Національний банк України

Платіжна організація
Національної платіжної системи “Український платіжний простір”

СХВАЛЕНО
Рішення Ради Платіжної організації
Національної платіжної системи
“Український платіжний простір”
протокол від 30.01.2018 № 57/2/2018

Методичні рекомендації щодо параметрів моніторингу операцій із використанням електронних платіжних засобів Національної платіжної системи “Український платіжний простір”

м. Київ

Зміст

СХВАЛЕНО
Рішення Ради Платіжної організації
Національної платіжної системи
“Український платіжний простір”
протокол від 30.01.2018 № 57/2/2018

Методичні рекомендації щодо параметрів моніторингу операцій із використанням електронних платіжних засобів Національної платіжної системи “Український платіжний простір”

І. Загальні положення

1. Методичні рекомендації щодо параметрів моніторингу операцій із використанням електронних платіжних засобів Національної платіжної системи “Український платіжний простір” (далі – Методичні рекомендації) підготовлені з метою реалізації емітентами та еквайрами (далі – учасники) вимог статті 40^1 Закону України “Про платіжні системи та переказ коштів в Україні”, Положення про порядок емісії електронних платіжних засобів і здійснення операцій з їх використанням, затвердженого постановою Правління Національного банку від 05.11.2014 № 705 (далі – Положення про порядок емісії), та інших нормативно-правових актів Національного банку України та нормативних документів Національної платіжної системи “Український платіжний простір” (далі – НПС “ПРОСТІР”).

2. Методичні рекомендації визначають загальний порядок та основні параметри щодо здійснення учасниками НПС “ПРОСТІР” моніторингу за операціями з використанням електронних платіжних засобів (далі – ЕПЗ) НПС “ПРОСТІР” (в тому числі їх реквізитів).

3. Терміни в Методичних рекомендаціях уживаються в такому значенні:

1) реквізити ЕПЗ НПС “ПРОСТІР” – основний номер (цифровий номер з 16 цифр), ім’я та прізвище держателя ЕПЗ, дата завершення терміну дії ЕПЗ, код перевірки достовірності ЕПЗ;

2) система моніторингу – поєднання програмно-технічних комплексів, а також технологічних, організаційних та інших заходів, які забезпечують систематичний контроль за операціями, що здійснені з використанням ЕПЗ;

3) спірна операція – операція, здійснена з використанням ЕПЗ (у тому числі його реквізитів) та відносно якої між еквайром і емітентом за ініціативою користувача ЕПЗ виникає спір;

4) сумнівна операція – операція, що зафіксована засобами системи моніторингу, яка не притаманна типовій поведінці користувача/торговця (наприклад, відрізняється суттю, часом, сумою, місцем здійснення тощо) та

критерії (параметри) якої визначені внутрішніми документами учасника платіжної системи;

5) точка компрометації – місце, де відбулось несанкціоноване отримання реквізитів ЕПЗ сторонніми особами;

6) фішинговий сайт – веб-ресурс (веб-сторінка), який використовується шахраями для несанкціонованого отримання персональних даних користувача та/або реквізитів його ЕПЗ під виглядом оплати неіснуючих послуг, який зазвичай виглядає за дизайном як сайт організації, якій користувач довіряє;

7) фолбек (fallback) – трансакція з використанням картки з чипом стандарту EMV, ініціювання якої спочатку відбувалось у платіжному пристрої зі зчитуванням даних чипа, проте, через нездатність пристрою зчитати дані з чипа та завершити трансакцію, її завершено з дозволу емітента зі зчитуванням та передачею даних магнітної смуги;

8) шахрайська операція – операція здійснена з використанням ЕПЗ (у тому числі його реквізитів), виконана без дозволу держателя ЕПЗ або авторизованої на проведення операції особи, що призвела до фінансової втрати одного або більше учасників платіжної системи та/або її користувачів.

