Офіційно опубліковано 09.05.2023

Правління Національного банку України

П О С Т А Н О В А

03 травня 2023 року Київ № 58

Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статті 68 Закону України “Про платіжні послуги”, з метою встановлення для надавачів платіжних послуг вимог щодо порядку застосування автентифікації і посиленої автентифікації та забезпечення електронної взаємодії між суб’єктами платіжних операцій Правління Національного банку України **постановляє:**

1. Затвердити Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку (далі – Положення), що додається.

2. Департаменту безпеки (Олександр Паламарчук) після офіційного опублікування довести до відома учасників платіжного ринку інформацію про прийняття цієї постанови.

3. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Андрія Пишного.

4. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування, крім розділу V Положення, який набирає чинності з дня набрання чинності та введення в дію глави 4 розділу IV Закону України “Про платіжні послуги”.

Голова Андрій ПИШНИЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
03 травня 2023 року № 58

Положення
про автентифікацію та застосування посиленої автентифікації на платіжному ринку

І. Загальні положення

1. Предмет правового регулювання та терміни

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про банки і банківську діяльність", "Про платіжні послуги" (далі – Закон про платіжні послуги), "Про захист інформації в інформаційно-комунікаційних системах", "Про основні засади забезпечення кібербезпеки України", "Про електронні довірчі послуги".

Засадничою основою цього Положення є принцип технологічної нейтральності до методів, які можуть використовувати надавачі платіжних послуг з метою застосування посиленої автентифікації користувачів платіжних послуг.

2. Це Положення встановлює для надавачів платіжних послуг вимоги до:

1) застосування автентифікації користувачів платіжних послуг, застосування посиленої автентифікації у випадках, встановлених Законом про платіжні послуги, а також у випадках, коли надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувачів;

2) захисту конфіденційності та цілісності вразливих платіжних даних;

3) електронної взаємодії на платіжному ринку України між суб'єктами платіжних операцій.

3. Терміни, що використовуються в цьому Положенні, вживаються в таких значеннях:

1) активація – процес, за допомогою якого вразливі платіжні дані, пристрої або програмне забезпечення для цілей автентифікації стають повністю функціональними і готовими до використання користувачем, який має/повинен мати законне право на їх використання;

2) багатоцільовий пристрій – пристрій (планшетний або персональний комп'ютер, мобільний телефон), що використовується для автентифікації користувача платіжної послуги. Після застосування процедури автентифікації

багатоцільовий пристрій набуває функціональних можливостей платіжного пристрою, якщо це потрібно для надання платіжної послуги;

3) безпечне інформаційне середовище – середовище, у якому надавач платіжних послуг забезпечує захист конфіденційності, цілісності, доступності та можливість спостережуваності вразливих платіжних даних;

4) віддалений канал – сукупність телекомунікаційних рішень та програмного забезпечення, призначених для інформаційного обміну між територіально віддаленими засобами дистанційної комунікації;

5) відповідальна особа – працівник надавача платіжних послуг, юридична особа, на яку покладено ведення на договірних засадах певного напряму, та/або позаштатний спеціаліст, зареєстрований як фізична особа – суб'єкт підприємницької діяльності, яка провадить підприємницьку діяльність без створення юридичної особи, або самозайнята особа, на яку органом управління надавача платіжних послуг покладено відповідні функції із забезпечення захисту інформації та кіберзахисту, та які володіють знаннями у сферах захисту інформації та кіберзахисту, безпеки переказу коштів та інформаційних технологій;

6) 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 несанкціоновані або шахрайські дії;

7) заходи безпеки – сукупність заходів з виконання вимог цього Положення та інших вимог, що визначені законами України та нормативно-правовими актами Національного банку України (далі – Національний банк) у сфері захисту інформації та кіберзахисту на платіжному ринку;

8) зловмисне програмне забезпечення – програмне забезпечення, функціонування якого може призвести до порушення безпеки інформації щодо виконання платіжних операцій та вразливих платіжних даних на будь-яких етапах формування, обробки, передавання та зберігання такої інформації, результатом чого є втрата цілісності, конфіденційності, доступності зазначеної інформації, та/або функціонування якого полягає у спостереженні за даними, що формуються, обробляються, передаються та зберігаються під час виконання платіжних операцій або пов'язаних з ними;

9) інтерфейс – сукупність програмно-апаратних засобів, призначених для здійснення функцій електронної взаємодії між різноманітними пристроями та різновидами програмного забезпечення учасників платіжного ринку в інформаційно-телекомунікаційних системах надавача платіжних послуг та/або

мережі загального користування з метою застосування процедур автентифікації та надання фінансових та/або нефінансових платіжних послуг;

10) керівник надавача платіжних послуг – призначена згідно зі статутом або рішенням керуючого органу, або безпосередньо власником надавача платіжних послуг посадова особа, відомості про яку внесені до Державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, та яка діє від імені надавача платіжних послуг, представляє його інтереси в органах державної влади і органах місцевого самоврядування, інших організаціях, а також у відносинах з юридичними особами та громадянами, формує адміністрацію надавача платіжних послуг і вирішує питання діяльності суб'єкта інформаційного захисту в межах та порядку, визначених установчими документами;

11) код автентифікації – результат виконання процедури посиленої автентифікації;

12) MOTO (Mail order/Telephone order) – платіжні операції, що здійснюються шляхом ручного введення реквізитів платіжного інструменту (не платником) та з використанням платіжного пристрою;

13) несанкціоновані або шахрайські дії – вчинення сторонніми особами та/або відповідальними особами дій із втручання в інформаційно-телекомунікаційну систему незаконним та/або протиправним шляхом, що можуть призвести до порушення цілісності, доступності та/або конфіденційності інформації, яка використовується під час надання платіжних послуг;

14) поведінкова модель платника – результат аналізу інформації, що міститься в платіжній інструкції, стосовно прийнятого платником рішення з ініціювання платіжної операції з урахуванням інформації про поведінку платника в минулому щодо використання платіжних послуг;

15) посилена автентифікація – процедура автентифікації користувача, яка передбачає використання двох чи більше сукупностей даних (елементів), що належать до таких різних категорій:

знань [володіння інформацією (даними), що відома лише користувачу];

володінь (застосування матеріального предмета, яким володіє лише користувач);

притаманність [перевірка біометричних даних або інших властивостей (рис, характеристик), притаманних лише користувачу, що відрізняють його від інших користувачів];

16) серія дистанційних платіжних операцій – періодично повторювані платіжні операції, що ініціюються з рахунку платника на користь одного або

декількох отримувачів, згоду на виконання яких було попередньо підтверджено платником за допомогою посиленої автентифікації;

17) список довірених отримувачів – перелік отримувачів, який створює користувач платіжних послуг;

18) сторонні особи – будь які фізичні особи та/або юридичні особи, фізичні особи-підприємці, які не є представниками надавача платіжних послуг та яким не надано керівником надавача платіжних послуг права на обробку інформації, пов’язаної з наданням платіжних послуг;

19) унікальний ідентифікатор сеансу електронної взаємодії – поєднання літер, чисел або символів, визначених надавачем платіжних послуг, відповідно до протоколів платіжних і розрахункових систем або систем обміну повідомленнями, що використовуються для електронної взаємодії з та між суб’єктами платіжних операцій, яке надає змогу відстежувати платіжну операцію.

