

ЗАТВЕРДЖЕНО
Рішенням Загальних зборів учасників
Товариства з обмеженою відповідальністю
«Фінансова компанія МБК»
протокол №113 від 17.12.2024 року

ВНУТРІШНІ ПРАВИЛА
ТОВ «ФК МБК»
про переказ коштів без відкриття рахунків

м. Київ 2024

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ	3
2. ВИЗНАЧЕННЯ ТЕРМІНІВ	3
3. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ В «КАРТКОВІЙ» ПС	5
4. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ В «НЕ КАРТКОВІЙ» ПС	16
5. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ З ВИКОРИСТАННЯМ ТЕХНІЧНОГО ПРОТОКОЛУ PORTMONE DIRECT	24
6. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ А2С (<i>account-to-card</i>) ТА А2А (<i>account-to-account</i>)	31
7. ФОРМА ТА ПОРЯДОК НАДАННЯ ЗГОДИ ПЛАТНИКА НА ВИКОНАННЯ ПЛАТІЖНОЇ ОПЕРАЦІЇ	36
8. ПОРЯДОК ПРИЙНЯТТЯ ДО ВИКОНАННЯ ПЛАТІЖНОЇ ІНСТРУКЦІЇ ТА НАСТАННЯ МОМЕНТУ БЕЗВІДКЛИЧНОСТІ ПЛАТІЖНОЇ ІНСТРУКЦІЇ, ПОРЯДОК ВІДКЛИКАННЯ ЗГОДИ ПЛАТНИКА НА ВИКОНАННЯ ПЛАТІЖНОЇ ОПЕРАЦІЇ	37
9. ДОКУМЕНТИ ЗА ОПЕРАЦІЯМИ З ВИКОРИСТАННЯМ ПЛАТІЖНИХ ІНСТРУМЕНТІВ	38
10. ІДЕНТИФІКАЦІЯ ПЛАТНИКА ТА ОТРИМУВАЧА. СУПРОВОДЖЕННЯ ПЛАТІЖНИХ ОПЕРАЦІЙ НЕОБХІДНОЮ ІНФОРМАЦІЄЮ	38
11. ПОРЯДОК ЗДІЙСНЕННЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ	44
12. УПРАВЛІННЯ РИЗИКАМИ	47
13. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ВИКОРИСТОВУЄТЬСЯ ПІД ЧАС НАДАННЯ ПЛАТІЖНИХ ПОСЛУГ (ВИКОНАННЯ ПЛАТІЖНИХ ОПЕРАЦІЙ)	53
14. СТРОКИ ТА ПОРЯДОК ЗБЕРІГАННЯ ІНФОРМАЦІЇ ПРО ПЛАТІЖНІ ОПЕРАЦІЇ	62
15. ПОРЯДОК ЗДІЙСНЕННЯ ВНУТРІШНЬОГО КОНТРОЛЮ	65
16. ВІДПОВІДАЛЬНІСТЬ ПРАЦІВНИКІВ	68
17. ЗАКЛЮЧНІ ПОЛОЖЕННЯ	68

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Метою діяльності Товариства з обмеженою відповідальністю «Фінансова компанія МБК» (надалі Товариство або ФК, або ННПП) є надання фінансових платіжних послуг, зокрема, здійснення переказу коштів без відкриття рахунків у національній валюті на всій території України.

1.2. Внутрішні правила ТОВ «ФК МБК» про переказ коштів без відкриття рахунків (далі – Правила) є обов'язковими для всіх працівників Товариства, які відповідно до покладених на них обов'язків прямо чи опосередковано залучені до процесів здійснення Товариством переказу коштів без відкриття рахунків.

1.3. Правила розроблені відповідно до вимог Цивільного кодексу України, Господарського кодексу України, Закону України «Про платіжні послуги», Закону України «Про фінансові послуги та фінансові компанії», Закону України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», Положення про порядок емісії та еквайрингу платіжних інструментів, затвердженого Постановою Правління НБУ №164 від 29.07.2022 р., Положення про порядок здійснення авторизації діяльності надавачів фінансових платіжних послуг та обмежених платіжних послуг, затвердженого Постановою НБУ №217 від 07.10.2022 р., Положення про здійснення установами фінансового моніторингу, затвердженого Постановою Правління НБУ №107 від 28.07.2020 р., та інших нормативно-правових актів Національного банку України.

1.4. Правила регламентують порядок та умови надання ФК фінансової платіжної послуги з переказу коштів без відкриття рахунків на користь фізичних та/або юридичних осіб на всій території України.

1.5. Вимоги цих Правил не поширюються на випадки виконання платіжних операцій з електронними грошима, а також на платіжні операції, умовами яких передбачено прийняття або видачу ФК готівкових коштів.

2. ВИЗНАЧЕННЯ ТЕРМІНІВ

2.1. У цих Правилах терміни та скорочення вживаються в такому значенні:

2.1.1. **Авторизація** – процедура отримання дозволу на проведення платіжної операції з використанням Платіжного інструменту. За результатами успішної Авторизації формується і надається код Авторизації (набір цифр або набір букв і цифр).

2.1.2. **ННПП** – небанківський надавач платіжних послуг – Товариство з обмеженою відповідальністю «Фінансова компанія МБК» (далі – ФК або ННПП, або ТОВ «ФК МБК»), код за ЄДРПОУ 37973945.

2.1.3. **ТО** – технологічний оператор – Товариство з обмеженою відповідальністю «Портмоне», код за ЄДРПОУ 31868613 (ТОВ «Портмоне»).

2.1.4. **Банк (Обслуговуючий банк)** – банківські установи, в яких відкриті розрахункові рахунки ФК для приймання та переказу коштів Платників.

2.1.5. **Розрахунковий банк** – уповноважений оператором відповідної Платіжної системи банк, що бере участь у проведенні розрахунків у Платіжній системі.

2.1.6. **Процесингова установа** – юридична особа, що здійснює процесинг.

2.1.7. **Еквайр** – надавач платіжних послуг, який надає послугу еквайрингу платіжних інструментів та має ліцензію на надання такої послуги. Еквайрами ФК є наступні банки: АТ «Ощадбанк» (код за ЄДРПОУ 00032129), АТ «Гаскомбанк» (код за ЄДРПОУ 09806443), АТ «ПУМБ» (код за ЄДРПОУ 14282829), АТ «Ідея Банк» (код за ЄДРПОУ 19390819), АТ «Райффайзен Банк» (код за ЄДРПОУ 14305909), АТ «СЕНС БАНК» (код за ЄДРПОУ 23494714), АТ КБ «Приватбанк» (код за ЄДРПОУ 14360570), Акціонерний банк «Південний» (код за ЄДРПОУ 20953647).

2.1.8. **ПС («карткова»)** – система для виконання платіжних операцій із формальними та стандартизованими домовленостями і загальними правилами щодо процесингу, клірингу та/або виконання розрахунків між учасниками платіжної системи. Так звана «карткова» ПС означає платіжну систему, в якій здійснюється емісія платіжних карток та приймання їх до розрахунків. ФК є непрямим учасником через банки-еквайри таких міжнародних платіжних систем як VISA (оператор Visa International Service Association) та MasterCard (оператор Mastercard International Incorporated), а також Національної платіжної системи «Український платіжний простір» («ПРОСТІР») (оператор Національний банк України). В межах зазначених «карткових» ПС ФК здійснює переказ коштів.

- 2.1.9. **СЕП** – державна платіжна система, що забезпечує проведення міжбанківських розрахунків через рахунки, відкриті банками в Національному банку України. Оператором та розрахунковим банком СЕП є Національний банк України.
- 2.1.10. **Емітент** – надавач платіжних послуг, який надає послугу емісії платіжних інструментів та має право на надання такої послуги відповідно до Закону України «Про платіжні послуги». Емітент є одночасно надавачем платіжних послуг з обслуговування рахунку Платника (НППЗОР). ФК надає можливість ініціювати платіжні операції з використанням платіжних інструментів у вигляді електронних платіжних засобів (ЕПЗ), емітованих як банками України, так і іноземними банками, які є учасниками «карткових» ПС VISA та MasterCard.
- 2.1.11. **НППЗОР Отримувача** – надавач платіжних послуг, у якому відкритий рахунок Отримувача для зарахування коштів за платіжною операцією.
- 2.1.12. **Платник** – особа, з рахунку якої ініціюється платіжна операція на підставі платіжної інструкції. Платником може бути фізична особа, фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність чи юридична особа.
- 2.1.13. **Отримувач** – особа, на рахунок якої зараховується сума платіжної операції. Отримувачами є:
1) фізичні особи-підприємці, фізичні особи, що здійснюють незалежну професійну діяльність та юридичні особи, з якими ФК уклала договори про надання платіжних послуг (договори про прийом платежів);
2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України);
3) фізичні особи, фізичні особи-підприємці, фізичні особи, що здійснюють незалежну професійну діяльність та юридичні особи, реквізити яких Платник зазначив в платіжній інструкції.
- 2.1.14. **Платіжний застосунок ННПП/сайт ННПП** – спосіб комунікації та ініціювання Платником платіжної операції. Платник переходить:
1) на сайт ФК за адресою <https://www.portmone.com.ua/> (далі – Сайт ФК);
2) або мобільний застосунок Portmone.com для операційних систем iOS та Android (далі – Мобільний застосунок ФК);
3) або платіжну сторінку ФК, розміщену на сайті та/або в мобільному застосунку Отримувача (так званий Payment Gateway та SDK відповідно);
4) або за посиланням (структурованим посиланням), створеним та виставленим Отримувачем для оплати (так званий інвойс), у тому числі з використанням QR коду, який веде на платіжну сторінку.
- 2.1.15. **ЕПЗ** – електронний платіжний засіб – платіжний інструмент, реалізований на будь-якому носії, що містить в електронній формі дані, необхідні для ініціювання платіжної операції та/або здійснення інших операцій, визначених договором з емітентом. Для ініціювання платіжної операції Платник може використовувати такі ЕПЗ як:
1) платіжна картка (електронний платіжний засіб у вигляді пластикової чи іншого виду картки), емітованої в «карткових» платіжних системах VISA, MasterCard, UnionPay International чи НПС «ПРОСТІР»;
2) токенізована платіжна картка – унікальний цифровий ідентифікатор, який створений відповідно до технологій платіжних систем, в результаті заміни реквізитів платіжних карток (віртуальних, фізичних) для здійснення платіжних та/або інших операцій (технології VTS, M4M, Click to Pay);
3) токенізована платіжна картка у застосунках Google Pay та Apple Pay.
- 2.1.16. **Платіжна інструкція** – розпорядження ініціатора надавачу платіжних послуг щодо виконання платіжної операції.
- 2.1.17. **Платіжний пристрій** – технічний пристрій (банківський автомат, платіжний термінал, програмно-технічний комплекс самообслуговування, програмно-апаратне середовище мобільного телефону, системи онлайн-банкінгу, клієнт-банку, каса банку, інший пристрій), що дає змогу Платнику ініціювати платіжну операцію, а також виконати інші операції згідно з функціональними можливостями цього пристрою.
- 2.1.18. **НПП** – надавач платіжних послуг.
- 2.1.19. **ПС («не карткова»)** – система для виконання платіжних операцій із формальними та стандартизованими домовленостями і загальними правилами щодо процесингу, клірингу та/або виконання розрахунків між учасниками платіжної системи, в межах якої не здійснюється емісія платіжних карток.

2.1.20. **Платіжний інструмент** – персоналізований засіб, пристрій та/або набір процедур, що відповідають вимогам законодавства та погоджені Платником і ФК для надання платіжних інструкцій. ФК приймає такі види Платіжних інструментів як: електронні платіжні засоби (ЕПЗ).

2.1.21. **Фактичний платник (ФП)** – особа, яка в платіжній інструкції НПП, що обслуговує Фактичного платника, та/або НПП (Учасника ПС) зазначена фактичним платником і грошові зобов'язання якої виконує НПП шляхом ініціювання платіжної операції зі свого рахунку.

2.1.22. Основною функцією ФК є надання Платникам та Отримувачам послуг з переказу коштів за платіжними операціями, що ініційовані через Платіжний застосунок НПП/сайт НПП з використанням ЕПЗ.

2.1.23. ФК є непрямим учасником, через банки-еквайри, таких «карткових» платіжних систем як VISA (оператор Visa International Service Association), MasterCard (оператор Mastercard International Incorporated), Національної платіжної системи «Український платіжний простір» («ПРОСТІР») (оператор Національний банк України) та прямим учасником «не карткових» платіжних систем «Фінансовий світ» (оператор ТОВ «Українська платіжна система») та «City24» (оператор ТОВ «ФК «ФЕНІКС»). ФК надає послуги під знаком для товарів та послуг TM Portmone та Portmone.com.

2.1.24. Порядок діяльності ФК в «карткових» та «не карткових» ПС визначається правилами, встановленими оператором відповідної ПС. При виконанні ФК переказу коштів в межах «не карткової» ПС може здійснюватися взаємозалік на основі клірингу або кожна платіжна інструкція виконуватися окремо.

Інші терміни вживаються у значенні, наведеному у Законі України «Про платіжні послуги» та нормативно-правових актах Національного банку України.

3. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ В «КАРТКОВІЙ» ПС

3.1. Виконання ФК платіжної операції з переказу коштів без відкриття рахунку в межах «карткової» ПС (**Графічна схема №1 – пункт 3.4. цих Правил**) відбувається наступним чином:

1) Платник за допомогою мобільного телефону (смартфону), персонального комп'ютера, планшета, ноутбука переходить (заходить) у Платіжний застосунок НПП/сайт НПП, де має можливість обрати (заповнити) необхідні поля (реквізити) для подання платіжної інструкції в електронній формі. Перелік реквізитів платіжної інструкції складається з обов'язкових реквізитів, без яких неможливе виконання платіжної операції, та факультативних реквізитів, наявність яких залежить від категорії Отримувача, на користь якого здійснюється платіжна операція (наприклад, у разі ініціювання платіжної операції на користь Отримувача, який надає житлово-комунальні послуги, в платіжній інструкції може бути інформація про покази лічильника та суму переплати/заборгованості тощо). До обов'язкових реквізитів платіжної інструкції належать:

- 1) дата складання і номер;
- 2) унікальний ідентифікатор Платника та/або найменування/прізвище, власне ім'я, по батькові (за наявності), код платника та номер його рахунку;
- 3) найменування надавача платіжних послуг платника;
- 4) суму цифрами та/або словами;
- 5) призначення платежу;
- 6) унікальний ідентифікатор отримувача або найменування/прізвище, власне ім'я, по батькові (за наявності), код отримувача та номер його рахунку;
- 7) найменування надавача платіжних послуг Отримувача.

Для платіжних операцій, ініційованих з використанням ЕПЗ без фізичної присутності Платника за місцезнаходженням ФК, не вимагається проставлення (накладання) підпису Платника.

У разі ініціювання платіжної операції з використанням ЕПЗ, що емітований нерезидентом України, додатковими реквізитами платіжної інструкції є інформація, що така платіжна операція є транскордонним переказом, ініційованим в іноземній валюті, та надає змогу НППзОР Отримувача отримати всі необхідні дані для виконання функцій агента валютного нагляду, зокрема, отримати інформацію про Платника, передбачену Законом України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 року №361-ІХ та Законом України «Про валюту і валютні операції» від 21.06.2018 року №2473-VIII.

ФК забезпечує фіксування в операційно-обліковій системі дати і часу надходження платіжної інструкції, прийняття її до виконання (або відмови в її прийнятті), виконання платіжної інструкції.

Після заповнення Платником реквізитів платіжної інструкції в електронній формі, Платник має право ще раз переглянути їх та за потреби змінити. Також у Платника є можливість відмовитися від подання платіжної інструкції та закрити сторінку сайту чи Платіжний застосунок, що не призведе до виконання ФК платіжної операції.

2) Якщо Платник заповнив (проставив, обрав) всі необхідні реквізити (поля) платіжної інструкції в електронній формі та згоден ініціювати платіжну операцію на користь Отримувача, то такий Платник переходить на захищену сторінку ФК, яка обслуговується технологічним оператором ТОВ «Портмоне» (ТОВ «Портмоне» щорічно проходить аудит безпеки PCI DSS (Payment Card Industry Data Security Standard)), для введення реквізитів ЕПЗ (PAN, термін дії, CVV/CVC-код) або вибору ЕПЗ у вигляді токенованої платіжної картки (токенована платіжна картка за технологією VTS, M4M або Click to Pay; токенована платіжна картка у застосунку Google Pay та Apple Pay)).

3) Після отримання від Платника інформації про реквізити ЕПЗ ТОВ «Портмоне» та/або ФК передає платіжну інструкцію Платника та надсилає запит про можливість здійснення авторизації ЕПЗ (процедура отримання дозволу на проведення платіжної операції з використанням ЕПЗ) засобами технічного протоколу до Процесингової установи. Далі Процесингова установа передає таку платіжну інструкцію та запит на здійснення авторизації відповідному еквайру, з яким ФК уклала договір.

4) Еквайр через інфраструктуру відповідної «карткової» ПС разом з платіжною інструкцією Платника надсилає емітенту ЕПЗ запит на авторизацію.

5-6) Емітент на підставі отриманої платіжної інструкції Платника та запиту на авторизацію від еквайра через інфраструктуру «карткової» ПС перевіряє інформацію про рахунок Платника та встановлює факт належності такому Платнику відповідного ЕПЗ, який пов'язаний з рахунком. Після цього емітент засобами технічного протоколу надає еквайру одну з відповідей: 1) відмова в авторизації (наприклад, але не обмежуючись, недостатньо коштів на рахунку Платника, некоректно введено термін дії чи CVV/CVC-код, не пройдено процедуру посиленої автентифікації (протокол 3D Secure та інші способи посиленої автентифікації)); 2) згода на авторизацію. У випадку відмови в авторизації, емітент передає через інфраструктуру «карткової» ПС зазначену відповідь еквайру, еквайр віддає інформацію процесинговій установі, а процесингова установа передає відповідь емітента про відмову в авторизації до ФК/ТОВ «Портмоне». ФК відображає Платнику у Платіжному застосунку ННПП/сайті ННПП інформацію про неуспішну спробу ініціювання платіжної операції, яка не призвела до списання коштів з рахунку платника. Залежно від причин відмови в авторизації ТОВ «ФК МБК» може відображати Платнику отриману від еквайра інформацію про код помилки та його розшифрування.

7) Емітент після успішної авторизації присвоює операції код авторизації. Інформація про згоду на авторизацію (успішна авторизація) передається емітентом ЕПЗ через інфраструктуру «карткової» ПС до еквайра, а від еквайра до процесингової установи, яка, в свою чергу передає інформацію про результати авторизації до ФК/ТОВ «Портмоне». Зазначена технічна взаємодія (обмін запитами-повідомленнями) відбувається в режимі реального часу, як правило, не більше 30 секунд. ФК відображає Платнику інформацію про успішно ініційовану платіжну операцію та надає квитанцію, яка засвідчує зазначений факт.

8) Через операційно-облікову систему ФК формуються платіжні інструкції щодо переказу коштів на користь відповідного Отримувача, які експортуються до клієнт-банку Обслуговуючого банку. Уповноважені особи ФК підписують такі платіжні інструкції з метою їх виконання Обслуговуючим банком.

9) Обслуговуючий банк передає платіжні інструкції ФК до системи СЕП.

10) НППЗОР Отримувача отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача.

11) НППЗОР Отримувача відображає Отримувачу інформацію про зарахування суми коштів на рахунок Отримувача.

3.2. Додатковий опис до Графічної схеми №1:

3.2.1. Платником може бути: фізична особа, фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність чи юридична особа, яка на законних підставах використовує ЕПЗ. Отримувачем може бути: 1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про

надання платіжних послуг (договори про прийом платежів); 2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України); 3) фізичні особи-підприємці, фізичні особи, що здійснюють незалежну професійну діяльність та юридичні особи, реквізити яких Платник зазначив в платіжній інструкції. Територія здійснення платіжних операцій – Україна. Платник в момент ініціювання платіжної операції фізично може знаходитися в будь-якій точці світу, а також використовувати ЕПЗ, що емітоване нерезидентом України.

3.2.2. ФК в режимі реального часу (онлайн) передає дані про ініційовану платіжну операцію відповідно до узгодженого з Отримувачем протоколу обміну даними. Отримувач в режимі онлайн (якщо інше не передбачено договором ФК з Отримувачем) підтверджує зарахування коштів на баланс Платника в Отримувача.

3.2.3. Ініціювання платіжної операції здійснюється із застосуванням ЕПЗ. ЕПЗ реалізований на будь-якому носії, що містить в електронній формі дані, необхідні для ініціювання платіжної операції (дистанційної платіжної операції).

3.2.4. ЕПЗ дозволяє ідентифікувати його держателя. ЕПЗ може передаватися у власність або надаватися в користування Платнику в порядку та на умовах, визначеному договором з емітентом.

3.3. Умови та обмеження, що виконуються ФК при наданні платіжних послуг:

3.3.1. ФК безпосередньо не приймає та не видає кошти у готівковій формі. ФК укладає договори з банками та небанківськими надавачами платіжних послуг – учасниками ПС про прийом платежів, а також з банками-еквайрами договори про здійснення еквайрингу операцій, ініційованих за допомогою ЕПЗ;

3.3.2. ФК отримує від еквайрів кошти на свій розрахунковий рахунок та виконує їх переказ на користь Отримувача виключно в безготівковій формі у національній валюті України – гривні;

3.3.3. Отримувачем може виступати виключно особа резидент України. ФК укладає з кожним Отримувачем договір, що визначає умови та порядок надання платіжних послуг та/або укладає з Платником договір (оферту) про виконання платіжних операцій у відповідності до платіжних реквізитів зазначених Платником у платіжній інструкції;

3.3.4. Валюта переказу – гривня;

3.3.5. Основними завданнями ФК при наданні платіжних послуг з переказу коштів без відкриття рахунків є: підключення Отримувача до банку-еквайру з метою Авторизації ЕПЗ Платника, заведення для Отримувача віртуальних платіжних терміналів, інформація щодо яких потрапляє до бази даних «карткової» ПС; обмін інформацією за платіжними операціями між еквайром, ФК та Отримувачем; переказ коштів за платіжними операціями Платників консолідованою платіжною інструкцією в розрізі кожного Отримувача; сервісна та інформаційна підтримка Платників та Отримувачів.

3.3.6. ФК належить до фінансових установ-посередників, а тому в рамках участі в ПС отримує кошти від еквайрів (принципових учасників «карткових» ПС) та перераховує на рахунки Отримувачів, що відкриті у банках України та небанківських надавачах платіжних послуг України, які мають право на відкриття платіжних рахунків.

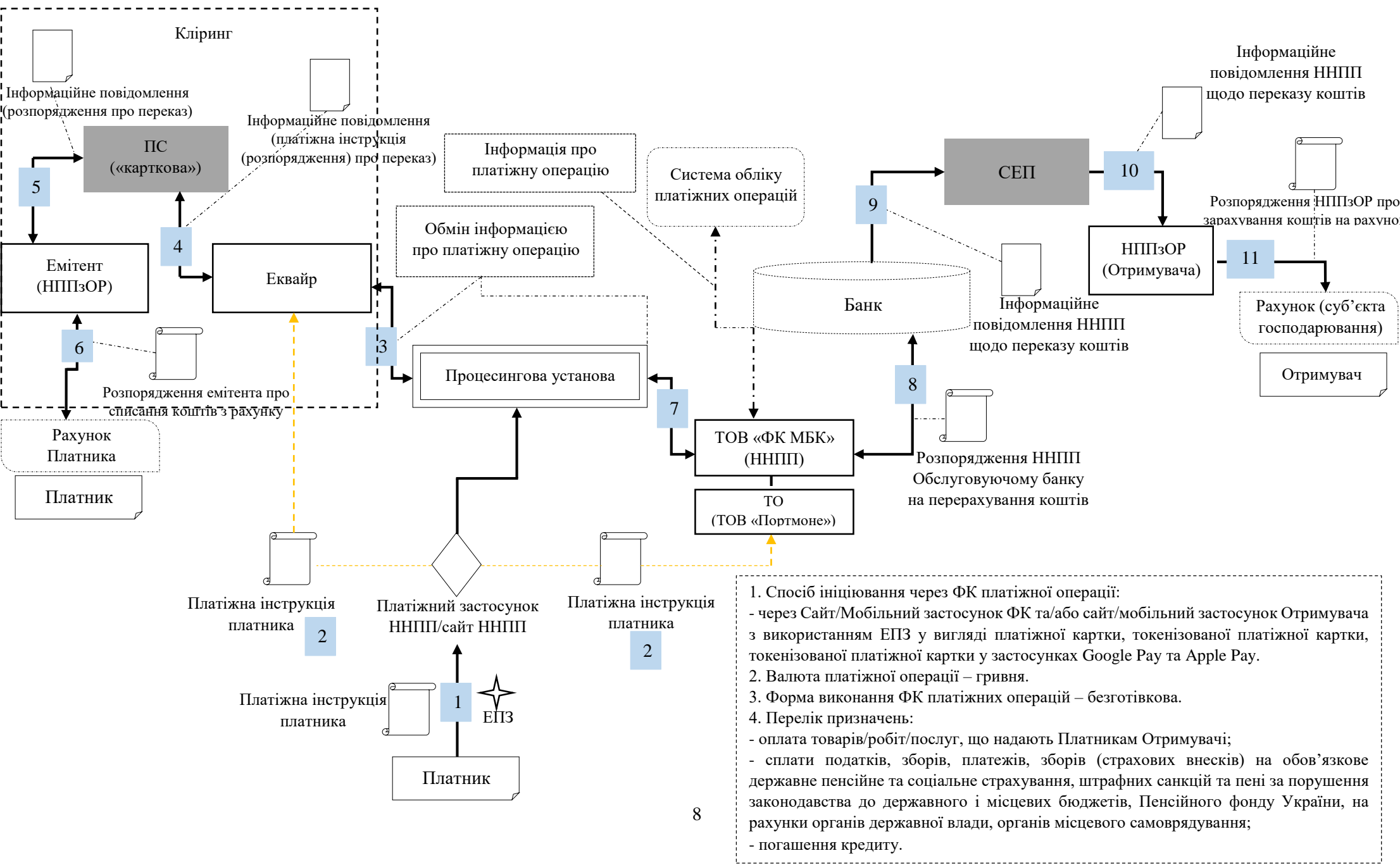
3.3.7. Така схема виконання платіжної операції використовується для: 1) оплати товарів, робіт, послуг в мережі Інтернет (так званий Е-Commerce); 2) погашення кредиту; 3) сплати житлово-комунальних послуг (в т. ч. ОСББ, ЖК, керуючі компанії, домофонні компанії, вивіз сміття та ін.); 4) поповнення мобільних; 5) сплати податків, зборів, платежів, зборів (страхових внесків) на обов'язкове державне пенсійне та соціальне страхування, штрафних санкцій та пені за порушення законодавства до державного і місцевих бюджетів, Пенсійного фонду України, на рахунки органів державної влади, органів місцевого самоврядування.

3.3.8. ФК в межах «карткової» ПС виконує наступні функції:

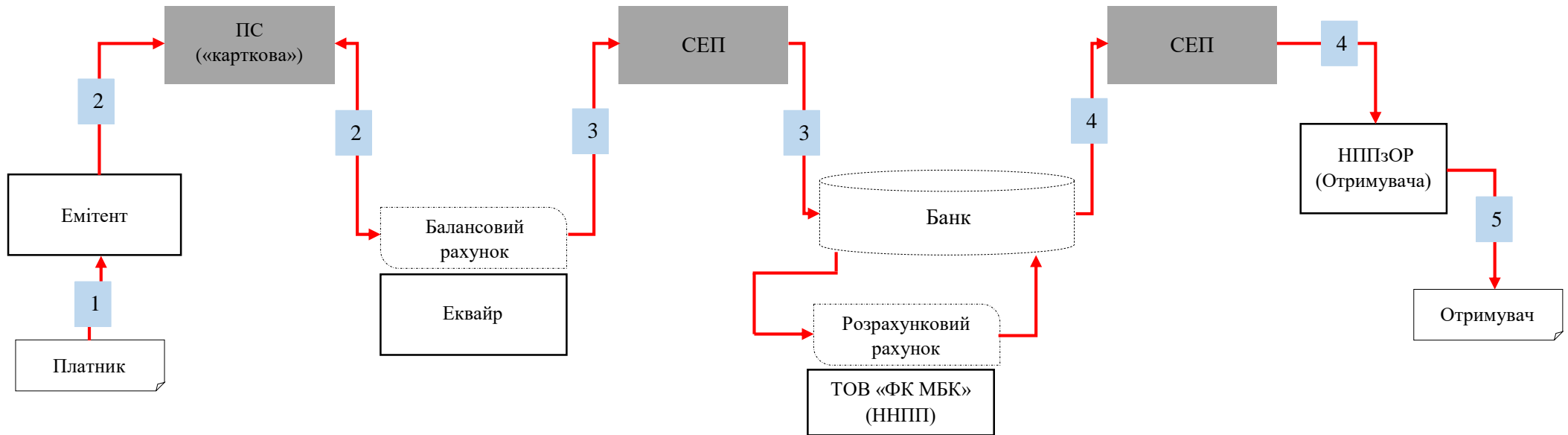
3.3.8.1. Технічного еквайрингу. ФК може надавати Отримувачам та/або еквайрам послуги щодо технологічного, інформаційного обслуговування операцій з використанням ЕПЗ.

3.3.8.2. Фінансового агрегатора (фасилітатора). Згідно з правилами «карткових» ПС ФК отримує консолідовані платіжні інструкції від еквайрів з подальшим перерахуванням коштів Отримувачам, що обслуговуються ФК.

3.4. Графічне зображення схеми виконання ФК платіжної операції з переказу коштів без відкриття рахунку в межах «карткової» ПС (інформаційні потоки) (Графічна схема №1):



3.5. Графічне зображення схеми виконання ФК платіжної операції з переказу коштів без відкриття рахунку в межах «карткової» ПС має наступний вигляд (схема руху коштів):



3.5.1. Фінансові взаєморозрахунки відбуваються у наступному порядку:

3.5.1.1. Після успішної Авторизації емітент блокує суму коштів за платіжною операцією на рахунку Платника та, в подальшому, списує кошти з рахунку Платника на транзитний рахунок емітента;

3.5.1.2. Емітент та еквайр здійснюють взаємні розрахунки шляхом клірингу;

3.5.1.3. Еквайр наступного операційного дня з моменту ініціювання платіжної операції з балансового рахунку перераховує через СЕП кошти ФК на розрахунковий рахунок в Банку ФК відповідно до контрольного реєстру, наданого ФК еквайром;

3.5.1.4. Після отримання коштів від еквайрів ФК відповідно до умов договорів про прийом платежів з кожним Отримувачем та з урахуванням строків передбачених Законом України «Про платіжні послуги», а також правилами відповідної ПС, переказує кошти Отримувачам в розрізі кожного Отримувача. Зазначені операції проходять через СЕП;

3.5.1.5. НППзОР Отримувача зараховує отримані від ФК кошти на рахунок Отримувача.

3.6. ФК в межах «карткової» ПС виконує наступні функції:

3.6.1. Технічного еквайрингу. ФК може надавати Отримувачам та/або еквайрам послуги щодо технологічного, інформаційного обслуговування операцій з використанням ЕПЗ.

3.6.2. Фінансового агрегатора (фасилітатора). Згідно з правилами «карткових» ПС ФК отримує консолідовані платіжні інструкції від еквайрів з подальшим перерахуванням коштів Отримувачам, що обслуговуються ФК.

