою робити відповідні записи в розділі VІІ журналу обліку адміністратора інформаційної безпеки (додаток 1).

27. Адміністратор інформаційної безпеки зобов’язаний зберігати ПМГК і його копію в неробочий час і в робочий час, якщо він не використовується в роботі, у сейфі. Адміністратор інформаційної безпеки зобов’язаний замкнути й опечатати сейф відбитком особистої печатки.

28. Після завершення строку використання ПМГК організація зобов’язана знищити ПМГК та його копію на місці методом, який унеможливлює їх відновлення, і скласти акт про знищення засобів захисту інформації Національного банку України (додаток 7) у двох примірниках та подати цей акт

Департаменту інформаційної безпеки під час отримання нового ПМГК у територіальному управлінні. Департамент інформаційної безпеки зберігає один примірник цього акта, організація – другий.

Адміністратор інформаційної безпеки зобов’язаний зробити відповідний запис про знищення ПМГК та його копії із зазначенням номерів і дат акта про знищення засобів захисту інформації Національного банку України у розділі ІІ журналу обліку адміністратора інформаційної безпеки (додаток 1).

29. Адміністратор інформаційної безпеки в разі псування носія з ПМГК до завершення строку його використання зобов’язаний:

1) відновити ПМГК із резервної копії;

2) зробити відповідний запис у розділі ІІ журналу обліку адміністратора інформаційної безпеки (додаток 1);

3) повідомити Департамент інформаційної безпеки засобами системи електронної пошти Національного банку про заміну копії ПМГК і нові номери сеансів генерації ключів, які надаватимуться цією копією ПМГК під час наступних сеансів генерації ключів.

30. Адміністратор інформаційної безпеки в разі втрати ПМГК (та/або його копії) або втрати контролю за місцезнаходженням ПМГК та/або його копії зобов’язаний:

1) проінформувати про це Департамент інформаційної безпеки засобами системи електронної пошти Національного банку і замовити новий ПМГК (додаток 8);

2) не проводити генерації ключів до отримання нового ПМГК;

3) провести службове розслідування, копію матеріалів якого подати Департаменту інформаційної безпеки;

4) отримати новий ПМГК відповідно до встановленого порядку і надалі вживати заходів, що передбачені в пунктах 24 – 28 розділу V цих Правил.

31. Організація зобов’язана здійснити заміну ПМГК відповідно до пункту 30 розділу V цих Правил без службового розслідування, не припиняючи роботи в СЕП та/або в інформаційних задачах, якщо один з адміністраторів інформаційної безпеки звільняється від обов’язків адміністратора інформаційної безпеки.

32. Відповідальна особа, яка працюватиме з ключем, зобов’язана генерувати кожен ключ за допомогою ПМГК на робочому місці, яке відповідає вимогам пункту 75 розділу VIII цих Правил, у присутності адміністратора інформаційної безпеки.

Адміністратор інформаційної безпеки зобов’язаний реєструвати всі спроби генерації ключів, у тому числі й невдалі, у розділі III журналу обліку адміністратора інформаційної безпеки (додаток 1).

33. З метою підвищення рівня інформаційної безпеки організація має право використовувати захищені носії ТК, використання яких погоджено Департаментом інформаційної безпеки.

Департамент інформаційної безпеки надає відповідні криптобібліотеки підтримки носіїв ТК, рекомендації щодо налаштування доступу до ТК програмної частини системи захисту інформації та програмне забезпечення для перенесення ТК з ГМД на захищений носій ТК. Відповідальна особа здійснює перенесення ТК за допомогою вищезазначеного програмного забезпечення з реєстрацією як операції зі створення копії ТК відповідно до пункту 34 розділу V цих Правил. Після перенесення ТК відповідальна особа зобов’язана знищити ТК на ГМД відповідно до пункту 46 розділу V цих Правил.

Відповідальна особа зобов’язана здійснювати перенесення власного ТК з ГМД на апаратний носій на окремому немережевому комп’ютері в присутності адміністратора інформаційної безпеки.

ВК після їх генерації (ключі операціоністів САБ сертифікації не потребують) підлягають сертифікації в Національному банку.

34. 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, і з обов’язковим здійсненням запису в розділі III журналу обліку адміністратора інформаційної безпеки (додаток 1).

35. Відповідальна особа, яка проводить генерацію ключа і надалі працює з ним, зобов’язана встановити індивідуальний пароль для ТК (за необхідності – його копії) і не має розголошувати пароль жодній особі (крім випадків, якщо передбачено передавання ТК робочого місця іншій відповідальній особі).

36. На створені копії ПМГК і ТК поширюються всі вимоги щодо інформаційної безпеки, як і на основні ЗЗІ.

37. У разі використання захищених носіїв ТК відповідальна особа самостійно забезпечує зберігання таких носіїв.

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

38. У разі використання на робочих місцях САБ та/або інформаційних задач, що функціонують в операційному середовищі UNIX із ЗЗІ, заборонено використовувати незахищені носії ТК.

