Офіційно опубліковано
17.06.2022

Правління Національного банку України

П О С Т А Н О В А

13 червня 2022 року Київ № 119

Про внесення змін до деяких нормативно-правових актів Національного банку України з питань захисту інформації та кіберзахисту

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, Закону України “Про платіжні послуги” та з метою приведення нормативно-правових актів Національного банку України з питань захисту інформації та кіберзахисту у відповідність до вимог законодавства України Правління Національного банку України **постановляє:**

1. Унести до постанови Правління Національного банку України від 19 травня 2021 року № 43 “Про затвердження Положення про захист інформації та кіберзахист у платіжних системах” такі зміни:

1) у заголовку слова “у платіжних системах” замінити словами “учасниками платіжного ринку”;

2) у пункті 1 слова “у платіжних системах” замінити словами “учасниками платіжного ринку”.

2. Затвердити Зміни до Положення про захист інформації та кіберзахист у платіжних системах, затвердженого постановою Правління Національного банку України від 19 травня 2021 року № 43, що додаються.

3. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Кирила Шевченка.

4. Постанова набирає чинності з дня введення в дію Закону України “Про платіжні послуги”.

Голова Кирило ШЕВЧЕНКО

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
13 червня 2022 року № 119

Зміни до Положення про захист інформації та кіберзахист у платіжних системах

1. У заголовку Положення слова “у платіжних системах” замінити словами “учасниками платіжного ринку”.

2. У розділі I:

1) у пункті 1 слова “Про платіжні системи та переказ коштів в Україні” замінити словами “Про платіжні послуги”;

2) у пункті 3:

підпункт 2 виключити;

у підпункті 7 слово “систем” замінити словом “послуг”;

підпункт 10 викласти в такій редакції:

“10) ключовий суб’єкт інформаційного захисту – суб’єкт інформаційного захисту, який належить до однієї категорії або більше:

оператор важливої платіжної системи, якщо він виконує функції технологічного оператора платіжних послуг у цій платіжній системі;

важливий технологічний оператор платіжних послуг;

технологічний оператор платіжних послуг, який надає послуги платіжній системі, створеній нерезидентом, та який отримав дозвіл Національного банку України (далі – Національний банк) надавати свої послуги в Україні;

технологічний оператор платіжних послуг, що надає послуги більше ніж одній платіжній системі;”;

у підпункті 13 слова “електронних документів на переказ,” замінити словами “платіжних інструкцій та їх”;

підпункти 14 та 16 викласти в такій редакції:

“14) критичні дані – дані, несанкціоноване використання або втрата яких призводить до порушення інформаційної безпеки або порушення прав користувачів платіжних послуг;”;

“16) суб’єкт інформаційного захисту – надавач платіжних послуг (крім установ електронних грошей, Національного банку, органів державної влади та органів місцевого самоврядування), оператор платіжної системи-резидент та технологічний оператор платіжних послуг у разі надання інших видів послуг, крім оброблення платіжних операцій в міжнародних карткових платіжних системах.”;

3) пункт 4 викласти в такій редакції:

“4. Вимоги цього Положення поширюються на суб’єктів інформаційного захисту, крім філій іноземних платіжних установ, що на законних підставах надають послуги в Україні та використовують засоби захисту інформації відповідно до своїх правил та з урахуванням вимог юрисдикцій, де ці правила були узгоджені, на банки, що є операторами платіжних систем, учасниками платіжних систем та/або надавачами платіжних послуг, у частині питань, що не врегульовані іншими нормативно-правовими актами Національного банку у сфері кіберзахисту та інформаційної безпеки в банківській системі.”;

4) у пункті 5 слова “платіжні системи, створені Національним банком” замінити словами “операторів платіжних систем, функції яких виконує Національний банк, та учасників таких платіжних систем”;

5) у пункті 6:

підпункт 1 викласти в такій редакції:

“1) критичні дані, а також бази даних та інформаційні повідомлення між суб’єктами інформаційного захисту, що містять такі дані;”;

підпункти 2, 3 виключити.

3. У розділі ІІІ:

1) у пункті 11:

в абзаці першому слова “в платіжних системах” замінити словами “під час надання платіжних послуг”;

підпункт 4 викласти в такій редакції:

“4) методику відновлення та захисту критичних даних у разі втрати, компрометації чи пошкодження криптографічних ключів або носіїв критичних даних.

До критичних даних належать:

платіжні інструкції в електронній формі;

вразливі платіжні дані (індивідуальна облікова інформація, особисті криптографічні ключі, паролі доступу, коди операцій, інша інформація, що зазначається в платіжній інструкції та за допомогою якої можуть вчинятися шахрайські дії);

персональні дані;

архіви всіх цих даних;”;

пункт доповнити новим підпунктом такого змісту:

“6) вимоги до захисту платіжних інструкцій в електронній формі від несанкціонованого знищення та модифікації.”;

2) у підпункті 3 пункту 12 слово “багатофакторної” замінити словом “посиленої”;

3) у пункті 13:

в абзаці першому слова “в платіжних системах” замінити словами “під час надання платіжних послуг”;

у підпункті 1 слова “електронних документів на переказ” замінити словами “критичних даних”.