3.7. Структура договірних відносин за участі ФК наступна:

3.7.1. ФК укладає з еквайром відповідний договір еквайрингу, який реєструється в НБУ та «картковій» ПС. Договір еквайрингу повинен містити: 1) платіжні інструменти, які приймаються для ініціювання платіжних операцій; 2) порядок оформлення документів, що підтверджують здійснення операції; 3) порядок і терміни/строки розрахунків між еквайром та ФК; 4) розмір комісійної винагороди, яку ФК сплачує еквайру; 5) процедури безпеки, яких має дотримуватися ФК під час приймання платіжних інструментів та передавання даних еквайру про проведені операції; 6) обов'язок ФК надавати інформацію, потрібну для виконання еквайром вимог законодавства України, що регулює відносини у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення; 7) відповідальність ФК та еквайра; 8) порядок розгляду спорів; 14) інші умови відповідно до законодавства України та вимог Положення про порядок емісії та еквайрингу платіжних інструментів, затвердженого Постановою Правління НБУ №164 від 29.07.2022 р.;

3.7.2. ФК укладає з Отримувачем договір про надання платіжних послуг (договір про прийом платежів). Договір про надання платіжних послуг укладається в письмовій формі (паперовій або електронній з використанням програмного комплексу ФК Portmone.Backoffice). Договір про надання платіжних послуг може укладатися шляхом приєднання Отримувача до договору про прийом платежів, розміщеного на веб-сайті ФК в мережі Інтернет за посиланням <http://www.fcmbk.com.ua/>. Усі поточні редакції публічної пропозиції укладення договору про прийом платежів зберігаються на зазначеному веб-сайті ФК із вказівкою строку їх дії. Отримувач має право в будь-який час отримати доступ до всіх редакцій публічної пропозиції укладення договору про прийом платежів. Прийняття Отримувачем публічної пропозиції укладення договору про прийом платежів відбувається шляхом підписання угоди-приєднання до договору про прийом платежів. Підписання Отримувачем та ФК угоди-приєднання до договору про прийом платежів відбувається з використанням засобів електронного підпису у порядку та з урахуванням вимог, передбачених законодавством у сфері електронного документообігу, електронних довірчих послуг, у тому числі, з урахуванням Положення про використання електронного підпису та електронної печатки, затвердженого Постановою Правління НБУ №172 від 20.12.2023 р.

3.7.3. Договір між ФК та Отримувачем повинен містити такі умови: 1) платіжні інструменти, які приймаються Отримувачем; 2) порядок оформлення документів, що підтверджують здійснення операції; 3) порядок і терміни/строки розрахунків між ФК та Отримувачем; 4) розмір комісійної винагороди, яку Отримувач сплачує ФК; 5) процедури безпеки, яких має дотримуватися ФК та Отримувач; 6) обов'язок Отримувача надавати інформацію, потрібну для виконання ФК вимог законодавства України, що регулює відносини у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення; 7) перелік інформації, що має надавати Отримувач ФК, включаючи інформацію про види діяльності Отримувача для призначення відповідного коду категорії його діяльності (МСС - Merchant category code), порядок та строки її надання; 8) обов'язок Отримувача надати ФК інформацію про зміну видів його діяльності, які повідомлялися ФК для призначення коду категорії його діяльності; 9) відповідальність Отримувача за надання недостовірної інформації про види своєї діяльності; 10) право ФК відмовитися від підтримання ділових відносин та порядок повідомлення ФК про намір використати таке право; 11) порядок та строк ініціювання Отримувачем повернення коштів за повернутий товар (ненадану послугу), який(а) був(ла) придбаний(а) з використанням платіжного інструменту (з урахуванням вимог законодавства України з питань захисту прав споживачів); 12) відповідальність ФК та Отримувача за порушення умов договору та/або правил ПС; 13) порядок розгляду спорів; 14) інші умови відповідно до законодавства України або на розсуд ФК та Отримувача.

3.8. Порядок виконання ФК платіжних операцій:

3.8.1. Інформаційні потоки:

3.8.1.1. ФК на підставі укладеного з Отримувачем договору звертається до еквайра для здійснення налаштування віртуальних платіжних терміналів еквайра під кожного Отримувача з метою обробки платіжних операцій (направлення авторизаційних/клірингових запитів) у «картковій» ПС, ініційованих за допомогою ЕПЗ;

3.8.1.2. ФК надає можливість Платнику у інтерфейсі Платіжного застосунку ННПП/С отримати рахунок від Отримувача та зазначити необхідну інформацію для ініціювання платіжної операції, що відбувається наступним чином:

- ФК через Білінгову систему направляє запит до системи Отримувача на отримання рахунку із зазначенням параметрів (перелік та формат полів зазначаються в Заяві на реєстрацію Отримувача в Білінговій системі, яка є додатком до договору про прийом платежів), що однозначно ідентифікують Платника. У відповідь на запит Отримувач надає інформацію про рахунок, яка може містити суму заборгованості платника, період за який виставлено рахунок, деталізацію нарахувань, показники лічильників, суму переоплати за попередній період тощо. У випадку передплати послуг Отримувача рахунок надається із сумою заборгованості «0 грн.» і сума платіжної операції може визначатись Платником самостійно.

- Обмін запитами/повідомленнями між ФК та Отримувачем відбувається у відповідності до протоколу взаємодії, який є невід'ємною частиною договору про прийом платежів та розміщується за посиланням <https://docs.portmone.com.ua/docs/uk/PaymentGatewayUa/>.

- Кожному рахунку в Білінговій системі присвоюється унікальний обліковий номер платіжної операції.

- Якщо Отримувач не зміг однозначно ідентифікувати Платника за наданими параметрами (або Платник знаходиться у Отримувача в статусі не активного) ФК отримує відповідний код помилки.

- Після успішної транзакції ФК відображає обліковий номер платіжної операції в Білінговій системі в статусі оплаченого в режимі реального часу (не пізніше 15 хвилин з моменту Авторизації).

- У випадку підтримки програмно-технічними засобами Отримувача функціоналу зарахування коштів в режимі реального часу, ФК передає за допомогою Білінгової системи відповідне повідомлення про здійснення успішної транзакції Отримувачу, що призводить до зарахування Отримувачем суми транзакції на особовий рахунок платника (інформаційний потік).

- ФК для контролю прийнятих коштів не пізніше 13 год. 00 хв. наступного банківського дня за днем переказу коштів від ФК, повинна надіслати контрольний реєстр Отримувачу. У випадку розбіжностей між контрольним реєстром ФК та даними в системі Отримувача, ФК та Отримувач вживають заходів для аналізу ситуації та виявлення зайвих та/або відсутніх транзакцій.

- Для ідентифікації Отримувача в Білінговій системі та внесення відомостей до Системи Portmone.com ФК може надати Отримувачу окремий логін та спеціальний цифровий ключ, а також виділену фіксовану ір-адресу.

- Під час обміну запитами/повідомленнями між Отримувачем та ФК використовується зашифрований канал зв'язку з використанням криптографічного захисту.

3.8.1.3. *Білінгова система* – це сукупність програмно-технічних засобів за допомогою яких відбувається інформаційно-технічний обмін між ФК та Платником, надавачами платіжних послуг, Отримувачем, платіжними системами.

Складовою частиною Білінгової системи є Система Portmone.com - сукупність програмно-технічних засобів, за допомогою яких відбувається інформаційний обмін між ФК та Отримувачем в процесі здійснення Платниками платіжних операцій на користь Отримувача, та яка призначена для: обробки даних за рахунками Отримувача, перевірки правильності даних про рахунок, підтвердження суми заборгованості Платника перед Отримувачем; передачі даних надавачам платіжних послуг; передачі даних про ініційовану платником платіжну операцію в базу даних Отримувача; формування і надання Отримувачу контрольного реєстру з даними про здійснені платіжні операції.

3.8.1.4. Під рахунком розуміється електронний документ, виставлений Отримувачем на оплату його послуг (наприклад, рахунок за житлово-комунальні послуги, рахунок за послуги доступу до мережі Інтернет тощо).

3.8.1.5. Після того, як Платник підтверджує намір ініціювати платіжну операцію відповідно до сформованих параметрів на користь обраного Отримувача, Платник перенаправляється на захищену платіжну сторінку ФК, що обслуговується технологічним оператором платіжних послуг Товариством

з обмеженою відповідальністю «Портмоне» (код за ЄДРПОУ 31868613), яке щорічно проходить аудит безпеки PCI DSS (Payment Card Industry Data Security Standard);

3.8.1.6. На платіжній сторінці Платник обирає метод оплати (платіжна картка; токенизована платіжна картка за технологією VTS, M4M або Click to Pay; токенизована платіжна картка у застосунку Google Pay та Apple Pay) та залежно від обраного методу оплати вводить необхідні реквізити ЕПЗ (номер платіжної картки (PAN), строк дії, CVV/CVC-код). Далі еквайр з використанням послуг процесингової установи обробляє ці дані та передає їх на Авторизацію. Еквайр та процесингова установа здійснюють обмін інформаційними повідомленнями за принципом «запит-відповідь» з емітентом. За результатами такого обміну відбувається Авторизація, тобто, отримання від емітента дозволу на проведення платіжної операції. Платіжна сторінка з рахунком Отримувача на Сайті ФК має такий вигляд (наведений приклад є виключно зразком, зміна дизайну сторінки не потребує внесення змін до цих Правил):

portmone.com Мобільний Перекази Оплата за реквізитами Страхування Кабінет

Дата рахунку: 09.04.2024, сума рахунку: 1.53 грн.

Реквізити платежу

	борг	з нього сплатити	нараховано	до сплати	разом
Газорозподіл	0.00	0.00	1.53	1.53	1.53

Зберегти без оплати Копіювати Попередні рахунки

Сума рахунку до сплати: 1.53
комісія 3.00

Всього до сплати: 4.53

Google Pay

sense bank

Картка відправника
SENSE **€0000

MM/PP
12/26

CVV




Оплатити

3.8.1.7. Емітент після успішної Авторизації присвоює транзакції код авторизації. Дані про успішну (не успішну) платіжну операцію передаються до еквайра, а останній перенаправляє їх ФК. ФК в режимі онлайн передає дані про ініційовану платіжну операцію відповідно до узгодженого з Отримувачем протоколу обміну даними. Отримувач в режимі онлайн (якщо інше не передбачено договором ФК з Отримувачем) підтверджує зарахування коштів на баланс Платника в Отримувача, а ФК в режимі онлайн використовуючи інтерфейс Сайту/Мобільного застосунку ФК повідомляє Платника про статус платіжної операції та надає можливість завантажити або надіслати на електронну адресу/в месенджер документ за операцією з використанням платіжного інструменту (квитанцію);

3.8.1.8. Платіжна сторінка, інтегрована до Сайту Отримувача (Payment Gateway) має наступний вигляд (наведений приклад є виключно зразком, зміна дизайну сторінки не потребує внесення змін до цих Правил):

Portmone.com
100.00 грн
Приховати ^

Описание заказа
№ замовлення: test_1
Сума: 100.00 грн

 Карта  Portmone.com  **NEW** Click to pay

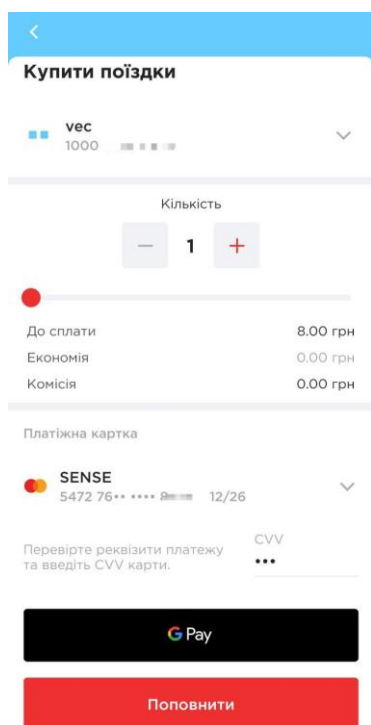
Номер картки _____ MM/PP CVV _____
Ваш e-mail (обов'язково) _____

Оплатити 100 грн

[Публічна оферта](#)
[Скасувати оплату](#)

3.8.1.9. У випадку неуспішної Авторизації повідомляється код помилки. Дані до системи Отримувача не передаються, а ФК в режимі онлайн, використовуючи інтерфейс Сайту/Мобільного застосунку, повідомляє текст помилки.

3.8.1.10. Зразок платіжної сторінки та сторінки після успішного ініціювання платіжної операції у Мобільному застосунку ФК має наступний вигляд:



Купити поїздки

vec 1000

Кількість: - 1 +

До сплати 8.00 грн
Економія 0.00 грн
Комісія 0.00 грн

Платіжна картка

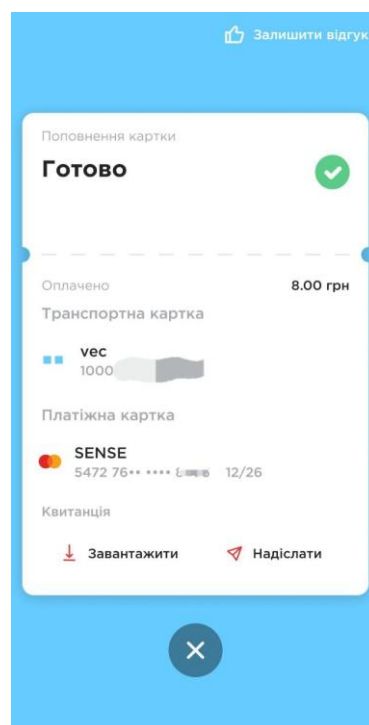
SENSE 5472 76** **** 12/26

Перевірте реквізити платежу та введіть CVV карти.

CVV

Г Pay

Поповнити



Залишити відгук

Поповнення картки

Готово

Оплачено 8.00 грн

Транспортна картка

vec 1000

Платіжна картка

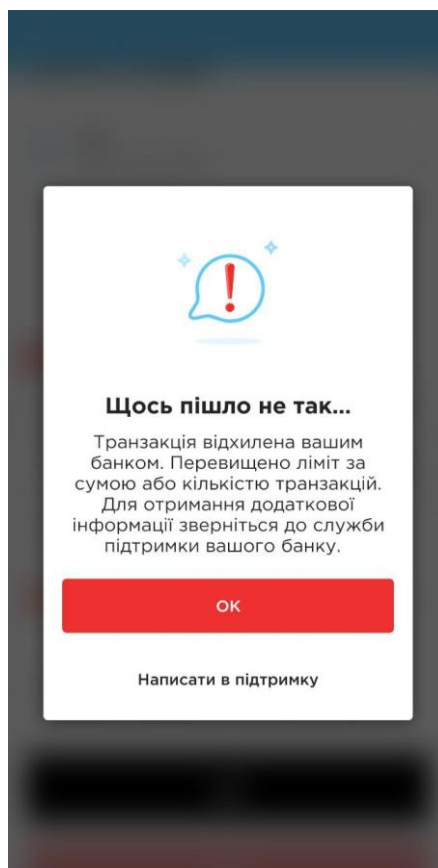
SENSE 5472 76** **** 12/26

Квитанція

Завантажити Надіслати

X

3.8.1.11. Зразок сторінки після неуспішного ініціювання платіжної операції у Мобільному застосунку ФК має наступний вигляд (наведено як приклад, текст помилки може суттєво відрізнятись залежно від причин відмови):



3.9. ФК для контролю платіжних операцій, ініційованих на користь кожного з Отримувачів, не пізніше 13 год. 00 хв. кожного операційного дня отримує від еквайра контрольний реєстр платіжних операцій за попередній(і) календарний(і) день(ні) в період з 00год. 00хв. 00сек. по 23год. 59хв. 59сек. за Київським часом). В контрольному реєстрі зазначається детальний перелік операцій та загальна сума всіх операцій за попередній календарний день в розрізі кожного Отримувача. У випадку розбіжностей між контрольним реєстром та даними в інформаційній системі ФК, проводяться заходи для аналізу ситуації та виявлення зайвих та/або відсутніх платіжних операцій.

3.10. Фінансові взаєморозрахунки відбуваються у наступному порядку:

3.10.1. У випадках передбачених договорами з Отримувачами, ФК може забезпечувати збереження коштів користувачів платіжних послуг шляхом перерахування Отримувачу авансового (гарантійного) платежу як засобу забезпечення виконання зобов'язань відповідно до ч. 2 ст. 546 Цивільного кодексу України або забезпечувати кошти користувачів банківською гарантією;

3.10.2. Ініціювання платіжної операції Платником відбувається в межах авансового (гарантійного) платежу, наданої банківської гарантії або в межах лімітів, затверджених кожним Отримувачем;

3.10.3. Після успішної Авторизації емітент блокує суму коштів за платіжною операцією на рахунку Платника та, в подальшому, списує кошти з рахунку Платника;

3.10.4. Після успішної Авторизації еквайр, наступного операційного дня, перераховує кошти ФК на розрахунковий рахунок в Банку ФК відповідно до контрольного реєстру, наданого ФК еквайром;

3.10.5. Після отримання коштів від еквайрів ФК відповідно до умов договорів про прийом платежів з кожним Отримувачем та з урахуванням строків передбачених Законом України «Про платіжні послуги», а також правилами відповідної ПС, перераховує консолідованими платіжними інструкціями кошти Отримувачам в розрізі кожного Отримувача. Зазначені операції проходять через СЕП;

3.10.6. Еквайр отримує від емітента компенсацію здійсненого платежу в рамках клірингових взаєморозрахунків в межах ПС.

3.11. Еквайр (учасник ПС) виконує наступні основні функції:

- 3.11.1. Проводить первинну обробку операцій ініційованих за допомогою ЕПЗ і бере на себе зобов'язання з організації розрахунків з Отримувачами;
- 3.11.2. Проводить налаштування Платіжних пристроїв та віртуальних платіжних терміналів під кожного окремого Отримувача;
- 3.11.3. Організовує інформаційно-технічну взаємодію з ФК та перерахування на розрахункові рахунки ФК коштів за платіжними операціями ініційованими Платниками на користь Отримувачів, з якими у ФК укладені відповідні договори про прийом платежів;
- 3.11.4. Здійснює моніторинг платіжних операцій, аналіз діяльності нових та вже існуючих Отримувачів, перевіряє Отримувачів щодо можливого ризику шахрайства з їх боку;
- 3.11.5. Здійснює постійний моніторинг операцій, ініційованих за допомогою ЕПЗ, з метою ідентифікації неакцептованих, помилкових, неналежних, підозрілих платіжних операцій та вжиття заходів із запобігання або припинення зазначених операцій. Моніторинг здійснюється з урахуванням критеріїв, що встановлені правилами відповідної ПС. Загальні правила моніторингу платіжних операцій, в першу чергу порогових та підозрілих, встановлюються чинним законодавством України та нормативно-правовими актами НБУ.
- 3.11.6. Бере участь у програмах лояльності, рекламно-маркетингових акціях ПС з метою популяризації нових сервісів, платіжних методів та інструментів.
- 3.11.7. Виконує інші функції, передбачені законодавством України та правилами ПС.
- 3.12. Банк ФК виконує наступні основні функції:
 - 3.12.1. відкриває розрахункові та поточні рахунки ФК як клієнту банку;
 - 3.12.2. з метою покриття ризиків технічної неплатоспроможності відкриває ФК кредитну лінію (овердрафт) для здійснення короткострокового кредитування;
 - 3.12.3. при здійсненні внутрішньобанківських платіжних операцій приймає сформовані платіжні інструкції і проводить їх виконання шляхом списання відповідних сум коштів з розрахункових рахунків ФК та їх зарахування на поточні рахунки Отримувачів, що відкриті в цьому Банку;
 - 3.12.4. при здійсненні міжбанківських платіжних операцій (за умови, якщо розрахунковий рахунок ФК та Отримувача в різних банках) приймає сформовані ФК платіжні інструкції і проводить їх виконання шляхом списання відповідних сум коштів з розрахункового рахунку ФК та їх переказ через СЕП на поточні рахунки Отримувачів, що відкриті в іншому банку;
 - 3.12.5. може виступати гарантом (банківська гарантія) завершення розрахунків ФК з Отримувачами згідно з порядком, визначеним умовами договорів;
 - 3.12.6. виконує інші функції, визначені законодавством України.
- 3.13. Процесингова установа виконує такі функції:
 - 3.13.1. забезпечує в межах повноважень, визначених оператором ПС виконання за платіжними операціями авторизації, моніторингу, збору, оброблення та зберігання інформації, надання обробленої інформації учасникам розрахунків, обмін інформацією між учасниками ПС, цілодобову безперервну Авторизацію платіжних операцій, ініційованих з використанням ЕПЗ;
 - 3.13.2. забезпечує маршрутизацію запитів на Авторизацію та підтримує ведення актуальних таблиць маршрутизації;
 - 3.13.3. обслуговує учасників ПС та модулі безпеки, підключені до ПС;
 - 3.13.4. проводить безперервний моніторинг надійності і безперервності функціонування Платіжних пристроїв учасників ПС;
 - 3.13.5. забезпечує збирання, зберігання та передавання до оператора Платіжної системи інформації щодо нештатних ситуацій, що виникали під час роботи;
 - 3.13.6. розраховує за поточну добу (або визначений розрахунковий період) нетто-позиції та формує і надсилає еквайру нетто-файл для виконання кінцевих розрахунків, надає детальну інформацію за усіма платіжними операціями, на підставі яких були розраховані нетто-позиції;
 - 3.13.7. формує та подає оператору та учасникам ПС звітність за формою та обсягами, що встановлена внутрішніми документами оператора ПС та інформаційні виписки про ініційовані платіжні операції, які були оброблені за участі Процесингової установи;
 - 3.13.8. забезпечує підтримку бази даних учасників ПС та формування встановлених форм звітності для них згідно з умовами укладених договорів з учасниками ПС;
 - 3.13.9. забезпечує згідно з регламентом ПС безперервну та якісне інформаційне обслуговування учасників ПС та надання їм необхідних послуг;

- 3.13.10. забезпечує конфіденційність інформації відповідно до умов укладених договорів;
- 3.13.11. бере участь та забезпечує відповідною інформацією оператора ПС при розгляді і вирішенні спірних питань та конфліктних ситуацій між учасниками ПС;
- 3.13.12. виконує інші функції, що не суперечать чинному законодавству України та правилам ПС.

3.14. Комісія (комісійна винагорода).

- 3.14.1. Розміри комісій та порядок їх обчислення та сплати визначаються у відповідних договорах, які укладаються ФК з Отримувачами та еквайрами.
- 3.14.2. Нарахування комісії здійснюється за платіжні послуги з переказу коштів без відкриття рахунків та комісійна винагорода може утримуватися з Платника та/або Отримувача.
- 3.14.3. Комісії можуть утримуватись у визначеному відсотку від суми платіжної операції або фіксованій сумі.
- 3.14.4. Кожний з учасників оброблення транзакції сплачують або отримують комісійну винагороду (інтерчейндж) за послуги з її оброблення у відповідності до правил ПС.
- 3.14.5. ФК зобов'язана:
- ознайомити держателя ЕПЗ з розміром власної комісійної винагороди за виконання платіжної операції (за наявності такої комісійної винагороди) безпосередньо перед ініціюванням такої операції;
 - забезпечити можливість держателю ЕПЗ відмовитись від розпочатої платіжної операції після ознайомлення з розміром комісійної винагороди ФК.

4. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ В «НЕ КАРТКОВІЙ» ПС

4.1. Опис виконання ФК платіжних операцій в межах «не карткової» ПС містить багато спільних рис з виконанням операцій в межах «карткової» ПС. Відмінності полягають у тому, що в межах «не карткової» ПС не здійснюється емісія платіжних карток; через ФК може відбуватися ініціювання Платником платіжної операції, або ФК завершуватиме платіжну операцію та перераховуватиме кошти Отримувачу; Учасник ПС, який має відповідну ліцензію, може приймати готівкові кошти від Платників та перераховувати ФК у безготівковій формі з метою переказу коштів на користь Отримувача.

Ініціювання платіжної операції може здійснюватися через Платіжні пристрої, в тому числі, через банківський автомат, платіжний термінал, програмно-технічний комплекс самообслуговування, програмно-апаратне середовище мобільного телефону, системи онлайн-банкінгу, клієнт-банку, каса банку, інший пристрій банку чи небанківського надавача платіжних послуг – Учасника ПС, а також за допомогою інших платіжних пристроїв, якщо це не заборонено чинним законодавством України.

4.2. Зазначені схеми виконання платіжних операцій має перевагу у тому, що учасники «не карткових» ПС мають можливість використовувати інфраструктуру інших учасників або приймати платежі на користь тих отримувачів, з якими не мають укладених договорів про надання платіжних послуг. Наприклад, учасників №1 має мережу ПТКС, а учасник №2 має укладені договори з отримувачами про надання платіжних послуг. Таким чином, учасник №1 здійснює прийом коштів від платників через ПТКС, переказує кошти на рахунок учасника №2, який, в свою чергу перераховує кошти на користь кінцевого отримувача. Зазначені операції здійснюються через розрахунковий банк ПС та під наглядом оператора ПС. Учасники ПС через розрахунковий банк ПС можуть здійснювати розрахунки шляхом клірингу.

Схема виконання платіжної операції використовується для (призначення платежу):

- оплата товарів, робіт, послуг, що надають Отримувачі Платникам/фактичним платникам;
- сплати податків, зборів, платежів, зборів (страхових внесків) на обов'язкове державне пенсійне та соціальне страхування, штрафних санкцій та пені за порушення законодавства до державного і місцевих бюджетів, Пенсійного фонду України, на рахунки органів державної влади, органів місцевого самоврядування;
- погашення кредиту.

4.3. Виконання ФК платіжних операцій в межах «не карткової» ПС можливе двома способами:

4.3.1. Через ФК відбувається ініціювання Платником платіжної операції – ФК не має договорів про надання платіжних послуг з Отримувачами, але інші Учасники «не карткової» ПС мають такі договори. ФК отримує від Учасників ПС засобами технічного протоколу обміну даними відомості про рахунки Отримувачів, які містять суму нарахувань, реквізити Отримувача, особовий рахунок/номер

договору абонента та інші дані, які дозволяють ідентифікувати Платника в системі Отримувача та виконати платіжну операцію. Платники звертаються до ФК та ініціюють платіжну операцію на користь такого Отримувача. ФК забезпечує приймання коштів Платників та подальший переказ на рахунок Учасника ПС у Розрахунковому банку, який, в свою чергу, переказує кошти на користь Отримувача;

4.3.2. ФК завершує платіжну операцію та перераховує кошти Отримувачу – ФК має укладені договори про надання платіжних послуг (прийом платежів) з Отримувачами та бажає надати таким Отримувачам можливість оплати їх послуг в додаткових каналах, наприклад ПТКС, чи готівкою. Оскільки, ФК не має мережі ПТКС чи ліцензії на здійснення готівкових операцій, ФК звертається до інших Учасників ПС, які мають такі платіжні пристрої та/або право приймати готівкові кошти від платників. Зазначені Учасники ПС здійснюють приймання коштів Платників (готівкових та безготівкових) та переказують прийняті кошти у безготівковій формі на рахунок ФК у Розрахунковому банку ПС. ФК в межах укладених договорів з Отримувачами або на підставі поданої платником платіжної інструкції здійснює переказ коштів на рахунки таких Отримувачів.

Виконання платіжних операцій в межах «не карткової» ПС здійснюється під наглядом оператора ПС та відповідно до правил такої платіжної системи, що погоджені з Національним банком України.

4.4. Розрахунковий банк «не карткової» ПС – уповноважений оператором відповідної платіжної системи банк, що бере участь у проведенні розрахунків у платіжній системі.

4.5. З метою спрощення, ФК не відображала на схемах рух інформаційних та грошових потоків в частині ініціювання Платником платіжної операції з використанням ЕПЗ, відомості про яку потрапляють до «карткових» ПС VISA, MasterCard, «ПРОСТІР».

4.6. Виконання ФК платіжної операції, ініційованої з використання ЕПЗ, в межах «не карткової» ПС (**Графічна схема №2**) відбувається наступним чином:

1) Фактичний платник за допомогою Платіжного пристрою (банківський автомат, платіжний термінал, програмно-технічний комплекс самообслуговування, програмно-апаратне середовище мобільного телефону, системи онлайн-банкінгу, клієнт-банку, каса банку, інший пристрій) Учасника ПС заповнює необхідні поля (реквізити) для подання платіжної інструкції. Перелік реквізитів та форма подання платіжної інструкції визначається, з урахуванням вимог законодавства України, Учасником «не карткової» ПС, який приймає від Фактичного платника платіжну інструкцію. При цьому ФК може надати Учаснику «не карткової» ПС інформацію про факультативні реквізити платіжної інструкції, необхідні для ідентифікації Отримувачем Фактичного платника (наприклад, у разі ініціювання платіжної операції на користь Отримувача, який надає житлово-комунальні послуги, в платіжній інструкції може бути інформація про покази лічильника та суму переплати/заборгованості тощо).

2) Після заповнення Фактичним платником всіх необхідних реквізитів платіжної інструкції та надання Учаснику ПС згоди на виконання платіжної інструкції, Фактичний платник зазначає Учаснику ПС реквізити ЕПЗ, з якого бажає ініціювати платіжну операцію. ФК не зображає на Графічній схемі №2 порядок використання Фактичним платником ЕПЗ, типи ЕПЗ, які приймаються Учасником ПС та порядок взаємодії Учасника ПС з еквайрами, процесинговими установами та емітентами, оскільки, такий порядок безпосередньо визначається Учасником ПС, який приймає до виконання платіжну операцію. Учасник ПС самостійно визначає способи, умови та порядок взаємодії з Фактичним платником, а також перелік ЕПЗ, які приймає Учасник ПС для ініціювання платіжних операцій.

3) Учасник ПС за результатами авторизації ЕПЗ передає через Процесингову установу відповідну інформацію про платіжну операцію до «не карткової» ПС.

4) Інформація про успішно ініційовану платіжну операцію Фактичного платника передається через Процесингову установу «не карткової» ПС до ТОВ «ФК МБК».

