

ЗАТВЕРДЖЕНО
Рішенням Правління АТ «КРЕДОБАНК»
№ 952 від «26» серпня 2026 року
Вводяться в дію «01» вересня 2026 року
Нова редакція!

APPROVED
by Resolution of the Management Board of
JSC «KREDOBANK»
No. 952 dated August 26, 2026
Effective from September 1, 2026
New version!

ПРАВИЛА КОРИСТУВАННЯ БАНКІВСЬКИМИ ПЛАТІЖНИМИ КАРТКАМИ
АТ «КРЕДОБАНК»

RULES FOR USE OF BANK PAYMENT CARDS OF
JSC «KREDOBANK»

1. Вступ Правила користування банківськими платіжними картками (надалі – Правила) визначають основні умови та вимоги безпеки під час користування банківськими платіжними картками, в тому числі корпоративними (бізнесовими) банківськими платіжними картками, емітованими АТ «КРЕДОБАНК». Дотримання цих Правил дасть змогу забезпечити держателям банківських платіжних карток надійне їх зберігання, нерозголошення реквізитів банківської платіжної картки, персонального ідентифікаційного номера та інших даних, а також зменшить можливі ризики під час здійснення операцій з використанням банківської платіжної картки в банкоматах або платіжних терміналах та інших операцій безготівкової оплати товарів і послуг, у тому числі через мережу Інтернет.	1. Introduction Rules for Use of Bank Payment Cards (hereinafter referred to as the Rules) set out the principal terms and security requirements applicable to the use of bank payment cards, including corporate (business) bank payment cards issued by JSC «KREDOBANK». Compliance with the Rules will enable Bank Payment Card Holders to ensure the secure safekeeping of their bank payment cards, maintain the confidentiality of Bank Payment Card details, Personal Identification Numbers (PINs) and other data, as well as mitigate potential risks when performing transactions using a Bank Payment Card at ATMs or payment terminals and other cashless payment transactions for goods and services, including transactions performed via the Internet.
2. Терміни та визначення 2.1 У Правилах наведені нижче терміни та визначення вживаються в такому значенні: Автентифікація - процедура підтвердження особи Клієнта (Держателя БПК) при зверненні останнього до Банку на телефон Контакт-центру, яка здійснюється шляхом звірки персональних даних Клієнта, включених до БПД, даним (відомостям), що повідомляються Клієнтом (Держателем БПК) особі, яка від імені Банку здійснює комунікацію з Клієнтом (Держателем БПК) по номеру телефону Контакт-центру. Автентифікація вважається успішною у випадку, якщо отримані в ході комунікації дані (відомості) від Клієнта (Держателя БПК) відповідають даним (відомостям) щодо Клієнта (Держателя БПК), наявним в БПД. Авторизація - процес отримання дозволу Процесингового центру Банку та/або відповідного	2. Terms and Definitions 2.1. The following terms and definitions used in the Rules shall have the meanings set out below: Authentication means a procedure for verifying the identity of the Client (BPC Holder) when the Client (BPC Holder) contacts the Bank by calling the Contact Centre telephone number. Authentication shall be performed by comparing the Client's personal data contained in the Personal Data Database (PDD) against the data (information) provided by the Client (BPC Holder) to the person who, acting on behalf of the Bank, communicates with the Client (BPC Holder) via the Contact Centre telephone number. Authentication shall be deemed successful if the data (information) obtained from the Client (BPC Holder) in the course of such communication corresponds to the data (information) concerning the Client (BPC Holder) available in the PDD. Authorisation means the process of obtaining permission from the Bank's Processing Centre and/or the relevant

учасника Платіжної системи на проведення операції з використанням БПК.

Банк – Акціонерне товариство «КРЕДОБАНК».

Банківська платіжна картка (БПК) - електронний платіжний засіб (вид платіжного інструменту) у вигляді емітованої в установленому Законодавством порядку пластикової чи іншого виду картки, який надає можливість Клієнтові (Держателю БПК) за його допомогою отримати інформацію про належні Клієнтові (Держателю БПК) кошти, які знаходяться на Поточному рахунку та ініціювати платіжні та інші операції, передбачені договором Клієнта і Банку.