Інші терміни в цьому Положенні вживаються в значеннях, наведених у законах України та нормативно-правових актах Національного банку з питань захисту інформації та кіберзахисту учасників платіжного ринку.

4. Вимоги цього Положення поширюються на надавачів платіжних послуг.

5. Вимоги цього Положення не поширюються на надавачів обмежених платіжних послуг.

6. Контроль за дотриманням вимог цього Положення, законів України та нормативно-правових актів Національного банку, що регламентують порядок проведення платіжних операцій, здійснює Національний банк.

2. Загальні вимоги до автентифікації

7. Електронна взаємодія надавача платіжних послуг із користувачем здійснюється лише після автентифікації користувача платіжних послуг, який є фізичною особою, або уповноваженого представника користувача, який є юридичною особою. Надавач платіжних послуг зобов’язаний застосовувати посилену автентифікацію користувачів платіжних послуг у випадках, визначених у статті 68 Закону про платіжні послуги.

8. Надавач платіжних послуг використовує механізми і процедури моніторингу операцій для виявлення несанкціонованих або шахрайських дій. Ці механізми і процедури ґрунтуються на аналізі операцій з урахуванням тих складових, що є типовими для користувача платіжних послуг, за умов належного використання вразливих платіжних даних.

9. Процедура автентифікації повинна включати механізми моніторингу спроб несанкціонованих або шахрайських дій з використанням вразливих платіжних даних. Також ця процедура повинна передбачати перевірку, чи має користувач платіжних послуг право доступу до рахунку.

Механізми і процедури моніторингу операцій з переказу коштів повинні враховувати кожний із таких факторів ризику:

1) списки пошкоджених, скомпрометованих або викрадених елементів автентифікації;

2) суму кожної платіжної операції;

3) сценарії шахрайства під час надання платіжних послуг;

4) ознаки зараження зловмисним програмним забезпеченням під час будь-яких сеансів процедури автентифікації;

5) нетипове (аномальне) використання багатоцільового пристрою або програмного забезпечення для здійснення автентифікації.

II. Безпека платіжних операцій із застосуванням посиленої автентифікації користувача платіжних послуг

3. Впровадження заходів безпеки

10. Надавач платіжних послуг відповідно до вимог пункту 2 глави 1 розділу I цього Положення забезпечує документування заходів безпеки із захисту платіжних операцій, оцінює та перевіряє ці заходи на відповідність вимогам Національного банку щодо захисту інформації, кіберзахисту та інформаційної безпеки під час надання платіжних послуг. Перевірки здійснюються відповідальними особами надавача платіжних послуг. Ці відповідальні особи не повинні брати участі в основній операційній діяльності надавача платіжних послуг або надавач платіжних послуг повинен залучати до таких перевірок інших осіб, які є незалежними від надавача платіжних послуг, на підставі відповідних договорів, укладених для цілей перевірки. Такі відповідальні особи повинні мати знання та досвід роботи не менше одного року у сферах захисту інформації та кіберзахисту, безпеки переказу коштів та інформаційних технологій.

11. Надавач платіжних послуг, який скористався правом не застосовувати посиленої автентифікації користувача платіжних послуг, виконавши вимоги, визначені в главі 12 розділу III цього Положення, здійснює не рідше одного разу на рік обов’язкову перевірку впроваджених заходів безпеки із захисту платіжних операцій, реєстрації випадків шахрайства та розрахованого загального коефіцієнта шахрайства для кожного виду платіжної операції. Відповідальні особи, які здійснюють цю перевірку, не повинні брати участі в основній операційній діяльності надавача платіжних послуг або надавач платіжних послуг

залучає до таких перевірок інших осіб, які є незалежними від надавача платіжних послуг, на підставі відповідних правових угод, укладених для цілей перевірки. Такі відповідальні особи повинні мати знання та досвід роботи не менше одного року у сферах захисту інформації та кіберзахисту, безпеки переказу коштів та інформаційних технологій.

12. Результатом перевірки надавача платіжних послуг є оцінка та звіт про відповідність і повноту заходів безпеки, вжитих надавачем платіжних послуг на виконання вимог цього Положення.

13. Надавач платіжних послуг повинен на запит Національного банку надати оцінку та звіт про відповідність і повноту заходів безпеки, вжитих надавачем платіжних послуг на виконання вимог цього Положення, отриманих за результатами проведення перевірки.

4. Код автентифікації

14. Надавач платіжних послуг за результатами процедури посиленої автентифікації користувача платіжної послуги створює код автентифікації. Для створення коду автентифікації надавач платіжних послуг використовує багатоцільові пристрої або програмне забезпечення, призначене для цілей автентифікації користувача платіжних послуг.

Код автентифікації повинен бути стійким до його підробки та стійким до розкриття будь-якого з елементів посиленої автентифікації, з використанням яких цей код було створено. Для забезпечення стійкості коду автентифікації надавач платіжних послуг застосовує такі технологічні рішення, як створення та перевірка справжності одноразових паролів, електронних підписів чи інші підтвердження з використанням криптографічних засобів захисту інформації, що містяться в елементах посиленої автентифікації.

15. Надавач платіжних послуг створює код автентифікації щоразу під час отримання користувачем доступу до рахунку за допомогою засобів дистанційної комунікації, ініціювання дистанційної платіжної операції або під час здійснення будь-яких інших дій у разі підозри вчинення шахрайства (або наявності ризику шахрайства) чи інших неправомірних дій (або наявності ризику вчинення інших неправомірних дій) з урахуванням вимог розділу ІІІ цього Положення.

16. Надавач платіжних послуг для застосування посиленої автентифікації користувача платіжної послуги повинен вжити заходів безпеки, що забезпечують виконання таких вимог:

1) інформація про будь-який з елементів посиленої автентифікації не може бути отримана у разі розкриття коду автентифікації;

2) немає можливості створити новий код автентифікації на основі знання про будь-який інший код автентифікації, що був створений раніше;

3) код автентифікації неможливо підробити.