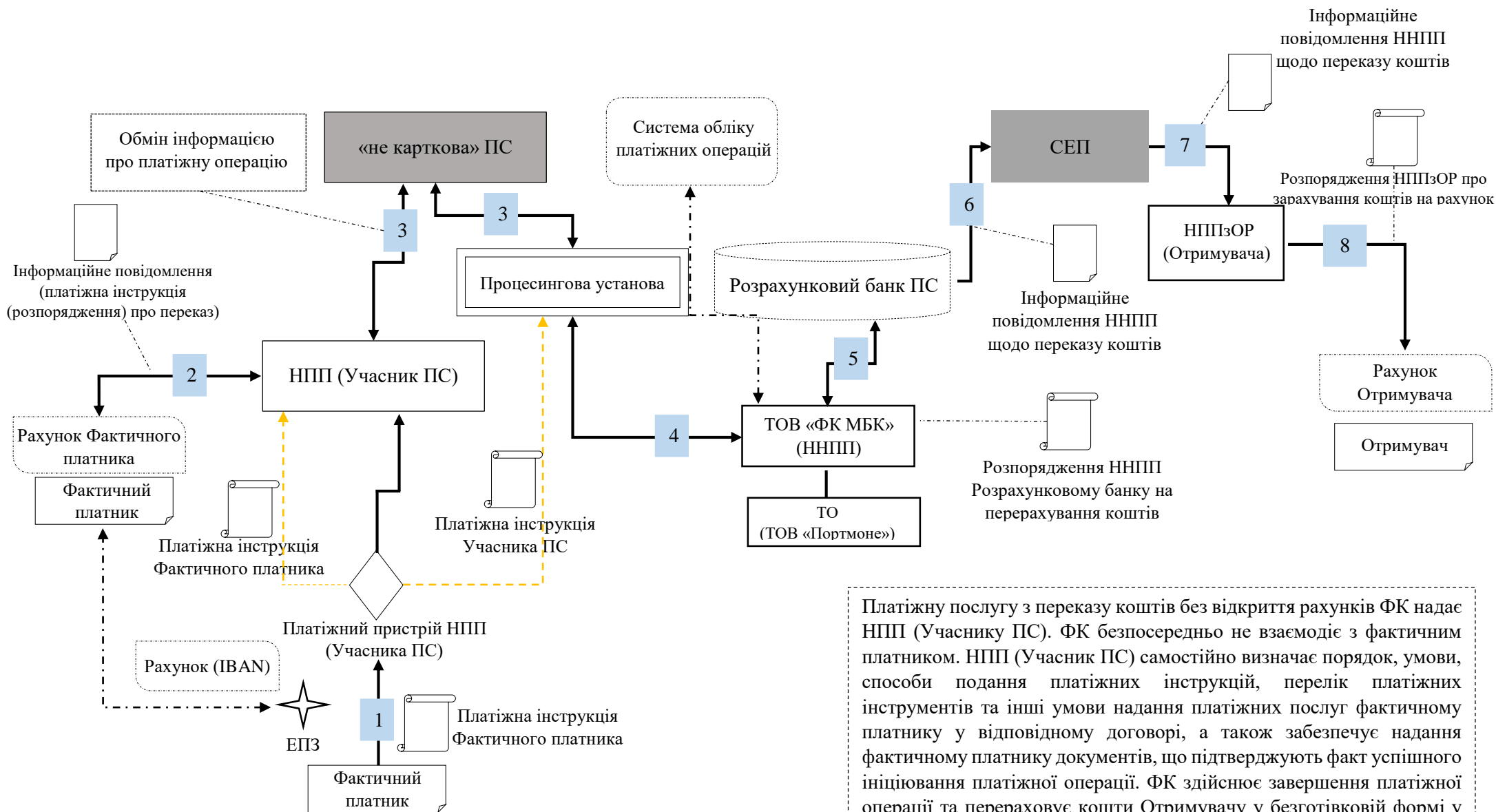
5) Через операційно-облікову систему ТОВ «ФК МБК» формуються платіжні інструкції щодо переказу коштів на користь відповідного Отримувача, які експортуються до клієнт-банку Розрахункового банку ПС. Уповноважені особи ТОВ «ФК МБК» підписують такі платіжні інструкції з метою їх виконання Розрахунковим банком ПС.

6) Розрахунковий банк ПС передає платіжні інструкції ТОВ «ФК МБК» до системи СЕП.

7) НППзОР Отримувача отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача.

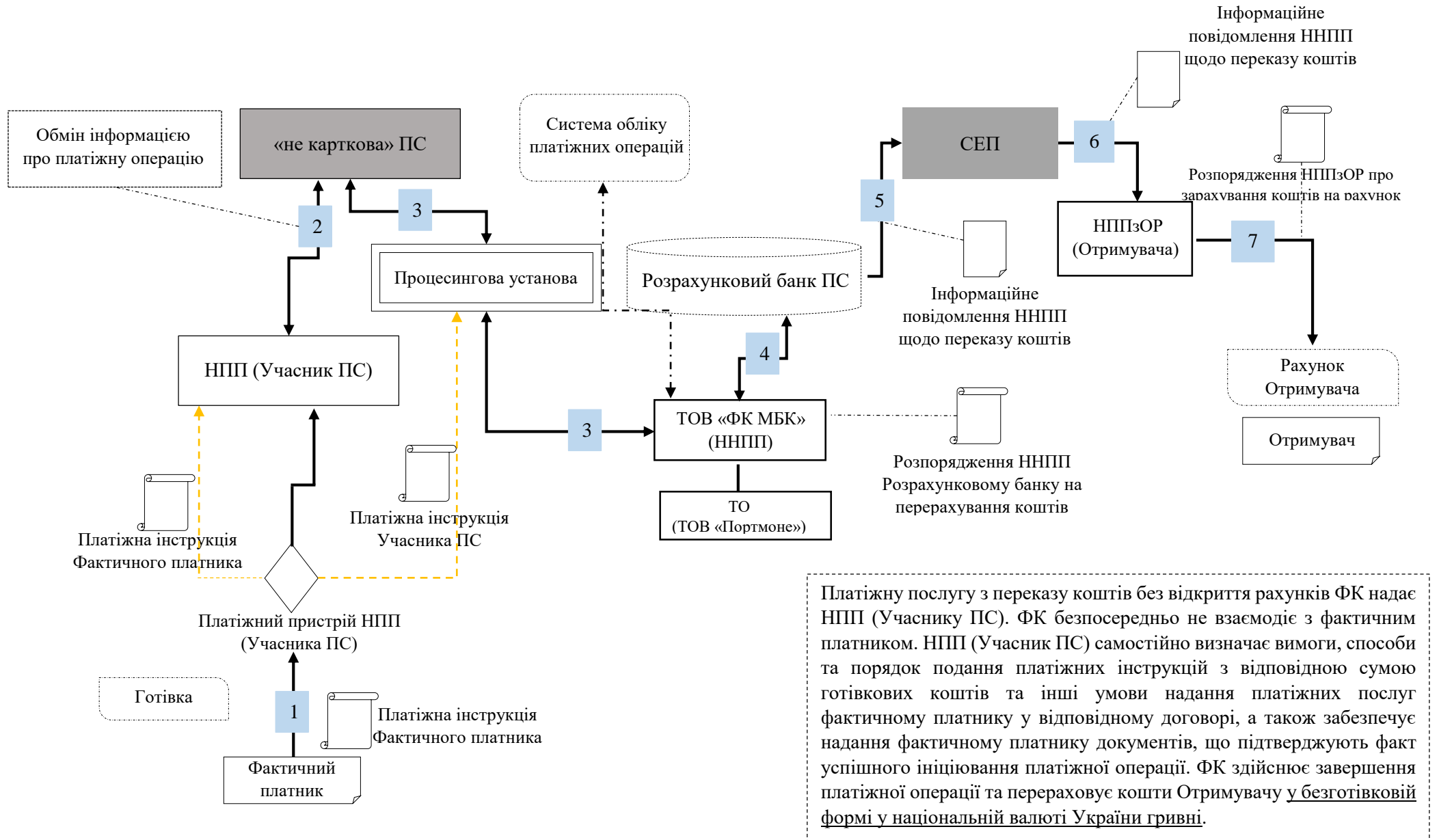
8) НППзОР Отримувача відображає Отримувачу інформацію про зарахування суми коштів на рахунок Отримувача.

4.7. Графічне зображення схеми звершення ФК платіжної операції, ініційованої з використання ЕПЗ, в межах «не карткової» ПС (*інформаційні потоки*) (далі – *Графічна схема №2*):

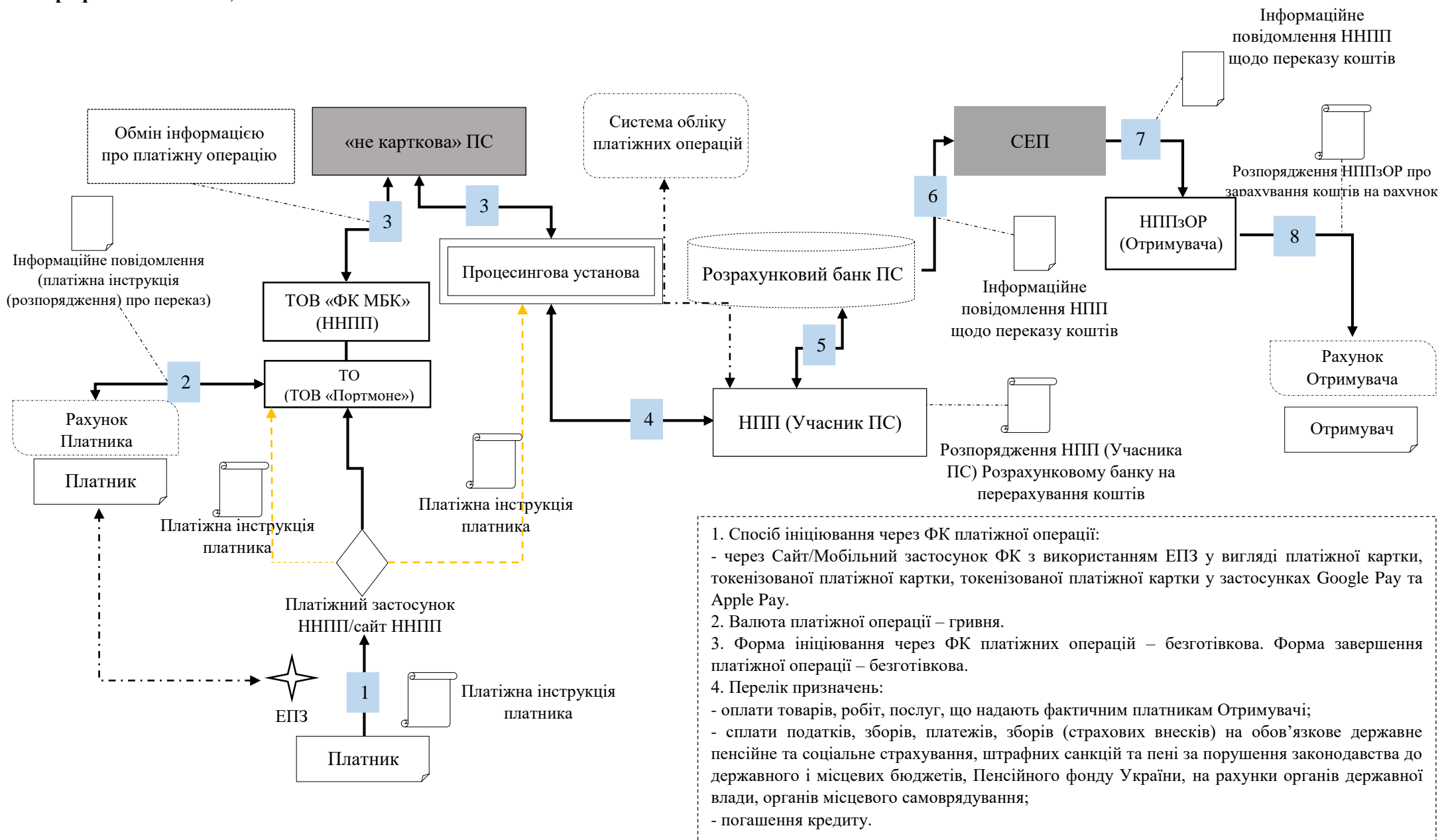


Платіжну послугу з переказу коштів без відкриття рахунків ФК надає НПП (Учаснику ПС). ФК безпосередньо не взаємодіє з фактичним платником. НПП (Учасник ПС) самостійно визначає порядок, умови, способи подання платіжних інструкцій, перелік платіжних інструментів та інші умови надання платіжних послуг фактичному платнику у відповідному договорі, а також забезпечує надання фактичному платнику документів, що підтверджують факт успішного ініціювання платіжної операції. ФК здійснює завершення платіжної операції та перераховує кошти Отримувачу у безготівковій формі у національній валюті України гривні.

4.8. Графічне зображення схеми звернення ФК платіжної операції, ініційованої шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів, в межах «не карткової» ПС (інформаційні потоки) (далі – Графічна схема №3):



4.9. Графічне зображення схеми ініціювання Платником через ФК платіжної операції в межах «не карткової» РС (інформаційні потоки) (далі – Графічна схема №4):



4.10. Додатковий опис до Графічної схеми №2:

4.10.1. Фактичний платник – особа, яка в платіжній інструкції НПП (Учасника ПС) зазначена фактичним платником і грошові зобов'язання якої виконує Учасник ПС шляхом ініціювання платіжної операції зі свого рахунку.

4.10.2. Фактичним платником може бути фізична особа, фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність чи юридична особа, яка на законних підставах використовує ЕПЗ. Отримувачем може бути: 1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про надання платіжних послуг (договори про прийом платежів); 2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України). Територія здійснення платіжних операцій – Україна.

4.11. Учасник ПС зобов'язаний надати Фактичному платнику документ, що підтверджує ініціювання платіжної операції (квитанція, чек тощо), який повинен відповідати вимогам законодавства.

4.12. Виконання ФК платіжної операції, ініційованої шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів, в межах «не карткової» ПС (**Графічна схема №3**) відбувається наступним чином:

1) Фактичний платник за допомогою Платіжного пристрою (банківський автомат, платіжний термінал, програмно-технічний комплекс самообслуговування) або через пункт надання фінансових послуг Учасника ПС заповнює необхідні поля (реквізити) для подання платіжної інструкції. Перелік реквізитів та форма подання платіжної інструкції визначається, з урахуванням вимог законодавства України, Учасником «не карткової» ПС, який приймає від Фактичного платника платіжну інструкцію. При цьому ФК може надати Учаснику «не карткової» ПС інформацію про факультативні реквізити платіжної інструкції, необхідні для ідентифікації Отримувачем Фактичного платника (наприклад, у разі ініціювання платіжної операції на користь Отримувача, який надає житлово-комунальні послуги, в платіжній інструкції може бути інформація про покази лічильника та суму переплати/заборгованості тощо). Після заповнення Фактичним платником всіх необхідних реквізитів платіжної інструкції та надання Учаснику ПС згоди на виконання платіжної інструкції, Учасник ПС отримує від Фактичного платника відповідну суму готівкових коштів та видає квитанцію (чек). Учасник ПС самостійно визначає способи, умови та порядок взаємодії з Фактичним платником, у тому числі порядок приймання готівкових коштів, з урахуванням вимог застосовного законодавства та правил відповідної «не карткової» ПС.

2) Учасник ПС засобами технічного протоколу через Процесингову установу передає в «не карткову» ПС інформацію про платіжну операцію (платіжну інструкцію) Фактичного платника, ініційовану шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів.

3) Інформація про успішно ініційовану платіжну операцію Фактичного платника шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів передається через Процесингову установу «не карткової» ПС до ТОВ «ФК МБК».

4) Через операційно-облікову систему ТОВ «ФК МБК» формуються платіжні інструкції щодо переказу коштів на користь відповідного Отримувача, які експортуються до клієнт-банку Розрахункового банку ПС. Уповноважені особи ТОВ «ФК МБК» підписують такі платіжні інструкції з метою їх виконання Розрахунковим банком ПС.

5) Розрахунковий банк ПС «не карткової» ПС передає платіжні інструкції ТОВ «ФК МБК» до системи СЕП.

6) НППзОР Отримувача отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача.

7) НППзОР Отримувача відображає Отримувачу інформацію про зарахування суми коштів на рахунок Отримувача.

4.13. Додатковий опис до Графічної схеми №3:

4.13.1. Фактичний платник – особа, яка в платіжній інструкції НПП (Учасника ПС) зазначена фактичним платником і грошові зобов'язання якої виконує Учасник ПС шляхом ініціювання платіжної операції зі свого рахунку.

4.13.2. Фактичним платником може бути фізична особа, фізична особа-підприємець чи фізична особа, що здійснює незалежну професійну діяльність. Отримувачем може бути: 1) фізична особа-

підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про надання платіжних послуг (договори про прийом платежів); 2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України). Територія здійснення платіжних операцій – Україна.

4.14. Ініціювання Платником через ТОВ «ФК МБК» платіжної операції з переказу коштів без відкриття рахунку в межах «не карткової» ПС (**Графічна схема №4**) відбувається наступним чином:

1) Платник за допомогою мобільного телефону (смартфону), персонального комп'ютера, планшета, ноутбука переходить (заходить) у Платіжний застосунок ННПП/сайт ННПП, де має можливість обрати (заповнити) необхідні поля (реквізити) для подання платіжної інструкції в електронній формі. Перелік реквізитів платіжної інструкції складається з обов'язкових реквізитів, без яких неможливе виконання платіжної операції, та факультативних реквізитів, рекомендації щодо яких надав Учасник ПС, який має укладений договір про надання платіжних послуг з Отримувачем;

2) Порядок використання Платником ЕПЗ та отримання ФК грошових коштів від Платника аналогічний до порядку зазначеного в описі до Графічної схеми №1 (підпункти 1-7 пункту 2.1.). У разі ініціювання платіжної операції з використанням ЕПЗ, що емітований нерезидентом України, додатковими реквізитами платіжної інструкції є інформація, що така платіжна операція є транскордонним переказом, ініційованим в іноземній валюті, та надає змогу НППЗОР Отримувача отримати всі необхідні дані для виконання функцій агента валютного нагляду, зокрема, отримати інформацію про Платника, передбачену Законом України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 року №361-ІХ та Законом України «Про валюту і валютні операції» від 21.06.2018 року №2473-VIII;

3) За результатами авторизації ЕПЗ ТОВ «ФК МБК» через Процесингову установу передає платіжну інструкцію та інформацію про ініційовану платіжну операцію до «не карткової» ПС;

4) З «не карткової» ПС через Процесингову установу платіжна інструкція Платника та інформація про ініційовану через ТОВ «ФК МБК» платіжну операцію передається до Учасника ПС;

5) Через відповідну операційно-облікову систему Учасника ПС формуються платіжні інструкції щодо переказу коштів на користь відповідного Отримувача, які експортуються до клієнт-банку Розрахункового банку ПС. Уповноважені особи Учасника ПС підписують такі платіжні інструкції з метою їх виконання Розрахунковим банком ПС.

6) Розрахунковий банк ПС передає платіжні інструкції Учасника ПС до системи СЕП.

7) НППЗОР Отримувача отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача.

8) НППЗОР Отримувача відображає Отримувачу інформацію про зарахування суми коштів на рахунок Отримувача.⁴

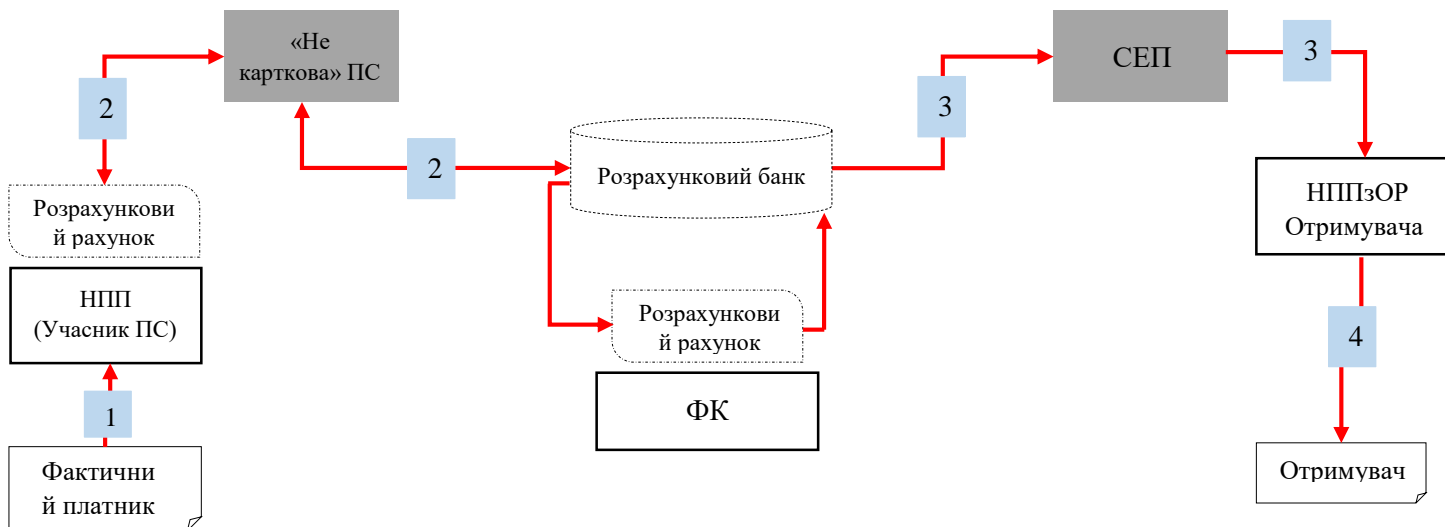
4.15. Додатковий опис до Графічної схеми №4:

4.15.1. Платником може бути: *фізична особа, фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність чи юридична особа, яка на законних підставах використовує ЕПЗ.*

4.15.2. Отримувачем може бути: *1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими Учасник ПС уклав договори про надання платіжних послуг (договори про приймання платежів); 2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України).*

4.15.3. Територія здійснення платіжних операцій – Україна. *Платник в момент ініціювання платіжної операції фізично може знаходитися в будь-якій точці світу, а також використовувати ЕПЗ, що емітоване нерезидентом України.*

4.16. Графічне зображення схеми звершення ФК платіжної операції, ініційованої з використанням ЕПЗ або шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів, в межах «не карткової» ПС (схема руху коштів до Графічної схеми №2 та Графічної схеми №3):



4.17. Фінансові взаєморозрахунки відбуваються у наступному порядку:

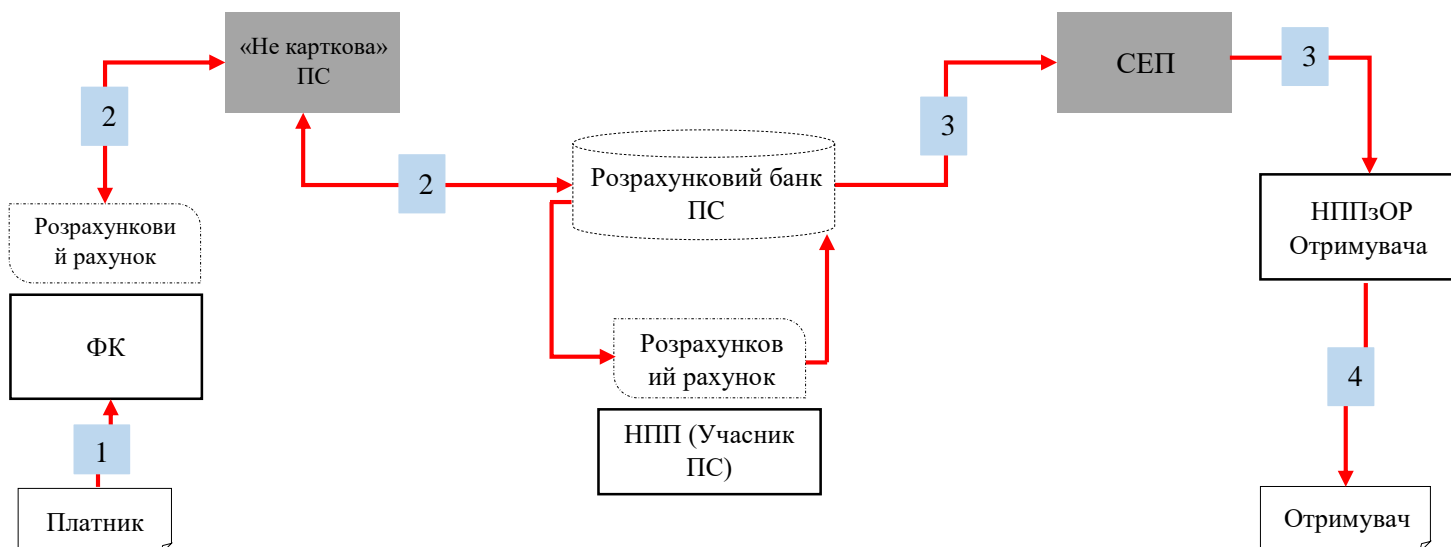
4.17.1. Учасник ПС, через якого ініціюється платіжна операція, отримує грошові кошти Фактичного платника. Схема руху коштів відображається у спрощеному вигляді, оскільки, порядок взаєморозрахунків Учасника ПС з еквайром (у разі ініціювання платіжної операції з використанням ЕПЗ) визначається умовами відповідного договору між таким Учасником ПС та еквайром. Порядок зарахування Учасником ПС готівкових коштів на свій розрахунковий рахунок в Розрахунковому банку ПС визначається законодавством та здійснюється Учасником ПС відповідно до внутрішніх правил (процедур, порядків);

4.17.2. Учасник ПС наступного операційного дня з моменту ініціювання платіжної операції Фактичним платником (як з використанням ЕПЗ, так і шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів) переказує кошти в безготівковій формі з розрахункового рахунку через Розрахунковий банк «не карткової» ПС на розрахунковий рахунок ФК в Розрахунковому банку у розрізі кожного Отримувача відповідно до контрольного реєстру, наданого таким Учасником ПС;

4.17.3. Після отримання коштів від Учасника ПС ФК відповідно до умов договорів про прийом платежів з кожним Отримувачем та з урахуванням строків передбачених Законом України «Про платіжні послуги», а також правилами відповідної ПС, переказує кошти Отримувачам в розрізі кожного Отримувача. Зазначені операції проходять через СЕП

4.17.4. НППзОР Отримувача зараховує отримані від ФК кошти на рахунок Отримувача.

4.18. Графічне зображення схеми ініціювання Платником через ФК платіжної операції в межах «не карткової» ПС (грошові потоки):



4.19. Фінансові взаєморозрахунки відбуваються у наступному порядку:

4.19.1. Отримання ФК на розрахунковий рахунок в Розрахунковому банку ПС коштів від Платника через еквайра відбувається у порядку, визначеному підпунктами 1-3 пункту 2.3.1. цього опису.

4.19.2. ФК наступного операційного дня з моменту ініціювання платіжної операції Платником з використанням ЕПЗ переказує кошти в безготівковій формі з розрахункового рахунку через Розрахунковий банк «не карткової» ПС на розрахунковий рахунок Учасника ПС у розрізі кожного Отримувача відповідно до контрольного реєстру, наданого ФК Учаснику ПС;

4.19.3. Після отримання коштів від ФК Учасник ПС відповідно до умов договорів про надання платіжних послуг з кожним Отримувачем та з урахуванням строків передбачених Законом України «Про платіжні послуги», а також правилами відповідної ПС, переказує кошти Отримувачам в розрізі кожного Отримувача. Зазначені операції проходять через СЕП;

4.19.4. НППзОР Отримувача зараховує отримані від Учасника ПС кошти на рахунок Отримувача.

5. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ З ВИКОРИСТАННЯМ ТЕХНІЧНОГО ПРОТОКОЛУ PORTMONE DIRECT

5.1. Portmone Direct – технічний протокол обміну даними, який використовує ФК для надання платіжної послуги з переказу коштів без відкриття рахунків НПП – банку або небанківському надавачу платіжних послуг (далі – НПП), що виступає у ролі Платника та діє від власного імені (не є комерційним агентом). ФК укладає з НПП договір за яким НПП своїми силами і засобами надає послуги з приймання та перерахування на розрахунковий рахунок ФК коштів у національній валюті, що надходять від фактичних платників з метою оплати товарів/робіт/послуг Отримувачів. Фактичним платником є особа, яка в платіжній інструкції Платника (НПП) зазначена фактичним платником і грошові зобов'язання якої виконує НПП шляхом ініціювання платіжної операції зі свого рахунку.

5.2. ФК, на виконання умов договорів з Отримувачами, може укладати договори з НПП, пов'язані із наданням послуг з переказу коштів з урахуванням положень Закону України «Про банки та банківську діяльність», при цьому, така форма відносин не носить характеру агентської. НПП забезпечують фактичним платникам можливість безпосереднього ініціювання платіжних операцій на користь Отримувачів, з якими ФК має договори про прийом платежів та виконує переказ коштів (завершення платіжних операцій).

5.3. Технологія оброблення та виконання платіжних операцій за протоколом Portmone Direct має наступний вигляд:

5.3.1. ФК укладає договори з НПП про надання платіжної послуги з переказу коштів без відкриття рахунків, яка полягає у завершенні платіжних операцій, ініційованих фактичними платниками на користь Отримувачів. НПП за такої схеми виступає у ролі Платника. Умовами договору з НПП передбачено, що НПП своїми силами і засобами (з використанням власних Платіжних пристроїв) надає послуги з приймання та перерахування на розрахунковий рахунок ФК коштів у національній валюті, що надходять від фактичних платників з метою оплати послуг/товарів/робіт, які надають таким фактичним платникам Отримувачі.

5.3.2. Приймання НПП коштів від фактичних платників здійснюється шляхом обробки платіжних операцій, що ініційовані фактичними платниками за допомогою ЕПЗ, або шляхом списання коштів з поточного/платіжного рахунку відповідно до поданої платіжної інструкції, або шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів згідно з внутрішніми нормативними документами НПП. НПП самостійно визначають способи ініціювання платіжних операцій, валюту платіжної операції, перелік платіжних інструментів, які приймаються НПП. При цьому, ФК виконує переказ коштів від НПП виключно у безготівковому вигляді у національній валюті України гривні. НПП забезпечують ініціювання через них платіжних операцій фактичними платниками з метою їх подальшого перерахування на розрахунковий рахунок ФК в Обслуговуючому банку не пізніше наступного операційного дня від дати приймання коштів від фактичних платників, якщо інше не передбачено умовами договорів ФК з НПП та Отримувачами, і не суперечить законодавству України.

5.3.3. Для інформаційного обслуговування фактичних платників, НПП та Отримувачів під час виконання платіжних операцій за протоколом Portmone Direct, ФК впровадила та використовує

сукупність програмно-технічних засобів у вигляді Білінгової системи, за допомогою якої відбувається інформаційний обмін між НПП, ФК та Отримувачами в процесі ініціювання фактичними платниками платіжних операцій та здійснення ФК переказу коштів на користь Отримувачів. Білінгова система ФК призначена для передачі/обміну даними між всіма учасниками руху коштів.

5.3.4. Для організації переказу коштів ФК надає НПП підтвердження своїх повноважень завершувати платіжні операції та переказувати кошти Отримувачам (таким підтвердженням є відповідний договір з Отримувачем про надання платіжних послуг).

5.4. Порядок інформаційно-технічної взаємодії під час виконання платіжних операцій за протоколом Portmone Direct:

5.4.1. НПП направляє запит до Білінгової системи на отримання рахунку із зазначенням параметрів (перелік та формат полів зазначаються в Заяві на реєстрацію Отримувача в системі НПП щодо кожного Отримувача), що однозначно ідентифікують фактичного платника. У відповідь на запит Білінгова система ФК надає інформацію про рахунок від Отримувача, яка може містити суму заборгованості фактичного платника, період за який виставлено рахунок, деталізацію нарахувань, показники лічильників, суму переплати за попередній період тощо. У випадку передплати послуг фактичний платник отримує рахунок із сумою заборгованості «0 грн.» та може самостійно визначити суму платіжної операції. У випадку утримання комісії безпосередньо з фактичного платника на користь ФК за переказ коштів в Заяві зазначається розмір такої комісії.

5.4.2. Обмін запитами/повідомленнями між НПП, ФК та Отримувачем відбувається у відповідності до протоколу Portmone Direct, що розміщено за посиланням: <https://docs.portmone.com.ua/docs/uk/PortmoneDirectUa/>. У випадку внесення ФК змін та доповнень до протоколу Portmone Direct, що не призводять до погіршення взаємодії сторін, такі зміни набирають чинності з дати оновлення протоколу Portmone Direct.

5.4.3. Кожному рахунку виданому з Білінгової системи присвоюється унікальний ідентифікатор (набір цифр та/або букв) - обліковий номер платіжної операції.

5.4.4. Якщо Отримувач не зміг однозначно ідентифікувати фактичного платника за наданими НПП параметрами (або фактичний платник знаходиться у Отримувача в статусі не активного) ФК направляє до НПП відповідний код помилки.

5.4.5. Після успішної транзакції НПП направляє відповідну команду до Білінгової системи в режимі реального часу відповідно до протоколу Portmone Direct. При цьому НПП обов'язково зазначає обліковий номер платіжної операції, присвоєний ФК відповідному рахунку.

5.4.6. У випадку технічного збою НПП зобов'язаний використовуючи засоби передбачені протоколом Portmone Direct перевірити коректність передачі інформації про рахунки фактичного платника до/з Білінгової системи перед її обробкою.