У такому разі після генерації ТК відповідальна особа, адміністратор інформаційної безпеки або адміністратор САБ забезпечують копіювання цього файла з ТК у захищену директорію, яка доступна для читання тільки з робочого місця саме цієї відповідальної особи, з відповідним записом у журналі обліку адміністратора інформаційної безпеки та обов’язковим підписом особи, яка копіювала ТК у захищену директорію.

39. У разі використання незахищеного носія ТК відповідальна особа зобов’язана зберігати ТК (і за необхідності їх копії) у неробочий час у власному сейфі, який має бути замкнутий і опечатаний відбитком її особистої печатки.

40. Відповідальні особи зобов’язані дотримуватися правил використання та зберігання ТК для унеможливлення їх несанкціонованого копіювання в разі використання незахищених носіїв ТК.

41. Адміністратор інформаційної безпеки має право забезпечити зберігання ТК відповідальних осіб у неробочий час у власному сейфі, якщо немає достатньої кількості особистих сейфів.

Адміністратор інформаційної безпеки зобов’язаний зберігати кожний ТК в окремій упаковці, що опечатується відбитком особистої печатки відповідальної особи, або в окремому запечатаному конверті з особистим підписом відповідальної особи.

Адміністратор інформаційної безпеки зобов’язаний видавати ТК відповідальним особам для роботи і приймати їх на зберігання з реєстрацією в розділі VIII журналу обліку адміністратора інформаційної безпеки (додаток 1).

42. Адміністратори АРМ-СЕП/АРМ-НБУ-інф зобов’язані передавати ТК АРМ-СЕП/АРМ-НБУ-інф (і за необхідності їх копії) між собою із здійсненням запису в журналі приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф (додаток 5).

43. ТК мають обмежений строк дії, що встановлюється під час сертифікації ВК. Для ключів операціоністів, які не підлягають сертифікації, строк дії ключа становить 100 днів.

Відповідальна особа зобов’язана здійснювати своєчасну генерацію ТК у зв’язку із закінченням строку його дії.

44. Адміністратор інформаційної безпеки організації зобов’язаний вести архів ВК операціоністів для забезпечення можливості перевірки ЕЦП операціоністів протягом усього строку зберігання архівів електронних банківських документів.

Строк зберігання архівів ВК операціоністів відповідає строку зберігання електронних банківських документів.

45. Адміністратор інформаційної безпеки зобов’язаний здійснювати контроль за строком дії ключів, забезпечувати своєчасну їх генерацію відповідальними особами і відправлення ВК на сертифікацію з метою уникнення невиправданої зупинки роботи організації.

46. Відповідальна особа зобов’язана знищувати ТК (та їх копії) після закінчення строку дії і здійснювати відповідний запис у розділі ІІІ журналу обліку адміністратора інформаційної безпеки (додаток 1).

ТК не вносяться до архіву електронних банківських документів.

47. Відповідальна особа в разі псування носія ТК до завершення строку його дії зобов’язана:

1) зняти ще одну копію ТК (у разі її наявності) або здійснити нову генерацію цього ключа;

2) здійснити відповідні записи в розділі ІІІ журналу обліку адміністратора інформаційної безпеки (додаток 1).

48. Відповідальна особа в разі компрометації ТК зобов’язана припинити використання цього ТК і повідомити адміністратора захисту інформації.

49. Адміністратор захисту інформації в разі компрометації ТК зобов’язаний:

1) повідомити системою електронної пошти Національного банку Департамент інформаційної безпеки, якщо це був ТК АРМ-СЕП або АРМ бухгалтера САБ;

2) забезпечити вилучення відповідного ВК з ТВК (за допомогою ПМГК) у встановленому порядку;

3) забезпечити генерацію нового ТК і надалі вживати заходів щодо його введення в дію.

50. Організація зобов’язана в разі втрати контролю за ТК провести службове розслідування, копії матеріалів якого подати до Департаменту інформаційної безпеки.

51. 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.

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

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

53. Організація зобов’язана вжити заходів для усунення загрози втрати ЗЗІ, електронних архівів, комп’ютерної техніки тощо в разі виникнення надзвичайної ситуації (пожежа, вибух, стихійне лихо тощо). Дії працівників організації, які використовують ЗЗІ, регламентуються відповідною довідкою про дії відповідальних осіб у разі виникнення надзвичайних ситуацій, що складається в довільній формі, підписується керівником організації і зберігається у справі адміністратора інформаційної безпеки. Відповідальні особи повинні зберігати виписку з цієї довідки на своїх робочих місцях.

54. Організація має право визначити тимчасовий порядок використання та зберігання ЗЗІ (за попереднім узгодженням з Департаментом інформаційної безпеки і дотриманням вимог цих Правил) за необхідності:

1) роботи протягом одного робочого дня в приміщенні іншої організації в разі виникнення аварійної ситуації (відключення електроживлення, пошкодження ліній зв’язку тощо);

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

3) проведення ремонтних робіт.
Організація в такому випадку зобов’язана затвердити цей порядок і його копію в паперовій або електронній формі надіслати Департаменту інформаційної безпеки.