17. Надавач платіжних послуг повинен забезпечити застосування процедури посиленої автентифікації зі створенням коду автентифікації, включаючи такі заходи безпеки:

1) визнати процедуру із застосування посиленої автентифікації помилковою, якщо під час застосування процедури посиленої автентифікації, з надання віддаленого доступу для здійснення дистанційних платіжних операцій або виконання будь-яких інших дій через віддалений канал з використанням засобів дистанційної комунікації, які можуть сприяти виникненню ризику шахрайства з переказу коштів чи інших зловживань, не вдалося створити код автентифікації відповідно до пункту 14 глави 4 розділу ІІ цього Положення через неможливість здійснення перевірки підтвердження справжності будь-якого елемента автентифікації чи визначити, який саме з елементів є некоректним, спотвореним;

2) кількість невдалих спроб застосування процедури посиленої автентифікації, що можуть здійснюватися послідовно, не повинна перевищувати п’яти. Після досягнення граничної кількості невдалих спроб можливість застосування процедури автентифікації повинно бути тимчасово або постійно заблоковано в порядку, визначеному надавачем платіжних послуг;

3) усі сеанси зв’язку повинні бути захищеними від несанкціонованого доступу до даних автентифікації, переданих під час застосування процедури посиленої автентифікації, та від дій не уповноважених на це сторонніх осіб відповідно до вимог розділу V цього Положення;

4) максимальний час без активності користувача платіжних послуг після проходження посиленої автентифікації та отримання доступу до рахунку з використанням засобів дистанційної комунікації через мережі загального користування не повинен перевищувати десяти хвилин.

18. Надавач платіжних послуг вважає процедуру посиленої автентифікації користувача успішно завершеною після підтвердження ним справжності коду автентифікації.

19. Надавач платіжних послуг не перевіряє справжності коду автентифікації в разі використання права не вимагати застосування посиленої автентифікації. Рішення про ініціювання дистанційної платіжної операції або надання доступу до рахунку за допомогою засобів дистанційної комунікації надавач платіжних послуг приймає за результатом застосування автентифікації користувача платіжних послуг.

20. Надавач платіжних послуг має право здійснювати тимчасове та постійне блокування користувача платіжної послуги. Тривалість тимчасового блокування

і кількість наступних повторних спроб встановлюються надавачем платіжних послуг у його внутрішніх документах, зважаючи на характеристику послуги, що надається, та всі ризики, ураховуючи вимоги глави 2 розділу I цього Положення.

Надавач платіжних послуг зобов'язаний надіслати користувачу платіжної послуги повідомлення, перед тим як встановити постійне блокування можливості застосування процедури автентифікації.

Надавач платіжних послуг зобов'язаний надати користувачу платіжної послуги безпечну процедуру розблокування відповідно до порядку, визначеного у своїх внутрішніх документах, яка дає змогу відновити можливість проходження посиленої автентифікації користувачем платіжної послуги в разі встановлення постійного блокування процедури автентифікації.

5. Динамічне пов'язування

21. Динамічне пов'язування використовується під час створення кодів автентифікації, що обмежується сукупністю суворих вимог безпеки. Щоб залишатися технологічно нейтральними, для впровадження кодів автентифікації не потрібна особлива технологія. Тому коди автентифікації потрібно запроваджувати з використанням таких рішень, як створення та перевірка справжності одноразових паролів, електронних підписів чи інших способів підтвердження з використанням ключів або криптографічних перетворень з урахуванням вимог пункту 91 глави 27 розділу V цього Положення, що зберігаються в елементах автентифікації під час виконання вимог безпеки.

22. Надавач платіжних послуг під час застосування процедури посиленої автентифікації користувача платіжної послуги впроваджує такі заходи:

1) платнику повідомляються ідентифікаційні дані отримувача та сума платіжної операції у спосіб, визначений договором;

2) створений код автентифікації є пов'язаним із сумою платіжної операції та отримувачем, які погоджені платником під час ініціювання операції;

3) код автентифікації, прийнятий надавачем платіжних послуг, підтверджує суму платіжної операції та ідентифікаційні дані отримувача;

4) будь-яка зміна суми або ідентифікаційних даних отримувача призводить до недійсності коду автентифікації та скасування ініціювання платіжної операції.

23. Надавач платіжних послуг зобов'язаний забезпечити конфіденційність, достовірність та цілісність індивідуальної облікової інформації користувача платіжних послуг для:

1) суми платіжної операції та інформацію про отримувача на всіх етапах автентифікації;

2) інформації, яка надається платнику на всіх етапах автентифікації, включаючи створення, передавання та використання коду автентифікації.

24. Надавач платіжних послуг для створення коду автентифікації за результатами застосування процедури посиленої автентифікації користувача платіжної послуги зобов’язаний забезпечити таке:

1) стосовно платіжної операції, відповідно до якої платник надав згоду на точну суму грошових коштів, що мають бути заблоковані на рахунку платника, код автентифікації повинен бути пов’язаним із отримувачем та сумою платіжної операції, на яку платник погодився під час ініціювання платіжної операції;

2) для платіжних операцій, які платник погодився провести як серію дистанційних платіжних операцій одному або кільком отримувачам, код автентифікації повинен бути пов’язаним із цими отримувачами та сумами платіжних операції на користь цих отримувачів.

6. Вимоги до елементів (даних) посиленої автентифікації, засобів та програмного забезпечення, пов’язаних з обробкою цих елементів

25. Надавач платіжних послуг для елементів (даних), віднесених до категорії знань, повинен застосовувати заходи безпеки щодо нерозголошення цих елементів стороннім особам.

26. Надавач платіжних послуг зобов’язаний застосовувати заходи безпеки, що мінімізують наслідки розголошення елементів (даних), віднесених до категорії знань, стороннім особам у разі використання платником цих елементів (даних).

27. Надавач платіжних послуг зобов’язаний застосовувати заходи безпеки, що забезпечують зменшення рівня ризику для елементів (даних), віднесених до категорії володіння, у частині того, що ці елементи (дані) не можуть бути використані сторонніми особами.

28. Надавач платіжних послуг зобов’язаний застосовувати заходи безпеки щодо запобігання дублюванню елементів (даних), віднесених до категорії володіння, у разі використання платником цих елементів (даних).

29. Надавач платіжних послуг для елементів (даних), віднесених до категорії притаманність, повинен застосовувати заходи безпеки до засобів дистанційної комунікації та програмного забезпечення багатоцільових пристроїв у частині унеможливлення використання цих елементів сторонніми особами.

30. Надавач платіжних послуг повинен забезпечити, щоб засоби дистанційної комунікації та програмне забезпечення, які надаються платнику,

гарантували належний рівень конфіденційності для елементів (даних) посиленої автентифікації, віднесених до категорії притаманність.

31. Надавач платіжних послуг зобов’язаний унеможливити реєстрацію сторонньої особи як платника засобами дистанційної комунікації.

7. Незалежність елементів (даних) посиленої автентифікації

32. Надавач платіжних послуг зобов’язаний вживати заходів безпеки з використання елементів посиленої автентифікації користувачем платіжної послуги, які гарантують, що компрометація одного з елементів посиленої автентифікації не створює загроз конфіденційності іншим елементам.