5.4.7. У випадку підтримки програмно-технічними засобами Отримувача функціоналу зарахування коштів в режимі реального часу, ФК передає за допомогою Білінгової системи відповідне повідомлення про здійснення успішної транзакції Отримувачу, що призводить до зарахування Отримувачем суми транзакції на особовий рахунок фактичного платника.

5.4.8. НПП для контролю прийнятих коштів не пізніше 10год. 00хв. поточного робочого дня, використовуючи засоби протоколу Portmone Direct, може запросити у ФК контрольний реєстр транзакцій за попередній календарний день (в період з 00год. 00хв. 00сек. по 23год. 59хв 59сек за київським часом) (надалі – Контрольний реєстр). В Контрольному реєстрі ФК зазначає детальний перелік транзакцій на користь кожного Отримувача та загальну суму всіх транзакцій за попередній календарний день, а також розмір комісій утриманих безпосередньо з фактичних платників на користь ФК за переказ коштів по кожному з Отримувачів. У випадку розбіжностей між Контрольним реєстром та даними в системі НПП, сторони вживають заходів для аналізу ситуації та виявлення зайвих та/або відсутніх транзакцій.

5.4.9. Для ідентифікації НПП в Білінговій системі ФК надає окремий логін та спеціальний цифровий ключ SSL, а також виділену фіксовану ір-адресу.

5.4.10. Під час обміну запитами/повідомленнями між НПП та ФК використовується зашифрований канал зв'язку з використанням SSL.

5.4.11. Документи у електронному вигляді, якими обмінюються НПП та ФК в порядку інформаційно-технічної взаємодії та електронного документообігу відповідно до Протоколу мають таку саму

юридичну силу, що і підписані уповноваженими особами НПП та ФК примірники таких документів у паперовій формі.

5.4.12. НПП забезпечує супроводження платіжної операції необхідними даними про фактичного платника, які передає до Білінгової системи, зокрема:

- у випадку ініціювання фактичним платником платіжної операції готівкою на суму, що дорівнює чи перевищує 5 000 грн., або
- у випадку ініціювання фактичним платником платіжної операції з рахунку або з використанням електронних платіжних засобів на суму, що дорівнює чи перевищує 30 000 гривень, якщо інше не передбачено Законом України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

НПП передає до Білінгової системи такий набір даних (параметрів) про фактичного платника:

- прізвище, ім'я та, за наявності, по батькові фактичного платника;
- номер рахунку або номер електронного платіжного засобу фактичного платника, а в разі відсутності - унікальний обліковий номер платіжної операції, який дає змогу здійснити відстеження операції;
- номер та, за наявності, серію паспорта громадянина України (або іншого документа, що посвідчує особу та відповідно до законодавства України може бути використаним на території України для укладення правочинів) або реєстраційний номер облікової картки платника податків.

5.4.13. У випадку, якщо ФК не отримала до Білінгової системи необхідних даних про фактичного платника, завершення платіжної операції та перерахування коштів на рахунок Отримувача зупиняється (до системи НПП надсилається повідомлення про відмову від подальшого проведення платіжної операції). При цьому ФК може повторно направити запит до системи НПП для отримання даних про фактичного платника та забезпечення проведення платіжної операції (оплати рахунку Отримувача).

5.5. Виконання ФК платіжної операції з переказу коштів без відкриття рахунків, ініційованої Фактичним платником з використанням ЕПЗ, що надається НПП за технічним протоколом ФК Portmone Direct (**Графічна схема №5**), відбувається наступним чином:

1) Фактичний платник за допомогою Платіжного пристрою НПП (банківський автомат, платіжний термінал, програмно-технічний комплекс самообслуговування, програмно-апаратне середовище мобільного телефону, системи онлайн-банкінгу, клієнт-банку, каса банку, інший пристрій) заповнює необхідні поля (реквізити) для подання платіжної інструкції. Перелік реквізитів та форма подання платіжної інструкції визначається, з урахуванням вимог законодавства України, НПП, який приймає від Фактичного платника платіжну інструкцію. При цьому ФК може надати НПП інформацію про факультативні реквізити платіжної інструкції, необхідні для ідентифікації Отримувачем Фактичного платника (наприклад, у разі ініціювання платіжної операції на користь Отримувача, який надає житлово-комунальні послуги, в платіжній інструкції може бути інформація про покази лічильника та суму переоплати/заборгованості тощо).

2) Після заповнення Фактичним платником всіх необхідних реквізитів платіжної інструкції та надання НПП згоди на виконання платіжної інструкції, Фактичний платник зазначає НПП реквізити ЕПЗ, з якого бажає ініціювати платіжну операцію. ФК не зображає на Графічній схемі №5 порядок використання Фактичним платником ЕПЗ, типи ЕПЗ, які приймаються НПП та порядок взаємодії НПП з еквайрами, процесинговими установами та емітентами, оскільки, такий порядок безпосередньо визначається НПП, через якого ініціюється платіжна операція Фактичного платника. НПП самостійно визначає способи, умови та порядок взаємодії з Фактичним платником, а також перелік ЕПЗ, які приймає НПП для ініціювання платіжних операцій.

3) НПП за результатами авторизації ЕПЗ передає через технічний протокол Portmone Direct відповідну інформацію про платіжну операцію до ТОВ «ФК МБК».

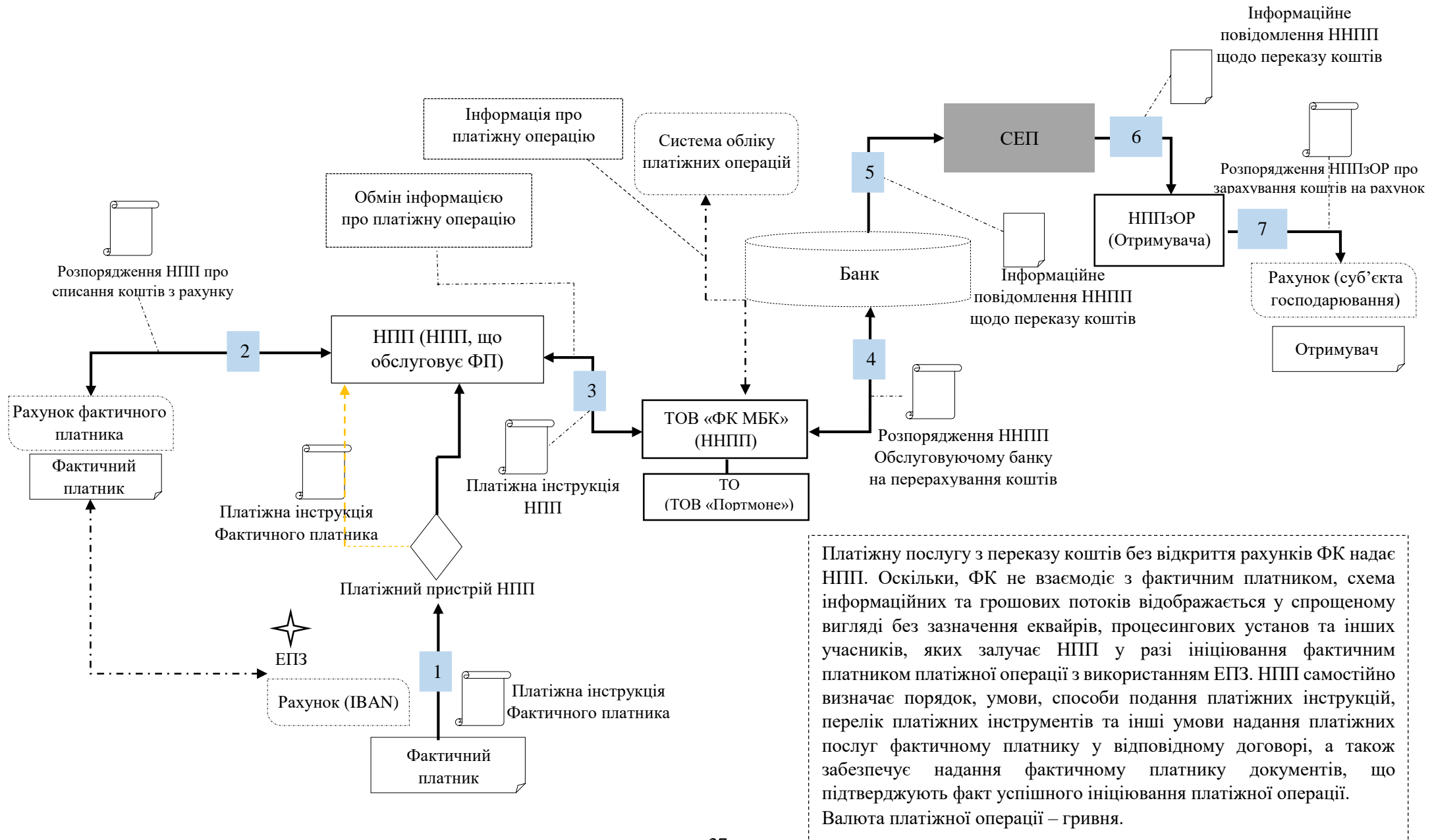
4) Через операційно-облікову систему ТОВ «ФК МБК» формуються платіжні інструкції щодо переказу коштів на користь відповідного Отримувача, які експортуються до клієнт-банку Обслуговуючого банку. Уповноважені особи ТОВ «ФК МБК» підписують такі платіжні інструкції з метою їх виконання Обслуговуючим банком.

5) Обслуговуючий банк передає платіжні інструкції ТОВ «ФК МБК» до системи СЕП.

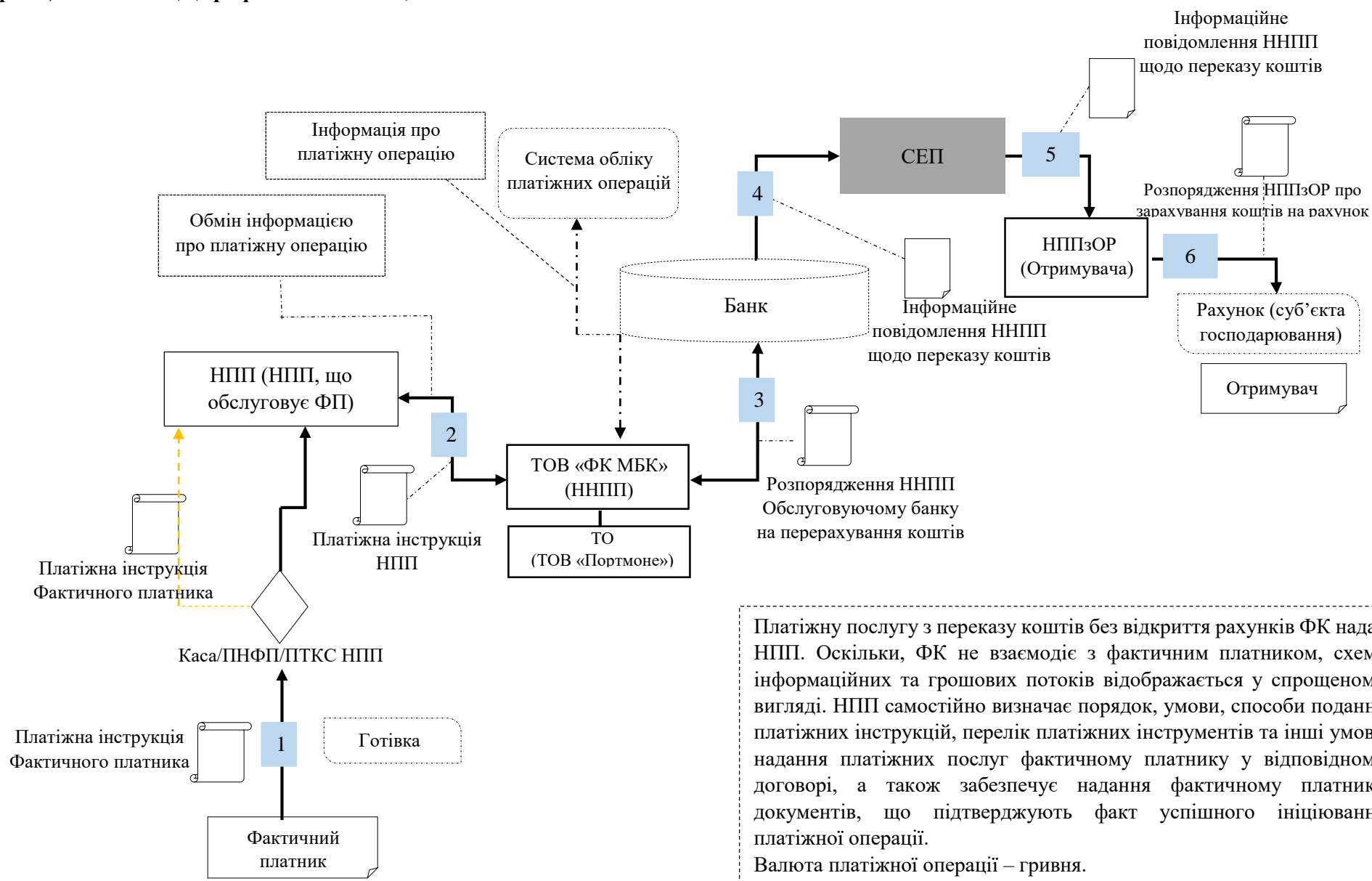
6) НППзОР Отримувача отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача.

7) НППзОР Отримувача відображає Отримувачу інформацію про зарахування суми коштів на рахунок Отримувача.

5.6. Графічне зображення схеми виконання ФК платіжної операції з переказу коштів без відкриття рахунків, ініційованої Фактичним платником з використанням ЕПЗ, що надається НПП за технічним протоколом ФК Portmone Direct (*інформаційні потоки*) (Графічна схема №5):



5.7. Графічне зображення схеми виконання ФК платіжної операції з переказу коштів без відкриття рахунків, ініційованої Фактичним платником шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів, що надається НПП за технічним протоколом ФК Portmone Direct (інформаційні потоки) (Графічна схема №6):



5.8. Додатковий опис до Графічної схеми №5:

5.8.1. Фактичний платник (ФП) – особа, яка в платіжній інструкції НПП (НПП, що обслуговує Фактичного платника) зазначена фактичним платником і грошові зобов'язання якої виконує НПП шляхом ініціювання платіжної операції зі свого рахунку. Фактичним платником може бути фізична особа, фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якою НПП уклав договір про надання платіжних послуг (наприклад, договір розрахунково-касового обслуговування, договір платіжного рахунку та інші).

5.8.2. НПП, що обслуговує Фактичного платника є: банк або небанківський надавач платіжних послуг, які є резидентами України. Отримувачем може бути: 1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про надання платіжних послуг (договори про прийом платежів); 2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України); 3) фізичні особи-підприємці, фізичні особи, що здійснюють незалежну професійну діяльність та юридичні особи, реквізити яких НПП, що обслуговує ФП, зазначив в платіжній інструкції. Територія здійснення платіжних операцій – Україна.

5.9. Виконання платіжної операції з переказу коштів від НПП використовується для:

- оплати товарів/робіт/послуг, що надають фактичним платникам Отримувачі;
- сплати податків, зборів, платежів, зборів (страхових внесків) на обов'язкове державне пенсійне та соціальне страхування, штрафних санкцій та пені за порушення законодавства до державного і місцевих бюджетів, Пенсійного фонду України, на рахунки органів державної влади, органів місцевого самоврядування;
- погашення кредиту.

5.10. Виконання ФК платіжної операції з переказу коштів без відкриття рахунків, ініційованої Фактичним платником шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів, що надається НПП за технічним протоколом ФК Portmone Direct (**Графічна схема №6**), відбувається наступним чином:

1) Фактичний платник через каси, відділення та інші пункти надання фінансових послуг НПП (Каса/ПНФП НПП), або через Платіжний пристрій НПП (банківський автомат, ПТКС) заповнює необхідні поля (реквізити) для подання платіжної інструкції. Перелік реквізитів та форма подання платіжної інструкції визначається НПП, який приймає від Фактичного платника платіжну інструкцію, з урахуванням вимог законодавства України. При цьому ФК може надати НПП інформацію про факультативні реквізити платіжної інструкції, необхідні для ідентифікації Отримувачем Фактичного платника (наприклад, у разі ініціювання платіжної операції на користь Отримувача, який надає житлово-комунальні послуги, в платіжній інструкції може бути інформація про покази лічильника та суму переплати/заборгованості тощо). Після заповнення Фактичним платником всіх необхідних реквізитів платіжної інструкції та надання НПП згоди на виконання платіжної інструкції, НПП отримує від Фактичного платника відповідну суму готівкових коштів та видає квитанцію (чек). НПП самостійно визначає способи, умови та порядок взаємодії з Фактичним платником, у тому числі порядок приймання готівкових коштів, з урахуванням вимог застосовного законодавства.

2) НПП засобами технічного протоколу Portmone Direct передає ФК інформацію про платіжну операцію (платіжну інструкцію) Фактичного платника, ініційовану шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів.

3) Через операційно-облікову систему ТОВ «ФК МБК» формуються платіжні інструкції щодо переказу коштів на користь відповідного Отримувача, які експортуються до клієнт-банку Обслуговуючого банку. Уповноважені особи ТОВ «ФК МБК» підписують такі платіжні інструкції з метою їх виконання Обслуговуючим банком.

4) Обслуговуючий банк передає платіжні інструкції ТОВ «ФК МБК» до системи СЕП.

5) НППзОР Отримувача отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача.

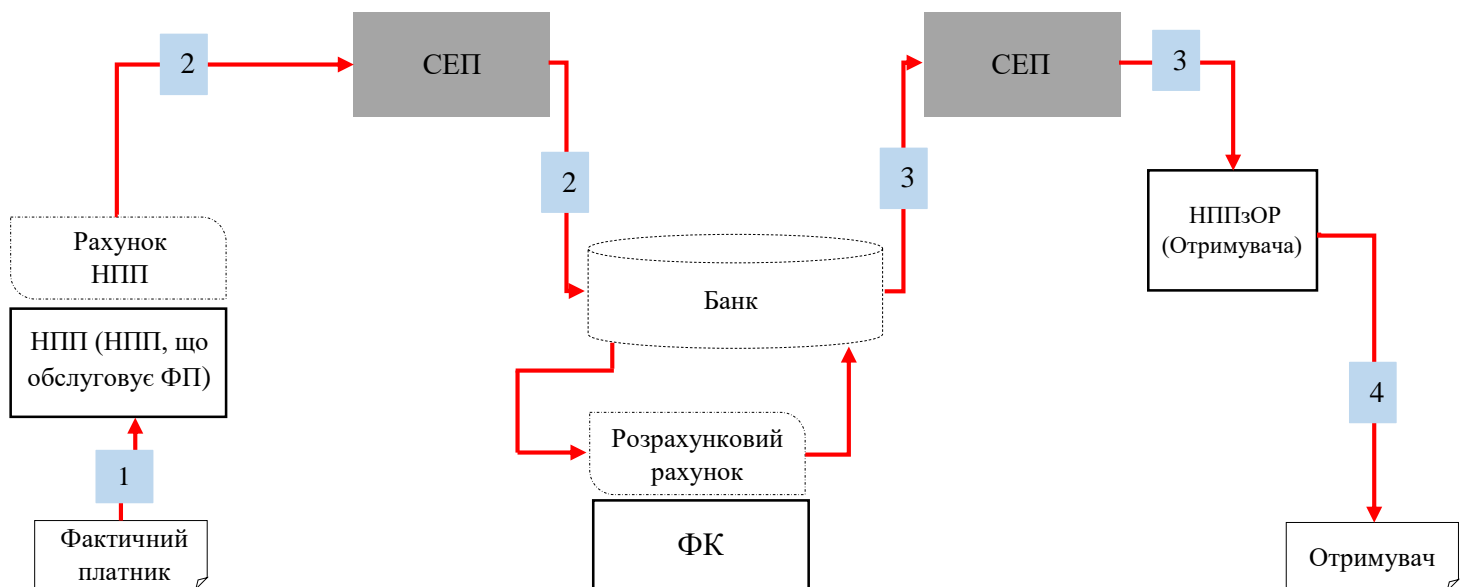
6) НППзОР Отримувача відображає Отримувачу інформацію про зарахування суми коштів на рахунок Отримувача.

5.11. Додатковий опис до Графічної схеми №6:

5.11.1. Фактичний платник (ФП) – особа, яка в платіжній інструкції НПП (НПП, що обслуговує ФП) зазначена фактичним платником і грошові зобов'язання якої виконує НПП шляхом ініціювання платіжної операції зі свого рахунку. Фактичним платником може бути: 1) фізична особа, фізична особа-підприємець та фізична особа, що здійснює незалежну професійну діяльність, з якою НПП встановлено ділові відносини; 2) фізична особа, фізична особа-підприємець та фізична особа, що здійснює незалежну професійну діяльність, яка ініціює разову платіжну операцію без встановлення ділових відносин з НПП.

5.11.2. НПП, що обслуговує Фактичного платника є: банк або небанківський надавач платіжних послуг, які є резидентами України. Отримувачем може бути: 1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про надання платіжних послуг (договори про прийом платежів); 2) органи державної влади України для зарахування коштів за сплатами податків, адміністративних штрафів та інших платежів до бюджету (рахунки Державної казначейської служби України); 3) фізичні особи, фізичні особи-підприємці, фізичні особи, що здійснюють незалежну професійну діяльність та юридичні особи, реквізити яких НПП, що обслуговує ФП, зазначив в платіжній інструкції. Територія здійснення платіжних операцій – Україна.

5.12. Графічне зображення схеми виконання ФК платіжної операції з переказу коштів без відкриття рахунків, що надається НПП за технічним протоколом ФК Portmone Direct (рух коштів для Графічної схеми №5 та Графічної схеми №6):



5.13. Фінансові взаєморозрахунки відбуваються у наступному порядку:

5.13.1. НПП, через якого ініціюється платіжна операція, отримує грошові кошти Фактичного платника. Схема руху коштів відображається у спрощеному вигляді, оскільки, порядок взаєморозрахунків НПП з еквайром/емітентом (у разі ініціювання платіжної операції з використанням ЕПЗ) визначається правилами відповідної «карткової» ПС. Порядок зарахування НПП готівкових коштів на свій транзитний рахунок визначається законодавством та здійснюється НПП відповідно до внутрішніх правил (процедур, порядків);

5.13.2. НПП наступного операційного дня з моменту ініціювання платіжної операції Фактичним платником (як з використанням ЕПЗ, так і шляхом подання платіжної інструкції разом з відповідною сумою готівкових коштів) переказує кошти в безготівковій формі з транзитного рахунку на розрахунковий рахунок ФК в Обслуговуючому банку у розрізі кожного Отримувача відповідно до контрольного реєстру, наданого таким НПП;

5.13.3. Після отримання коштів від НПП ФК відповідно до умов договорів про прийом платежів з кожним Отримувачем та з урахуванням строків передбачених Законом України «Про платіжні послуги», переказує кошти Отримувачам в розрізі кожного Отримувача. Зазначені операції проходять через СЕП;

5.13.4. НППзОР Отримувача зараховує отримані від ФК кошти на рахунок Отримувача.

5.14. Виконання платіжної операції з переказу коштів від НПП використовується для:

- оплати товарів/робіт/послуг, що надають фактичним платникам Отримувачі;
- сплати податків, зборів, платежів, зборів (страхових внесків) на обов'язкове державне пенсійне та соціальне страхування, штрафних санкцій та пені за порушення законодавства до державного і місцевих

бюджетів, Пенсійного фонду України, на рахунки органів державної влади, органів місцевого самоврядування;

- погашення кредиту.

5.15. Документами, що підтверджують факт виконання ФК платіжної операції з переказу коштів є відповідні Контрольні реєстри та щомісячні акти наданих послуг, які укладаються між НПП та ФК.

5.16. Рух коштів від НПП до Отримувачів з використанням протоколу Portmone Direct наступний:

5.16.1. Не пізніше 15:00 поточного операційного дня НПП перераховує на розрахунковий рахунок ФК прийняті платіжні операції відповідно до Контрольного реєстру за попередній календарний день/попередні календарні дні;

5.16.2. Приймання безготівкових коштів від фактичних платників здійснюється НПП шляхом обробки транзакцій, що ініційовані фактичними платниками за допомогою Платіжних пристроїв, із подальшим перерахуванням коштів на розрахунковий рахунок ФК. НПП перераховує кошти фактичних платників за платіжними операціями, ініційованими протягом операційного дня НПП, єдиною платіжною інструкцією з призначенням платежу «Покриття згідно договору про прийом платежів № _____ від _____ 202_ р. на суму _____, утримана комісія 0 грн.»;

5.16.3. Приймання готівкових коштів від фактичних платників здійснюється через каси, платіжні термінали, термінали самообслуговування НПП тощо, відповідно до внутрішніх положень НПП, із подальшим перерахуванням коштів на розрахунковий рахунок ФК;

5.16.4. З метою забезпечення належного виконання НПП власних зобов'язань щодо здійснення переказу грошових коштів на користь ФК НПП може перерахувати гарантійний платіж у розумінні ч. 2 ст. 546 Цивільного кодексу України у розмірі обсягу коштів, які планує приймати НПП протягом 3 (трьох) операційних днів.

6. УМОВИ ТА ПОРЯДОК ЗДІЙСНЕННЯ ПЕРЕКАЗУ КОШТІВ A2C (account-to-card) ТА A2A (account-to-account)

6.1. Схема виконання платіжної операції з переказу коштів на рахунок за реквізитами платіжної картки Отримувача ФО (так звана A2C (account-to-card) операція) (**Графічна схема №7**) здійснюється ФК наступним чином:

1) До ФК звертається суб'єкт господарювання або орган державної влади, що виступає в ролі Платника, який має потребу у здійсненні виплат коштів фізичним особам (страхові виплати, грошова компенсація вартості товарів, надана платнику в разі їх повернення продавцю, соціальна та державна допомога, доходи у вигляді процентів нараховані на державні цінні папери або облігації, грошова компенсація вартості товарів у разі їх повернення та інші випадки передбачені ст. 165 Податкового кодексу України). Платник зі свого рахунку, який відкрито у надавача платіжних послуг з обслуговування рахунку (банк), здійснює перерахування коштів на розрахунковий рахунок ФК, який відкрито у банка-еквайра. Зазначене перерахування Платник може здійснювати за допомогою дистанційних засобів комунікації (клієнт-банк);

2) Технологічний оператор ТОВ «Портмоне» забезпечує технічну взаємодію шляхом підключення технічного протоколу обміну даними API до сайту/мобільного застосунку Платника, який використовують Отримувачі фізичні особи (Отримувачі ФО). Платник засобами API протоколу надсилає ТОВ «Портмоне» відповідну нотифікацію (повідомлення) про те, що до Платника звернувся Отримувач ФО, який бажає отримати виплату коштів за номером ЕПЗ. Платник здійснює перенаправлення (редирект) такого Отримувача ФО на сторінку ТОВ «Портмоне», де ТОВ «Портмоне» отримує реквізити ЕПЗ і забезпечує ФК можливість здійснення ідентифікації та верифікації Отримувача ФО у випадках, передбачених законодавством.

3) ФК здійснює ідентифікацію та верифікацію Отримувача ФО, а також перевіряє Отримувача ФО за санкційними списками. В подальшому ФК контролює загальні суми перерахування коштів на користь такої фізичної особи протягом певного періоду часу з метою контролю та виявлення досягнення сумою перерахувань коштів певних порогових значень. За результатами успішної ідентифікації та верифікації Отримувача ФО та відсутності збігу даних з даними санкційної особи, ФК надсилає з використанням технічного протоколу взаємодії повідомлення Процесинговій установі про ініційовану платіжну операцію A2C (account-to-card). Процесингова установа через інфраструктуру «карткових» ПС надсилає до еквайра платіжну інструкцію та запит на авторизацію ЕПЗ.

4) Еквайр через інфраструктуру відповідної «карткової» ПС разом з платіжною інструкцією надсилає емітенту ЕПЗ запит на авторизацію.

5-6) Емітент на підставі отриманої платіжної інструкції та запиту на авторизацію від еквайра через інфраструктуру «карткової» ПС перевіряє інформацію про рахунок Отримувача ФО та встановлює факт

належності такому Отримувачу ФО відповідного ЕПЗ, який пов'язаний з рахунком. Після цього емітент засобами технічного протоколу надає еквайру одну з відповідей: 1) відмова в авторизації (наприклад, але не обмежуючись, некоректні реквізити ЕПЗ, рахунок закрито/заблоковано); 2) згода на авторизацію. У випадку відмови в авторизації, емітент передає через інфраструктуру «карткової» ПС зазначену відповідь еквайру, еквайр віддає інформацію процесинговій установі, а процесингова установа передає відповідь емітента про відмову в авторизації до ТОВ «ФК МБК»/ТОВ «Портмоне». ТОВ «ФК МБК» відображає Платнику через АРІ протокол інформацію про неуспішну спробу ініціювання платіжної операції, яка не призвела до виконання платіжної операції. Залежно від причин відмови в авторизації ТОВ «ФК МБК» може відображати Платнику отриману від еквайра інформацію про код помилки та його розшифрування.

Емітент після успішної авторизації присвоює операції код авторизації. Інформація про згоду на авторизацію (успішна авторизація) передається емітентом ЕПЗ через інфраструктуру «карткової» ПС до еквайра, а від еквайра до процесингової установи, яка, в свою чергу передає інформацію про результати авторизації до ТОВ «ФК МБК»/ТОВ «Портмоне». Зазначена технічна взаємодія (обмін запитами-повідомленнями) відбувається в режимі реального часу, як правило, не більше 15 хв. ТОВ «ФК МБК» відображає Платнику інформацію про успішно ініційовану платіжну операцію та надає квитанцію, яка засвідчує зазначений факт.

6.2. Додатковий опис до Графічної схеми №7:

6.2.1. Платником може бути: 1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про надання платіжних послуг; 2) органи державної влади України у разі здійснення виплат суми державної та соціальної матеріальної допомоги, державної допомоги, компенсацій, вартості соціальних послуг та реабілітаційної допомоги, грошової компенсації особам з інвалідністю, фінансової допомоги та інших видів виплат відповідно до статті 165 Податкового кодексу України. Територія здійснення платіжних операцій – Україна. Отримувач є фізичною особою, резидентом України. Платник є резидентом України.

6.3. Схема виконання платіжної операції з переказу коштів з рахунку на рахунок (так звана А2А (account-to-account) операція) (Графічна схема №8) здійснюється ФК наступним чином:

1) До ФК звертається суб'єкт господарювання або орган державної влади, що виступає в ролі Платника, який має потребу у здійсненні виплат коштів фізичним особам (страхові виплати, грошова компенсація вартості товарів, надана платнику в разі їх повернення продавцю, соціальна та державна допомога, доходи у вигляді процентів нараховані на державні цінні папери або облігації, грошова компенсація вартості товарів у разі їх повернення та інші випадки передбачені ст. 165 Податкового кодексу України). Платник зі свого рахунку, який відкрито у надавача платіжних послуг з обслуговування рахунку (банк), здійснює перерахування коштів на розрахунковий рахунок ФК, який відкрито у Обслуговуючого банку. Зазначене перерахування Платник може здійснювати за допомогою дистанційних засобів комунікації (клієнт-банк);

2) Технологічний оператор ТОВ «Портмоне» забезпечує технічну взаємодію шляхом підключення технічного протоколу обміну даними АРІ до сайту/мобільного застосунку Платника, який використовують Отримувачі фізичні особи (Отримувачі ФО). Платник засобами АРІ протоколу надсилає ТОВ «Портмоне» відповідну нотифікацію (повідомлення) про те, що до Платника звернувся Отримувач ФО, який бажає отримати виплату коштів за номером ЕПЗ. Платник здійснює перенаправлення (редирект) такого Отримувача ФО на сторінку ТОВ «Портмоне», де ТОВ «Портмоне» отримує реквізити ЕПЗ і забезпечує ФК можливість здійснення ідентифікації та верифікації Отримувача ФО у випадках, передбачених законодавством.