4. У першому реченні абзацу першого пункту 18 розділу V слова “електронних документів на переказ, персональних даних користувачів платіжних систем та архівів цих даних” замінити словами “критичних даних”.

5. У пункті 21 розділу VI:

1) в абзаці першому слова “платіжних систем” замінити словами “платіжних послуг”;

2) у підпункті 2 слово “багатофакторна” замінити словом “посилена”.

6. У розділі VII:

1) у пункті 22 слова “, узгодження з платіжною організацією платіжної системи” та “у платіжній системі” виключити;

2) у пункті 24:

у підпункті 1 слова “платіжних систем” замінити словами “платіжних послуг”;

у підпункті 8 слово “облікових” замінити словами “вразливих платіжних”.

7. Розділ IX доповнити новим пунктом такого змісту:

“30[1]. Обмін інформацією між користувачами, надавачами платіжних послуг з обслуговування рахунку та іншими надавачами платіжних послуг (надавачами платіжних послуг, що отримали право на надання нефінансових платіжних послуг, та надавачами послуг із надання відомостей з рахунків) під час доступу до рахунків користувачів забезпечується за допомогою засобів захисту мережі. Суб’єкт інформаційного захисту зобов’язаний в таких випадках здійснювати шифрування інформації за допомогою криптографічних алгоритмів, які є національними стандартами або які мають позитивний експертний висновок Адміністрації Держспецзв’язку.”.

8. У розділі XI:

1) заголовок розділу після слів “захисту інформації” доповнити словами “, електронних платіжних засобів”;

2) підпункт 3 пункту 34 виключити;

3) розділ доповнити новим пунктом такого змісту:

“35^1. Суб’єкт інформаційного захисту повинен використовувати електронні платіжні засоби, що відповідають таким вимогам:

1) дані в електронній формі, що містяться в електронному платіжному засобі, зберігаються в захищеному від НСД вигляді;

2) дані, що містяться в електронному платіжному засобі, не можуть бути доступними в повному обсязі без додаткового підтвердження права на доступ до цих даних;

3) обмін даними, що містяться в електронному платіжному засобі, між учасниками платіжного ринку може здійснюватися лише в захищеному від НСД вигляді;

4) платіжні додатки, розміщені в апаратно-програмному середовищі електронного платіжного засобу, не можуть використовувати дані інших додатків цього електронного платіжного засобу;

5) у разі використання електронного платіжного засобу в кількох платіжних системах, потрібних для ініціювання платіжної операції, дані кожної окремої платіжної системи повинні зберігатися незалежно одні від одних;

6) криптографічні ключі, що вносяться до електронного платіжного засобу під час його емісії, не можуть бути скопійовані та можуть бути використані лише для шифрування/розшифрування даних або для створення/перевірки електронного підпису;

7) якщо електронний платіжний засіб здійснює генерацію криптографічних ключів або виконує інші криптографічні операції, то проводиться зовнішня незалежна перевірка стійкості до атак цього електронного платіжного засобу.”.

9. Розділ XII викласти в такій редакції:

“XII. Умови використання електронного підпису

36. Філії іноземних платіжних установ або технологічний оператор платіжних послуг, який забезпечує взаємодію з міжнародною платіжною системою, оператором якої є нерезидент, повинні (повинен) укласти договір з оператором такої платіжної системи про визнання електронного підпису.

37. Суб’єкт інформаційного захисту (філія іноземної платіжної установи або технологічний оператор платіжних послуг), якщо платіжна інструкція у формі електронного документа, одержана від оператора міжнародної платіжної системи, не містить визнаного електронного підпису, зобов’язаний створити свій електронний підпис для такої платіжної інструкції відповідно до вимог законодавства України.

38. Суб’єкт інформаційного захисту має право використовувати удосконалений електронний підпис без сертифіката відкритого ключа або чинність відкритого ключа підписувача засвідчується сертифікатом відкритого ключа на договірних засадах. Термін використання особистих ключів та сертифікатів відкритих ключів удосконаленого електронного підпису не повинен перевищувати трьох років.”.

10. Пункт 39 розділу XIII викласти в такій редакції:

“39. Суб’єкт інформаційного захисту зобов’язаний забезпечити розроблення, документування та періодичне оновлення політики управління інцидентами під час надання платіжних послуг, а також заходів, пов’язаних із реалізацією цієї політики.”.

11. У тексті Положення слова “переказ коштів” у всіх відмінках замінити словами “надання платіжних послуг” у відповідних відмінках.