Банкомат – спеціалізований електронний механізм для самообслуговування Держателя БПК за платіжними операціями, ініційованими БПК щодо одержання коштів у готівковій формі, одержання інформації щодо стану Поточного рахунку, а також виконання інших операцій згідно з функціональними можливостями цього механізму.

Блокування БПК – зміна статусу БПК, яка унеможливає здійснення платіжних операцій з використанням цієї БПК з проведенням Авторизації. Блокування БПК не перешкоджає здійсненню з використанням БПК тих платіжних операцій, які можуть проводитися без Авторизації. Блокування може бути постійним або тимчасовим. У випадку постійного Блокування БПК її використання в подальшому є неможливим. У випадку тимчасового Блокування є можливість зняття Держателем БПК Блокування БПК шляхом звернення в Контакт-центр.

Виписка – звіт/підтвердження руху коштів на Поточному рахунку за проведеними платіжними операціями, стан Поточного рахунку, який надається Банком на вимогу Клієнта.

Держатель БПК - фізична особа, яка на законних підставах використовує БПК для ініціювання платіжних операцій з відповідного Поточного рахунку в Банку або здійснює інші операції із застосуванням БПК.

Добовий авторизаційний ліміт – ліміт на здійснення операцій за допомогою БПК, встановлений Банком та/або Клієнтом (Держателем БПК) з метою уникнення фінансових втрат через несанкціоноване використання БПК.

Контакт-центр - структурний підрозділ Банку, що за допомогою телефонного зв'язку проводить процедуру Автентифікації Клієнта (Держателя БПК) та, у разі успішного проходження такої процедури, приймає звернення/дистанційні розпорядження Клієнта (Держателя БПК), розкриває Клієнтові (Держателю БПК) інформацію, передбачену умовами Правил надання комплексних банківських послуг фізичним особам у Акціонерному Товаристві «КРЕДОБАНК» та/або Правил надання комплексних банківських послуг юридичним особам та фізичним особам-підприємцям в АТ «КРЕДОБАНК» та здійснює інші комунікації з Клієнтом (Держателем БПК) з метою надання та/або у зв'язку із наданням Клієнту (Держателю БПК) банківських та/або інших

Payment System Participant to perform a transaction using a BPC.

Bank means Joint Stock Company «KREDOBANK».

Bank Payment Card (BPC) means an electronic payment instrument (a type of payment instrument) in the form of a plastic or other type of card issued in accordance with the procedure prescribed by the Legislation, which enables the Client (BPC Holder) to obtain information on the funds belonging to the Client (BPC Holder) and held in the Current Account, and to initiate payment and other transactions provided for by the agreement between the Client and the Bank.

ATM means a specialised electronic self-service device for the BPC Holder to perform BPC-initiated payment transactions involving cash withdrawal, obtain information on the status of the Current Account, and perform other transactions subject to the functionality of such device.

BPC Blocking means a change of the BPC status that makes it impossible to perform payment transactions using such BPC with BPC Authorisation. BPC Blocking does not prevent payment transactions using the BPC that may be performed without BPC Authorisation. Blocking may be permanent or temporary. In the event of permanent BPC Blocking, further use of the BPC shall be impossible. In the event of temporary BPC Blocking, the Holder may unblock the BPC by contacting the Contact Centre.

Statement means a report/confirmation of the movement of funds in the Current Account in respect of payment transactions performed and of the status of the Current Account, provided by the Bank at the Client's request.

BPC Holder means an individual who uses a BPC on legal grounds to initiate payment transactions from the relevant Current Account held with the Bank or performs other transactions using the BPC.

Daily Authorisation Limit means a limit on transactions performed using a BPC, established by the Bank and/or the Client (BPC Holder) to prevent financial losses resulting from the unauthorised use of the BPC.

Contact Centre means a structural unit of the Bank that, by means of telephone communication, performs the Authentication procedure in respect of the Client (BPC Holder) and, upon successful completion of such procedure, accepts requests/remote instructions from the Client (BPC Holder), discloses to the Client (BPC Holder) the information provided for by Terms and Conditions for Provision of Comprehensive Banking Services to Individuals at Joint Stock Company «KREDOBANK» and/or Terms and Conditions for Provision of Comprehensive Banking Services to Legal Entities and Sole Proprietors at JSC «KREDOBANK», and otherwise communicates with the Client (BPC Holder) for the purpose of providing and/or in connection with the provision to the Client (BPC Holder) of banking and/or other services stipulated by Terms and Conditions for Provision of