33. Надавач платіжних послуг зобов’язаний, якщо елементи посиленої автентифікації або код автентифікації обробляються за допомогою багатоцільового пристрою, застосовувати заходи безпеки, що повинні включати таке:

1) використання відокремлених безпечних інформаційних середовищ для забезпечення безпечної роботи багатоцільового пристрою;

2) механізми, які забезпечують неможливість того, що платник чи інша сторонняя особа може змінювати програмне забезпечення або платіжний пристрій;

3) заходи безпеки, що забезпечать зменшення впливу наслідків несанкціонованих змін.

III. Право надавача платіжних послуг не застосувати посиленої автентифікації

8. Інформація про рахунок

34. Надавач платіжних послуг з обслуговування рахунків не вимагає застосування посиленої автентифікації користувачів платіжної послуги за умови дотримання вимог пунктів 8 та 9 глави 2 розділу I цього Положення в таких випадках:

1) посилена автентифікація користувача була (під час першого доступу до інформації про рахунок) застосована надавачем платіжних послуг з обслуговування рахунку в процесі отримання через іншого надавача платіжних послуг згоди користувача на доступ до інформації про рахунок користувача;

2) після здійснення посиленої автентифікації користувача, визначеної в підпункті 1 пункту 34 глави 8 розділу III цього Положення, минуло не більше 180 днів;

3) надавачу нефінансових платіжних послуг з обслуговування рахунків не розкриваються вразливі платіжні дані.

35. Надавач платіжних послуг з обслуговування рахунків зобов'язаний застосувати посилену автентифікацію, якщо виконується будь-яка з таких умов:

1) користувач платіжних послуг вперше отримує доступ до інформації, зазначеної в підпункті 1 пункту 34 глави 8 розділу III цього Положення;

2) минуло більше 180 днів з моменту, коли користувач платіжної послуги останній раз здійснював доступ з мережі Інтернет до інформації про рахунок, зазначеної в підпункті 1 пункту 34 глави 8 розділу III цього Положення, та була застосована посилена автентифікація користувача платіжної послуги.

36. Надавач платіжних послуг, що отримав право на надання нефінансових платіжних послуг, зобов'язаний застосовувати посилену автентифікацію користувачів під час кожного входу користувача до платіжного застосунку.

9. Невеликі суми переказу та довірені отримувачі

37. Надавач платіжних послуг та інші задіяні у відповідній платіжній операції надавачі платіжних послуг мають право не вимагати застосування посиленої автентифікації користувачів платіжної послуги за умови дотримання вимог пунктів 8 та 9 глави 2 розділу I цього Положення в таких випадках:

1) сума дистанційної платіжної операції не перевищує 2 000 гривень;

2) загальна сума попередніх платіжних операцій, ініційованих платником з часу застосування останньої посиленої автентифікації користувача платіжної послуги, не перевищує 10 000 гривень або кількість попередніх операцій, ініційованих платником з часу застосування останньої посиленої автентифікації користувача платіжної послуги, не перевищує п'яти послідовних окремих операцій.

38. Надавач платіжних послуг з обслуговування рахунку зобов'язаний застосовувати посилену автентифікацію, якщо платник створює або вносить зміни до списку довірених отримувачів через надавача платіжних послуг з обслуговування рахунку.

39. Надавач платіжних послуг має право не вимагати застосування посиленої автентифікації за умови дотримання загальних вимог автентифікації, визначених у розділі II цього Положення, якщо платник ініціює платіжну операцію, а отримувач включений до списку довірених отримувачів, який раніше був створений цим платником.

10. Повторювані/регулярні платіжні операції та кредитові перекази між рахунками однієї фізичної або юридичної особи

40. Надавач платіжних послуг зобов’язаний застосовувати посилену автентифікацію, якщо платник вперше створює, ініціює або вносить зміни до списку (шаблону) платіжних операцій, що періодично повторюються.

41. Надавач платіжних послуг не вимагає застосування посиленої автентифікації користувача платіжної послуги для ініціювання всіх наступних платіжних операцій, що входять до серії дистанційних платіжних операцій, які відповідають списку (шаблону), зазначеному в пункті 40 глави 10 розділу III цього Положення, за умови дотримання загальних вимог щодо автентифікації, визначених у главі 2 розділу I цього Положення, та застосування посиленої автентифікації користувача для першої платіжної операції з цієї серії.

42. Надавач платіжних послуг не вимагає застосовування посиленої автентифікації платника за умови дотримання вимог, визначених у пунктах 8 та 9 глави 2 розділу I цього Положення, у разі ініціювання платником кредитового переказу між власними рахунками, що обслуговуються одним надавачем платіжних послуг.

11. Операції МОТО, дебетові перекази та делегування автентифікації

43. Надавач платіжних послуг з обслуговування рахунку самостійно приймає рішення щодо застосування посиленої автентифікації користувача платіжної послуги за операціями МОТО.

44. Надавач платіжних послуг з обслуговування рахунків не вимагає застосування посиленої автентифікації користувачів платіжної послуги за дебетовим переказом за умови отримання згоди платника на виконання такої платіжної операції або в разі здійснення дебетового переказу стягувачем.

45. Надавач платіжних послуг з обслуговування рахунків не вимагає застосування посиленої автентифікації користувача платіжної послуги, якщо інший надавач платіжних послуг виконав автентифікацію цього користувача.

12. Аналіз ризику для платіжних операцій

46. Надавач платіжних послуг не вимагає застосовування посиленої автентифікації платника в разі ініціювання платником дистанційної платіжної операції, що має низький рівень ризику, з урахуванням виконання вимог до механізмів моніторингу операцій, визначених у пунктах 8, 9 глави 2 розділу I та пункті 47 глави 12 розділу III цього Положення.

47. Дистанційна платіжна операція вважається такою, що має низький рівень ризику, якщо надавачем платіжних послуг дотримано такі вимоги:

1) рівень шахрайства для платіжної операції, розрахований відповідно до глави 13 розділу ІІІ цього Положення, еквівалентний або нижче референтного коефіцієнта рівня шахрайства, визначеного в додатку до цього Положення для обраного виду платіжних операцій;

2) сума операції не перевищує відповідного порогового значення, визначеного в додатку до цього Положення;

3) надавач платіжних послуг за результатами моніторингу операцій у режимі реального часу не виявив жодної з таких ознак:

нетипових (аномальних) витрат або нетипової (аномальної) поведінкової моделі платника;

використання платником платіжних пристроїв/програмного забезпечення, які раніше платник не використовував;

виконання коду зловмисного програмного забезпечення під час застосування процедури автентифікації;

застосування відомих сценаріїв вчинення несанкціонованих або шахрайських дій під час надання платіжних послуг;

місцезнаходження платника, яке зафіксовано вперше;

місцезнаходження отримувача в зоні підвищеного ризику (місцезнаходження, де раніше траплялися шахрайські операції).

Перелік, зазначений у підпункті 3 пункту 47 глави 12 розділу ІІІ цього Положення, не є вичерпним, надавач платіжних послуг під час надання платіжних послуг має право доповнювати цей перелік іншими ознаками з огляду на досвід боротьби з шахрайськими діями.