VII. Організація діловодства з питань інформаційної безпеки

55. Діловодство з питань інформаційної безпеки в організації ведуть:

1) адміністратор інформаційної безпеки;

2) адміністратор АРМ-СЕП/АРМ-НБУ-інф;

3) відповідальні особи, які використовують єдиний ТК.

56. Адміністратор інформаційної безпеки зобов’язаний вести:

1) справу адміністратора інформаційної безпеки;

2) журнал обліку адміністратора інформаційної безпеки (додаток 1).

57. Адміністратор інформаційної безпеки зобов’язаний зберігати в справі адміністратора інформаційної безпеки такі документи:

1) копії нормативно-правових актів та рекомендації Національного банку з питань інформаційної безпеки;

2) довідку про останню перевірку Департаментом інформаційної безпеки стану інформаційної безпеки;

3) зобов’язання відповідальних осіб (додатки 2, 3);

4) акти про приймання-передавання апаратних засобів захисту інформації Національного банку України (додаток 2 до Положення про захист) та/або супровідні листи до ЗЗІ, які перебувають у використанні;

5) акт про знищення засобів захисту інформації Національного банку України (додаток 7);

6) листи про надання ЗЗІ (додаток 8);

7) акт про повернення до Департаменту інформаційної безпеки, знищення і передавання до архіву засобів захисту інформації Національного банку України, справ і журналів обліку (додаток 3 до Положення про захист);

8) довідку про дії відповідальних осіб у разі виникнення надзвичайних ситуацій з підписом керівника організації;

9) інші документи з питань інформаційної безпеки.
До справи адміністратора інформаційної безпеки не включаються документи, що не стосуються інформаційної безпеки.

58. Листи Національного банку (або їх копії) з питань інформаційної безпеки, експлуатації СЕП у частині, що стосується захисту інформації в СЕП, які надходять системою електронної пошти Національного банку, повинні або включатися до справи адміністратора інформаційної безпеки або реєструватися, зберігатися і знищуватися відповідно до правил діловодства організації.

59. Адміністратор АРМ-СЕП/АРМ-НБУ-інф зобов’язаний вести журнал приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф (додаток 5), у якому реєструються всі переміщення і зміни ЗЗІ на АРМ-СЕП/АРМ-НБУ-інф.

60. Відповідальні особи зобов’язані вести журнал приймання-передавання таємних ключів робочих і технологічних місць (додаток 6) у разі передавання ТК робочого місця іншій відповідальній особі.

VIII. Вимоги до приміщень

61. Організація, яка використовує АРМ-СЕП/АРМ-НБУ-інф, зобов’язана розмістити їх в одному або окремих приміщеннях (крім приміщення адміністратора інформаційної безпеки) з обмеженим доступом, двері яких повинні бути оснащені кодовим або автоматичним замком і місцем для опечатування або системою контролю доступу, яка забезпечуватиме персоніфіковану реєстрацію входу/виходу осіб у спеціальному електронному журналі.

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

62. Дозволяється розміщувати комп’ютер з АРМ-СЕП/АРМ-НБУ-інф у серверному приміщенні, якщо цей програмно-апаратний комплекс працює в автоматичному режимі. У цьому разі адміністратор АРМ-СЕП зобов’язаний реагувати на інформаційні повідомлення, які надсилаються на АРМ-СЕП.

63. Організація зобов’язана установити ґрати на вікно (вікна) у приміщенні АРМ-СЕП, якщо воно:

1) внутрішнє і виходить в інше приміщення або коридор організації;

2) зовнішнє і розташовується на першому чи останньому поверсі організації;

3) зовнішнє і розташовується на інших поверхах організації, до яких є доступ з прилеглих об’єктів.

64. Організація зобов’язана обладнати приміщення з АРМ-СЕП/АРМ-НБУ-інф системою охоронної сигналізації з двома рубежами захисту:

1) перший – датчики охорони периметра;

2) другий – датчики контролю за переміщенням об’єктів у приміщенні.

65. Організація зобов’язана встановити в приміщенні з АРМ-СЕП/АРМ-НБУ-інф сейфи (металеві шафи), призначені для зберігання в неробочий час ЗЗІ і документів до них.

66. Адміністратор інформаційної безпеки зобов’язаний обліковувати ключі від сейфів (металевих шаф) і печатки для їх опечатування в розділах V і VI журналу обліку адміністратора інформаційної безпеки (додаток 1).

67. Адміністратор АРМ-СЕП/АРМ-НБУ-інф під час виконання своїх обов’язків зобов’язаний:

1) зберігати ключі від вхідних дверей приміщення з АРМ-СЕП/АРМ-НБУ-інф і сейфів (металевих шаф) у робочий час;

2) замикати або блокувати системою доступу приміщення з АРМ-СЕП/АРМ-НБУ-інф у разі своєї відсутності.