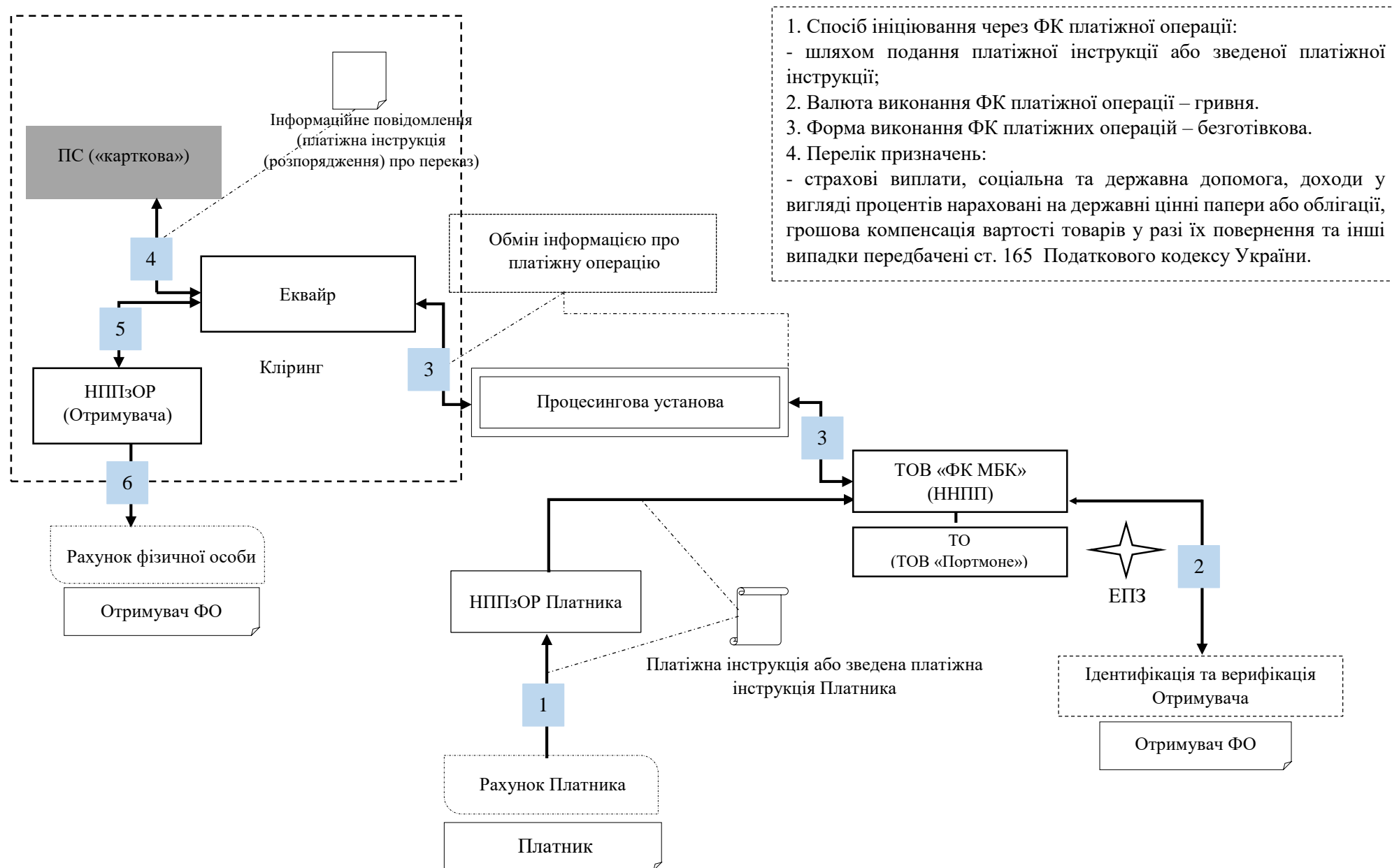
3) ФК здійснює ідентифікацію та верифікацію Отримувача ФО, а також перевіряє Отримувача ФО за санкційними списками. В подальшому ФК контролює загальні суми перерахування коштів на користь такої фізичної особи протягом певного періоду часу з метою контролю та виявлення досягнення сумою перерахувань коштів певних порогових значень. За результатами успішної ідентифікації та верифікації Отримувача ФО та відсутності збігу даних з даними санкційної особи, ФК через операційно-облікову систему ТОВ «ФК МБК» формує платіжні інструкції щодо переказу коштів на користь відповідного Отримувача ФО за номером ІВАН, які експортуються до клієнт-банку Обслуговуючого банку. Уповноважені особи ТОВ «ФК МБК» підписують такі платіжні інструкції з метою їх виконання Обслуговуючим банком.

4) Обслуговуючий банк передає платіжні інструкції ТОВ «ФК МБК» до системи СЕП.

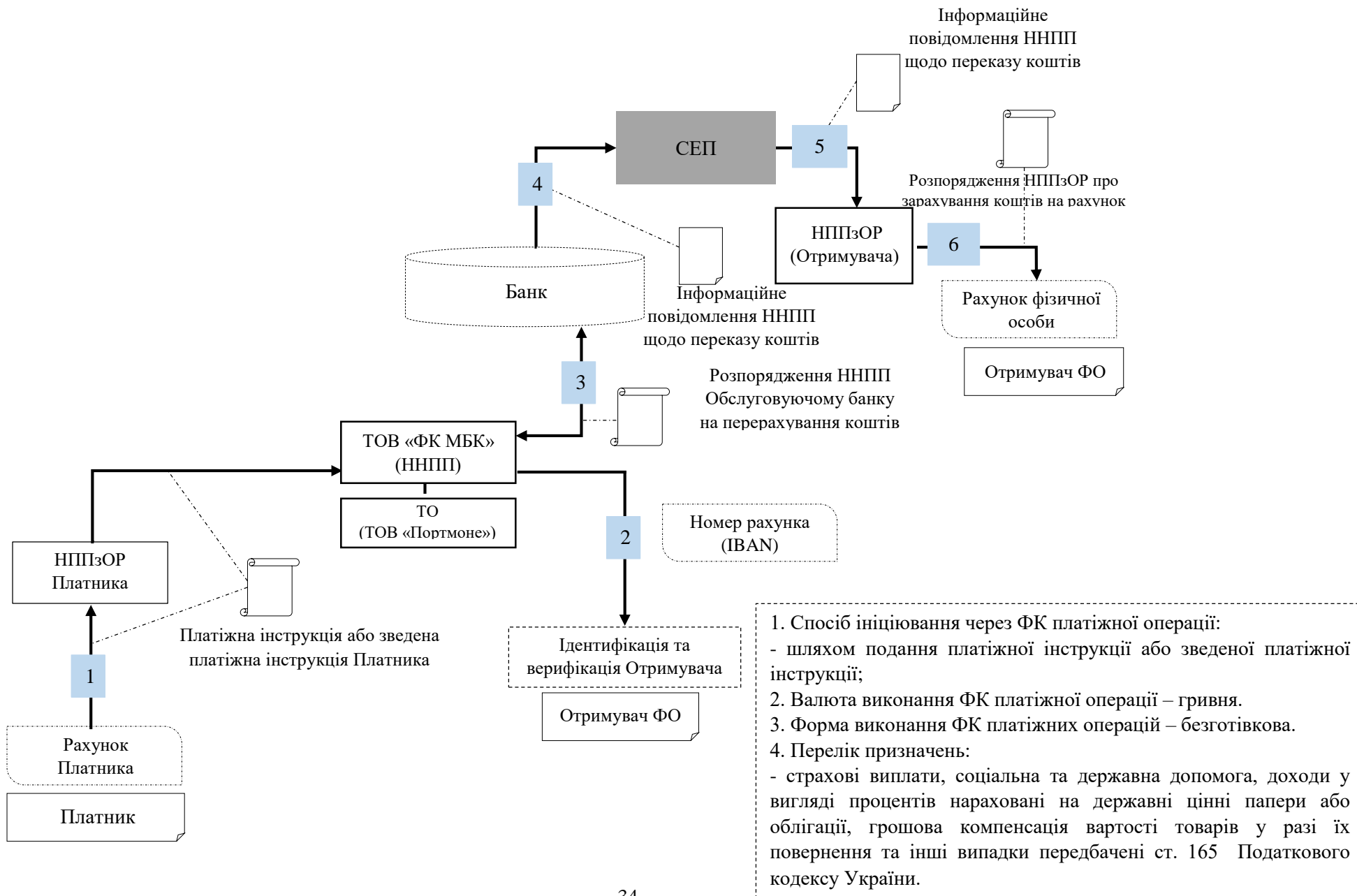
5) НППЗОР Отримувача ФО отримує через СЕП інформацію про переказ коштів на користь відповідного Отримувача ФО.

6) НППЗОР Отримувача ФО відображає Отримувачу ФО інформацію про зарахування суми коштів на рахунок Отримувача ФО.

6.4. Графічне зображення схеми виконання ФК платіжної операції переказу коштів з рахунку на рахунок за реквізитами платіжної картки (A2C) (*інформаційні потоки*) (далі – Графічна схема №7):



6.5. Графічне зображення схеми виконання ФК платіжної операції переказу коштів з рахунку на рахунок (A2A) (*інформаційні потоки*) (далі – Графічна схема №8):

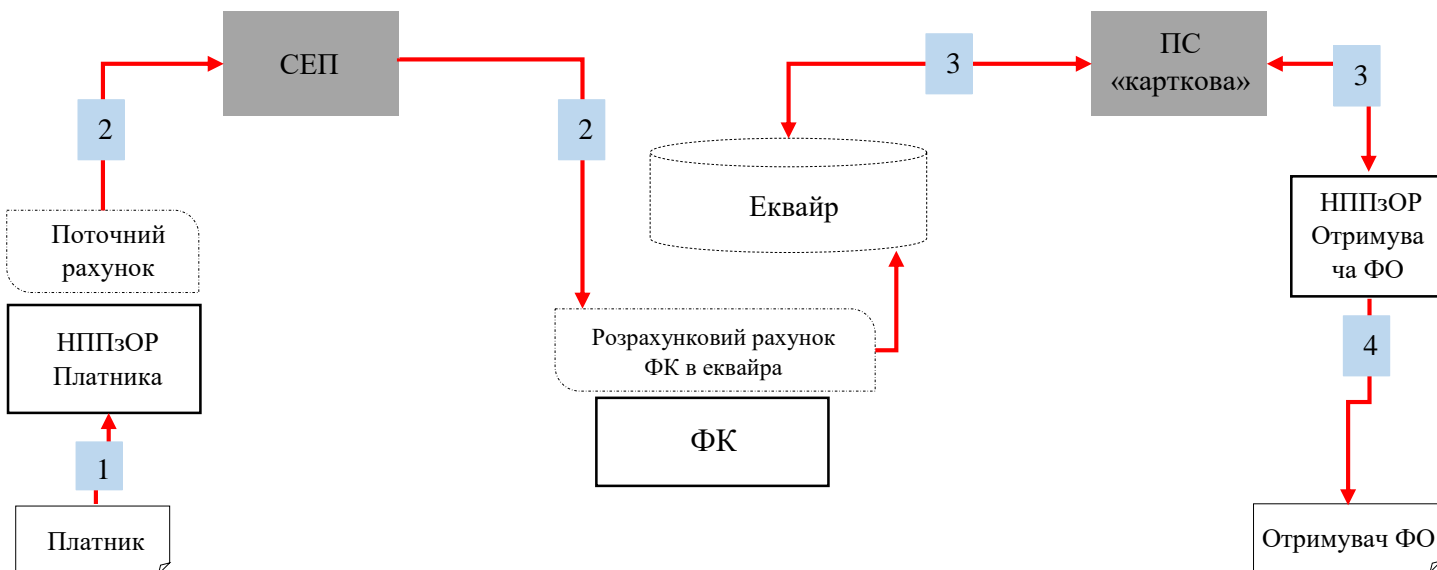


6.6. Перед встановленням ділових відносин ФК здійснює належну перевірку та вживає всіх заходів, виконання яких вимагає Закон України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 року №361-IX (далі – Закон про ПВК/ФТ). Після здійснення належної перевірки ФК укладає з таким Платником договір про надання платіжних послуг – виконання операцій А2С (account-to-card) або А2А (account-to-account), який передбачає перерахування Платником на розрахунковий рахунок ФК певної суми для здійснення операцій з переказу коштів фізичним особам.

6.7. **Додатковий опис до Графічної схеми №8:**

6.7.1. **Платником може бути:** 1) фізична особа-підприємець, фізична особа, що здійснює незалежну професійну діяльність та юридична особа, з якими ФК уклала договори про надання платіжних послуг; 2) органи державної влади України у разі здійснення виплат суми державної та соціальної матеріальної допомоги, державної допомоги, компенсації, вартості соціальних послуг та реабілітаційної допомоги, грошової компенсації особам з інвалідністю, фінансової допомоги та інших видів виплат відповідно до статті 165 Податкового кодексу України. Територія здійснення платіжних операцій – Україна. Отримувач є фізичною особою, резидентом України. Платник є резидентом України.

6.8. Графічне зображення схеми виконання ФК платіжної операції переказу коштів з рахунку на рахунок за реквізитами ЕПЗ (А2С) за номером ЕПЗ Отримувача ФО (схема руху коштів до Графічної схеми №7):



6.9. Фінансові взаєморозрахунки відбуваються у наступному порядку:

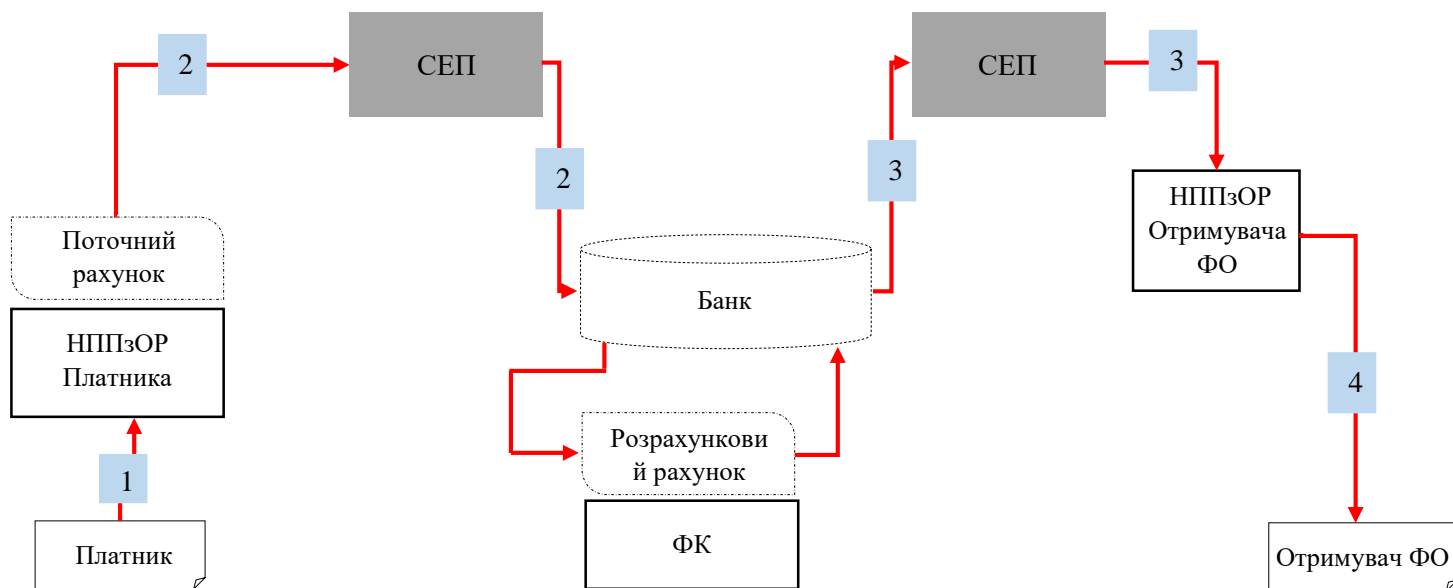
6.9.1. Платник подає НППЗО платіжну інструкцію про перерахування коштів на розрахунковий рахунок ФК в Обслуговуючому банку;

6.9.2. НППЗО Платника протягом операційного часу у той самий операційний день, в якому було подано платіжну інструкцію Платником, виконує платіжну операцію з перерахування коштів на розрахунковий рахунок ФК в Обслуговуючому банку. НППЗО зобов'язаний прийняти до виконання платіжну інструкцію Платника, що надійшла до нього після закінчення операційного часу, не пізніше наступного операційного дня;

6.9.3. Еквайр протягом операційного часу того самого операційного дня, у якому надійшов запит від ФК про виконання платіжної операції з розрахункового рахунку ФК у банка-еквайра здійснює розрахунки з емітентом ЕПЗ Отримувача ФО відповідно до правил «карткових» ПС (у тому числі шляхом клірингу);

6.9.4. НППЗО Отримувача ФО (емітент ЕПЗ) зараховує кошти на рахунок Отримувача ФО.

6.10. Графічне зображення схеми виконання ФК платіжної операції з переказу коштів з рахунку на рахунок (А2А) за номером ІВАН отримувача (схема руху коштів до Графічної схеми №8):



6.11. Фінансові взаєморозрахунки відбуваються у наступному порядку:

6.11.1. Платник подає НППЗОР платіжну інструкцію про перерахування коштів на розрахунковий рахунок ФК в Обслуговуючому банку;

6.11.2. НППЗОР Платника протягом операційного часу у той самий операційний день, в якому було подано платіжну інструкцію Платником, виконує платіжну операцію з перерахування коштів на розрахунковий рахунок ФК в Обслуговуючому банку. НППЗОР зобов'язаний прийняти до виконання платіжну інструкцію Платника, що надійшла до нього після закінчення операційного часу, не пізніше наступного операційного дня;

6.11.3. Після отримання коштів від Платника ФК з урахуванням строків передбачених Законом України «Про платіжні послуги», подає Обслуговуючому банку платіжні інструкції для виконання платіжних операцій з переказу коштів на користь Отримувачів ФО в розрізі кожного Отримувача за номером ІВАН. Обслуговуючий банк виконує платіжні інструкції ФК протягом операційного часу у той самий операційний день, в якому було подано платіжну інструкцію. Зазначені платіжні операції проходять через СЕП;

6.11.4. НППЗОР Отримувача ФО зараховує отримані від ФК кошти на рахунок Отримувача ФО.

7. ФОРМА ТА ПОРЯДОК НАДАННЯ ЗГОДИ ПЛАТНИКА НА ВИКОНАННЯ ПЛАТІЖНОЇ ОПЕРАЦІЇ

7.1. Форми надання згоди Платника на виконання ФК платіжної операції:

7.1.1. Електронна форма з використанням Платіжного застосунку ННПП/сайту ННПП – у випадку ініціювання платіжної операції з використанням ЕПЗ, платіжна інструкція надається в електронному вигляді шляхом заповнення і обрання полів, що пропонуються на відповідній платіжній сторінці і необхідні для виконання платіжної операції, що ініціюється Платником;

7.1.2. Електронна форма з використанням платіжних пристроїв - у випадку ініціювання платіжної операції через Платіжні пристрої (банківський автомат, платіжний термінал, програмно-технічний комплекс самообслуговування, програмно-апаратне середовище мобільного телефону, система дистанційного обслуговування банку, інший пристрій, що належить надавачам платіжних послуг, з ФК уклала відповідні договори), платіжна інструкція надається в електронному вигляді шляхом заповнення і обрання полів, що пропонуються у відповідному платіжному пристрої і необхідні для виконання платіжної операції, у порядку та спосіб, що передбачені вимогами надавача платіжних послуг, якому належить такий Платіжний пристрій;

7.1.3. Паперова форма – у разі ініціювання платіжної операції через Касу/ПНФП/ПТКС ННПП (технічний протокол Portmone Direct). У такому разі платіжна інструкція подається платником

безпосередньо до Каси/ПНФП/ПТКС НПП. У випадку ініціювання платіжної операції через Касу/ПНФП/ПТКС НПП, платіжна інструкція подається за формою, затвердженою нормативно-правовими актами Національного банку України щодо порядку організації касової роботи банками та проведення платіжних операцій надавачами платіжних послуг в Україні.

8. ПОРЯДОК ПРИЙНЯТТЯ ДО ВИКОНАННЯ ПЛАТІЖНОЇ ІНСТРУКЦІЇ ТА НАСТАННЯ МОМЕНТУ БЕЗВІДКЛИЧНОСТІ ПЛАТІЖНОЇ ІНСТРУКЦІЇ, ПОРЯДОК ВІДКЛИКАННЯ ЗГОДИ ПЛАТНИКА НА ВИКОНАННЯ ПЛАТІЖНОЇ ОПЕРАЦІЇ

8.1. Згода на виконання платіжної операції (пов'язаних між собою платіжних операцій) може бути надана Платником ФК особисто (у разі ініціювання платіжної операції з використанням ЕПЗ) або через іншого надавача платіжних послуг, з яким ФК уклала договір (схема Portmone Direct). Згодою Платника на виконання платіжної операції є здійснення дій, які однозначно свідчать про його бажання здійснити переказ коштів на зазначених умовах на користь зазначеного ним Отримувача, у тому числі: підтвердження згоди в інтерфейсі веб-сайту Отримувача, платіжної сторінки ФК, Платіжного пристрою, відповідно до їхнього функціоналу шляхом заповнення форм, натискання кнопок тощо, введення даних ЕПЗ Платника, підтвердження згоди на операцію на боці емітента ЕПЗ та ін.

8.2. ФК передбачає у певних договорах про надання платіжних послуг з Платниками виконання платіжних операцій, пов'язаних між собою спільними ознаками, у визначений Платником період часу (автоматичні платежі). У такому разі згода надається перед виконанням першої платіжної операції.

8.3. ФК приймає до виконання надану Платником платіжну інструкцію, за умови, що вона оформлена належним чином та немає законних підстав для відмови в її прийнятті, цілодобово (з 00 години 00 хвилин 00 секунд за Київським часом до 23 години 59 хвилин 59 секунд за Київським часом поточної доби), незалежно від часу та вихідних чи святкових днів.

8.4. Згода на виконання платіжної операції (пов'язаних між собою платіжних операцій) може бути відкликана Платником не пізніше настання моменту безвідкличності платіжної інструкції відповідно до Закону України «Про платіжні послуги». Після списання коштів з рахунку Платника або настання дати валютування платіжної інструкції настає момент безвідкличності платіжної інструкції.

8.5. Платник має право відкликати згоду на виконання платіжної операції з використанням ЕПЗ до 23:00 дня, в якому було ініційовано таку платіжну операцію та за умови підтвердження ФК можливості відкликання такої платіжної операції, шляхом усного чи письмового звернення до ФК в довільній формі, але із зазначенням реквізитів платіжної інструкції.

8.6. Повернення Платнику прийнятих ФК коштів може відбуватись:

8.6.1. шляхом ініціювання однією стороною (ФК або Отримувачем) та лише за умови підтвердження технічної можливості такого повернення іншою стороною, засобами передбаченими в технічному протоколі з обов'язковим направленням письмового повідомлення про повернення коштів за відповідною платіжною операцією.

8.6.2. у випадку застосування еквайром процедури чарджбек, про що ФК інформує Отримувача електронною поштою. Для встановлення правомірності платіжної операції еквайр має право призупинити завершення транзакції не більше ніж на сто вісімдесят днів від дати Авторизації. У разі встановлення правомірності платіжної операції, ФК з ініціативи еквайра має завершити транзакцію, а у разі встановлення неправомірності платіжної операції за результатами моніторингу або в разі опротестування платіжної операції держателем Платіжного інструменту, емітентом або ПС – сума операції повертається держателю Платіжного інструменту, про що ФК письмово інформує Отримувача з посиланням на відповідне рішення ПС.

8.7. Після обробки операції повернення коштів Платнику, з відображенням в Білінговій системі та системі Отримувача (що відображається в контрольному реєстрі), ФК здійснює операцію з повернення коштів Платнику протягом 10-и операційних днів та в подальшому утримує їх із сум оплат на користь Отримувача, що відображається в акті наданих послуг. У випадку відсутності наступних платіжних операцій на користь Отримувача, Отримувач зобов'язується протягом 10 (десяти) робочих днів з дати отримання письмової заяви ФК, здійснити відшкодування на повну суму проведених повернень на користь Платника. Отримувач здійснює відшкодування на рахунок ФК зазначений в письмовій заяві, а ФК проводить взаєморозрахунки з еквайрами.

9. ДОКУМЕНТИ ЗА ОПЕРАЦІЯМИ З ВИКОРИСТАННЯМ ПЛАТІЖНИХ ІНСТРУМЕНТІВ

9.1. Документ, який підтверджує ініціювання Платником платіжної операції через ФК (квитанція) – це документ, що підтверджує факт успішного ініціювання платіжної операції через ФК.

9.2. Квитанції, що оформлені ФК відповідно до вимог законодавства та нормативно-правових актів Національного банку України, мають статус первинного документа, і можуть використовуватися у разі врегулювання спірних питань між держателем ЕПЗ і Отримувачем, а також між держателем і емітентом.

9.3. Квитанції складаються ФК та друкуються державною мовою. У разі необхідності, квитанції можуть бути складені іншою мовою за домовленістю сторін (Платника та ФК) відповідно до законодавства України або якщо Платіжний пристрій дає Платнику технічну можливість здійснити вибір мови.

9.4. Квитанції повинні містити такі обов'язкові реквізити:

- 1) номер платіжної інструкції;
- 2) інформацію про ФК;
- 3) інформацію про Платника та Отримувача;
- 4) дату та час здійснення операції;
- 5) суму та валюту операції;
- 6) суму комісійної винагороди ФК (за наявності);
- 7) призначення платіжної операції;
- 8) ідентифікатор еквайра або інші реквізити, за допомогою яких є можливість ідентифікувати еквайра;
- 9) ідентифікатор Отримувача;
- 10) ідентифікатор Платіжного пристрою;
- 11) унікальний код операції / у разі використання платіжного інструменту в платіжній системі – найменування платіжної системи та код авторизації або інший код, що ідентифікує операцію в платіжній системі;

9.5. Квитанції оформлюються ФК у вигляді електронних документів з накладанням електронної печатки ФК для засвідчення чинності та достовірності такого документа. На вимогу Платника ФК може оформити квитанцію у паперовому вигляді з власноручним підписом уповноваженої особи ФК.

9.6. Для платіжних операцій, ініційованих не з використанням ЕПЗ, зокрема, у випадках, коли Платником є юридична особа чи НПП, яким ФК надає послугу переказу коштів, документами, які підтверджують ініціювання платіжної операції через ФК є контрольні реєстри (реєстри), за умови, що вони містять всі необхідні реквізити, передбачені пунктом 6.4. Крім зазначено, Платник та ФК щомісяця укладають акти наданих послуг, акти звіряння та інші документи, передбачені договором між ФК та таким Платником, які підтверджуються факт належного надання ФК платіжних послуг з переказу коштів.

10. ІДЕНТИФІКАЦІЯ ПЛАТНИКА ТА ОТРИМУВАЧА. СУПРОВОДЖЕННЯ ПЛАТІЖНИХ ОПЕРАЦІЙ НЕОБХІДНОЮ ІНФОРМАЦІЄЮ

10.1. Детальний порядок здійснення ФК заходів належної перевірки клієнтів (користувачів платіжних послуг), супроводження платіжних операцій необхідною інформацією та виконання інших функцій суб'єкта первинного фінансового моніторингу визначений внутрішніми Правилами проведення фінансового моніторингу в ТОВ «ФК МБК» (далі - Правила), що розроблені відповідно до вимог Закону України від 06.12.2019 № 361-ІХ «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», зі змінами та доповненнями (далі – Закон), Закону України № 1591-ІХ від 30 червня 2021 року «Про платіжні послуги», Положення про здійснення установами фінансового моніторингу, затвердженого Постановою Правління Національного банку України № 107 від 28 липня 2020 року (далі – Положення № 107) та інших нормативно-правових актів Національного банку України.

10.2. Порядок виконання ФК функцій суб'єкта реалізації санкцій під час надання платіжних послуг визначений внутрішнім Порядком реалізації персональних спеціальних економічних та інших обмежувальних заходів (санкцій) в ТОВАРИСТВІ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ФІНАНСОВА КОМПАНІЯ МБК», який розроблено з урахуванням вимог Закону України «Про

санкції» від 14 серпня 2014 року №1644-VII, Положення про реалізацію спеціальних економічних та інших обмежувальних заходів (санкцій), затвердженого Постановою Правління Національного банку України від 11.05.2023 року №65 та інших нормативно-правових актів.

10.3. Відповідальним за організацію дотримання вимог законодавства України у сфері запобігання та протидії легалізації (відмиванню) кримінальних доходів/фінансування тероризму, розповсюдження зброї масового знищення (ПВК/ФТ) та належну організацію внутрішньої системи ПВК/ФТ є Генеральний директор Товариства та Відповідальний працівник Товариства, який призначається на посаду у порядку визначеному законодавством.

10.4. Належна перевірка клієнтів (будь-яка особа, яка звертається за наданням послуг або користується послугами ФК) здійснюється ФК у разі:

- встановлення ділових відносин;
- наявності підозри;
- здійснення платіжних операцій (у тому числі міжнародних) без відкриття рахунка;
- проведення фінансової операції з віртуальними активами на суму, що дорівнює чи перевищує 30 000 гривень;
- виникнення сумнівів у достовірності чи повноті раніше отриманих ідентифікаційних даних клієнта;
- проведення разової фінансової операції без встановлення ділових відносин з клієнтами, якщо сума фінансової операції дорівнює або перевищує 400 000 грн.

Залежно від рівня ризику проведення фінансової операції належна перевірка клієнта здійснюється також у разі проведення ним кількох фінансових операцій, що можуть бути пов'язані між собою, на загальну суму, що дорівнює або перевищує 400 000 грн.

10.5. Ідентифікація та верифікація клієнта здійснюються до/або під час встановлення ділових відносин, вчинення правочинів (крім випадків, передбачених Законом), але до проведення фінансової операції.

10.6. Повторна ідентифікація та верифікація клієнта (його представника) не є обов'язковими, якщо ця особа раніше була ідентифікована та верифікована згідно з вимогами Закону, за умови відсутності у ФК підозр та/або підстав вважати, що наявні документи, дані та/або інформація про клієнта (представника клієнта) є нечинними (недійсними) та/або неактуальними.