Інші терміни, які вживаються у Методичних рекомендаціях, застосовуються в значеннях, визначених Законом України “Про платіжні системи та переказ коштів в Україні”, Положенням про порядок емісії, іншими законами та нормативно-правовими актами Національного банку України (далі – Національний банк), Правилами НПС “ПРОСТІР”, затверджених рішенням Ради Платіжної організації НПС “ПРОСТІР” від 07.06.2013 № 213, (із змінами) (далі – Правила НПС “ПРОСТІР”) та іншими нормативними документами НПС “ПРОСТІР”.

ІІ. Класифікація способів компрометації електронних платіжних засобів

4. Основні способи компрометації ЕПЗ НПС “ПРОСТІР”:

1) вішинг (голосовий фішинг) – різновид фішингу, метою якого є отримання доступу до персональних даних держателя ЕПЗ та/або реквізитів його ЕПЗ за допомогою засобів телекомунікаційного зв’язку, сервісу інтерактивного голосового меню тощо;

2) скіммінг – несанкціоноване копіювання та збереження даних за допомогою спеціального технічного пристрою (скіммера) з магнітної смуги ЕПЗ. Скіммер може розміщуватися перед (над) отвором для приймання електронних платіжних засобів на платіжному пристрої;

3) фармінг – процедура прихованої переадресації користувача на фішинговий сайт;

4) фішинг – різновид соціальної інженерії, метою якого є отримання доступу до персональних даних держателя та/або реквізитів його ЕПЗ засобами електронної пошти та/або фішингових сайтів;

5) шиммінг – різновид скімінгу, при реалізації якого спеціальний технічний пристрій для копіювання та збереження даних розміщується в отворі для приймання ЕПЗ всередині платіжного пристрою;

6) шкідливе програмне забезпечення – таке, що здатне перехоплювати дані ЕПЗ та/або персональні дані держателя та зберігати/поширювати для подальшого несанкціонованого використання.

Цей перелік способів компрометації ЕПЗ НПС "ПРОСТІР" не є вичерпним. Учасники НПС "ПРОСТІР" під час здійснення моніторингу можуть враховувати також інші можливі способи компрометації ЕПЗ НПС "ПРОСТІР".

ІІІ. Моніторинг

5. Моніторинг операцій з використанням ЕПЗ НПС "ПРОСТІР" (в тому числі його реквізитів) рекомендується здійснювати в режимі 24/7 з урахуванням прикладів параметрів моніторингу, наведених у Додатку 1, Додатку 2 та Додатку 3 до цього документу, але не обмежуючись ними.

6. Моніторинг здійснюється структурними підрозділами учасників НПС "ПРОСТІР", відповідальними за банківську та інформаційну безпеку, за допомогою системи моніторингу, яка дозволяє виявляти сумнівні операції та вживати заходи для зменшення потенційних ризиків.

7. Моніторинг рекомендується здійснювати на підставі інформації, наданої незалежними процесинговими центрами та/або інформації з власного процесингового центру, з урахуванням внутрішньобанківських правил, розроблених відповідно до законодавства України, у т. ч. нормативно-правових актів Національного банку, Правил НПС "ПРОСТІР" та з урахуванням цих Методичних рекомендацій.

8. За типами аналізу система моніторингу може поділятись на:

онлайнову, в якій аналіз авторизацій та прийняття рішення про її схвалення або відхилення здійснюється в режимі реального часу;

офлайнову, в якій рішення про віднесення авторизацій/операцій до категорії сумнівних здійснюється на підставі аналізу звітів за параметрами моніторингу авторизацій, що вже відбулись, та операцій у клірингових файлах.

9. За типами реагування система моніторингу може поділятись на:

автоматичну – віднесення операції до категорії сумнівних здійснюється автоматично на підставі параметрів моніторингу;

автоматизовану – рішення про віднесення операції до категорії сумнівних приймає співробітник відповідального підрозділу банку на підставі параметрів моніторингу.