48. Надавач платіжних послуг, який прийняв рішення не вимагати застосовування посиленої автентифікації користувача платіжної послуги для дистанційних платіжних операцій на підставі того, що він має низький ризик, зобов’язаний ураховувати такі фактори ризику:

1) попередні схеми/моделі витрат окремого користувача платіжних послуг;

2) історію платіжних операцій кожного з користувачів платіжних послуг надавача платіжних послуг;

3) місцезнаходження платника та отримувача платежу на момент здійснення платіжної операції, якщо багатоцільовий пристрій надається надавачем платіжних послуг;

4) ідентифікацію аномальної схеми оплати користувача платіжних послуг з урахуванням історії платіжних операцій користувача.

Надавач платіжних послуг для проведення оцінки ризику повинен поєднувати фактори, зазначені в пункті 48 глави 12 розділу ІІІ цього Положення, для кожної окремої платіжної операції з метою визначення того, чи можливо

надати дозвіл на проведення конкретного платежу без застосування посиленої автентифікації користувача платіжної послуги.

13. Розрахунок коефіцієнта рівня шахрайства

49. Надавач платіжних послуг повинен забезпечити такий коефіцієнт рівня шахрайства, який буде еквівалентним або нижчим за референтний коефіцієнт рівня шахрайства, визначений у додатку до цього Положення для кожного виду платіжних операцій, незалежно від того, чи ініціювання таких операцій здійснено із застосуванням посиленої автентифікації, чи з використанням будь-яких винятків, визначених у главах 8–10 розділу ІІІ цього Положення.

50. Коефіцієнт рівня шахрайства для кожного виду платіжних операцій обчислюється як загальна сума несанкціонованих або шахрайських дистанційних платіжних операцій без урахування фактів повернення коштів та способу застосування їх автентифікації, яка ділиться на загальну суму всіх дистанційних платіжних операцій для цього виду операцій, незалежно від того, чи була застосована посилена автентифікація, чи ні.

51. Надавач платіжних послуг зобов’язаний проводити розрахунок коефіцієнта рівня шахрайства щомісяця в перший робочий день наступного місяця.

52. Результати розрахунку коефіцієнта рівня шахрайства надаються надавачем платіжних послуг за окремим запитом Національного банку.

14. Відмова від використання права не вимагати застосовування посиленої автентифікації користувача платіжної послуги

53. Надавачу платіжних послуг забороняється не вимагати застосовування посиленої автентифікації користувача платіжної послуги для будь-якого виду платіжних операцій, якщо розрахований коефіцієнт рівня шахрайства протягом двох кварталів поспіль для цього виду платіжних операцій перевищує референтний коефіцієнт рівня шахрайства, визначений у додатку до цього Положення.

54. Надавач платіжних послуг у разі перевищення референтного коефіцієнта рівня шахрайства протягом двох кварталів поспіль має право не вимагати застосовування посиленої автентифікації користувача платіжної послуги тільки після того, як розрахований коефіцієнт рівня шахрайства для визначеного виду платіжних операцій протягом двох кварталів поспіль буде рівним або нижчим за референтний коефіцієнт рівня шахрайства, визначений у додатку до цього Положення.

55. Надавач платіжних послуг має право не вимагати застосовування посиленої автентифікації користувача платіжної послуги відповідно до вимог,

визначених у главах 8–10 розділу ІІІ цього Положення, для платіжних операцій, до яких були застосовані вимоги пункту 53 глави 14 розділу ІІІ цього Положення, після виконання вимог пункту 54 глави 14 розділу ІІІ цього Положення.

15. Моніторинг

56. Надавач платіжних послуг повинен щоквартально реєструвати та контролювати нижчезазначені дані для кожного виду платіжних операцій, групуючи їх на недистанційні та дистанційні платіжні операції, а саме:

1) загальну суму платіжних операцій, вчинених внаслідок несанкціонованих або шахрайських дій, а також загальну суму всіх платіжних операцій із розподілом на платіжні операції, що ініційовані шляхом застосування посиленої автентифікації користувача платіжної послуги та ініційовані з використанням будь-яких виключень, визначених у главах 8–10 розділу ІІІ цього Положення, з розподілом за кожним типом операцій;

2) середню суму платіжної операції, включаючи розподіл платіжних операцій, ініційованих шляхом застосування посиленої автентифікації користувача платіжної послуги та ініційованих з використанням будь-яких винятків, визначених у главах 8–10 розділу ІІІ цього Положення, з розподілом за кожним типом операцій;

3) кількість платіжних операцій, до яких надавач платіжних послуг не застосував посиленої автентифікації користувача платіжної послуги, та їх відсоток від загальної кількості платіжних операцій.

57. Надавач платіжних послуг зобов’язаний надавати на запит Національного банку результати моніторингу, проведеного відповідно до вимог пункту 56 глави 15 розділу ІІІ цього Положення.

IV. Конфіденційність і цілісність вразливих платіжних даних

16. Вимоги до конфіденційності та цілісності

58. Надавач платіжних послуг зобов’язаний забезпечити на всіх етапах застосування автентифікації конфіденційність та цілісність вразливих платіжних даних, а також кодів автентифікації.

59. Надавач платіжних послуг зобов’язаний забезпечити дотримання таких вимог:

1) вразливі платіжні дані маскуються під час відображення та не відображаються в повному обсязі під час їх введення користувачем платіжних послуг у процесі автентифікації;

2) вразливі платіжні дані, а також криптографічні ключі, що використовуються для шифрування вразливих платіжних даних, зберігаються у вигляді, захищеному від несанкціонованого перегляду та модифікації;

3) особисті криптографічні ключі повинні бути захищені від несанкціонованого доступу.

60. Методологія та порядок управління криптографічними ключами, що використовуються для шифрування або іншим чином забезпечують захист вразливих платіжних даних, затверджуються керівником надавача платіжних послуг.

17. Створення та передавання вразливих платіжних даних

61. Надавач платіжних послуг зобов’язаний забезпечити створення вразливих платіжних даних у безпечному інформаційному середовищі відповідно до вимог нормативно-правових актів Національного банку з питань захисту інформації та кіберзахисту на платіжному ринку.

62. Надавач платіжних послуг запроваджує заходи щодо зменшення ризику несанкціонованого використання вразливих платіжних даних та багатоцільових пристроїв і програмного забезпечення для цілей автентифікації після їх втрати, крадіжки або копіювання до моменту їх надання користувачу платіжних послуг.

63. Надавач платіжних послуг зобов’язаний забезпечити обробку та маршрутизацію вразливих платіжних даних та кодів автентифікації в безпечному інформаційному середовищі відповідно до вимог нормативно-правових актів Національного банку з питань захисту інформації та кіберзахисту на платіжному ринку.