10.7. Для здійснення належної перевірки клієнта (представника клієнта) при встановленні ділових відносин (укладанні договору про надання платіжних послуг), оформлених у письмовій формі, виникненні підозри, проведення разової фінансової операції без встановлення ділових відносин з клієнтами на суму, що дорівнює чи перевищує 400 000 гривень, або суму, еквівалентну зазначеній сумі, у тому числі в іноземній валюті, банківських металах, інших активах, працівник фронт-офісу ФК встановлює наступну інформацію:

Особа, що ідентифікується, верифікується та вивчається	Інформація, що встановлюється	Документи, що є підставою для ідентифікації, верифікації та вивчення
Фізична особа-резидент	1) прізвище, ім'я та по батькові; 2) дата народження; 3) номер (та за наявності - серію) паспорта громадянина України (або іншого документа, що посвідчує особу та відповідно до законодавства України може бути використаним на території України для укладення правочинів), дату видачі та орган, що його видав; 4) реєстраційний номер облікової картки платника податків, номер (та за наявності - серію) паспорта громадянина України, в якому проставлено відмітку про відмову від прийняття реєстраційного номера	1) паспорт громадянина України або інший документ, що посвідчує особу та відповідно до законодавства України може бути використаним на території України для укладення правочинів; 2) довідка про присвоєння ідентифікаційного номеру <i>або</i> картка платника податків, <i>або</i> дані про реєстраційний номер облікової картки платника податків, що вноситься до паспорта громадянина України у формі книжечки за формою, наведеною у додатку 4 до Положення про реєстрацію фізичних

	<p>облікової картки платника податків, чи номер паспорта із записом про відмову від прийняття реєстраційного номера облікової картки платника податків в електронному безконтактному носії;</p> <p>5) місце проживання або місце перебування фізичної особи - резидента України;</p> <p>б) належність до політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами;</p> <p>7) унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).</p>	<p>осіб у Державному реєстрі фізичних осіб - платників податків, затвердженого наказом Міністерства фінансів України від 29.09.2017 № 822 або дані про реєстраційний номер облікової картки платника податків, що містяться на звороті</p> <p>паспорта громадянина України у формі ID-картки;</p> <p>3) Анкета фінансового моніторингу фізичної особи (додаток до Правил)</p>
Фізична особа-нерезидент	<p>1) прізвище, ім'я та (за наявності) по батькові;</p> <p>2) дата народження;</p> <p>3) номер (та за наявності - серію) паспорта (або іншого документа, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів), дату видачі та орган, що його видав;</p> <p>4) громадянство;</p> <p>5) місце проживання або місце тимчасового перебування фізичної особи - нерезидента в Україні</p> <p>б) належність до політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами;</p> <p>7) унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).</p>	<p>1) національний паспорт громадянина іншої держави або інший документ, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів;</p> <p>2) Анкета фінансового моніторингу фізичної особи (додаток до Правил).</p>
Фізична особа-підприємець	<p>1) прізвище, ім'я та (за наявності) по батькові;</p> <p>2) дата народження;</p> <p>3) номер (та за наявності - серію) паспорта громадянина України (або іншого документа, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів), дату видачі та орган, що його видав;</p> <p>4) реєстраційний номер облікової картки платника податків, номер (та за наявності - серію) паспорта громадянина України, в якому проставлено відмітку про відмову від прийняття реєстраційного номера облікової картки платника податків, чи номер паспорта із записом про відмову від прийняття реєстраційного номера</p>	<p>1) паспорт громадянина України або інший документ, що посвідчує особу та відповідно до законодавства України може бути використаний на території України для укладення правочинів;</p> <p>2) довідка про присвоєння ідентифікаційного номеру або картка платника податків, або дані про реєстраційний номер облікової картки платника податків, що вноситься до паспорта громадянина України у формі книжечки за формою, наведеною у додатку 4 до Положення про реєстрацію фізичних осіб у Державному реєстрі фізичних осіб - платників податків, затвердженого наказом Міністерства фінансів України від 29.09.2017 № 822 або дані про реєстраційний номер облікової картки</p>

	<p>облікової картки платника податків в електронному безконтактному носії; 5) дату та номер запису в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань про проведення державної реєстрації; 6) місце проживання або місце перебування; 7) реквізити банку, в якому відкрито рахунок, і номер поточного рахунка (за наявності); 8) види діяльності відповідно до КВЕД; 9) належність до політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами; 10) унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).</p>	<p>платника податків, що містяться на звороті паспорта громадянина України у формі ID-картки; 3) документ, який підтверджує реєстрацію особи в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань (Виписка (або Витяг) з Єдиного державного реєстру юридичних та фізичних осіб-підприємців або Електронний витяг); 4) Анкета фінансового моніторингу фізичної особи – підприємця (додаток до Правил) 5) Додаток до ID картки громадянина України (витяг з Державного демографічного реєстру).</p>
<p>Юридична особа-резидент</p>	<p>1) повне найменування; 2) місцезнаходження; 3) дату та номер запису в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань про проведення державної реєстрації; 4) відомості про виконавчий орган (органи управління); 5) ідентифікаційні дані осіб, які мають право розпоряджатися рахунками та/або майном; 6) ідентифікаційний код згідно з Єдиним державним реєстром підприємств та організацій України; 7) реквізити банку, в якому відкрито рахунок, і номер поточного рахунка; 8) дані, що дають змогу встановити кінцевих бенефіціарних власників (контролерів); 9) структура власності клієнта; 10) види діяльності відповідно до КВЕД; 11) характеристика операції, що планує проводити клієнт; 12) розмір зареєстрованого та сплаченого статутного капіталу юридичної особи; 13) кількість працівників; 14) належність до політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами; 15) фінансовий стан; 16) наявність ліцензій (за наявності).</p>	<p>1) документ, який підтверджує реєстрацію особи в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань (Виписка (або Витяг) з Єдиного державного реєстру юридичних та фізичних осіб-підприємців або Електронний витяг); 2) документи, що підтверджують обрання керівника юридичної особи та його повноваження; 3) опис документів, що надаються державному реєстратору для проведення реєстраційної дії пов'язаної з реєстрацією статуту (нові редакції статуту) або установчі документи; 4) документи, що засвідчують осіб, які мають право підпису платіжних/розрахункових та інших документів від імені юридичної особи (в разі їх наявності); 5) структура власності юридичної особи; 6) Фінансова звітність станом на останню звітну дату. (Показники фінансової звітності юридичної особи, (баланс (Ф1) та звіт про фінансові результати (Ф2), Звіт про використання доходів (прибутків) неприбуткових організацій (в разі наявності); 7) ліцензії (за наявності); 8) Анкета фінансового моніторингу юридичної особи (додаток до Правил).</p>

Юридична особа-нерезидент	<ol style="list-style-type: none"> 1) повне найменування; 2) місцезнаходження; 3) реквізити банку, в якому відкрито рахунок, номер банківського рахунка; 4) відомості про виконавчий орган (органи управління); 5) ідентифікаційні дані осіб, які мають право розпоряджатися рахунками та/або майном; 6) дані, що дають змогу встановити кінцевих бенефіціарних власників (контролерів); 7) структура власності клієнта; 8) види діяльності та характеристика операцій, що планує проводити клієнт; 9) розмір зареєстрованого та сплаченого капіталу юридичної особи; 10) кількість працівників; 11) належність до політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами. 	<ol style="list-style-type: none"> 1) копія легалізованого витягу з торгового, банківського чи судового реєстру або нотаріально засвідчене реєстраційне посвідчення уповноваженого органу іноземної держави про реєстрацію відповідної юридичної особи; 2) копії легалізованих установчих документів; 3) копії легалізованих документів, які посвідчують осіб уповноважених діяти від імені Клієнта та документи, що підтверджують їх повноваження; 4) Анкета фінансового моніторингу юридичної особи (додаток до Правил).
Траст та інше подібне правове утворення, що не є юридичною особою	<ol style="list-style-type: none"> 1) повне найменування; 2) мета та цілі діяльності; 3) об'єкти управління, що належать нерезиденту; 4) країна заснування, місцезнаходження; 5) реквізити банку, в якому відкрито рахунок, номер банківського рахунка; 6) ідентифікаційний номер (у разі наявності), що нерезидент використовує при поданні податкових декларацій та інших податкових документів до податкових органів у країні, резидентом якої він є; 7) належність до політично значущих осіб, членів їх сімей та осіб, пов'язаних з політично значущими особами. 	<ol style="list-style-type: none"> 1) копія легалізованого витягу з торгового, банківського чи судового реєстру або нотаріально засвідчене реєстраційне посвідчення уповноваженого органу іноземної держави про реєстрацію нерезидента (засновника трасту або іншого подібного правового утворення); 2) засвідчена копія документа або його витяг про утворення (заснування) трасту або іншого подібного правового утворення; 3) копії легалізованих документів, які посвідчують осіб уповноважених діяти від імені клієнта та документи, що підтверджують їх повноваження; 4) копії легалізованих установчих документів; 5) Анкета фінансового моніторингу юридичної особи (додаток до Правил).

10.8. ФК з метою виконання вимог, передбачених статтею 14 Закону забезпечує наявність у платіжних інструкціях усіх необхідних полів для внесення інформації про Платника та/або Отримувача за платіжною операцією; супроводження платіжної операції обов'язковою інформацією про Платника і Отримувача коштів; за допомогою програмного комплексу запроваджує заходи моніторингу наявності обов'язкової інформації про платіжну операцію та виявлення реквізитів, заповнених із використанням символів, які не допускаються ПС.

Інформація, що супроводжує платіжну операцію	Документи, що є підставою для верифікації
- прізвище, ім'я та (за наявності) по батькові такої особи;	- паспорт громадянина України або інший документ, що посвідчує особу та відповідно до законодавства України може бути використаним на території України для укладення правочинів;

<ul style="list-style-type: none"> - обліковий номер фінансової операції, що присвоюється автоматично в системі та дає змогу відстежити рух коштів; - місце проживання (або місце перебування) або номер (та за наявності - серію) паспорта громадянина України (або іншого документа, що посвідчує особу та відповідно до законодавства України може бути використаним на території України для укладення правочинів), або реєстраційний номер облікової картки платника податків, або дату і місце народження; - номер засобу зв'язку (за наявності). 	<ul style="list-style-type: none"> - довідка про присвоєння ідентифікаційного номеру або картка платника податків, або дані про реєстраційний номер облікової картки платника податків, що внесені до паспорта громадянина України; - електронна Анкета Клієнта.
--	--

10.9. ФК може здійснити верифікацію клієнта – фізичної особи шляхом використання одного з таких способів:

1) за допомогою Системи BankID НБУ в такому порядку:

- отримати ідентифікаційні дані такої фізичної особи за допомогою засобів Системи BankID НБУ;
- отримати від фізичної особи копію ідентифікаційного документа (копії сторінок ідентифікаційного документа, що містять ідентифікаційні дані), на яку накладений КЕП клієнта;
- здійснити перевірку ідентифікаційних даних, що містяться в копії ідентифікаційного документа, КЕП та файлі, отриманому за допомогою Системи BankID НБУ від банку, що є абонентом-ідентифікатором, на їх відповідність;

2) шляхом отримання електронної копії ідентифікаційного документа, в такому порядку:

- отримати е-паспорт/е-паспорт для виїзду за кордон, завірений кваліфікованою електронною печаткою ДП «ДІА» з відповідною кваліфікованою електронною позначкою часу, що відповідатиме даті здійснення верифікації особи, та:

- отримати копію ідентифікаційного документа або опитувальника, на який накладений КЕП клієнта. ФК вважає верифікацію клієнта – фізичної особи завершеною лише за умови здійснення ним успішної перевірки відповідності отриманих ідентифікаційних даних.

10.10. ФК на підставі чинного договору доступу до СЕІ з ДП «Дія» здійснює верифікацію ФОП або представника клієнта – суб'єкта господарювання та перевіряє наявність у представника суб'єкта господарювання відповідних повноважень в такому порядку:

1) отримує документи для встановлення ділових відносин за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, які підписані/засвідчені КЕП клієнта, який є ФОП, або КЕП фізичної особи як представника відповідного суб'єкта господарювання;

2) здійснює перевірку наявності необхідного обсягу повноважень у такої фізичної особи як представника відповідного суб'єкта господарювання за допомогою підсистеми верифікації СЕІ (для суб'єктів господарювання);

3) встановлює факт відповідності ідентифікаційних даних, що містяться в підсистемі верифікації СЕІ, ідентифікаційним даним, що містяться в КЕП такої особи;

4) документує факти здійснення вищезазначених перевірок.

10.11. З метою не допущення уникнення певних порогових значень, виконання вимог, визначених чинним законодавством з питань фінансового моніторингу, зокрема дроблення платіжної операції на кілька пов'язаних між собою платіжних операцій, що здійснюються на менші суми з метою уникнення верифікації Платника при проведенні платіжної операції на суму, що дорівнює чи перевищує 30 тис. грн., в тому числі за наявності ознак пов'язаності такої платіжної операції з іншими платіжними операціями, що в сумі перевищують 30 тис. грн., ФК запроваджено обов'язкову верифікацію Платника (за умови, що він не був верифікований протягом останніх 12 місяців).

10.12. Ліміти (обмеження) на використання платіжних інструментів:

№	Вид платіжної операції	Ліміти (обмеження) платіжної операції*
1	2	3
1	Переказ коштів від фізичної особи на користь отримувача-суб'єкта господарювання (юридична особа чи	Від 0,05 грн. до 4 000 000 грн.**

	фізична особа-підприємець), що ініціюється за допомогою електронного платіжного засобу (ЕПЗ)	
2	Переказ коштів від фізичної особи з метою сплати податків, зборів, платежів, зборів (страхових внесків) на обов'язкове державне пенсійне та соціальне страхування, штрафних санкцій та пені за порушення законодавства до державного і місцевих бюджетів, Пенсійного фонду України, на рахунки органів державної влади, органів місцевого самоврядування або платіжної операції з метою оплати житлово-комунальних послуг	Від 0,05 грн. до 5 000 000 грн.**

*Зазначений перелік лімітів (обмежень) не є вичерпним. ФК як суб'єкт первинного фінансового моніторингу залишає за собою право встановлювати інші обмеження з метою управління ризиками та недопущення використання послуг ФК у протиправних цілях. На виконання вимог Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», для проведення платіжної операції на суму що дорівнює чи перевищує 30 000 грн., ФК здійснює належну перевірку (ідентифікацію та верифікацію) платника.

**Отримувачі коштів можуть встановлювати інші обмеження щодо мінімальної та максимальної суми платіжної операції.

10.13. Відповідно до ст. 23 Закону ФК:

- має право зупинити здійснення фінансової операції, якщо вона є підозрілою;
- зобов'язана зупинити фінансові операції в разі виникнення підозри, що вони містять ознаки вчинення кримінального правопорушення, визначеного Кримінальним кодексом України.

10.14. ФК здійснює заходи, що забезпечують можливість замороження активів терористів, в тому числі за допомогою засобів автоматизації програмного комплексу ФК, а саме:

- завантаження переліку терористів та змін до нього на постійній основі;
- здійснення скринінгових процедур, які дають змогу виявити в клієнтській базі та в фінансових операціях індикатори пов'язаності з особами з переліку терористів;
- розгляд та порядок ескалації випадків виявлення індикаторів пов'язаності з особами з переліку терористів, зокрема збігу окремих даних (комбінацій даних) із клієнтської бази та фінансових операцій з даними осіб із переліку терористів;
- призупинення здійснення фінансових операцій та/або замороження/розмороження відповідних активів.

11. ПОРЯДОК ЗДІЙСНЕННЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ

11.1. Облікова політика ФК визначає сукупність принципів, методів та процедур, що використовуються для фінансового та управлінського обліку, складання звітності та організацію процесу бюджетування.

11.2. Облікова політика розробляється у відповідності до законів, положень, інструкцій й інших нормативних актів, що регулюють порядок ведення бухгалтерського обліку, складання і представлення фінансової звітності в Україні, та затверджується керівником ФК.

11.3. Для обліку платіжних операцій використовується комп'ютерна програма, що дозволяє заводити відомості про Банки, Отримувачів, договори, фінансові умови співпраці, централізовано змінювати налаштування в базі даних, здійснювати моніторинг проведених операцій, отримувати та перевіряти реєстри за визначений проміжок часу в розрізі по кожному Отримувачу та/або Банку, формувати звіти за проведеними платіжними операціями.

11.4. **План рахунків, особливості обліку платіжних операцій та основні засади ціноутворення.**

11.4.1. План рахунків бухгалтерського обліку розробляється відповідно до Плану рахунків бухгалтерського обліку активів, капіталу, зобов'язань і господарських операцій підприємств і організацій, затвердженого наказом Міністерства фінансів України №291 від 21.12.1999 р. «Про затвердження Плану рахунків бухгалтерського обліку та Інструкції про його застосування». Робочий план рахунків наводиться в додатку до облікової політики. Відображення господарських операцій ФК в бухгалтерському обліку здійснюється з використанням синтетичних рахунків, субрахунків та аналітичних рахунків.

11.4.2. Аналітичні рахунки відкриваються в залежності від потреби та рівня аналітики.

11.4.3. Ведеться облік витрат з використанням 8 та 9 класів рахунків.

11.4.4. Облік платіжних операцій:

11.4.4.1. Кожного дня о 8:00 за Київським часом в шлюз обміну даними надходять файли які містять інформацію про суму прийнятих від Платників платіжних операцій, в розрізі Банків, Отримувачів та укладених договорів. Дані файли завантажуються в Програму Business automation software PROF (далі по тексту – BAS) та формують наступні кореспонденції:

Дт 374-Банк-договір-сума : Кт 683-Отримувач-договір-логін-сума.

Дана кореспонденція відображає дебіторську заборгованість Банків за прийнятими платіжними операціями та кредиторську заборгованість ФК перед Отримувачами за кожен день. На основі оборотів за рах. 374, щомісячно (період з 00:00:00 першого дня по 23:59:59 останнього дня місяця) формуються акти по прийнятих платіжних операціях з Банками. В актах вказується сума прийнятих операцій за звітний період та комісія за прийом платежів. Акти надсилаються на електронну адресу Банків для узгодження в перші два робочі дні, наступного місяця за звітним. На основі оборотів за рах. 683 формуються акти прийнятих платіжних операцій з Отримувачами. В актах вказується сума прийнятих коштів та комісія ФК за прийом платежів. Акти надсилаються на електронну адресу Отримувачів для узгодження в перші три робочі дні місяця наступного за звітним.

Комісія ФК є доходом підприємства та формує кореспонденцію:

Дт 361-Отримувач-договір-сума: Кт703-Дохід від операцій по прийому платежів-сума

Комісія Банків за прийом платежів є затратами підприємства та формує кореспонденцію:

Дт 903 – витрати на еквайринг та прийом платежів-сума: Кт 631-Банк-Договір-сума

Через великий потік операцій в секунду, а також через те що в Банків, ФК та Отримувачів сервери можуть бути не синхронізовані, виникає тимчасова різниця між даними Банків та Отримувачів про прийняті платіжні операції. Дана різниця відображається на рахунках 374 та 683 по субконто Перехідні транзакції.

11.5. Основні засади ціноутворення. Винагородою ФК є комісія, яка встановлюється як процент від суми прийнятих (в окремих випадках перерахованих) платіжних операцій, або фіксована сума. Розмір комісії визначається в договорі з кожним Отримувачем окремо. У разі, якщо розмір комісії яку сплачує Отримувач не покриває прямих витрат ФК на прийом платежів, може вводиться комісія з Платника (ініціатора платіжної операції). Розмір і порядок утримання комісії з Платника визначається наказом про тарифну політику ФК. Платник попереджається перед проведення (ініціюванням) платіжної операції про наявність та розмір комісії за проведення платіжної операції на користь конкретного Отримувача.

11.6. Форма обліку.

11.6.1. Бухгалтерський облік здійснюється з використанням комп'ютерної бухгалтерської програми BAS.

11.6.2. Фіксування фактів здійснення господарських операцій здійснюється шляхом оформлення первинних документів. Форми первинних документів можуть розроблятися ФК самостійно і використовуватись після затвердження Генеральним директором ФК.

11.6.3. Відповідальність за рівень відповідності реєстрів обліку, порядку і способу реєстрації й узагальнення інформації, передбаченого даною комп'ютерною програмою вимогам законодавства, покладається на головного бухгалтера ФК. Регістри обліку зберігаються в електронному вигляді, в програмі BAS.

11.6.4. Відповідно до пункту 1.3 «Положення про документальне забезпечення записів у бухгалтерському обліку», затвердженого наказом Міністерства фінансів України від 24.05.1995 р. № 88, усі первинні документи, облікові реєстри, фінансова, статистична й інша звітність складаються українською мовою. Документи, що служать підставою для записів у бухгалтерському обліку і

складені іноземною мовою, повинні мати погоджений переклад українською мовою відповідно до вимог Закону України «Про забезпечення функціонування української мови як державної».

11.6.5. При відображенні в бухгалтерському обліку господарських операцій і подій застосовуються норми (міжнародних стандартів) бухгалтерського обліку фінансової звітності, затверджених Міністерством фінансів України.

11.6.7. ФК складає фінансову звітність у відповідності до вимог МСБО 1 «Подання фінансової звітності».

11.7. ФК розробляє та встановлює межі суттєвості: операції, об'єкти обліку та статті звітності, за якими встановлюється поріг суттєвості; величини порога суттєвості; бази для визначення порога суттєвості.

11.8. ФК відображає відстрочені податкові активи й відстрочені податкові зобов'язання у річній фінансовій звітності.

11.9. При перерахуванні доходів, витрат і грошових коштів, виражених в іноземній валюті застосовується валютний курс НБУ на дату складання звіту.

11.10. ФК встановлює тривалість операційного циклу для визнання доходів і витрат в один місяць.

11.11. В порядку здійснення бухгалтерського обліку пов'язаними сторонами вважаються як юридичні, так і фізичні особи, які прямо або опосередковано здійснюють контроль над підприємством або суттєво впливають на його діяльність, та підприємства, які перебувають під його контролем або суттєвим впливом. Перелік таких осіб наводиться в додатках до облікової політики ФК та при необхідності оновлюється.

11.12. Облік основних засобів та нематеріальних активів.

11.12.1. ФК в обліковій політиці затверджує порядок визначення основних засобів; визначення вартісного бар'єру при визнанні основним засобом; спосіб ведення обліку основних засобів тощо.

11.12.2. ФК в обліковій політиці затверджує порядок визначення матеріальних активів; визначення терміну корисного використання; визначення малоцінних необоротних матеріальних активів.

11.12.3. Придбані (створені) основні засоби зараховуються на баланс ФК за первісною вартістю. Одиницею обліку основних засобів є об'єкт основних засобів.

11.12.4. ФК визначає правила нарахування амортизації, встановлює строки корисного використання основних засобів, умови проведення переоцінки основних засобів, відображення і облік ремонту основних засобів, відображення витрат на поліпшення основних засобів (модернізація, добудова, дообладнання, реконструкція тощо).

11.12.5. Нематеріальні активи зараховуються на баланс за первісною вартістю. При придбанні (створенні) нематеріального активу строк його корисного використання визначається комісією і затверджується наказом керівника підприємства. При нарахуванні амортизації нематеріальних активів застосовується прямолінійний метод.

11.13. ФК в обліковій політиці визначає порядок обліку запасів, порядок зарахування на баланс, порядок продажу (відпуск у виробництво, вибуття) та здійснення оцінки, порядок списання запасів тощо.

11.14. Облік дебіторської та кредиторської заборгованості.

11.14.1. ФК в обліковій політиці визначає порядок відображення дебіторської заборгованості за товари (роботи, послуги), порядок розрахунку величини резерву кредитного ризику, порядок визнання дебіторської заборгованості безнадійною, порядок проведення звіряння взаєморозрахунків, порядок визнання заборгованості погодженої, дії при порушенні дебіторами термінів сплати заборгованості, методи звіряння з Банками та порядок оформлення бухгалтерської довідки, в разі наявності розбіжностей.

11.14.2. ФК веде єдиний реєстр всіх покупців та постачальників (контрагентів), які мають унікальний ідентифікаційний номер. По кожному контрагенту повинна вестися наступна інформація:

- повне найменування контрагента;
- юридична та фактична адреса;
- банківські реквізити;
- код за ЄДРПОУ;
- код платника ПДВ (за наявності);
- РНОКПП;
- контактна інформація;
- свідоцтво про право сплати єдиного податку;

- ліцензії та дозволи на здійснення виду діяльності, що є предметом договору;
- реквізити договору, якщо договір з контрагентом укладався.

11.15. ФК в обліковій політиці визначає випадки та порядок створення резервів на покриття збитків через можливі шахрайські дії з платіжними інструментами, на відпустки співробітників, на додаткове пенсійне забезпечення, реструктуризацію, виконання зобов'язань за обтяженими контрактами тощо.

11.16. Облік доходів та витрат.

11.16.1 Дохід від реалізації товарів (продукції) визнається у відповідності до вимог МСФЗ 15 «Дохід від договорів з клієнтами».

11.16.2. Оцінка ступеня завершеності операції з надання послуг (виконання робіт) здійснюється шляхом вивчення наданої послуги, при цьому в бухгалтерському обліку доходи відображаються у звітному періоді підписання акту наданих послуг.

11.16.3. Проценти визнаються у тому звітному періоді, до якого вони належать, виходячи з бази їх нарахування та строку користування відповідними активами.

11.16.4. Роялті визнаються за принципом нарахування згідно з економічним змістом відповідної угоди.

11.16.5. Дивіденди визнаються в періоді прийняття рішення про їх виплату.

11.16.6. Витрати визнаються витратами певного періоду одночасно з визнанням доходу, для отримання якого вони здійснені. Витрати, які неможливо прямо пов'язати з доходом певного періоду, відображаються у складі витрат того звітного періоду, в якому вони були здійснені: адміністративні витрати, витрати на збут, інші витрати операційної діяльності.

11.16.7. ФК веде облік витрат з використанням 8 та 9 класів рахунків у відповідності до статей витрат визначених в обліковій політиці, що уточнюються щорічно. Порядок капіталізації фінансових витрат визначається в обліковій політиці ФК.

11.16.8. Доходи і витрати включаються до складу звіту про фінансові результати на підставі принципів нарахування та відповідності і відображаються в бухгалтерському обліку та фінансових звітах тих періодів, до яких вони відносяться. При цьому доходи і витрати відображаються в обліку і звітності у момент їх виникнення, незалежно від часу надходження або сплати грошових коштів.

12. УПРАВЛІННЯ РИЗИКАМИ

12.1. Управління ризиками – систематичний процес, завдяки якому ФК виявляє (ідентифікує) власні ризики, оцінює їх величину, здійснює їх моніторинг, контролює свої ризикові позиції та бере до уваги відносини між різними категоріями ризику.

Основні види ризиків, що можуть виникати, умовно поділяються ФК на операційні, комплаєнс-ризиків, ризиків безпеки та кіберризиків, регуляторні ризиків, ризиків ліквідності, кредитні ризиків, ринкові ризиків та інші види ризиків, детальний опис яких наведений у Політиці управління ризиками ТОВ «ФК МБК».

№	Вид ризику	Операції (події), що створюють ризики	Вірогідність настання (низька, середня, висока)	Заходи ФК щодо запобігання та мінімізації ризику
1	Операційний ризик	<ul style="list-style-type: none"> - управління персоналом; - управління ліквідністю; - виконання платіжних операцій; - забезпечення проведення розрахунків та зберігання документів; - операції з основними засобами та нематеріальними активами; - управління безперервністю діяльності - управління проектами; - управління бюджетом; 	низька	Обов'язкове приведення у відповідність до вимог нормативної бази своїх внутрішніх документів, а також технологічних інструкцій для співробітників, здійснення регулярне навчання та тестування співробітників, контроль за виконанням технологічних інструкцій і правил забезпечення інформаційної безпеки,

		<ul style="list-style-type: none"> - кваліфікація та компетентність працівників, посадових осіб Товариства; - злочинні та шахрайські дії, пов'язані з порушенням внутрішніх процедур (втрати внаслідок шахрайських дій, незаконного привласнення майна або навмисного порушення норм законодавства України та здійснених працівниками Товариства); - низький рівень задоволеності співробітників умовами праці; - порушення в процесах та продуктах Товариства, що можуть призвести до виникнення збитків/санкцій, додаткових втрат. 		застосування надійних програмно-апаратних засобів, резервування ліній зв'язку та програмно-апаратних засобів.
2	Комплаєнс-ризик	<ul style="list-style-type: none"> - порушення законодавства про платіжні послуги, фінансові послуги, міжнародних правил та стандартів, дія яких поширюється на Товариство; - порушення в сфері організації внутрішньої структури та/або процесу прийняття рішень, недоліки в сфері організації внутрішньої структури та процесу прийняття рішень (прийняття рішень не відповідним органом управління та /або з порушенням процедури щодо прийняття відповідного рішення), недоліки в сфері прийняття своєчасних та адекватних управлінських рішень щодо пом'якшення та / або мінімізації ризиків Товариства; - порушення обмежень в операціях з пов'язаними особами; - порушення антимонопольного законодавства; - порушення законодавства в сфері захисту персональних даних; - порушення вимог Національного банку України; - порушення вимог щодо своєчасності та достовірності подання звітності; 	низька	Своєчасне, точне та неухильне дотримання вимог законодавства України, ринкових стандартів та внутрішніх документів ФК. Постійний моніторинг поведінки працівників та запобігання випадкам конфлікту інтересів, неетичній чи недоброчесній поведінці. Внутрішній контроль та експертна оцінка рівня відповідності діяльності ФК вимогам законодавства, ринковим стандартам та внутрішнім документам ФК.