послуг, передбачених Правилами надання комплексних банківських послуг фізичним особам у Акціонерному Товаристві «КРЕДОБАНК» та/або Правил надання комплексних банківських послуг юридичним особам та фізичним особам-підприємцям в АТ «КРЕДОБАНК», у т. ч. з метою надання Клієнту (Держателю БПК) відомостей інформаційного/рекламного характеру. Звернення в Контакт-центр здійснюється за наступними номерами телефонів - 0 800 500 850 (безкоштовно по Україні) та + 38 032 297 6470 - з-за кордону.

Клієнт – фізична особа, суб'єкт господарювання (юридична особа або фізична особа-підприємець) тощо, на ім'я якої / якого відкрито Поточний рахунок, за яким здійснюються платіжні та/або інші операції з використанням БПК.

Платіжна система або МПС – міжнародні платіжні системи Visa incorporated (далі VISA), Mastercard International Incorporated тощо, членом яких є Банк, які здійснюють свою діяльність на території двох і більше країн та забезпечує проведення переказу коштів у межах цієї платіжної системи, у тому числі з однієї країни в іншу.

ПІН-код - набір цифр, відомий лише Клієнту (Держателю БПК) і потрібний для його Ідентифікації та Автентифікації під час здійснення платіжних та інших операцій із використанням електронного платіжного засобу.

Програмно-технічний комплекс самообслуговування (ПТКС) - технічний пристрій, що дає змогу Клієнту (Держателю БПК) ініціювати платіжну операцію готівкою, а також виконувати інші операції відповідно до функціональних можливостей цього пристрою;

Поточний рахунок – рахунок, що відкривається Банком Клієнту на договірній основі для зберігання коштів і виконання платіжних операцій, в тому числі за допомогою БПК.

Система – програмний комплекс, в тому числі Мобільний застосунок (система онлайн банкінгу «КРЕДОБАНК» або інший визначений Банком програмний комплекс), – який забезпечує можливість дистанційного обслуговування Клієнта Банком, шляхом надання Клієнту (Користувачу) послуг (на підставі електронних документів) через мережу Internet та/або корпоративну мережу Банку, а також забезпечує приймання-передачу іншої інформації через мережу Internet в електронній формі. Для цілей цих Правил Система не включає засіб дистанційного обслуговування «Клієнт-Інтернет-Банк («iFOBS»)

Фінансовий номер телефону - номер телефону (для послуг мобільного зв'язку) Клієнта – фізичної особи, в тому числі підприємця, або Держателя корпоративної (бізнесової) БПК), який за результатами проведеної Сторонами процедури верифікації Фінансового номеру телефону зареєстрований в БПД, як єдиний (крім випадків, визначених договором Клієнта і Банку) номер телефону відповідного Клієнта/Держателя БПК, за

Comprehensive Banking Services to Individuals at Joint Stock Company «KREDOBANK» and/or Terms and Conditions for Provision of Comprehensive Banking Services to Legal Entities and Sole Proprietors at JSC «KREDOBANK», including for the purpose of providing the Client (BPC Holder) with data of an informational/advertising nature. The Contact Centre may be contacted at the following telephone numbers: 0 800 500 850 (toll-free within Ukraine) and +38 032 297 6470 (for calls from abroad).

Client means an individual or an economic entity (a legal entity or a sole proprietor), etc., in whose name a Current Account has been opened and on which payment and/or other transactions are performed using a BPC.

Payment System or IPS means international payment systems such as Visa incorporated (hereinafter referred to as VISA), Mastercard International Incorporated, etc., operating in two or more countries, of which the Bank is a member, and which enable funds transfers within the relevant payment system, including from one country to another.

Personal Identification Number (PIN) means a set of digits known only to the Client (BPC Holder) and required to identify and authenticate the Client (BPC Holder) when performing payment and other transactions using an electronic payment instrument.

Self-service hardware-software complex (SHSC) means a technical device enabling the Client (BPC Holder) to initiate a cash payment transaction and perform other transactions subject to the functionality of such device.

Current Account means an account opened by the Bank for the Client on a contractual basis for the safekeeping of funds and the execution of Payment Transactions, including those performed using a BPC.