68. Адміністратор АРМ-СЕП/АРМ-НБУ-інф має право зберігати ключі від сейфів (металевих шаф) адміністратора АРМ-СЕП/АРМ-НБУ-інф в опечатаному вигляді в тому самому приміщенні.

69. Організація зобов’язана призначати працівників, які мають допуск до приміщення з АРМ-СЕП/АРМ-НБУ-інф з правом самостійної роботи, внутрішнім документом, у якому повинні зазначатися всі відповідальні особи і ЗЗІ, які вони використовують.

Адміністратор інформаційної безпеки обліковує призначених осіб у розділі VI журналу обліку адміністратора інформаційної безпеки (додаток 1).

70. Право допуску до приміщення з АРМ-СЕП/АРМ-НБУ-інф під контролем відповідальних осіб відповідно до пункту 69 мають:

1) керівник організації (або особа, яка виконує його обов’язки);

2) заступник керівника організації, який призначений відповідальним за організацію інформаційної безпеки;

3) адміністратори інформаційної безпеки;

4) інші працівники організації, які обслуговують приміщення й АРМ-СЕП/АРМ-НБУ-інф;

5) представники Департаменту інформаційної безпеки, які здійснюють перевірку стану інформаційної безпеки в організації.

71. Працівники служби інформаційної безпеки організації (якщо вони не призначені внутрішнім документом організації як відповідальні особи за роботу із ЗЗІ) мають право доступу до приміщення з АРМ-СЕП/АРМ-НБУ-інф лише для вирішення питань, що належать до їх компетенції.

72. Працівники організації, які мають право доступу до приміщення з АРМ-СЕП/АРМ-НБУ-інф, зобов'язані перебувати в приміщенні з АРМ-СЕП/АРМ-НБУ-інф лише в присутності адміністратора АРМ-СЕП/АРМ-НБУ-інф та на час виконання своїх обов'язків, пов'язаних з роботою АРМ-СЕП/АРМ-НБУ-інф або обслуговуванням приміщення.

Працівники організації мають право доступу до приміщення з АРМ-СЕП/АРМ-НБУ-інф для вирішення окремих питань на підставі усного розпорядження керівника організації (або особи, яка виконує його обов'язки) лише в присутності адміністратора АРМ-СЕП/АРМ-НБУ-інф.

73. У разі зміни свого місцезнаходження або місцезнаходження АРМ-СЕП/АРМ-НБУ-інф організація зобов'язана повідомляти Департамент інформаційної безпеки про місця розташування АРМ-СЕП/АРМ-НБУ-інф протягом трьох робочих днів із часу настання цих змін.

Департамент інформаційної безпеки зобов'язаний організувати перевірку виконання вимог до приміщень протягом п'яти робочих днів із дня надходження цього повідомлення зі складанням відповідної довідки.

74. Організація зобов'язана розмістити робоче місце адміністратора інформаційної безпеки в окремому приміщенні з обмеженим доступом та обладнати його сейфом для зберігання ЗЗІ, справ і журналу обліку адміністратора інформаційної безпеки тощо. Це приміщення повинно обладнуватися системою охоронної сигналізації з одним рубежем захисту та в неробочий час опечатуватися.

75. Робоче місце адміністратора інформаційної безпеки повинно бути обладнане комп'ютером, не підключеним до локальної мережі організації, для копіювання носіїв ТК і генерування ключів відповідальними особами.

76. Забороняється розміщувати АРМ-СЕП, АРМ бухгалтера САБ та робоче місце адміністратора інформаційної безпеки в одному приміщенні (у будь-яких комбінаціях).

77. Організація зобов’язана розмістити робочі місця САБ, на яких використовуються ЗЗІ, у приміщеннях з обмеженим доступом, та в разі використання незахищених носіїв ТК обладнати робочі місця окремими або багатосекційними сейфами чи багатосекційними металевими шафами з засобами опечатування для зберігання ТК.

Сейф з кодовим замком також має обладнуватися місцем для опечатування, що дасть змогу виявляти спроби його несанкціонованого відкривання.

78. Організація зобов’язана забезпечити надійне кріплення сейфа для зберігання ЗЗІ, який має вагу менше ніж 100 кг і хоча б один з габаритів якого менший ніж 500 мм, до підлоги, стіни тощо.

79. Організація зобов’язана здійснити заміну відповідного замка або сейфа і провести службове розслідування в разі втрати ключів від сейфів (металевих шаф), у яких зберігаються ЗЗІ.

Адміністратор інформаційної безпеки зобов’язаний зберігати матеріали розслідування в справі адміністратора інформаційної безпеки.

80. Керівник організації відповідає за виконання вимог до приміщень.