		<ul style="list-style-type: none"> - порушення вимог у сфері інформаційної безпеки та кіберзахисту; - порушення вимог щодо роботи з інформацією з обмеженим доступом; - недотримання принципів професійної поведінки (етики) керівниками та працівниками Товариства (порушення положень Кодексу поведінки), конфлікт інтересів (підлеглисть, отримання подарунків); - порушення вимог у сфері трудових відносин (порушення трудового законодавства, внутрішнього трудового розпорядку, тривалість робочого дня, суперечки з приводу заробітної плати, компенсації у разі звільнення, інші трудові спори); - порушення/невідповідність законодавству в інших сферах; 		
3	Ризик безпеки та кіберризик	<ul style="list-style-type: none"> - порушення систем захисту інформації, не забезпечення безпеки інформації з обмеженим доступом; - несанкціоноване втручання (доступ) третіх осіб до інформаційних систем та програмних комплексів Товариства; - не забезпечення належного рівня безпеки інформації з обмеженим доступом (витік інформації про користувачів платіжних послуг та ін.); - кібератаки, DDoS-атаки; - витік інформації, даних або несанкціонований доступ третіх осіб до інформаційних систем Товариства внаслідок недобросовісної/зловмисної поведінки працівників; - незабезпечення фізичного захисту центрів оброблення даних, дата-центрів, нездійснення резервного копіювання даних. 	низька	<p>Резервування всіх систем, наявність дзеркальних серверних потужностей, використання хмарних рішень, використання сертифікованих криптографічних та інших засобів системи захисту інформації, ведення трастових IP-адрес, правила доступу та регулювання прав доступу, логування доступу, система постійних навчань та перевірки знань, проходження на кварталній та щорічній основі віддалених пенетрейшн тестів та аудиту PCI DSS, щоденні звірки з іншими учасниками обміну даних, тощо.</p> <p>Організаційні заходи щодо можливого управління системами віддалено в т. ч. за межами України, забезпечення резервними потужностями електропостачання та доступу до мережі Інтернет.</p>

				<p>Побудова інфраструктури відкритої для подальшої її модернізації та розвитку з урахуванням вимог державних та міжнародних стандартів, організація і проведення постійного моніторингу (протоколювання) основних подій, що виникають у системі та аудиту системи та її складових для аналізу та оцінки її основних показників, використання сертифікованого та/або ліцензійного програмного забезпечення та основних програмно-апаратних засобів.</p>
4	Регуляторний ризик	<p>Регуляторний ризик не пов'язаний з конкретним типом операцій. Його генерують зміни у законодавстві та нормативних актах регулюючих органів. Передбачити усі фактори регуляторного ризику неможливо. Можливі приклади виникнення такого ризику (але не виключно) наступні:</p> <ul style="list-style-type: none"> - обмеження окремих видів діяльності на ринку платіжних послуг; - обмеження або встановлення додаткових зборів та платежів на ринку платіжних послуг; - обмеження/заборона окремих типів платіжних операцій/платіжних інструментів; - тиск на надавачів платіжних послуг, обов'язкове узгодження тих чи інших управлінських рішень з регулятором. 	середня	<p>Моніторинг змін законодавства на етапі законопроектів, активна участь в процесі ініціювання змін до регулювання платіжних послуг, вивчення європейського законодавства та практик, залучення зовнішніх консультантів та фахівців і експертів до моменту запровадження послуг та на етапі вирішення юридичних питань. Дотримання вимог законодавства та регулювання НБУ. Впровадження ефективного механізму вирішення спірних ситуацій.</p>
5	Ризик ліквідності	<p>- операції, що чинять вплив на статті балансу Товариства та/або позабалансу у визначених проміжках часу та призводять до збільшення невідповідності між активами та пасивами, розподіленими за датами очікуваного виконання розрахунків;</p>	низька	<p>Запровадження резервних відрахувань, часткове переведення резервів в валюти першої категорії, страхування співробітників, використання інструментів додаткового залучення коштів, в т. ч. кредитних. Залучення коштів з альтернативних джерел, контроль за ліквідністю,</p>

		<ul style="list-style-type: none"> - значне погіршення фінансових показників, пруденційних нормативів; - істотне скорочення частки на ринку, відтік користувачів платіжних послуг; - значні виплати внаслідок штрафів та негативних судових рішень; - значні обсяги сплати дивідендів та, як наслідок, обмеження можливості зростання капіталу Товариства за рахунок прибутку. 		<p>отримання передоплат, робота з простроченою заборгованістю, робота щодо отримання боргів від банків, що були виведені з ринку, реінвестиція прибутку за попередні періоди з боку акціонерів, партнерські проекти з банками. оптимізація структури капіталу (співвідношення між власними та позичковими джерелами формування фінансових ресурсів) та мінімізація боргових зобов'язань, що досягається шляхом диверсифікації кредиторів та мінімізацією платежів за користування позичковим капіталом.</p>
6	Кредитний ризик	<p>Кредитний ризик представляє собою елемент невизначеності при виконанні контрагентом (користувачем, надавачем платіжних послуг) своїх грошових зобов'язань за договором перед Товариством. До складу кредитного ризику входить (але не виключно):</p> <ul style="list-style-type: none"> - невиконання/несвоєчасне виконання контрагентом (користувачем, надавачем платіжних послуг) зобов'язань з оплати винагороди Товариства за надані платіжні послуги; - невиконання/несвоєчасне виконання контрагентом (користувачем, надавачем платіжних послуг) зобов'язань з повернення коштів за платіжною операцією, яку було визнано шахрайською (Chargeback), операцією за якою платнику не було надано товарів, робіт або послуг, або операцією, за якою платник відмовився від товарів, робіт або послуг; - невиконання/несвоєчасне виконання контрагентом (користувачем, надавачем платіжних послуг) зобов'язань 	низька	<p>Ідентифікація окремих видів фінансових ризиків здійснюється за трьома етапами:</p> <p>На першому етапі в розрізі окремих видів фінансових операцій визначаються властиві їм зовнішні чи систематичні види фінансових ризиків.</p> <p>На другому етапі визначається перелік внутрішніх або несистематичних фінансових ризиків, які властиві окремим видам фінансових операцій (ризик зниження фінансової стабільності, ризик неплатоспроможності, структурний ризик, кредитний ризик).</p> <p>На третьому етапі формується запропонований загальний портфель фінансових ризиків, що пов'язані з майбутньою фінансовою діяльністю.</p> <p>Аналіз виявлених ризиків передбачає виявлення джерел і причин їх виникнення, встановлення потенційних зон ризику,</p>

		з повернення коштів за неакцептованими, неналежними, помилковими операціями.		виявлення можливих вигод та негативних наслідків від реалізації ризикового рішення. Після ідентифікації ризику запроваджується захід мінімізації (отримання забезпечення, гарантії, передплати тощо) або усунення ризику (розірвання ділових відносин, робота за передплатою тощо). Запровадження обмеження обсягів розрахунків шляхом застосування відповідних лімітів щодо обмеження виконання фінансових операцій, в т. ч. для забезпечення виконання контрольних процедур протидії легалізації коштів, одержаних злочинним шляхом
7	Ринковий ризик	Ринковий ризик пов'язаний з невизначеністю коливань ринкової кон'юнктури - ціновими та курсовими ризиками, змінами ставок інтерчейндж та інших складових комісійної винагороди, ліквідністю і т.п. До складу ринкового ризику входить (але не виключно): - збільшення ставок міжбанківської комісійної винагороди (інтерчейндж), комісійної винагороди еквайрів та інших тарифів надавачів платіжних послуг; - монополізація ринку платіжних послуг одним гравцем; - зниження рівня конкурентоспроможності послуг, продуктів Товариства.	середня	Залучення споживачів платіжних послуг, які раніше не користувались онлайн платежами, пошук джерел доходів на інших ринках, розвиток платіжних рішень на інших ринках всередині країни, зменшення собівартості надання послуг. Ретельна перевірка фінансових показників та застосування поточного та/або періодичного моніторингу фінансового стану незалежно декількома підрозділами компанії. Розроблення та впровадження нових платіжних сервісів та послуг, проведення маркетингових заходів, направлених на розвиток бізнесу, поліпшення якості та доступності своїх послуг.

12.2. Крім перелічених ризиків, продовження широкомасштабної російської агресії проти України створює сприятливе підґрунтя для вчинення злочинів у сфері відмивання коштів/фінансування тероризму/фінансування розповсюдження зброї масового знищення (далі – ВК/ФТ/ФРЗМЗ або окремо – ВК, ФТ, ФРЗМЗ), інформаційної безпеки та кіберзахисту, санкційних обмежень. Держави, що здійснюють збройну агресію проти України, постійно створюють нові та удосконалюють поточні

схеми приховування активів, уникнення дії санкційних обмежень, постачання озброєння з третіх країн. Ключовим обов'язком ФК як суб'єкта первинного фінансового моніторингу є забезпечення функціонування належної системи управління ризиками, застосування у своїй діяльності ризик-орієнтовного підходу та вжиття належних заходів з метою мінімізації ризиків. В умовах війни такий обов'язок набуває особливого значення.

12.3. З метою належного застосування у своїй діяльності ризик-орієнтованого підходу відповідно до Закону України від 06.12.2019 № 361-IX «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» ФК щороку переглядає власний ризик-профіль та ризик-апетит.

12.4. ФК застосовує класичний спосіб диференціації ризиків, який передбачає наявність трьох рівнів: **низький, середній та високий** рівень ризику. Для побудови матриці ризиків ФК використовуються критерії впливу (**impact**) та ймовірності ризиків (**likelihood**):

Вплив		Ймовірність	
Рівень	Наслідки ризиків ВК/ФТ	Рівень	Ймовірність
Високий	Тяжкі наслідки ризику	Високий	Висока вірогідність наявності ризику ВК/ФТ/ФРЗМЗ
Середній	Середні наслідки ризику	Середній	Розумні підстави для припущення ризику ВК/ФТ/ФРЗМЗ
Низький	Незначні наслідки ризику / Відсутність будь-якого впливу	Низький	Низька вірогідність наявності ризику ВК/ФТ/ФРЗМЗ

12.5. Наслідки ризиків стосуються результатів, які виникають внаслідок настання ризикових подій. Наслідки можуть проявлятися як завдані збитки, втрати активів, підрив репутації ФК, втрата довіри клієнтів, втрати в доходах ФК. Узагальнено можна стверджувати, що процеси ВК і ФТ генерують два типи наслідків: перший – асоціюється безпосередньо із здійсненням операцій, пов'язаних із ВК та ФТ (наприклад, скоєння предикатних злочинів, залучення фінансових установ до відмивання, скоєння терористичних актів); другий – асоціюється з використанням активів після того, як вони були легалізовані (відмиті).

Факторами для оцінки ризик-профілю ФК є:

1. Характер та масштаб діяльності ФК;
2. Послуги, що надаються ФК;
3. Види клієнтів та їх ризик-профілі;
4. Географічне розташування Товариства та держави реєстрації клієнта ФК;
5. Канали/способи надання (отримання) послуг;
6. Інші значущі фактори.

12.6. ФК використовує систему оцінки ризику ВК/ФТ/ФРЗМЗ, яка характеризується поєднанням якісно-скорингових (бальних) показників. Вказана система фокусується на головних ризикових подіях, пов'язаних із процесом ВК/ФТ/ФРЗМЗ, які в свою чергу впливають на формування профілю ризику.

13. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ВИКОРИСТОВУЄТЬСЯ ПІД ЧАС НАДАННЯ ПЛАТІЖНИХ ПОСЛУГ (ВИКОНАННЯ ПЛАТІЖНИХ ОПЕРАЦІЙ)

13.1. Система захисту інформації, що використовується ФК під час виконання платіжних операцій, базується на вимогах міжнародного Стандарту безпеки даних індустрії платіжних карт (Payment Card Industry (PCI) Data Security Standard (DSS)). Стандарт PCI DSS представляє собою сукупність деталізованих вимог щодо забезпечення безпеки даних про держателів платіжних карток, які передаються, зберігаються і обробляються в інформаційній інфраструктурі ФК. Дані вимоги застосовуються до всіх компонентів системи, зокрема: мережевий пристрій, сервер або додаток, що входить до складу або підключений до середовища даних про держателів ЕПЗ.

13.2. Порядок захисту та використання засобів захисту інформації щодо платіжних операцій визначається законами України, нормативно-правовими актами Національного банку України та правилами ПС. В ФК розроблені та впроваджені Політика інформаційної безпеки, Концепція забезпечення інформаційної безпеки, Фізичний захист, а також інші внутрішні документи: Парольна політика; Політика управління доступом до ресурсів мережі ФК; Правила забезпечення інформаційної безпеки при роботі користувачів в мережі ФК та інші.

13.3. При виконанні платіжних операцій ФК здійснює в межах своїх повноважень захист відповідної інформації від:

13.3.1. несанкціонованого доступу до інформації – доступу до інформації про платіжну операцію, що є банківською таємницею або конфіденційною інформацією, осіб, які не мають на це прав або повноважень;

13.3.2. несанкціонованих змін інформації – внесення змін або часткового чи повного знищення інформації щодо платіжних операцій особами, які не мають на це права або повноважень;

13.3.3. несанкціонованих операцій з компонентами інформаційної системи ФК – використання або внесення змін до компонентів інформаційної системи протягом її функціонування особами, які не мають на це права або повноважень.

13.4. Система захисту інформації забезпечує:

- цілісність інформації, що передається в інформаційну систему та компонентів інформаційної системи;

- конфіденційність інформації під час її обробки, передавання та зберігання;

- забезпечення постійного та безперешкодного доступу до компонентів інформаційної системи ФК особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором.

13.5. Система захисту інформації базується на таких принципах:

13.5.1. чіткий розподіл прав доступу до інформаційних систем між співробітниками ФК, а також персоніфікація здійснення операцій і їх протоколювання;

13.5.2. автоматичне ведення захищених журналів, що містять логи (записи) використання компонентів системи, процесингу та виконання платіжних і деяких службових операцій;

13.5.3. сертифікація;

13.5.4. шифрування даних і обчислювання хеш-функцій, аудит операцій, що здійснюється в інформаційних системах ФК;

13.5.5. засоби діагностики та самодіагностики, що дають змогу визначити порушення цілісності баз даних і програмного забезпечення, відсутність та спроби повторення операцій, спроби несанкціонованого доступу до компонентів системи;

13.5.6. захищені засоби резервного копіювання системних компонентів, операційних даних та визначених критичних компонентів у відповідності із затвердженого політикою та процедурами резервного копіювання та забезпечення безперебійної роботи та/або відновлення роботи ФК.

13.6. Комплекс заходів по захисту інформації в ФК включає в себе наступне:

- призначення ролей і розподіл відповідальності;
- розробка, реалізація, впровадження та контроль виконання планів заходів, політик безпеки та інших документів щодо забезпечення інформаційної безпеки;
- підготовка користувачів і технічних фахівців до вирішення проблем, пов'язаних із забезпеченням інформаційної безпеки;
- проектування, розгортання і вдосконалення технічної інфраструктури інформаційної безпеки;
- аудит інформаційної безпеки.

13.7. Технічна інфраструктура інформаційної безпеки ФК вирішує наступні завдання:

13.7.1. Захист зовнішнього периметра мережі ФК від загроз з боку зовнішніх мереж за рахунок використання міжмережевого екранування, контролю віддаленого доступу та моніторингу інформаційних взаємодій. Використовується апаратно-програмний комплекс захисту інформації Fortinet FortiGate 300, що був неодноразово протестований та отримав підтвердження найкращої продуктивності та ефективності захисту, що засвідчується відповідними сертифікатами NSS Labs, ICSA, Virus Bulletin та AV Comparatives і відповідає вимогам міжнародного стандарту якості ISO-9001:2000 та українського стандарту ДСТУ ISO 9001-2001.

13.7.2. ФК забезпечує підтримку конфігурацій міжмережевих екранів для захисту даних про держателів ЕПЗ. Розроблені стандарти конфігурації міжмережевих екранів, які включають в себе:

- формальний процес затвердження та тестування всіх зовнішніх з'єднань і змін в конфігурації брандмауера;
- актуальну схему мережі із зазначенням всіх каналів доступу до даних про держателів ЕПЗ;
- вимоги до міжмережевих екранів для кожного Інтернет-з'єднання і кожного з'єднання між демілітаризованою зоною (DMZ) і внутрішньою мережею ФК;
- опис груп, ролей і відповідальності за керування мережевими пристроями;
- документований перелік сервісів і портів, необхідних для роботи бізнес-додатків;
- документування використання будь-якого небезпечного протоколу передачі даних (наприклад, FTP), яке включає в себе опис причини використання протоколу і застосовуваних при цьому засобів захисту;
- щоквартальний перегляд налаштувань міжмережевих екранів і маршрутизаторів;
- стандарти конфігурації для маршрутизаторів.

13.7.3. Створена конфігурація міжмережевих екранів, яка забороняє будь-які з'єднання, які виходять від недовірих мереж і вузлів, за винятком протоколів, необхідних для середовища даних про держателів ЕПЗ.

13.7.4. Створена конфігурація міжмережевих екранів, що обмежує з'єднання між загальнодоступними серверами і будь-яким компонентом системи, що зберігають дані про держателів ЕПЗ. Ця конфігурація включає наступне:

- обмеження вхідного трафіку на IP- адреси, розташовані в DMZ (вхідні фільтри);
- заборона на з'єднання з внутрішніх адрес з Інтернету до адрес, розташованих в DMZ;
- включення динамічної пакетної фільтрації із запам'ятовуванням стану (дозвіл проходження пакетів тільки для встановлених з'єднань);
- розміщення баз даних у внутрішньому сегменті мережі, відокремленому від DMZ;
- обмеження вхідного і вихідного трафіку: дозволений тільки необхідний для середовища даних про держателів ЕПЗ;
- забезпечення безпеки і синхронізації файлів конфігурації маршрутизаторів. Так, файли поточної робочої конфігурації (для нормального функціонування маршрутизаторів) і файли ініціалізації (використовувані при перезавантаженні) містять однаково безпечну конфігурацію;
- заборона всього вхідного і вихідного трафіку, який явно не дозволений встановленими правилами;
- заборона на використання бездротової мережі;
- установку персональних міжмережевих екранів на всі мобільні і ті, що належать співробітникам комп'ютери, які мають доступ в Інтернет і використовуються для доступу до локальної мережі ФК.

13.7.5. Заборонено будь-який прямий доступ із зовнішнього середовища до будь-якого з компонентів системи, що містять дані про держателів ЕПЗ (баз даних, журналам протоколювання подій, файлів трасування). Використовується DMZ для фільтрації будь-якого трафіку і заборони прямих маршрутів для вхідного і вихідного Інтернет-трафіку. Будь-який вихідний трафік від додатків обробки ЕПЗ обмежений тільки IP-адресами, розташованими в DMZ.

13.7.6. Реалізований механізм трансляції IP-адрес для запобігання розкриття внутрішніх адрес. Для цього використовуються такі технології, як PAT і NAT.

13.7.7. Захист корпоративних серверів за рахунок використання механізмів управління доступом до серверів баз даних, файловим, інформаційним і поштових серверів, реєстрації та обліку подій, пов'язаних із здійсненням доступу до ресурсів корпоративних серверів, механізмів моніторингу та аудиту безпеки.

13.7.8. Розроблені стандарти конфігурації для всіх системних компонентів, з метою врахування відомих проблем безпеки, а також положення загальноприйнятих галузевих стандартів (SANS, NIST, CIS).

13.7.9. Кожен сервер має одну основну функцію (веб-сервер, сервер баз даних і сервер DNS встановлені на різних віртуальних серверах).

13.7.10. Відключені всі сервіси та протоколи, використання яких не потрібно для виконання пристроєм своєї основної функції. З системи вилучена вся непотрібна функціональність: сценарії, драйвери тощо, непотрібні для роботи відповідних сервісів.

13.7.11. Комплексний антивірусний захист систем за такими рівнями: 1) захист зовнішнього шлюзу в мережу Інтернет; 2) захист серверів; 3) захист робочих місць користувачів.

Антивірусні механізми підтримуються в актуальному стані, мають централізовані сервери оновлень, постійно увімкнені та ведуться журнали протоколювання подій.

13.7.12. Моніторинг мережевого трафіку в реальному часі з метою виявлення підозрілих дій користувачів мережі і спроб здійснення несанкціонованого доступу до ресурсів корпоративної мережі з боку зовнішніх зловмисників.

13.7.13. Захист прикладних підсистем, що функціонують, забезпечення доступності наданих ними прикладних сервісів.

13.7.14. На всі системні компоненти та програмне забезпечення встановлені найсвіжіші оновлення безпеки.

13.7.15. Впроваджено процес визначення знову виявлених вразливостей безпеки та оновлення стандартів конфігурації системних компонентів;

13.7.16. Застосунки та додатки розробляються з урахуванням вимог інформаційної безпеки протягом усього циклу розробки:

- всі оновлення безпеки та зміни в конфігурації тестуються перед впровадженням;
- середовища розробки, тестування та виробничого функціонування програмного забезпечення відокремлені один від одного;
- обов'язки з розробки, тестування і виробничого функціонування програмного забезпечення відокремлені один від одного;
- виробничі дані (наприклад, чинні дані ЕПЗ) не використовуються для тестування і розробки;
- всі тестові дані і платіжні рахунки вилучаються із системи перед переведенням її у виробничий режим;
- всі індивідуальні облікові записи, імена користувачів і паролі видаляються перед передачею програмного забезпечення замовникам або переведенням його у виробничий режим;
- програмний код застосунків досліджується на наявність потенційних вразливостей перед передачею готових застосунків замовникам або переведенням їх у виробничий режим.

13.7.17. Розроблені та впроваджені процедури управління змінами, які включають в себе: 1) документування впливу зміни на систему; 2) погодження зміни з керівництвом; 3) тестування виробничої функціональності; 4) процедуру скасування зміни.

13.7.18. Розробка веб-додатків проходить відповідно до посібників з безпечного програмування. Програмний код додатків досліджується на наявність потенційних вразливостей, зокрема таких:

- відсутність перевірки вхідних даних;
- обхід системи контролю доступу;
- обхід системи автентифікації і управління сесіями;
- атаки типу XSS;
- переповнення буфера;
- ін'єкції (наприклад, SQL-ін'єкції);
- некоректна обробка помилок;
- небезпечне зберігання даних;
- відмова в обслуговуванні;
- небезпечне управління конфігурацією.

13.8. Заходи забезпечення інформаційної безпеки організаційного рівня:

13.8.1. Організаційні заходи полягають в заходах адміністративного рівня і процедурних заходах захисту інформації.

Основою заходів адміністративного рівня, тобто заходів, що вживаються керівництвом ФК, є політика інформаційної безпеки. Під політикою інформаційної безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації.

13.8.2. Політика інформаційної безпеки ФК визначається нормативними та організаційно-розпорядчими документами, до числа яких належать такі:

- Політика паролів;
- Політика управління доступом до ресурсів мережі;
- Правила забезпечення інформаційної безпеки при роботі користувачів в мережі;
- Політика забезпечення інформаційної безпеки при взаємодії з мережею Інтернет;

- Політика резервного копіювання і відновлення даних;
- Регламенти роботи служб адміністрування мережі;
- План забезпечення безперервності бізнесу;
- Процедура реагування на інциденти, пов'язані з порушенням інформаційної безпеки;
- Конфіденційність та Перелік конфіденційних відомостей;
- Інші організаційно-розпорядчі документи.

13.8.3. Планування відновлювальних робіт дозволяє підготуватися до аварій, зменшити шкоду від них і зберегти здатність до функціонування.

13.8.4. Програма безпеки ФК передбачає набір оперативних заходів, спрямованих на виявлення і нейтралізацію порушень режиму безпеки. В ній передбачена та спланована заздалегідь послідовність дій кожного відповідального співробітника, оскільки заходи передбачають прийняття невідкладних та скоординованих рішень. Реакція на порушення режиму безпеки переслідує дві головні цілі:

- блокування порушника і зменшення завданої ним шкоди;
- недопущення повторних порушень.

13.9. Заходи забезпечення інформаційної безпеки програмно-технічного рівня:

13.9.1. Програмно-технічні засоби захисту розташовуються на наступних кордонах:

- захист зовнішнього периметру корпоративної мережі;
- захист внутрішніх мережевих сервісів і інформаційних обмінів;
- захист серверів і робочих станцій;
- захист системних ресурсів і локальних застосунків на серверах і робочих станціях.

13.9.2. На програмно-технічному рівні виконання захисних функцій в інформаційній системі здійснюється наступними сервісами безпеки:

- ідентифікація/автентифікація;
- розмежування доступу;
- протоколювання/аудит;
- екранування;
- тунелювання;
- шифрування;
- контроль цілісності;
- контроль захищеності;
- управління.

13.10. Критична інформація (дані про держателів ЕПЗ) передається через відкриті загальнодоступні мережі тільки в зашифрованому вигляді.

13.10.1. Для захисту критичних даних про держателів ЕПЗ під час передачі їх через загальнодоступні мережі в ПК використовуються стійкі криптографічні алгоритми та протоколи, такі як TLS і IPSEC. До загальнодоступних мереж відноситься Інтернет.

13.10.2. Незашифровані дані ЕПЗ не пересилається по електронній пошті.

13.11. Обов'язковими є регулярні перевірки систем і процесів забезпечення безпеки та захисту інформації.

13.11.1. Заходи забезпечення безпеки і мережеві з'єднання щорічно тестуються на їх здатність виявляти спроби несанкціонованого доступу і протистояти їм.

13.11.2. Сторонньою сертифікованою компанією проводиться зовнішнє і внутрішнє сканування мережі на наявність вразливостей не рідше одного разу на квартал, а також після внесення значних змін.

13.11.3. Проводиться тест на проникнення не рідше одного разу на рік, а також після будь-якої значимої зміни або оновлення інфраструктури та програм. Ці тести на проникнення включають:

- тести на проникнення мережевого рівня;
- тести на проникнення рівня додатків.

13.11.4. Використовуються системи виявлення вторгнень на рівні вузла і на рівні мережі, а також системи попередження вторгнень для контролю всього мережевого трафіку і оповіщення персоналу про підозрілі дії.

13.11.5. Використовуються додатки контролю цілісності файлів для оповіщення персоналу про несанкціоновані зміни критичних системних файлів і файлів даних. Перевірка цілісності критичних файлів проводиться не рідше одного разу на тиждень.

13.12. Заходи забезпечення інформаційної безпеки процедурного рівня.

13.12.1. Виділяються наступні групи процедурних заходів, спрямованих на забезпечення інформаційної безпеки:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

13.12.2. В ФК на процедурному рівні обмежено доступ до даних про держателів ЕПЗ тільки службовою необхідністю.

13.12.2.1. Доступом до обчислювальних ресурсів та інформації про держателів ЕПЗ володіють тільки ті співробітники, яким такий доступ необхідний відповідно до їх посадових обов'язків.

13.12.2.2. Для багатокористувацьких систем встановлюється механізм розмежування доступу, заснований на факторі знання, і застосовує принцип «заборонено все, що явно не дозволено».

13.12.3. Носії з резервними копіями даних зберігаються в безпечних місцях – центрах обробки даних або в компаніях, що забезпечують їх безпечно зберігання

13.13. Опис системи захисту інформації, що використовується під час виконання платіжних операцій.

13.13.1. Під час обміну інформацією з учасниками ПС застосовується система захисту інформації, що визначена правилами відповідної ПС та описується у договорах з еквайрами.

13.13.2. На зовнішньому кордоні мережі ФК розташовуються засоби виявлення зловмисної активності та контролю захищеності від лідера галузі захисту інтернет ресурсів Cloudflare. Далі йдуть міжмережеві екрани, що захищають зовнішні підключення. Вони, разом із засобами підтримки віртуальних приватних мереж, що об'єднуються з міжмережевими екранами, утворюють периметр безпеки, що відокремлює від зовнішнього світу.

13.13.3. Сервіс активного аудиту (як і управління) присутній у всіх критично важливих компонентах і, зокрема, в захисних. Це дозволяє швидко виявити атаку, навіть якщо з якихось причин вона виявиться успішною.

13.13.4. Управління доступом присутнє на всіх сервісах, функціонально корисних і інфраструктурних. Перед доступом здійснюється ідентифікація і автентифікація суб'єктів доступу (користувачів і процесів).

13.13.5. Засоби шифрування і контролю цілісності інформації, що передається по каналах зв'язку, винесено на спеціалізовані сервіси захисту інформації та з використанням спеціалізованого програмного забезпечення – система криптографічного захисту «ІТ Користувач ЦСК-1», де їм забезпечується кваліфіковане адміністрування.

13.13.6. Останній кордон утворюють засоби пасивного аудиту, що допомагають оцінити наслідки порушення безпеки, знайти винного, з'ясувати, чому успіх атаки став можливим.

13.14. Робота системи захисту інформації, яка реалізована у мережі ФК по обробці операції ініційованої Платником за допомогою ЕПЗ, може бути поділена на такі елементи:

13.14.1. Запит від зовнішнього Платника направляється через Платіжний пристрій, в т. ч. Сайт/Мобільний застосунок ФК/Отримувача. Доступ відбувається зашифрованим протоколом TLS версії не нижче 1.2 та ідентичність якого затверджена сертифікатом виданим міжнародним центром сертифікації Sectigo www.sectigo.com. Доступ до Платіжних пристроїв визначається Банками, яким належать такі Платіжні пристрої.

13.14.2. Передані дані Платника обробляються серверами обробки інформації. Інформаційні потоки захищені системою криптографічного захисту АТ «ІТ» «ІТ Користувач ЦСК-1».

13.14.3. Далі запит направляється до еквайра. Інформаційні потоки захищені відповідно до вимог еквайрів.

13.14.4. Відповідь Платнику відправляється в зворотному напрямку на екрані Сайту/Мобільного застосунку ФК або Платіжного пристрою Банку.

13.15. На зовнішніх та внутрішніх каналах зв'язку та під час обміну даними з іншими учасниками ПС, ФК дотримується індивідуальних процедур та правил взаємодії, що вимагаються, зокрема, еквайрами, процесинговими центрами та Отримувачами в рамках правил ПС.

13.15.1. ФК самостійно визначає порядок забезпечення захисту інформації з урахуванням національних вимог до забезпечення захисту інформації під час виконання платіжних операцій, а також вимог правил ПС та міжнародних стандартів інформаційної безпеки PCI DSS, зокрема:

- склад та порядок застосування організаційних заходів захисту інформації;
- склад та порядок використання технічних засобів захисту інформації, включаючи інформацію про конфігурацію технічних засобів захисту інформації, що визначає параметри їх роботи;
- порядок реєстрації та зберігання інформації на паперових носіях або в електронному вигляді, яка містить підтвердження виконання порядку застосування організаційних заходів захисту інформації та використання технічних засобів захисту інформації.

13.15.2. Для проведення робіт по забезпеченню захисту інформації ФК може залучати організації, що мають ліцензії на діяльність з технічного захисту конфіденційної інформації та (або) на діяльність з розробки та виробництва засобів захисту конфіденційної інформації.

13.15.3. Захисту підлягає наступна інформація:

- інформація про платіжні повідомлення;
- інформація, необхідна для засвідчення права розпорядження платіжним інструментом, у тому числі:
 - вся інформація, що міститься на магнітній смужці, платіжній картці, мікропроцесорі або іншому ЕПЗ;
 - перевірочне значення (CVV2), що використовується для підтвердження ініціювання операції за відсутності платіжної картки.
- ключова інформація засобів криптографічного захисту інформації, що використовуються при здійсненні платіжної операції;
- інформація про конфігурацію, що визначає параметри роботи технічних засобів по захисту інформації;
- інформація обмеженого доступу, у тому числі персональні дані та інша інформація, що підлягає обов'язковому захисту відповідно до чинного законодавства України під час здійснення платіжної операції.

13.15.4. Будь-який учасник ПС негайно повідомляє про всі можливі або підтверджені випадки втрати, крадіжки або компрометації будь-яких матеріалів і записів, що містять дані про рахунки і операції.

13.15.5. Для належної ідентифікації суб'єктів неакцептованих, помилкових, неналежних, підозрілих платіжних операцій та вжиття заходів щодо запобігання або припинення зазначених переказів учасники ПС повідомляють інших учасників ПС про таких суб'єктів та перекази в обсягах, встановлених правилами ПС або договорами між ними.

13.16. Особливості криптографічного захисту інформації на внутрішніх каналах зв'язку та під час її зберігання.

13.16.1. Для криптографічного захисту інформації використовуються програмні, апаратно-програмні та апаратні засоби, призначені для криптографічного захисту інформації (далі – КЗІ), які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

13.16.2. Передача засобів КЗІ здійснюється до ФК на підставі ліцензійного договору та окремих ліцензій з АТ «ІТ». Зазначеними документами передбачено порядок установаження засобів КЗІ в користувачів та обслуговування цих засобів, забезпечення ключовими документами (ключовими даними), а також ужиття заходів щодо забезпечення режиму безпеки тощо. АТ «ІТ» зазначене в переліку суб'єктів господарювання, має ліцензію Держспецзв'язку України від 15.02.2017 р. на провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації (у тому числі і інформації, що становить державну таємницю)..

13.16.3. Кожний екземпляр засобу КЗІ береться на облік та ведеться журнал обліку КЗІ. Одиницею обліку кожного екземпляра засобу КЗІ є:

- для апаратних та апаратно-програмних засобів - конструктивно закінчений технічний засіб;
- для програмних засобів - компакт-диск (CDROM) тощо.

13.16.4. При застосуванні КЗІ використовуються наступні стандарти:

13.16.4.1. Кожна ланка інформаційних потоків захищена системою КЗІ АТ «ІТ» «ІТ Користувач ЦСК-1»

До складу «ІТ Користувач ЦСК-1» входять бібліотеки взаємодії та допоміжне програмне забезпечення. Бібліотеки взаємодії забезпечують взаємодію «ІТ Користувач ЦСК-1» та комплексу обробки та передачі інформації, в складі якого цей засіб використовується, завдяки підтримці стандартних криптографічних інтерфейсів Windows CryptoAPI, PKCS#11, Java Cryptography Architecture (JCA).

13.16.4.1.1. В бібліотеках «ІТ Користувач ЦСК-1» використовуються такі криптографічні алгоритми та протоколи:

- алгоритми шифрування за ДСТУ ГОСТ 28147:2009, ДСТУ 7624-2014 та TDEA і AES за ДСТУ ISO/IEC 18033-3:2015 в режимах, що визначені ДСТУ ISO/IEC 10116:2014;
- алгоритми електронного підпису (ЕП) за ДСТУ 4145-2002, RSA за PKCS#1 (IETF RFC 3447) та ECDSA за ДСТУ ISO/IEC 14888-3:2019;
- алгоритми гешування за ГОСТ 34.311-95, ДСТУ 7564-2014 та SHA (SHA-1 і SHA-2) за ДСТУ ISO/IEC 10118-3:2005;
- протоколи розподілу ключів за ДСТУ ISO/IEC 11770-3:2015 (пп. 11.1) та RSA за PKCS#1 (IETF RFC 3447).
- Протоколи розподілу ключових даних реалізуються згідно ДСТУ ISO/IEC 11770-3:2015 (пп. 11.1) та технічних специфікацій до технічних рекомендацій IETF RFC 5652, затверджених наказом Адміністрації Держспецзв'язку №687 від 27.10.2020 р., і за алгоритмом направленою шифрування RSA згідно PKCS#1 (IETF RFC 3447). Генерація ключових даних повинна здійснюватися згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку.