System means a software suite, including the Mobile Application (the «KREDOBANK» online banking system or another software suite designated by the Bank), which enables the Bank to provide remote services to the Client by rendering services to the Client (User), on the basis of electronic documents, via the Internet and/or the Bank's corporate network, and also enables the receipt and transmission of other information in electronic form via the Internet. For the purposes of these Rules, the System shall not include the Client-Internet-Bank («iFOBS») remote banking facility.

Financial Phone Number means the Subscriber Number (used for mobile communication services) by a Client who is an individual, including a sole proprietor, or by a Corporate BPC (Business Card) Holder, which, following completion by the Parties of the Financial Phone Number verification procedure, is registered in the Personal Data Databases (PDD) as the single Subscriber Number (except in cases specified by the agreement between the Client and the Bank) of the relevant Client/BPC Holder through which the Bank provides the

яким Банк надає Клієнту банківські та/або інші послуги, передбачені договором Клієнта і Банку, а також за яким здійснюються необхідні комунікації між Банком та Клієнтом з метою надання та/або у зв'язку із наданням Клієнту банківських та/або інших послуг, передбачених договором Клієнта і Банку, у т.ч. з метою надсилання Клієнту повідомлень інформаційного та/або рекламного характеру.

CVC2/CVV2 – це тризначний код для перевірки справжності Банківської платіжної картки при оплаті через Інтернет.

POS-термінал – електронний пристрій, що дозволяє зчитувати інформацію з магнітної смуги або чіпу БПК та/або із застосуванням технології бездротового високочастотного зв'язку малого радіусу дії (NFC) і здійснювати зв'язок з Банком для проведення Авторизації з метою здійснення платіжних та інших операцій ініційованих за допомогою БПК, визначених функціональними можливостями такого пристрою.

PUSH-повідомлення – повідомлення Банку інформаційного та/або рекламного характеру та повідомлення, що надсилаються з метою надання та/або у зв'язку із наданням Банком банківських та/або інших послуг передбачених договорами укладеними між Банком та Клієнтом, які відображаються як спливаюче вікно на екрані Мобільного пристрою Клієнта на якому встановлено Мобільний застосунок Система онлайн-банкінгу «КРЕДОБАНК».

Off-line операція - операція з використанням БПК, технологічна схема виконання якої не потребує під час виконання операції безперервного зв'язку в режимі реального часу з Банком та еквайром. Під час здійснення Off-line операцій використовується залишок коштів відповідного платіжного додатку БПК а Авторизація операції проводиться POS-терміналом/ Банкоматом, на якому виконується ця операція з використанням модуля безпеки терміналу.

3D Secure - технологія, розроблена МПІС MasterCard Worldwide (MasterCard SecureCode) для забезпечення Клієнту (Держателю БПК) максимально високого рівня захисту операцій, які здійснюються у мережі Інтернет з використанням БПК та мінімізації рівня шахрайства за такими операціями. Ця технологія передбачає перевірку здійснення операції з використанням БПК у мережі Інтернет, в т.ч. засобами інтернет-банкінгу, Держателем БПК шляхом надсилання одноразового пароля на Мобільний пристрій Держателя БПК, використання якого (одноразового пароля) є необхідним для підтвердження Держателем БПК здійснення такої операції.

2.2. Інші терміни, які використовуються в Правилах, вживаються в значеннях, визначених у Правилах надання комплексних банківських послуг фізичним особам у Акціонерному Товаристві «КРЕДОБАНК» та/або Правилах надання комплексних банківських послуг юридичним особам та фізичним особам-підприємцям в АТ «КРЕДОБАНК». Терміни,

Client with banking and/or other services stipulated by the agreement between the Client and the Bank and through which necessary communications between the Bank and the Client are carried out for the purpose of and/or in connection with the provision of banking and/or other services to the Client under the agreement between the Client and the Bank, including the sending of informational and/or advertising messages to the Client.

CVC2/CVV2 means a three-digit code used to verify the authenticity of a Bank Payment Card when making payments over the Internet.

POS Terminal means an electronic device capable of reading information from the magnetic stripe or chip of a BPC and/or using Near-Field Communication (NFC) technology and communicating with the Bank to obtain BPC Authorisation for the purpose of performing payment and other transactions initiated using the BPC, subject to the functionality of such device.