Директор Департаменту інформаційної безпеки Д. О. Лук’янов

ПОГОДЖЕНО
Заступник Голови
Національного банку України
________________ Я. В. Смолій
(підпис)
“_26_” ___11______ 2015 року
(дата)

Додаток 1
до Правил
(підпункт 6 пункту 4 розділу II)

Журнал обліку адміністратора інформаційної безпеки

Розділ I. Перелік відповідальних за роботу із засобами захисту інформації Національного банку України осіб:

№ з/п	Прізвище, ініціали відповідальної особи	Функціональні обов’язки	Дата і номер документа про призначення	Дата і номер документа про звільнення від функціональних обов’язків	Причина звільнення
1	2	3	4	5	6

Розділ II. Перелік засобів захисту інформації Національного банку України:

№ з/п	Дата отримання (копіювання)	Назва	Дата і підпис відповідальної особи про отримання	Дата і підпис відповідальної особи про повернення	Примітки
1	2	3	4	5	6

Примітка: у колонці 6 за потреби робляться короткі робочі записи про факти втрати контролю за засобами захисту інформації тощо.

Розділ III. Перелік таємних ключів, що генерувалися в організації відповідальними особами:

№ з/п	Назва ТК	Назва файла ТК або номер захищеного носія ТК	Операція (генерація/ копіювання/генерація на видалення)	Дата і підпис відповідальної особи, яка генерувала/ копіювала та отримала ТК	Дата і підпис відповідальної особи, яка знищувала ТК	Дата і підпис відповідальної особи, яка вилучила ВК з ТВК
1	2	3	4	5	6	7

Продовження додатка 1

Розділ IV. Перелік осіб, які мають допуск до приміщення з АРМ-СЕП/АРМ-НБУ-інф:

№ з/п	Прізвище, ініціали особи, яка має допуск до приміщення з АРМ-СЕП/АРМ-НБУ-інф	Функціональні обов’язки	Дата і номер документа про допуск	Дата і номер документа про скасування допуску	Примітки
1	2	3	4	5	6

Розділ V. Перелік ключів від сейфів (металевих шаф) відповідальних осіб, у яких зберігаються засоби захисту інформації Національного банку України:

№ з/п	Призначення ключа	№ ключа	Прізвище, ініціали відповідальної особи, яка зберігає ключ	Примітки
1	2	3	4	5

Розділ VI. Перелік особистих печаток (штампів, пломбіраторів) відповідальних осіб для опечатування засобів захисту інформації Національного банку України:

№ з/п	№ печатки (штампів, пломбіраторів)	Прізвище, ініціали відповідальної особи	Примітки
1	2	3	4

Розділ VII. Облік приймання-передавання засобів захисту інформації Національного банку України, за які несе відповідальність адміністратор інформаційної безпеки:

№ з/п	Назва, версія, дата виготовлення засобів захисту інформації	Дата, час отри-мання	Підпис адміністратора інформаційної безпеки 1-ї зміни	Дата, час отри-мання	Підпис адміністратора інформаційної безпеки 2-ї зміни
1	2	3	4	5	6

Примітка.

Відмітки про приймання-передавання засобів захисту інформації Національного банку України робляться щодня в разі двозмінної роботи адміністратора інформаційної безпеки або у зв’язку з відсутністю основного адміністратора інформаційної безпеки – відпустка, навчання, хвороба тощо.

Розділ VIII. Облік приймання-передавання таємних ключів відповідальних осіб, що зберігаються в адміністратора інформаційної безпеки організації:

№ з/п	Назва файла ТК або номер захищеного носія ТК	Дата, час отримання	Підпис відповідальної особи	Дата, час повернення	Підпис адміністратора інформаційної безпеки	Примітки
1	2	3	4	5	6	7

Примітки:

не враховуються таємні ключі тих операторів робочих і технологічних місць САБ, які зберігають власні таємні ключі в особистих сейфах;

якщо оператор (операціоніст) не отримав власного таємного ключа для роботи, то в колонках 3 і 4 ставиться прочерк;

якщо строк дії таємного ключа закінчився, то в колонках 5 і 6 робиться відмітка про це;

у разі потреби допускається ведення не загального обліку таємних ключів, а індивідуального – за кожною відповідальною особою;

допускається зберігання облікових форм у швидкозшивачах. У цьому разі швидкозшивач є додатком до журналу обліку.

Розділ IX. Облік перевірок дотримання правил використання і зберігання засобів захисту інформації Національного банку України, проведених адміністратором інформаційної безпеки організації:

№ з/п	Дата перевірки	Порушення виявлено/не виявлено	Опис порушення	Підпис адміністратора інформаційної безпеки
1	2	3	4	5

Додаток 2
до Правил
(пункт 6 розділу ІІ)

Зобов’язання
адміністратора інформаційної безпеки

____
(найменування організації)

Я, ____, який призначений
(посада, прізвище, ім’я, по батькові)
згідно з внутрішнім документом від “___” _____________ 20__ р. № _______ адміністратором інформаційної безпеки організації, ознайомлений з правилами використання, зберігання й обліку засобів захисту інформації та інформаційної безпеки під час роботи з електронними банківськими документами і зобов’язуюся:

1. Забезпечувати та контролювати виконання режимних вимог до приміщень, у яких обробляються електронні документи, використовуються і зберігаються засоби захисту інформації Національного банку України.