IV. Загальні підходи до організації моніторингу

10. Учасникам НПС “ПРОСТІР” рекомендується визначити правила проведення моніторингу, які можуть містити, зокрема, наступне:

1) порядок управління ризиками;

2) порядок взаємодії учасників процесу (емітентів, еквайрів, торговців, держателів електронних платіжних засобів тощо);

3) вимоги до захисту інформації під час здійснення моніторингу;

4) порядок оброблення та зберігання інформації;

5) порядок проведення моніторингу за операціями з використанням електронних платіжних засобів НПС “ПРОСТІР” (в тому числі їх реквізитів);

6) порядок реагування на сумнівні операції;

7) порядок проведення розслідування фактів шахрайства;

8) інші.

11. Емітенту НПС “ПРОСТІР при розробці параметрів моніторингу авторизацій пропонується використовувати перелік параметрів моніторингу авторизацій емітента, наведений у табл.1 Додатка 1 до цього документу.

Також емітентом зокрема можуть бути встановлені такі додаткові параметри моніторингу:
кількість спроб введення неправильного ПІН;
відмови за результатами перевірок коду достовірності ЕПЗ;
авторизації з використанням платіжних терміналів самообслуговування;
авторизації з використанням ЕПЗ з терміном дії, що минув;
авторизації за неіснуючими та/або недостовірними номерами ЕПЗ;
авторизації з підбором сум;
авторизації за ЕПЗ емітента в точках компрометації (в тому числі можливих).

12. Еквайру НПС “ПРОСТІР” при розробці параметрів моніторингу авторизацій пропонується використовувати перелік параметрів моніторингу авторизацій еквайра, наведений у табл.2 Додатка 2 до цього документу.

Еквайром можуть бути встановлені додаткові параметри моніторингу, зокрема, відсоток відмін авторизацій (реверсалів).

13. Для визначення цільових значень параметрів моніторингу можуть використовуватися абсолютні та середньозважені значення показників. У разі використання в параметрі моніторингу часового періоду, рекомендується використовувати для порівняння середньозважене значення показника, попередньо обчислене за відповідний період.

14. Учаснику НПС “ПРОСТІР”, при розробці параметрів офлайн-моніторингу авторизацій/трансакцій пропонується використовувати перелік параметрів офлайн-моніторингу авторизацій та трансакцій у клірингових файлах, наведений у табл.3 Додатка 3 до цього документу.

Також учасником, зокрема, можуть бути встановлені такі додаткові параметри моніторингу:

максимальна сума однієї операції для торговця;

кількість/сума спірних операцій за окремим торговцем/платіжним пристроєм;

відсутність операцій у торговця за визначений період;

надходження коштів до торговця, що не проводив операцій за визначений період;

надходження коштів до торговця після розірвання договору еквайрингу.

16. Учасникам НПС “ПРОСТІР” доцільно формувати та супроводжувати базу даних інцидентів з електронними платіжними засобами на підставі даних системи моніторингу.

17. Учасникам НПС “ПРОСТІР” під час здійснення заходів щодо оперативного обміну інформацією, розслідувань фактів шахрайства, протидії/попередження злочинам із ЕПЗ (в тому числі за їх реквізитами), поданні інформації, заяв за вказаними фактами до правоохоронних органів, слід дотримуватись вимог законодавства з питань захисту даних (клієнтів, банків, торговців тощо).

Директор Департаменту
платіжних систем та інноваційного розвитку О. М. Яблунівський

Заступник начальника управління – начальник відділу
роботи з учасниками платіжного ринку Департаменту
платіжних систем та інноваційного розвитку В. С. Дикий

Заступник начальника відділу підтримки і розвитку Центрального маршрутизатора Управління інноваційного розвитку
Департаменту платіжних систем та інноваційного розвитку О. М. Алєксєєва

Заступник начальника відділу забезпечення діяльності
платіжної системи Національного банку України
Департаменту платіжних систем та інноваційного розвитку В. І. Харченко

Головний економіст відділу роботи з учасниками платіжного ринку
Департаменту платіжних систем та інноваційного розвитку А. В. Самойленко