Push Notification means an informational and/or advertising notification from the Bank, as well as a notification sent for the purpose of and/or in connection with the provision by the Bank of banking and/or other services stipulated by the agreements entered into between the Bank and the Client, which is displayed as a pop-up window on the screen of the Client's Mobile Device on which the «KREDOBANK» Online Banking System Mobile Application is installed.

Off-line Transaction means a transaction performed using a BPC, the technological processing scheme of which does not require a continuous real-time connection with the Bank and the acquirer while the transaction is being performed. When an Off-line Transaction is performed, the available balance of the relevant BPC payment application is used, and the Transaction is Authorised by the POS Terminal/ATM at which such Transaction is performed, using the terminal's security module.

3D Secure means a technology developed by the MasterCard Worldwide International Payment System (**MasterCard SecureCode**) to ensure the highest possible level of protection for the Client (BPC Holder) in respect of Transactions performed online using a BPC and to minimise the risk of fraud in connection with such Transactions. This technology provides for verification that a Transaction using a BPC online, including through online banking facilities, is performed by the BPC Holder by sending a one-time password to the BPC Holder's Mobile Device. The BPC Holder must use such one-time password to confirm the performance of the relevant Transaction.

2.2. Other terms used in the Rules shall have the meanings assigned to them in Terms and Conditions for Provision of Comprehensive Banking Services to Individuals at JSC «KREDOBANK» and/or Terms and Conditions for Provision of Comprehensive Banking Services to Legal Entities and Sole Proprietors at JSC «KREDOBANK». Terms not defined in the Rules, Terms and Conditions for Provision of Comprehensive

значення яких не визначено у Правилах, Правилах надання комплексних банківських послуг фізичним особам у Акціонерному Товаристві «КРЕДОБАНК та/або Правилах надання комплексних банківських послуг юридичним особам та фізичним особам-підприємцям в АТ «КРЕДОБАНК», вживаються у значеннях, визначених законами України та нормативно-правовими актами Національного банку.	Banking Services to Individuals at JSC «KREDOBANK» and/or Terms and Conditions for Provision of Comprehensive Banking Services to Legal Entities and Sole Proprietors at JSC «KREDOBANK» shall have the meanings assigned to them by the laws of Ukraine and regulations of the National Bank of Ukraine.
3. Правила отримання БПК та ПІН-коду, активації БПК 3.1. Під час отримання БПК рекомендуємо Вам (тут і далі звертання «Ви» у відповідних відмінках застосовується до Держателя БПК, в тому числі такого, який є Клієнтом) поставити підпис на її зворотному боці в місці, яке призначене для підпису Держателя БПК. Це зменшить ризик незаконного використання БПК. 3.2. Запишіть номер своєї БПК та номери телефонів Контакт-центру. У випадку втрати БПК, Вам слід негайно повідомити Банк за цими номерами. 3.3. Для встановлення та отримання ПІН-коду Вам необхідно надіслати СМС-запит на номер: +380931777744 - для абонентів усіх мобільних операторів України. Формат СМС - запиту наступний: 2+****, де **** – останні 4 цифри картки Держателя, для якої необхідно встановити та отримати ПІН-код 3.4. Вам слід врахувати наступне: СМС – повідомлення слід відправляти з Фінансового номеру телефону або іншого номеру мобільного телефону, який Ви вказали при оформленні БПК та /або підключенні Послуги Мобінформ (СМС-інформування). для успішного надсилання СМС-повідомлення, необхідна наявність залишку коштів на Вашому особовому рахунку мобільного оператора України, вартість відправки такої СМС згідно тарифів Вашого оператора. 3.5. Також Ви можете самостійно отримати ПІН-код, надіславши запит за допомогою Системи ПІН-код надійде на Ваш Фінансовий номер телефону. 3.6. У випадку, якщо Ви не маєте можливості відправити СМС-запит, Ви можете звернутись у будь-яке відділення Банку або Контакт-центр, після чого Вам буде згенеровано СМС-повідомлення/ PUSH-повідомлення з ПІН-кодом. 3.7. Після отримання СМС – повідомлення/ PUSH-повідомлення із ПІН-кодом, Вам необхідно запам'ятати комбінацію цифр та одразу видалити цю інформацію з Мобільного пристрою. 3.8. Ви можете самостійно змінити ПІН-код, отриманий в СМС-повідомленні / PUSH-повідомленні, на будь-яку іншу чотиризначну комбінацію цифр. Ця опція є у головному меню Банкомату АТ «КРЕДОБАНК». 3.9. У випадку відкриття цифрової (віртуальної) БПК як первинного інструменту, для підвищення	3. Rules for Receiving a BPC and PIN code and Activating the BPC 3.1. Upon receipt of the BPC, we recommend that you (hereinafter, references to «You» in the relevant grammatical forms shall mean the BPC Holder, including a BPC Holder who is also the Client) sign the reverse side of the BPC in the space designated for the BPC Holder's signature. This will reduce the risk of unauthorised use of the BPC. 3.2. Write down your BPC number and the Contact Centre telephone numbers. If the BPC is lost, you should immediately notify the Bank by calling these numbers. 3.3. To set and receive your PIN code, you must send an SMS request to +380 93 177 77 44. This number is available to subscribers of all Ukrainian mobile operators. An SMS request shall be in the following format: 2+****, where **** – are the last 4 digits of the BPC Holder for which the PIN code is to be set and received 3.4. Please note the following: An SMS request shall be sent from the Financial Telephone Number or another mobile telephone number specified by You when applying for the BPC and/or activating the Mobinform Service (SMS notifications). To successfully send an SMS request, You must have sufficient funds in your personal account with a Ukrainian mobile network operator. The cost of sending such SMS shall be charged in accordance with your mobile network operator's tariffs. 3.5. You may also obtain a PIN code independently by submitting a request via the System. The PIN code will be sent to your Financial Telephone Number. 3.6. If You are unable to send an SMS request, you may contact any branch of the Bank or the Contact Centre, following which an SMS/Push Notification containing the PIN code will be generated and sent to You. 3.7. Upon receipt of SMS/Push Notification containing the PIN code, You must memorise the combination of digits and immediately delete such information from your Mobile Device. 3.8. You may change the PIN code received in an SMS/Push Notification to any other four-digit combination. This option is available in the main menu of JSC «KREDOBANK» ATMs. 3.9. Where a digital (virtual) BPC is issued as the primary payment instrument, obtain the PIN code in advance to