2. Забезпечувати отримання, зберігання, облік і контроль за використанням засобів захисту інформації Національного банку України.

3. Виконувати правила використання і зберігання засобів захисту інформації Національного банку України та здійснювати контроль за технологією оброблення електронних банківських документів.

4. Знати нормативно-правові акти Національного банку України з питань інформаційної безпеки та здійснювати контроль за їх виконанням відповідальними особами.

5. Надавати інформацію щодо інформаційної безпеки Департаменту інформаційної безпеки Національного банку України на його запити.

6. Підтримувати зв’язок з Департаментом інформаційної безпеки Національного банку України з питань інформаційної безпеки.

7. Передати всі засоби захисту інформації, ключі від сейфів, особисті печатки тощо в установленому порядку в останній день роботи в разі звільнення з роботи.

8. Забезпечувати конфіденційність системи захисту інформації організації, постійно вживати заходів щодо підвищення рівня захищеності інформації в організації.

Продовження додатка 2

____

(дата, підпис)

Знання нормативно-правових актів Національного банку України з питань інформаційної безпеки, затверджених постановою Правління Національного банку України від __ ________ 2015 року № _____, перевірено.

Представник Департаменту
інформаційної безпеки
Національного банку України ______________________________

(підпис, ініціали, прізвище)

Додаток 3
до Правил
(пункт 7 розділу II)

Зобов’язання

Я, ____, який призначений
(посада, прізвище, ім’я, по батькові)
згідно з внутрішнім документом____
(найменування організації)
від “___” _____ 20__ р. № ___ виконувати обов’язки _______________________
(адміністратора/оператора та назва АРМ)
ознайомлений з правилами використання засобів захисту інформації під час роботи з електронними банківськими документами і зобов’язуюся:

1. Виконувати правила використання та зберігання власних таємних ключів і дотримуватися технології оброблення електронних банківських документів.

2. Не передавати іншим особам власні таємні ключі.

3. Не розголошувати мережеві паролі, паролі входу до системи автоматизації банку, інших програмно-технічно комплексів і пароль власного таємного ключа.

4. У разі спроби інших осіб отримати від мене засоби захисту інформації, підозри щодо втрати контролю за своїми таємними ключами або їх втрати негайно повідомити про це адміністратора інформаційної безпеки організації.

5. У разі звільнення з роботи в останній день роботи повернути адміністратору інформаційної безпеки організації всі засоби захисту інформації, ключі від сейфів, особисті печатки тощо.

6. Дотримуватися вимог щодо забезпечення конфіденційность системи захисту інформації організації.

Я, _________________________________, попереджений про те, що всі
(прізвище, ім’я, по батькові)
електронні банківські документи, які мають електронний цифровий підпис, зроблений з використанням мого таємного ключа, уважаються підтвердженими мною, а електронний цифровий підпис – накладеним мною.

____
(дата, підпис)

Знання правил використання та зберігання таємних ключів перевірено.
Адміністратор інформаційної безпеки _____________________________
(підпис, ініціали, прізвище)

Додаток 4
до Правил
(пункт 10 розділу II)

Таблиця
суміщення функціональних обов’язків

№ з/п	Функціональні обов’язки	Адміністратор інформаційної безпеки	Адміністратор АРМ-СЕП/ АРМ-НБУ-інф	Оператор АРМ бухгалтера (ключ типу В)	Оператор АРМ технолога (ключ типу А)	Операціоніст САБ	Оператор АРМ інформаційних задач	Адміністратор САБ	Відповідальний за розроблення САБ	Адміністратор локальної мережі	Адміністратор електронної пошти
1	2	3	4	5	6	7	8	9	10	11	12
1	Адміністратор інформаційної безпеки	-	Х	Х	Х	Х	Х	В	Х	В	В
2	Адміністратор АРМ-СЕП/АРМ-НБУ-інф	Х	-	Х	В	Д	Д	Х	Х	В	В
3	Оператор АРМ бухгалтера (ключ типу В)	Х	Х	-	Х	Х	Д	Х	Х	В	В
4	Оператор АРМ технолога (ключ типу А)	Х	В	Х	-	Х	Д	Д	Х	В	В