18. Пов’язування користувача з платіжною операцією

64. Надавач платіжних послуг зобов’язаний забезпечити безпечне пов’язування користувача платіжних послуг з призначеними для нього вразливими платіжними даними та багатоцільовими пристроями і програмним забезпеченням для цілей автентифікації.

65. Надавач платіжних послуг зобов’язаний забезпечити дотримання таких вимог:

1) пов’язування особи користувача платіжної послуги з вразливими платіжними даними, багатоцільовими пристроями та програмним забезпеченням для цілей автентифікації здійснюється в безпечному інформаційному середовищі;

2) пов’язування за допомогою засобів дистанційної комунікації користувача платіжної послуги з вразливими платіжними даними та з багатоцільовими пристроями або програмним забезпеченням для цілей автентифікації здійснюється з використанням посиленої автентифікації користувача платіжної послуги.

66. Відповідальність за здійснення безпечного пов’язування особи користувача платіжної послуги з вразливими платіжними даними покладається на надавача платіжних послуг. Межі такої відповідальності включають приміщення надавача платіжних послуг, інтернет-середовище, що надається надавачем платіжних послуг, або інші захищені вебсайти, що використовуються надавачем платіжних послуг та його автоматизованими сервісами, а також ризики, пов’язані з багатоцільовими пристроями та програмним забезпеченням для цілей автентифікації, які використовуються під час процесу автентифікації.

19. Постачання вразливих платіжних даних, багатоцільових пристроїв та програмного забезпечення для цілей автентифікації

67. Надавач платіжних послуг зобов’язаний забезпечити, щоб постачання вразливих платіжних даних, багатоцільових пристроїв та програмного забезпечення для цілей автентифікації користувача платіжних послуг здійснювалось у спосіб, що унеможливлює несанкціоноване використання через втрату, крадіжку або копіювання вразливих платіжних даних.

68. Надавач платіжних послуг зобов’язаний забезпечити виконання таких заходів:

1) впровадження безпечних механізмів передавання даних, що забезпечують постачання вразливих платіжних даних, багатоцільових пристроїв та програмного забезпечення для цілей автентифікації користувачу, який на законних підставах використовує платіжну послугу;

2) використання механізмів, що дають змогу перевіряти цілісність програмного забезпечення для цілей автентифікації, наданого користувачу платіжних послуг за допомогою мережі Інтернет;

3) створення умов, що забезпечують надання вразливих платіжних даних поза межами приміщень надавача платіжних послуг або з використанням засобів дистанційної комунікації та забезпечують таке:

сторонні особи не можуть отримати більше однієї зі складових вразливих платіжних даних або функцій багатоцільових пристроїв та програмного забезпечення для цілей автентифікації у разі надання їх з використанням засобів дистанційної комунікації;

вразливі платіжні дані, багатоцільові пристрої або програмне забезпечення для цілей автентифікації потребують активації перед їх використанням;

4) здійснення активації вразливих платіжних даних, багатоцільових пристроїв або програмного забезпечення для цілей автентифікації перед їх першим використанням у безпечному інформаційному середовищі з урахуванням вимог, визначених у главі 18 розділу IV цього Положення.

20. Відновлення, знищення, блокування та відкликання вразливих платіжних даних та засобів автентифікації

69. Надавач платіжних послуг зобов'язаний забезпечити оновлення або повторну активацію вразливих платіжних даних відповідно до вимог створення і використання вразливих платіжних даних та багатоцільових пристроїв для цілей автентифікації, викладених у главах 17–19 розділу IV цього Положення.

70. Надавач платіжних послуг зобов'язаний впровадити процеси, у межах яких потрібне виконання таких заходів:

1) забезпечення безпечного знищення, блокування або відкликання вразливих платіжних даних, багатоцільових пристроїв та програмного забезпечення для цілей автентифікації;

2) якщо надавач платіжних послуг надає багатоцільові пристрої та програмне забезпечення з автентифікації для багаторазового використання, то безпечне повторне використання багатоцільового пристрою або програмного забезпечення регламентується та впроваджується перед наданням до нього доступу іншому користувачеві платіжних послуг. Такий регламент затверджується керівником надавача платіжних послуг перед наданням в багаторазове використання багатоцільових пристроїв або програмного забезпечення для цілей автентифікації користувачу платіжних послуг;

3) забезпечення видалення та/або блокування інформації, що стосується вразливих платіжних даних, які зберігаються в інформаційних системах і базах даних надавача платіжних послуг, а в разі потреби – в загальнодоступних сховищах.

V. Вимоги до електронної взаємодії між суб'єктами платіжних операцій та до заходів безпеки під час електронної взаємодії

21. Загальні вимоги до електронної взаємодії під час автентифікації

71. Надавач платіжних послуг зобов'язаний забезпечити безпечну ідентифікацію платіжних пристрів платника та одержувача платежів під час електронної взаємодії з ними.

72. Надавач платіжних послуг зобов'язаний впровадити заходи, що мінімізують ризик помилкового надсилання повідомлень стороннім особам платіжними пристроями, програмним забезпеченням та іншими інтерфейсами.

22. Контроль платіжних операцій

73. Надавач платіжних послуг зобов’язаний впровадити процеси щодо контролю всіх платіжних операцій на всіх етапах їх формування, обробки, передавання та зберігання, а також всіх видів електронної взаємодії з та між суб’єктами платіжних операцій у частині надання платіжної послуги.

74. Надавач платіжних послуг зобов’язаний забезпечити, щоб будь-яка електронна взаємодія з та між суб’єктами платіжних операцій містила:

1) унікальний ідентифікатор сеансу електронної взаємодії;

2) механізми реєстрації платіжної операції, що включають номер операції, позначку часу та іншу інформацію платіжної операції для її контролю;

3) позначки часу, які ґрунтуються на уніфікованій системі відліку часу та синхронізуються із Всесвітнім координованим часом із точністю до секунди.

75. Надавач платіжних послуг забезпечує використання електронного підпису відповідно до вимог нормативно-правових актів Національного банку з питань застосування електронного підпису та електронної печатки.

23. Вимоги та параметри доступу до інтерфейсів

76. Надавач платіжних послуг з обслуговування рахунку для забезпечення доступу до рахунків у режимі реального часу зобов’язаний використати інтерфейси, що забезпечують виконання таких вимог:

1) надавач платіжних послуг з надання відомостей з рахунків, надавач платіжних послуг з ініціювання платіжної операції та емітент платіжних інструментів здійснюють взаємну автентифікацію з надавачем платіжних послуг з обслуговування рахунку за допомогою кваліфікованих сертифікатів відкритих ключів;

2) надавач платіжних послуг з надання відомостей з рахунків має можливість здійснювати безпечну електронну взаємодію щодо обміну інформацією про один або більшу кількість рахунків та пов’язаних із ними платіжних операцій;

3) надавач платіжних послуг з ініціювання платіжної операції здійснює безпечну електронну взаємодію з метою ініціювання платіжної операції з рахунку, отримання інформації про ініціювання платіжної операції та стосовно виконання платіжної операції.