Протокол встановлення захищеного сеансу передачі даних реалізовано на основі протоколу взаємної автентифікації з двома проходками згідно ДСТУ ISO/IEC 9798-3 (п. 5.2.1) та включає:

- формування користувачем та передачу даних автентифікації (запиту) на сервер, при цьому користувач виконує наступні дії:
 - генерує випадкове число;
 - підписує випадкове число та власний сертифікат (за необхідності) власним особистим ключем ЕП;
 - передає сформовані дані автентифікації (запит) на сервер;
 - обробку запиту від користувача сервером, при цьому сервер виконує наступні дії:
 - отримує дані автентифікації від користувача;
 - здійснює пошук (за відсутності сертифіката у запиті) та перевірку чинності сертифіката користувача;
 - перевіряє ЕП на даних;
 - у разі успішної обробки отриманих даних автентифікації – генерує сеансові ключі шифрування та вектори початкової ініціалізації;
 - підписує отримане випадкове число та сеансові ключі з векторами початкової ініціалізації власним особистим ключем ЕП;
 - зашифровує сформовані дані разом з ЕП спрямовано на користувача;
 - передає підписані та зашифровані дані автентифікації (відповідь) користувачу;
- прийом та обробку відповіді користувача від сервера, при цьому користувач виконує наступні дії:
- отримує відправлені дані автентифікації (відповідь) від сервера;
 - здійснює пошук та перевірку чинності сертифіката сервера;
 - розшифровує дані автентифікації;
 - перевіряє ЕП на даних;
 - перевіряє відповідність випадкового числа у отриманих даних;
 - у разі успішної обробки отриманих даних автентифікації (відповіді) завершує роботу протоколу.

13.16.4.1.2. Бібліотеки «ІТ Користувач ЦСК-1» забезпечують виконання високорівневих функцій:

- формування та перевірка підпису криптографічного конверта;
- формування та розшифрування криптографічного конверта;
- перевірки сертифікатів та ланцюгів сертифікатів;

- використання списків відізнаних сертифікатів або протоколу інтерактивного визначення статусу сертифікатів для їх перевірки;
 - формування запиту та перевірка відповіді протоколу фіксації часу.
- 13.16.4.2. «ІТ Користувач ЦСК-1» використовується для формування та перевірки електронних підписів, захисту конфіденційної та відкритої інформації, збереження її цілісності та автентичності, з використанням електронних підписів. Отриманий за допомогою «ІТ Користувач ЦСК-1» електронний підпис додається до первісних даних та забезпечує цілісність, а також можливість ідентифікації підписанта;
- 13.16.4.3. Ключові документи, які використовуються для перевірки електронного підпису, зберігають один або декілька сертифікатів кваліфікованого надавача електронних довірчих послуг/центру сертифікації ключів (далі - ЦСК) і розміщуються на носіях ключових даних, файлах комп'ютерної системи або спеціалізованих сховищах сертифікатів.
- 13.16.4.4. Використання ключових документів:
- користувач має змогу згенерувати персональний ключ електронного підпису за допомогою сервісного або прикладного програмного забезпечення;
 - порядок використання персонального ключа електронного підпису викладено в окремій інструкції щодо відповідного КЗІ, про ознайомлення з якою користувач розписується;
 - сертифікати використовуються засобом КЗІ «ІТ Користувач ЦСК-1» автоматично. Сертифікати ЦСК не є конфіденційними, але забезпечується їх захист від навмисного пошкодження або несанкціонованої зміни. Сертифікати ЦСК не потребують знищення після закінчення строку їх дії;
 - у разі компрометації ключів ЦСК, відповідний сертифікат підлягає видаленню із сховища сертифікатів, або переноситься у список заблокованих сертифікатів;
 - під час переходу до використання нового персонального ключа відбувається автоматичне знищення поточного ключа;
 - перед встановленням на комп'ютерну систему користувача виконується перевірка цілісності засобу КЗІ «ІТ Користувач ЦСК-1»;
 - сертифікати ЦСК доставляються користувачеві способом, що унеможлиблює їх модифікацію.
- 13.16.4.5. Допоміжне програмне забезпечення включає драйвери апаратного забезпечення, утиліти контролю стану носія ключової інформації, утиліти адміністративного обслуговування, утиліти завантаження та виконує наступні функції:
- зміна кодів доступу до носіїв;
 - генерацію персонального ключа користувача та створення самопідписного сертифіката цього ключа;
 - підписання бінарного файлу;
 - перевірку підпису на бінарний файл на підставі зазначеного сертифіката.
- 13.16.4.6. Засіб електронного підпису «ІТ Користувач ЦСК-1» підтримує роботу з наступними операційними системами: Microsoft Windows Server, Linux, Mac OS.
- 13.16.4.7. Обов'язки осіб, відповідальних за забезпечення безпеки експлуатації засобів КЗІ:
- ініціалізація засобів КЗІ;
 - контроль за виконанням процедур введення в експлуатацію засобів КЗІ;
 - контроль за виконанням процедур знищення ключових даних засобів КЗІ;
 - проведення службового розслідування у разі виникнення позаштатних ситуацій під час ініціалізації засобів КЗІ, генерації або використання ключових даних;
 - видалення сертифікатів ЦСК у разі компрометації ключів ЦСК;
 - контроль за цілісністю операційного середовища.
- 13.16.4.8. Обов'язки користувачів засобів КЗІ:
- генерація ключових даних;
 - перехід на використання нових ключових даних;
 - знищення ключових даних;
 - використання засобу КЗІ виключно за призначенням;
 - зберігання значення кодів доступу до засобу КЗІ у таємниці;
 - зберігання значення кодів розблокування засобу КЗІ у таємниці;
 - періодична зміна, або в разі потреби, коду доступу до засобу КЗІ;
 - не допускання зберігання разом засобів КЗІ та кодів доступу до них;

- не допускання використання засобу КЗІ іншими особами, що не мають відповідних повноважень;
- якщо засіб КЗІ був загублений або є підозра стосовно компрометації персонального ключа, негайно сповістити відповідальну за безпеку особу;
- у разі виявлення порушення в роботі засобу КЗІ негайно сповістити відповідальну за безпеку особу.

13.16.4.9. Дії співробітників в умовах надзвичайних ситуацій, стихійного лиха та підозри компрометації ключів:

- за надзвичайних ситуацій засоби КЗІ можуть залишатись в місці звичайного використання за умови зберігання кодів доступу у таємниці;
- змінні носії персональних ключів підлягають від'єднанню від комп'ютерної системи;
- завершити роботу програмного забезпечення, що використовує носії персональних ключів, або від'єднати електроживлення комп'ютерної системи;
- інші дії викладені в окремих інструкціях до відповідних засобів КЗІ.

13.16.5. Система захисту журналів та засоби резервного копіювання захищені «ІТ Користувач ЦСК-1».

13.16.6. Процедура ідентифікації та автентифікації здійснюється на основі відкритих ключів, сертифікатів «ІТ Користувач ЦСК-1», що відповідає прийнятим в Україні стандартам, який повністю сумісний зі стандартом ANSI X.509v3.

13.16.7. ЦСК забезпечує реєстрацію звернень користувачів і підготовку даних для формування сертифікатів відкритих ключів, підтверджує їх дійсність, виконує їх обслуговування, генерує ключові пари. Він може видавати, припиняти і відновлювати дію, відкликати сертифікати, генерувати список відкликаних сертифікатів і публікувати сертифікати та списки відкликаних сертифікатів.

13.16.8. Порядок використання ЦСК в ФК:

13.16.8.1. Генерація ключів ЦСК, введення даних, необхідних для створення запиту на формування сертифіката відкритого ключа ЦСК, здійснюється адміністратором сертифікації у присутності начальника ЦСК та під контролем керівника ФК.

13.16.8.2. Відразу після генерації ключів ЦСК автоматично створюється (у електронному вигляді) запит на формування сертифіката відкритого ключа ЦСК, що містить дані (в тому числі, значення відкритого ключа ЦСК), підписані особистим ключем ЦСК, необхідні для формування сертифіката ЦСК.

13.16.8.3. В подальшому цей запит використовується при підготовці документів для сертифікації відкритого ключа ЦСК та його видачі. Згенероване значення особистого ключа ЦСК записується у зашифрованому вигляді.

13.16.8.4. Після формування запиту до серверу сертифікатів на пошук відповідного сертифікату, сервер сертифікатів здійснює пошук в своїй базі необхідного сертифікату і передає його в центр обробки.

13.16.8.5. Крипто бібліотека «ІТ Користувач ЦСК-1» центру обробки виконує перевірку приналежності сертифікату, розшифровує електронні документи, перевіряє відповідність електронного підпису електронного документа цьому сертифікату і повідомляє центру обробки про чинність або нечинність електронного підпису. Після цього центр обробки надає інформацію користувачам в розшифрованому вигляді з відміткою про чинність електронного підпису.

14. СТРОКИ ТА ПОРЯДОК ЗБЕРІГАННЯ ІНФОРМАЦІЇ ПРО ПЛАТІЖНІ ОПЕРАЦІЇ

14.1. ФК вживає заходи щодо забезпечення високого рівня захисту інформації системи. Правила (політики) інформаційної безпеки та їх реалізація ФК здійснюються у відповідності до правил ПС, чинного законодавства України та вимог, встановлених нормативно-правовими актами Національного банку України.

14.2. Головними об'єктами захисту інформації, що зберігається є:

14.2.1. платіжні операції;

14.2.2. платіжні інструкції та документи за операціями з використанням платіжних інструментів;

14.2.3. електронні підписи, паролі та системна інформація і дані, що використовуються у ФК (базі даних, довідники, архіви, інформація про клієнтів (користувачів платіжних послуг) та здійснені ними операції тощо).

14.3. Для ефективного зберігання інформації про платіжні операції в ФК здійснюються такі організаційні заходи:

14.3.1. проведення аналізу можливих загроз та втрат для системи, а також підготовка даних для прийняття рішень щодо нештатних ситуацій;

14.3.2. розроблення інструкцій та рекомендацій щодо забезпечення захисту інформації;

14.3.3. розроблення інструкцій щодо дій працівників зі збереження конфіденційної інформації під час виникнення стихійних лих;

14.3.4. організація навчання працівників та контроль за їх роботою;

14.3.5. керування розподілом прав доступу користувачів та працівників до інформаційних джерел, облік засобів доступу до них;

14.3.6. керування генерацією, обліком та поширенням ключової інформації;

14.3.7. регламентація порядку внесення змін до технологічної інфраструктури системи;

14.3.8. організація обліку, зберігання і знищення документів та носіїв з конфіденційною інформацією.

14.4. Для запобігання порушенням, що можуть загрожувати інформаційній безпеці системи, в ФК застосовуються такі програмно-технічні та організаційні заходи щодо зберігання інформації:

14.4.1. чіткий розподіл прав доступу до інформаційних джерел між працівниками, а також персоніфікація здійснення операцій і їх протоколювання;

14.4.2. розвинута ключова система, що дає змогу контролювати транзакції та запити двома незалежними шляхами;

14.4.3. апаратно-програмні комплекси, що здійснюють криптографічний захист: комплекс захисту інформації Fortinet FortiGate 300 та програмне забезпечення «ІТ Користувач ЦСК-1»;

14.4.4. автоматичне ведення захищених журналів, що містять записи використання компонентів системи, процесингу та виконання платіжних і деяких службових операцій;

14.4.5. засоби діагностики та самодіагностики, що дають змогу визначати порушення цілісності баз даних і програмного забезпечення, відсутність та спроби повторення транзакцій, спроби несанкціонованого доступу до компонентів системи;

14.4.6. захищені засоби резервного копіювання системи, даних та визначених критичних компонентів у відповідності до затвердженої політики та процедури резервного копіювання та забезпечення безперебійної роботи ФК.

14.5. Порядок зберігання архівів документів та даних про проведені платіжні операції. Інформація про проведені платіжні операції, як і будь-яка інформація та/або електронні документи, що супроводжують процес переказу коштів від його ініціювання до перерахування на рахунок Отримувача, підлягає обов'язковій реєстрації в архіві даних на сервері резервування ФК.

14.6. Заходи, що виконуються в ФК для належного зберігання інформації про здійснені платіжні операції:

14.6.1. архітектура програмного забезпечення і апаратна реалізація забезпечують довгострокове зберігання всієї отриманої інформації та виключають несанкціонований доступ до неї, будь-яку її зміну чи перетворення;

14.6.2. сервери ФК розміщуються в окремому пристосованому для цього приміщенні;

14.6.3 в паперовій формі інформація про проведені платіжні операції зберігається не менше 5 (п'яти) років після завершення операції (при цьому строки зберігання документів можуть бути продовжені ФК відповідно до порядку, встановленого законодавством та внутрішніми документами ФК);

14.6.4. в електронному вигляді інформація про проведені платіжні операції зберігається постійно (не менше 10 років) в базах даних серверної системи ФК у вигляді, необхідному для її відтворення у разі необхідності;

14.6.5. за результатами операційного дня забезпечене щоденне створення резервних копій на резервних носіях (жорсткому диску) накопичених за операційний день електронних документів та інформації про проведені протягом операційного дня платіжні операції;

14.6.6. резервні копії електронних документів та інформації про платіжні операції зберігаються у порядку та протягом строків, які встановлені чинним законодавством України для відповідних груп документів у паперовій формі;

14.6.7. відповідальні працівники зобов'язані здійснювати перевірку цілісності та схоронності резервних копій електронних документів та інформації про платіжні операції щонайменше один раз на 6 місяців, у випадку необхідності поновлюючи зіпсовані резервні копії. Пошкоджені або зіпсовані

резервні копії підлягають окремому обліку та знищенню в межах строків зберігання електронних документів.

14.7. В ФК розроблена Політика збереження та поводження з даними.

14.7.1. Кількість даних держателів ЕПЗ і терміни їх зберігання обмежені тільки для виконання вимог бізнесу та регулюючих вимог до зберігання даних. В ФК вони зберігаються постійно (не менше 10 років).

14.7.2. Забороняється зберігати критичні автентифікаційні дані після авторизації (навіть у зашифрованому вигляді), зокрема елементи даних, що містять код CVC.

14.7.3. PAN (номер платіжної картки) підлягає маскуванню при його відображенні (максимально можлива кількість знаків PAN для відображення - перші 6 і останні 4 знаки).

14.7.4. З усіх даних про держателя ЕПЗ, як мінімум PAN надається у маскованому вигляді у всіх місцях зберігання. Для цього використовується будь-який з таких методів:

- стійка однонаправлена хеш-функція;
- укорочення (truncation);
- використання механізмів One-Time-Pad («одноразові блокноти») і використання та зберігання посилань на дані замість самих даних (index token);
- стійкі криптографічні алгоритми, спільно з процесами і процедурами управління ключами.

14.7.5. Забезпечується захист ключів шифрування даних про держателів ЕПЗ від їх компрометації або неправильного використання такими заходами:

- доступ до ключів шифрування дозволений тільки відповідальним за їх зберігання і використання співробітникам;
- ключі зберігаються в суворо визначених захищених сховищах і у суворо визначеному вигляді.

14.7.6. Задokumentовані всі процеси і процедури управління ключами шифрування даних про держателів ЕПЗ, у тому числі:

- генерація стійких ключів;
- безпечне поширення ключів;
- безпечне зберігання ключів;
- періодична зміна ключів здійснюється автоматично та не рідше одного разу на рік;
- знищення старих (прострочених) ключів;
- роздільне володіння частинами ключів (для розшифрування даних потрібний складний ключ, компоненти якого зберігаються у 2-х співробітників);
- захист від неавторизованої зміни ключа;
- заміна скомпрометованого ключа, а також імовірно скомпрометованого ключа;
- відкликання прострочених і недійсних ключів;
- визначення обов'язків і відповідальності співробітників щодо зберігання і використання ключів з письмовим підтвердженням їхньої згоди з ознайомленням і прийняттям таких обов'язків і відповідальності.

14.8. Безпека збереження даних про держателів ЕПЗ забезпечується шифруванням. Інші способи захисту збережених даних розглядаються як засоби зменшення ризику. Методи мінімізації ризику включають в себе: заборону зберігання даних про держателів ЕПЗ, крім випадків крайньої необхідності; зберігання укороченого PAN; уникнення пересилання PAN електронною поштою у відкритому вигляді.

14.9. ФК супроводжує платіжні операції необхідним обсягом інформації, при цьому інформація, одержана від Платника/еквайру/Банку зберігається в ФК не менше п'яти років після завершення операції.

14.10. В ФК забезпечена фізична безпека всіх паперових та електронних засобів (включаючи комп'ютери, електронні носії інформації, мережеве обладнання, лінії телекомунікацій, паперові звіти, чеки тощо), що містять дані про держателів ЕПЗ.

14.11. В ФК забезпечений суворий контроль над переміщенням носіїв інформації, які містять дані про держателів ЕПЗ, що включає:

- 14.11.1. класифікацію носіїв інформації, їх маркування, що містять конфіденційну інформацію;
- 14.11.2. пересилку носіїв тільки довіреним кур'єром або іншим способом, який може бути ретельно проконтрольований.

14.12. В ФК впроваджена процедура отримання дозволу від керівництва винесення за межі охоронюваної території носіїв, що містять дані про держателів ЕПЗ.

14.13. В ФК забезпечений суворий контроль за зберіганням носіїв, що містять дані про держателів ЕПЗ, і доступом до них:

14.13.1. носії, що містять дані про держателів ЕПЗ, інвентаризовано, а також забезпечена їх фізична безпека.

14.13.2. носії, що містять дані про держателів ЕПЗ, зберігання яких більше не потрібно для виконання бізнес-завдань або вимог законодавства, знищуються.

15. ПОРЯДОК ЗДІЙСНЕННЯ ВНУТРІШНЬОГО КОНТРОЛЮ

15.1. Для забезпечення належного контролю ФК за операціями визначено перелік операцій, що підлягають додатковому контролю, а також посади працівників, яким надане право виконувати контрольні функції. Детальний опис системи внутрішнього контролю ФК визначено у Положенні про внутрішній контроль ТОВ «ФК МБК».

15.2. Робочі місця відповідальних виконавців організовані таким чином, щоб сторонні особи не мали доступу до екранів програмно-апаратних засобів, ключової інформації, паролів, печаток, штампів, документів і бланків ФК.

15.3. Відповідальність за належну організацію системи внутрішнього контролю та її функціонування в процесі операційної діяльності ФК покладається на керівництво Товариства.

15.4. Система внутрішнього контролю ФК – це сукупність процедур, що спрямовані на попередження, виявлення і виправлення суттєвих помилок, а також забезпечення захисту і збереження активів, повноти і точності облікової документації. Внутрішній контроль є невід'ємною частиною операційної діяльності ФК та поєднувати адміністративний і бухгалтерський контроль за активами та пасивами ФК.

15.5. Внутрішній контроль включає попередній, первинний (поточний) і подальший контроль.

15.6. Будь-яка операція починається з попереднього контролю та передбачає перевірку:

- відповідності вимогам законодавства України;
- наявності відповідних дозволів і лімітів тощо.

15.7. Первинний (поточний) контроль у процесі проведення операцій забезпечується шляхом виконання встановлених процедур контролю за операціями ФК і передбачає візуальну перевірку правильності документів у паперовій формі та наявності підписів на них, а також перевірку наявності електронного підпису на електронних документах.

15.8. Зниження операційних ризиків під час введення даних в автоматизовані системи обліку забезпечується шляхом повторного введення відповідальним виконавцем обов'язкових реквізитів первинного документа.

15.9. Додатковий контроль запроваджується ФК самостійно залежно від операції і визначається відповідно до її виду і суми.

За операціями, що потребують додаткового контролю, записи в регістрах бухгалтерського обліку здійснюються лише після перевірки оформленого документа особою, на яку покладено функції контролера. У разі використання електронних документів додатковий контроль здійснюється лише після одержання позитивного результату перевірки електронного підпису, оформленого відповідальним виконавцем.

15.10. Подальший контроль здійснюється для забезпечення систематичної перевірки стану організації операційної діяльності ФК, правильності реєстрації, належного оформлення виконаних операцій, дотримання порядку звіряння аналітичного обліку та формування первинних документів.

15.11. Подальший контроль здійснюють працівники бек-офісу та/або інші служби відповідно до їх функціональних обов'язків, визначених внутрішніми документами ФК.

15.12. У процесі подальшого контролю слід з'ясувати причини порушення правил здійснення операцій та вживати заходів щодо їх усунення.

15.13. ФК застосовує такі процедури внутрішнього контролю:

15.13.1. з адміністративного контролю:

- організаційні процедури контролю;
- управлінські процедури контролю;
- розподіл функцій;

- фізичні заходи контролю (захист і збереження активів, матеріальних цінностей і облікових реєстрів).

15.13.2. з бухгалтерського контролю:

- облік операцій у повному обсязі;
- своєчасне звіряння;
- оцінка вартості.

15.14. Організаційні заходи адміністративного контролю передбачають таке:

- визначення короткострокових та довгострокових цілей ФК;
 - визначення організаційної структури ФК;
 - затвердження правил внутрішнього трудового розпорядку ФК та правил, що стосуються конфлікту інтересів;
 - розроблення процедур здійснення операцій;
 - відбір компетентних та надійних працівників, їх навчання, застосування системи заохочення тощо.
- Працівники, які залучені до укладання договорів, управління ризиками, контролю за ризиками, оброблення та обліку операцій, аналізу та фінансового контролю за операціями, а також особи, які заміщують їх, повинні мати необхідні знання, що відповідають кваліфікаційним вимогам.

15.15. Управлінські заходи адміністративного контролю мають забезпечувати таке:

- забезпечення своєчасного виконання платіжних операцій;
- забезпечення кваліфікованими кадрами, що здійснюють виконання платіжних операцій, та підвищення їх кваліфікації.

15.16. Заходи внутрішнього бухгалтерського контролю мають передбачати облік операцій у повному обсязі, а саме:

- усі операції мають обліковуватися відповідно до вимог законодавства України;
 - усі операції мають відображатися в балансі ФК в тому періоді, протягом якого вони були здійснені.
- Підтвердженням повного та своєчасного здійснення операції є документи, які свідчать про те, що ця операція була виконана та інформація про неї внесена в облікові реєстри. До письмових підтверджень належать і самі записи в облікових реєстрах.

15.17. Системи ведення бухгалтерського обліку в ФК забезпечують таке:

- зазначення детальної інформації про операцію;
- визначення її вартості та часу проведення;
- перевірка правильності відображення операцій, зокрема, забезпечення арифметичної точності записів, підбиття підсумків та перевірка і узгодження бухгалтерських записів, перевірка повідомлення про помилки і розбіжності.

15.18. Контроль за системою автоматизації обліку в процесі операційної діяльності ФК. Заходи контролю за системою автоматизації обліку мають передбачати перевірку:

- відповідності програмного забезпечення вимогам нормативно-правових актів Національного банку України;
- виконання вимог розробників програмних продуктів щодо технічного та технологічного забезпечення;
- виконання вимог щодо організації захисту інформації під час використання програмного забезпечення згідно з нормативно-правовими актами НБУ та вимогами розробників систем захисту інформації.

15.19. За допомогою програмно-технічних заходів забезпечується:

- хронологічне та систематичне відображення всіх операцій на аналітичних рахунках бухгалтерського обліку на підставі первинних документів;
- своєчасне та повне відображення всіх операцій ФК на балансі;
- дотримання правил складання і подання фінансової та статистичної звітності ФК;
- взаємозв'язок даних синтетичного та аналітичного обліку;
- накопичення та систематизація даних обліку в розрізі економічних показників, потрібних для складання звітності;
- автоматизований розрахунок економічних показників (нормативів), що визначені відповідними методиками НБУ;
- можливість оперативного аналізу фінансової діяльності ФК в розрізі структурних підрозділів;
- можливість нарощування функціональних характеристик програмного забезпечення, а також його адаптація в разі зміни законодавчої бази щодо обліку операцій.

15.20. ФК відслідковує та контролює будь-який доступ до мережевих ресурсів і даних про держателів ЕПЗ. Для цього розроблений процес розподілу доступу до компонентів системи між співробітниками.

15.21. Для кожного системного компонента включений механізм протоколювання таких подій:

- Будь-який доступ користувача до даних про держателів ЕПЗ;
- Будь-які дії, вчинені з використанням адміністративних повноважень;
- Будь-який доступ до записів про події в системі;
- Неуспішні спроби логічного доступу;
- Використання механізмів ідентифікації і автентифікації;
- Ініціалізація журналів протоколювання подій;
- Створення та видалення об'єктів системного рівня.

15.22. Для кожної події кожного системного компонента записуються наступні параметри:

- Ідентифікатор користувача;
- Тип події;
- Дата і час;
- Успішною чи неуспішною була подія;
- Джерело події;
- Ідентифікатор або назва даних, системного компонента або ресурсу, на які вплинула подія.

15.23. Журнали протоколювання подій захищені від змін. Впроваджено наступні заходи:

- 1) Доступом до журналів протоколювання подій володіють тільки ті співробітники, яким такий доступ необхідний відповідно до їх посадових обов'язків.
- 2) Журнали протоколювання подій захищені від неавторизованої зміни.
- 3) Резервні копії журналів протоколювання подій оперативно зберігаються на централізований сервер протоколювання або окремий носій, де їх зміна була б ускладнена.
- 4) Копії журналів протоколювання активності в бездротових мережах зберігаються на сервер протоколювання, що знаходиться всередині локальної мережі.
- 5) Використовуються додатки контролю цілісності файлів для захисту журналів протоколювання подій від несанкціонованих змін.
- 6) Журнали протоколювання подій переглядаються не рідше одного разу на день.
- 7) Журнали протоколювання подій зберігаються не менше одного року, а також в оперативному доступі не менше трьох місяців.

15.24. ФК дотримується правила призначення унікального ідентифікатора кожній особі, що має доступ до комп'ютерної мережі.

- 1) Кожному користувачеві призначено унікальне ім'я облікового запису для надання йому доступу до компонентів системи і даних про держателів ЕПЗ.
- 2) Крім ідентифікатора, застосовується один з наступних методів для автентифікації всіх користувачів:
 - Пароль;
 - Ключі (наприклад, SecureID, сертифікати, відкритий ключ).
- 3) Всі паролі зберігаються і передаються тільки в зашифрованому вигляді.
- 4) Встановлено контроль над виконанням процедур аутентифікації і управління паролями облікових записів співробітників та адміністраторів, що включає в себе:
 - Контроль над додаванням, видаленням і зміною ідентифікаторів, автентифікаційних даних і інших об'єктів ідентифікації.
 - Перевірку автентичності користувача перед зміною пароля.
 - Установку унікального початкового пароля для кожного користувача і його негайну зміну при першому вході користувача.
 - Негайне скасування доступу при звільненні користувача.
 - Видалення заблокованих облікових записів не рідше одного разу на 90 днів.
- 5) Доведення правил і процедур використання і зберігання пароля до всіх користувачів, що мають доступ до даних про держателів ЕПЗ.
- 6) Заборона використання групових, поділених і стандартних облікових записів і паролів.
- 7) Зміна пароля користувача не рідше одного разу на 90 днів.
- 8) Вимога використання в паролі не менше семи символів.
- 9) Вимога використання в паролі як цифр, так і букв.

10) Заборона при зміні пароля вибору в якості нового будь-якого з останніх чотирьох, що використовувалися даним користувачем паролів.

11) Блокування облікового запису після шести невдалих спроб введення пароля.

12) Установку періоду блокування облікового запису рівним 30 хвилинам або до розблокування облікового запису адміністратором.

13) Блокування робочої сесії користувача через 15 хвилин простою з вимогою введення пароля для розблокування.

14) Автентифікацію всіх варіантів доступу до будь-якої бази даних, яка містить дані про держателів ЕПЗ, у тому числі доступ з боку додатків, адміністраторів і будь-яких інших користувачів.

15.25. ФК запровадила правила інформаційної безпеки для співробітників і партнерів (політика інформаційної безпеки), що враховує вимоги стандарту PCI DSS.

1) Політика інформаційної безпеки описує щорічні процеси ідентифікації загроз, вразливостей і результатів їх реалізації, в рамках формальної оцінки ризиків;

2) Політика інформаційної безпеки переглядається у міру необхідності і оновлюється в разі зміни інфраструктури.

15.26. В ФК розроблені правила експлуатації для критичних пристроїв, з якими безпосередньо працюють співробітники (таких як модеми та бездротові мережі), щоб визначити коректний порядок використання цих пристроїв співробітниками. Такі правила включають наступне:

1) Процедуру явного схвалення керівництвом;

2) Автентифікацію перед використанням пристрою;

3) Перелік використовуваних пристроїв і співробітників, що мають доступ до таких пристроїв;

4) Маркування пристроїв, із зазначенням власника, контактної інформації та призначення;

5) Допустимі варіанти використання пристроїв;

6) Допустимі точки розміщення пристроїв в мережі;

7) Перелік схвалених ФК пристроїв;

8) Автоматичне відключення модемних сесій після певного періоду простою;

9) Включення модемів для доступу служби підтримки виробників, тільки у разі потреби такого доступу, з негайним вимиканням модемів після використання.

10) Заборона зберігання даних про держателів ЕПЗ на локальних дисках, дискетах та інших переносних носіях при віддаленому доступі до даних, а також заборону використання функцій копіювання-вставки даних і виведення даних на принтер під час сеансу віддаленого доступу.

15.27. Всім співробітникам ФК і всім відвідувачам забороняється використання мобільних пристроїв (ноутбуків, смартфонів, мобільних телефонів з картами пам'яті) з підключенням в корпоративну мережу.

16. ВІДПОВІДАЛЬНІСТЬ ПРАЦІВНИКІВ

16.1. Працівники ФК, до посадових обов'язків яких належить безпосередня робота з Платниками та/або Отримувачами щодо здійснення платіжних операцій з переказу коштів, несуть відповідальність, встановлену їх посадовими інструкціями відповідно до вимог трудового законодавства України чи адміністративну або кримінальну відповідальність відповідно до Кодексу України про адміністративні правопорушення та Кримінального кодексу України.

16.2. Працівники ФК виконуючи свої обов'язки щодо роботи з Платниками та Отримувачами при здійсненні платіжних операцій з переказу коштів, зобов'язані чітко виконувати обов'язки, що передбачені цими Правилами та узгоджувати свої дії з нормами чинного законодавства України.

16.3. За неналежне виконання своїх обов'язків працівники ФК, що беруть участь у безпосередньому забезпеченні виконання платіжних операцій з переказу коштів, несуть дисциплінарну відповідальність згідно з Кодексом законів України про працю за порушення трудової дисципліни.

17. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

17.1. Ці Правила набувають чинності з моменту їх затвердження вищим органом ФК – Загальними зборами учасників ТОВ «ФК МБК», з урахуванням наявної в ФК чинної ліцензії на надання фінансових платіжних послуг з переказу коштів без відкриття рахунків.

17.2. У разі потреби, в Правила можуть бути внесені зміни, які затверджуються вищим органом ФК.

17.3. Контроль за дотриманням та виконанням цих Правил покладається на Генерального директора ФК.

174.4. У разі невідповідності будь-якої частини цих Правил чинному законодавству України, у тому числі у зв'язку з прийняттям нових законодавчих актів, ці Правила діють лише в тій частині, що не суперечить законодавству України.

**Генеральний директор
ТОВ «ФК МБК»**

Володимир ХАЯН