Старший інженер відділу проектування і розробки
перспективних систем захисту банківської інформації
та електронних платіжних систем Департаменту безпеки В. В. Федотенко

Додаток 1

Параметри моніторингу емітентом авторизацій з використанням ЕПЗ

Таблиця 1. Перелік параметрів моніторингу авторизацій емітента

Кількість/сума/ відсоток	Успішність (так/ні)	ЕПЗ/ ІНЕ	Торговець/пристрій (Т/П)	Тип отримання даних ЕПЗ (чип/ фолбек/безконтакт/ магнітна стрічка/ ручне введення)	Метод автентифікації (підпис/PIN)	Період (день/місяць/тощо)	Приклади параметрів моніторингу (для порівняння)
Сума	так	ІНЕ	-	-	-	місяць	Сума успішних авторизацій за окремим ІНЕ за місяць
Сума	ні	ЕПЗ	П	-	-	день	Сума неуспішних (відхилених) авторизацій за окремим ЕПЗ в окремому платіжному пристрої за день
Сума	-	ЕПЗ	-	-	-	-	Сума авторизації за окремим ЕПЗ
Кількість	-	ЕПЗ	-	ручне введення	-	день	Кількість авторизацій за окремим ЕПЗ з використанням ручного введення за день
Кількість	так	ЕПЗ	Т	безконтакт	без PIN	день	Кількість успішних авторизацій за окремим ЕПЗ з використанням безконтактної технології без PIN у окремого торговця за день
Відсоток	-	ЕПЗ	-	ручне введення	-	місяць	Відсоток авторизацій за окремим ЕПЗ з використанням ручного введення за місяць

Додаток 2

Параметри моніторингу еквайром авторизацій за окремими торговцями/платіжними пристроями

Таблиця 2. Перелік параметрів моніторингу авторизацій еквайра

Кількість/сума/ відсоток	Успішність (так/ні)	ЕПЗ/ ІНЕ	Торговець/пристрій (Т/П)	Тип отримання даних ЕПЗ (чип/ фолбек/безконтакт/ магнітна стрічка/ ручне введення)	Метод автентифікації (підпис/PIN)	Період (день/місяць/тощо)	Приклади параметрів моніторингу (для порівняння)
Кількість	так	-	П	-	без PIN	місяць	Кількість успішних авторизацій без PIN в окремому платіжному пристрої за місяць
Сума	ні	-	Т	-	-	день	Сума неуспішних авторизацій у окремого торговця за день
Кількість	-	-	Т	фолбек	-	день	Кількість авторизацій з використанням фолбек у окремого торговця за день
Відсоток	-	-	-	ручне введення	-	місяць	Відсоток авторизацій з використанням ручного введення за місяць

Додаток 3

Параметри офлайн-моніторингу авторизацій та трансакцій у клірингових файлах

Таблиця 3. Перелік параметрів офлайн-моніторингу авторизацій та трансакцій у клірингових файлах

Кількість/сума/ відсоток	ЕПЗ/ ІНЕ	Торговець/пристрій (Т/П)	Тип отримання даних картки (чип/ фолбек/безконтакт/ магнітна стрічка/ ручне введення)	Метод автентифікації (підпис/PIN)	Період (день/місяць/тощо)	Приклади параметрів моніторингу (для порівняння)
Сума	ЕПЗ	-	-	без PIN	день	Сума операцій за окремим ЕПЗ за день
Кількість	ЕПЗ	П	-	-	день	Кількість операцій за окремим ЕПЗ в окремому платіжному пристрої за день
Сума	ЕПЗ	Т	ручне введення	-	місяць	Сума операцій за окремим ЕПЗ у окремого торговця з ручним введенням номера картки за місяць
Кількість	-	П	-	-	день	Кількість операцій в окремому платіжному пристрої за день
Сума	-	Т	-	-	місяць	Сума операцій у окремого торговця за місяць