77. Інтерфейс повинен відповідати таким вимогам:

1) емітент електронного платіжного засобу, надавач платіжних послуг з ініціювання платіжної операції та/або надавач платіжних послуг з надання відомостей з рахунків повинні мати можливість надати доручення надавачу платіжних послуг з обслуговування рахунку розпочати та застосувати автентифікацію користувача платіжної послуги;

2) між надавачем платіжних послуг з обслуговування рахунку та надавачем платіжних послуг з ініціювання платіжної операції, емітентом електронного платіжного засобу, а також надавачем платіжних послуг з надання відомостей з рахунків та будь-яким користувачем платіжних послуг протягом усієї процедури автентифікації встановлюється та підтримується безперервна електронна взаємодія;

3) під час електронної взаємодії забезпечується цілісність і конфіденційність вразливих платіжних даних та кодів автентифікації.

78. Надавач платіжних послуг з обслуговування рахунку забезпечує в режимі реального часу налаштування інтерфейсів доступу до рахунків, що надані користувачам платіжних послуг, відповідно до вимог цього Положення.

Надавач платіжних послуг з обслуговування рахунку повинен розробити опис, у якому документувати технічні характеристики будь-якого з інтерфейсів із зазначенням набору процедур, протоколів та інструментів, потрібних для надавачів платіжних послуг з ініціювання платіжної операції, надавачів платіжних послуг з надання відомостей з рахунків та емітентів електронних платіжних засобів. Цей опис надавач платіжних послуг з обслуговування рахунку повинен опублікувати на власному вебсайті.

24. Вимоги до спеціалізованих інтерфейсів

79. Надавач платіжних послуг з обслуговування рахунку забезпечує наявність окремо виділеного інтерфейсу для автентифікації та встановлення сеансу зв’язку з рахунком користувача платіжних послуг (далі – спеціалізований інтерфейс) або надає можливість надавачам платіжних послуг з ініціювання платіжної операції, надавачам платіжних послуг з надання відомостей з рахунків та емітентам електронних платіжних засобів самостійно встановлювати власні інтерфейси, що призначені для застосування процедур автентифікації та електронної взаємодії з користувачами платіжних послуг.

80. Надавач платіжних послуг з обслуговування рахунку, який встановив спеціалізований інтерфейс, зобов’язаний забезпечити умови, за яких цей інтерфейс забезпечує належний рівень доступності та продуктивності, включаючи підтримку інтерфейсів доступних користувачу платіжних послуг, призначених для надання доступу до рахунку в режимі реального часу.

81. Надавач платіжних послуг з обслуговування рахунку, який встановив та використовує спеціалізований інтерфейс, зобов’язаний встановити основні показники ефективності та цілі з обслуговування щодо доступності та цілісності даних, наданих відповідно до вимог глави 28 розділу V цього Положення.

82. Надавач платіжних послуг з обслуговування рахунку, який встановив та використовує спеціалізований інтерфейс, зобов’язаний забезпечити, щоб цей інтерфейс не створював перешкод для надання послуг з ініціювання платежів та послуг з інформаційного обслуговування рахунків.

83. Надавач платіжних послуг з обслуговування рахунку зобов’язаний здійснювати моніторинг доступності та ефективності спеціалізованого інтерфейсу. Також надавач платіжних послуг зобов’язаний опублікувати на своєму вебсайті щоквартальну статистику щодо порушень доступності та ефективності спеціалізованого інтерфейсу та інтерфейсу, що використовується користувачами платіжних послуг.

25. Заходи щодо надзвичайних ситуацій для спеціалізованого інтерфейсу

84. Надавач платіжних послуг з обслуговування рахунку повинен враховувати в описі використання спеціалізованого інтерфейсу стратегію і плани заходів щодо дій у надзвичайних ситуаціях, якщо є запланована недоступність інтерфейсу та/або виявлення факту непрацездатності інтерфейсу. Виявлення непередбаченої недоступності або непрацездатності інтерфейсу відбувається, якщо п’ять послідовних запитів на доступ до послуги з ініціювання платежу або послуги з надання відомостей з рахунку не отримали відповіді протягом 30 секунд.

85. Плани заходів щодо дій у надзвичайних ситуаціях повинні включати планування комунікацій з інформування надавачів платіжних послуг, які використовують спеціалізований інтерфейс, про заходи з відновлення такого інтерфейсу та інструкції щодо використання інших резервних спеціалізованих інтерфейсів.

86. Надавач платіжних послуг у разі виникнення надзвичайної ситуації має право використовувати інші інтерфейси, доступні користувачу платіжних послуг, для забезпечення для користувача можливості проходження автентифікації, управління рахунком та ініціювання платіжних операцій до моменту відновлення функціонування спеціалізованого інтерфейсу.

26. Перевірка авторизації діяльності надавача платіжних послуг

87. Надавач платіжних послуг з обслуговування рахунку перед наданням сторонньому надавачу платіжних послуг доступу до рахунку користувача зобов’язаний перевірити авторизацію діяльності такого стороннього надавача платіжних послуг щодо відповідної платіжної послуги шляхом:

1) перевірки чинності кваліфікованого сертифіката відкритого ключа стороннього надавача платіжних послуг;

2) автентифікації стороннього надавача платіжних послуг з використанням його кваліфікованого сертифіката відкритого ключа;

3) перевірки наявності інформації про стороннього надавача платіжних послуг у Реєстрі платіжної інфраструктури (далі – Реєстр); порівняння інформації про стороннього надавача платіжних послуг, що міститься у Реєстрі, з інформацією, що міститься у кваліфікованому сертифікаті відкритого ключа стороннього надавача платіжних послуг [порівнюються ідентифікаційні дані та відомості про вид (види) фінансової платіжної послуги].

Надавач платіжних послуг з обслуговування рахунку має право надавати доступ до рахунку користувача сторонньому надавачу платіжних послуг, якщо результати всіх зазначених перевірок є успішними.

88. Кваліфіковані сертифікати ключів надавачів платіжних послуг повинні містити:

1) для банків – ідентифікаційний код/номер, що дає змогу ідентифікувати банк у Державному реєстрі банків;

2) для небанківських надавачів платіжних послуг:

ідентифікаційний код/номер надавача платіжних послуг, що дає змогу ідентифікувати надавача платіжних послуг у Реєстрі;

інформацію про види нефінансових платіжних послуг, на які авторизовано небанківського надавача платіжних послуг.

89. Надавач платіжних послуг зобов’язаний надати Національному банку інформацію про кваліфікованого надавача електронних довірчих послуг, у якого він обслуговується.