Продовження додатка 4

Продовження таблиці

1	2	3	4	5	6	7	8	9	10	11	12
5	Операціоніст САБ	Х	Д	Х	Х	-	Д	Х	Х	В	В
6	Оператор АРМ інформаційних задач	Х	Д	Д	Д	Д	-	Д	Д	Д	Д
7	Адміністратор САБ	В	Х	Х	Д	Х	Д	-	В	Д	Д
8	Відповідальний за розроблення САБ	Х	Х	Х	Х	Х	Д	В	-	Х	Х
9	Адміністратор локальної мережі	В	В	В	В	В	Д	Д	Х	-	Д
10	Адміністратор електронної пошти	В	В	В	В	В	Д	Д	Х	Д	-

Примітки:

Д – суміщення обов’язків дозволено (не більше двох обов’язків одночасно);

В – суміщення можливе як виняток (не більше двох обов’язків одночасно) на час тимчасової відсутності відповідальної особи (хвороба, відпустка), яка виконує ці функції. Якщо суміщення викликано іншими причинами, то необхідно звернутися до Департаменту інформаційної безпеки Національного банку України для отримання відповідного дозволу на таке суміщення;

Х – суміщення обов’язків не дозволено.

Додаток 5
до Правил
(підпункт 12 пункт 12
розділу ІІІ)

Журнал
приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф

№ з/п	Дата	Час отримання засобів захисту з сейфа	Прізвище, ініціали, підпис адміністратора АРМ-СЕП/ АРМ-НБУ-інф 1-ї зміни	Час отримання засобів захисту від 1-ї зміни	Прізвище, ініціали, підпис адміністратора АРМ-СЕП/ АРМ-НБУ-інф 2-ї зміни	Час повернення засобів захисту до сейфа	Прізвище, ініціали, підпис адміністратора АРМ-СЕП/ АРМ-НБУ-інф 2-ї зміни	№ печатки
1	2	3	4	5	6	7	8	9

Примітки.

Адміністратори АРМ-СЕП/АРМ-НБУ-інф вносять до журналу записи про всі переміщення і зміни засобів захисту інформації Національного банку України АРМ-СЕП/АРМ-НБУ-інф.

Адміністратори АРМ-СЕП мають право не відключати АКЗІ від комп’ютера під час передавання зміни та після закінчення роботи.

Додаток 6
до Правил
(підпункт 11 пункту 13
розділу IV)

Журнал
приймання-передавання таємних ключів робочих і технологічних місць

№ з/п	Назва ТК	Дата, час отримання	Підпис відповідальної особи 1-ї зміни	Дата, час отримання	Підпис відповідальної особи 2-ї зміни
1	2	3	4	5	6

Примітка.

Відповідальні особи зобов’язані вносити до журналу записи про приймання-передавання таємних ключів щодня в разі їх двозмінної роботи або у зв’язку з відсутністю основної відповідальної особи – відпустка, навчання, хвороба тощо.

Додаток 7
до Правил
(пункт 28 розділу V)

ЗАТВЕРДЖЕНО
Керівник (заступник керівника)
організації
____
(підпис, ініціали, прізвище)
“___” ___________ 20__ р.
М. П.

Акт
про знищення засобів захисту інформації Національного банку України

м. __________ “___” _________ 20__ р.

Я, ____, адміністратор
(прізвище, ім’я, по батькові)
інформаційної безпеки відповідно до листа Департаменту інформаційної безпеки Національного банку України від “___” ________ 20__ р. № _____ знищив програмний модуль генерації ключів та його копію (версія ________, дата виготовлення ____________) згідно з Правилами організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженими постановою Правління Національного банку України від ___ ___________ 2015 року № _____.

Адміністратор інформаційної безпеки ________________________________
(підпис, ініціали, прізвище)

Додаток 8
до Правил
(пункт 30 розділу V)

ЕЛЕКТРОННА ПОШТА

Найменування організації Національний банк України
Департамент інформаційної безпеки

____
(дата, № документа)

Просимо надати новий програмний модуль генерації ключів у зв’язку із звільненням (переведенням на іншу посаду) адміністратора інформаційної безпеки ____
(ініціали, прізвище)
(або у зв’язку з утратою чи компрометацією діючого ПМГК. Після вивчення всіх обставин копії матеріалів службового розслідування будуть надіслані на вашу адресу).

Керівник (заступник керівника)
організації _____________________________
(підпис, ініціали, прізвище)

Виконавець __________________
(ініціали, прізвище)
роб. тел. _______________________

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
26 листопада 2015 року № 829

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

І. Загальні положення

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

2. У цьому Положенні терміни та скорочення вживаються в значеннях, визначених Законом України "Про електронні документи та електронний документообіг", Положенням про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженим постановою Правління Національного банку від 26 листопада 2015 року № 829 (далі – Положення про захист), 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 регламентує порядок проведення планових та позапланових перевірок стану інформаційної безпеки в організаціях, які отримали ЗЗІ відповідно до Положення про захист.

4. Виїзні перевірки щодо дотримання організаціями вимог інформаційної безпеки здійснюються Департаментом інформаційної безпеки Національного банку (далі – Департамент інформаційної безпеки) відповідно до Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджених постановою Правління Національного банку від 26 листопада 2015 року № 829 (далі – Правила).