90. Національний банк повідомляє кваліфікованого надавача електронних довірчих послуг про припинення надання окремого виду (видів) платіжних послуг, зазначеного (зазначених) у Реєстрі щодо відповідного надавача платіжних послуг (надавача платіжних послуг з ініціювання платіжної операції, надавача платіжних послуг з надання відомостей з рахунків, емітента платіжних інструментів, надавача платіжних послуг з обслуговування рахунку).

27. Безпека сеансу зв’язку

91. Надавач платіжних послуг з метою надання фінансових та/або нефінансових платіжних послуг зобов’язаний забезпечити захист даних із використанням криптографічних алгоритмів шифрування, що є національними стандартами, або такими, на які за результатами державної експертизи Державної служби спеціального зв’язку та захисту інформації України надано

позитивний експертний висновок під час обміну даними через мережі загального користування.

92. Надавач платіжних послуг, який надає фінансові та/або нефінансові платіжні послуги, зобов’язаний завершити будь-який сеанс зв’язку одразу після виконання запиту.

93. Надавач платіжних послуг з надання відомостей з рахунків та надавач платіжних послуг з ініціювання платіжної операції для підтримання паралельних сеансів зв’язку з надавачем платіжних послуг з обслуговування рахунку зобов’язані забезпечити умови, за яких ці сеанси безпечним чином пов’язані з відповідними сеансами, встановленими з користувачами платіжних послуг, з метою запобігання помилкової адресації будь-яких повідомлень або інформації.

94. Надавач платіжних послуг з надання відомостей з рахунків, надавач платіжних послуг з ініціювання платіжної операції та емітент платіжних інструментів спільно з надавачем платіжних послуг з обслуговування рахунку для забезпечення безпеки сеансу зв’язку зобов’язані впровадити таке:

1) сеанс зв’язку під час проведення платіжної операції повинен бути пов’язаний з відповідним користувачем або користувачами платіжної послуги з метою виділення кількох запитів від одного і того самого користувача або користувачів платіжної послуги;

2) для надання послуги з ініціювання платежів ініційована платіжна операція повинна бути ідентифікована;

3) для надання підтвердження наявності грошових коштів ідентифіковано запит, який пов’язано із сумою, потрібною для виконання платіжної операції.

95. Надавач платіжних послуг з обслуговування рахунку, надавач платіжних послуг з надання відомостей з рахунків, надавач платіжних послуг з ініціювання платіжної операції та емітент платіжних інструментів зобов’язані забезпечити, щоб під час передавання вразливих платіжних даних та кодів автентифікації ця інформація була захищена засобами криптографічного захисту інформації або представлена в такому вигляді, який унеможливлює зчитування цієї інформації, прямо чи опосередковано, у будь-який час.

Надавач платіжних послуг, до сфери відповідальності/компетенції якого належить подія порушення конфіденційності та/або цілісності вразливих платіжних даних, зобов’язаний невідкладно повідомити про це пов’язаного з ним користувача платіжних послуг та емітента цих вразливих платіжних даних у разі настання цієї події у визначений договором спосіб.

28. Обмін даними

96. Надавач платіжних послуг з обслуговування рахунку зобов’язаний дотримуватися таких вимог:

1) надавач платіжних послуг з надання відомостей з рахунків отримує таку саму інформацію з рахунків та пов’язаних з ними платіжних операцій, яка надається користувачу платіжних послуг під час запиту на доступ до інформації щодо рахунку, за умови, що ця інформація не містить вразливих платіжних даних;

2) після отримання платіжної інструкції надає надавачу платіжних послуг з ініціювання платіжної операції таку саму інформацію про ініціювання та виконання платіжної операції, яка надається в розпорядження ініціатору платіжної операції, якщо операція ініційована безпосередньо користувачем платіжних послуг;

3) надає підтвердження в простому форматі “так” або “ні” на запит стосовно наявності на рахунку платника потрібної суми коштів для здійснення платіжної операції;

4) після отримання надавачем платіжних послуг з надання відомостей з рахунків розпорядження користувача платіжних послуг про відкликання згоди на надання доступу до рахунків користувача, раніше отриманої від іншого надавача платіжних послуг з надання відомостей з рахунків, цей надавач платіжних послуг з надання відомостей з рахунків припиняє доступ до рахунків користувача та надає іншому надавачу платіжних послуг інформацію про скасування цього доступу.

97. Надавач платіжних послуг з обслуговування рахунку у разі виникнення непередбачуваної події або помилки, яка сталася під час процесу ідентифікації, автентифікації та/або обміну даними, надсилає надавачам платіжних послуг з надання відомостей з рахунків та надавачам платіжних послуг з ініціювання платіжної операції, а також емітентам платіжних інструментів повідомлення/сповіщення з поясненнями стосовно причини непередбачуваної події або помилки. Якщо надавач платіжних послуг з обслуговування рахунку використовує під час процесу ідентифікації, автентифікації та/або обміну даними спеціалізований інтерфейс відповідно до глави 24 розділу V цього Положення, то цей спеціалізований інтерфейс повинен мати можливість надання повідомлень/сповіщень стосовно причини непередбачуваної події або помилки, що повинні надаватися будь-яким надавачем платіжних послуг, який виявив подію або помилку, іншим надавачам платіжних послуг, які є учасниками процесу ідентифікації, автентифікації та/або обміну даними.

98. Надавач платіжних послуг з надання відомостей з рахунків зобов’язаний унеможливити доступ до інформації, що не стосується рахунків та пов’язаних з ними платіжних операцій користувача.

99. Надавач платіжних послуг з ініціювання платіжної операції надає надавачам платіжних послуг з обслуговування рахунку ту саму інформацію, яку надає користувач платіжних послуг під час безпосереднього ініціювання платіжної операції.

100. Надавач платіжних послуг з надання відомостей із рахунків повинен мати доступ до інформації щодо призначення рахунків та пов’язаних із ними платіжних операцій, що проводяться надавачами платіжних послуг з обслуговування рахунку, для цілей здійснення інформаційного обслуговування рахунків за будь-якої з таких обставин:

1) щоразу, коли користувач платіжних послуг запитує таку інформацію;

2) користувач платіжних послуг вимагає таку інформацію не більше чотирьох разів протягом 24 годин, якщо тільки між надавачем платіжних послуг з надання відомостей з рахунків та надавачем платіжних послуг з обслуговування рахунку не встановлено домовленості щодо більш високої частоти надання інформації, що погоджено користувачем платіжної послуги.

Додаток
до Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку
(підпункт 1 пункту 47 глави 12 розділу III)

Референтний коефіцієнт рівня шахрайства

№ з/п	Порогове значення суми платіжної операції	Референтний коефіцієнт для дистанційних платіжних операцій з використанням платіжних карток, (%)	Референтний коефіцієнт для дистанційних кредитових переказів, (%)
1	2	3	4
1	Сума операції не перевищує розміру 20 000 гривень	0,01	0,005
2	Сума операції не перевищує розміру 7 000 гривень	0,06	0,01
3	Сума операції не перевищує 2 000 гривень	0,13	0,015