5. Департамент інформаційної безпеки здійснює аналіз стану інформаційної безпеки в організаціях з метою забезпечення безперервного, надійного та ефективного функціонування СЕП та інформаційних задач шляхом:

збору результатів внутрішніх перевірок та оцінювання стану інформаційної безпеки в організаціях;

оцінювання стану інформаційної безпеки в організаціях за результатами виїзних перевірок.

6. Департамент інформаційної безпеки має право вимагати від організацій надання інформації та документів для здійснення контролю за станом інформаційної безпеки шляхом направлення відповідного запиту.

7. Організація зобов’язана надавати Департаменту інформаційної безпеки повну та достовірну інформацію і документи та їх копії належної якості у встановлені строки у визначених порядку та форматі відповідно до Положення про захист та Правил.

8. Департамент інформаційної безпеки забезпечує нерозголошення інформації, отриманої ним під час контролю за станом інформаційної безпеки в організації, третім особам, за винятком випадків, передбачених законодавством України.

II. Контроль за станом інформаційної безпеки в організації

9. Працівник Департаменту інформаційної безпеки, який здійснює перевірку, зобов’язаний мати документи, що підтверджують його особу, і розпорядчий акт про проведення перевірки.

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

11. Працівник Департаменту інформаційної безпеки, який здійснює перевірку, має право:

1) перевіряти використання, облік і зберігання ЗЗІ адміністратором інформаційної безпеки, журнали, справи і документи з питань організації інформаційної безпеки;

2) відвідувати приміщення з АРМ-СЕП/АРМ-НБУ-інф, вивчати умови використання і зберігання ЗЗІ адміністраторами АРМ-СЕП/АРМ-НБУ-інф;

3) відвідувати робочі місця всіх відповідальних за роботу із ЗЗІ осіб (далі – відповідальні особи) в організації і вивчати умови використання та зберігання ними ЗЗІ;

4) перевіряти знання відповідальними особами нормативно-правових актів Національного банку, що регламентують забезпечення інформаційної безпеки, виконання ними рекомендацій Національного банку, їх уміння працювати із ЗЗІ;

5) ознайомлюватися з внутрішніми документами, актами, журналами діяльності автоматизованих програмно-апаратних систем та іншими документами організації, що дають змогу проконтролювати виконання вимог щодо інформаційної безпеки.

12. Департамент інформаційної безпеки проводить планові (не рідше ніж один раз на два роки) і позапланові перевірки.

Підставами для проведення позапланових перевірок є включення організації в СЕП та/або інформаційні задачі, перехід на роботу з однієї моделі обслуговування консолідованого кореспондентського рахунку на іншу, зміна місцезнаходження організації, усунення недоліків, виявлених під час попередньої перевірки.

13. За результатами перевірки складається довідка про результати перевірки стану інформаційної безпеки в організації у двох примірниках. Один примірник цієї довідки зберігається в Департаменті інформаційної безпеки, другий – в організації.

14. У разі виявлення недоліків (порушень) організація зобов’язана повідомити Департамент інформаційної безпеки в установлений термін про вжиття заходів щодо їх усунення.

III. Перевірка готовності організації до включення в СЕП та інформаційні задачі

15. Департамент інформаційної безпеки зобов’язаний перевірити готовність організації до включення в СЕП та інформаційні задачі після вжиття організацією необхідних первинних заходів щодо організації захисту

електронної банківської інформації відповідно до вимог, що визначаються Правилами.

16. Підставою для перевірки є відповідний розпорядчий акт Департаменту інформаційної безпеки.

17. Під час перевірки розглядаються такі питання:

1) наявність технічних можливостей для організації робочих місць відповідальних осіб згідно з розділом VIII Правил;

2) відповідність приміщення з АРМ-СЕП/АРМ-НБУ-інф, з робочим місцем адміністратора інформаційної безпеки, інших приміщень, де використовуватимуться ЗЗІ, вимогам розділу VIII Правил;

3) наявність відповідальних осіб, внутрішнього документа організації про їх призначення і підписаних ними зобов’язань згідно з розділом II Правил;

4) наявність копій нормативно-правових актів Національного банку щодо забезпечення інформаційної безпеки під час роботи із ЗЗІ відповідно до розділу VII Правил;

5) перевірка знань нормативно-правових актів, що регламентують порядок забезпечення інформаційної безпеки під час роботи із ЗЗІ, відповідно до розділу III Правил.

18. За результатами перевірки складається відповідна довідка.
За наявності недоліків, що можуть впливати на безпеку електронних банківських документів, складається довідка із зазначенням виявлених недоліків (зауважень, порушень) та строків їх усунення.

Директор Департаменту інформаційної безпеки Д. О. Лук’янов

ПОГОДЖЕНО
Заступник Голови
Національного банку України
________________ Я. В. Смолій
(підпис)
“_26_” ___11______ 2015 року
(дата)