успішності здійснення операцій зі зняття коштів в банкоматах отримайте ПІН-код заздалегідь. 3.10. Активація БПК проводиться: – самостійно в Системі; – автоматично, за умови виконання Вами операції, що вимагає введення ПІН-коду (зняття готівки в касі/банкоматі Банку/інших банків, перегляд залишку; – шляхом здійснення дзвінка в Контакт-центр в автоматичному телефонному меню. 3.11. У випадку неможливості Активації БПК одним із способів, зазначених у п. 3.10. даних Правил, Ви можете Активувати БПК шляхом здійснення телефонного дзвінка до служби Контакт-центру та проходження Вами процедури Автентифікації як Держателя БПК. 3.12. Для можливості здійснення безготівкових off-line операції по БПК з безконтактною технологією, Активацію такої БПК потрібно проводити лише шляхом здійснення операції, яка вимагає введення ПІН-коду в Банкоматі Банку/інших банків.	increase the likelihood of successful cash withdrawal transactions at ATMs. 3.10. BPC shall be activated: – independently via the System; – automatically, provided that you perform a transaction requiring the entry of the PIN code (cash withdrawal at a cash desk or an ATM of the Bank/another bank, or balance enquiry); – by calling the Contact Centre and using the automated telephone menu. 3.11.If the BPC cannot be activated by any of the methods specified in clause 3.10 of the Rules, You may activate the BPC by calling the Contact Centre and completing the Authentication procedure as the BPC Holder. 3.12. To enable cashless off-line transactions using a contactless BPC, such BPC shall be activated exclusively by performing a Transaction requiring the entry of the PIN code at an ATM of the Bank or another bank.
4. Загальні правила використання БПК та ПІН-коду 4.1 БПК використовується в будь-якій торговій точці та пункті видачі готівки, де розташований логотип відповідної МПС. 4.2. Ви не повинні розголошувати ПІН-код стороннім особам (членам родини, знайомим, працівникам Банку, особам, які намагаються допомогти під час використання БПК). 4.3. ПІН-код необхідно запам'ятати або записати та зберігати його окремо від БПК у місці, недоступному для сторонніх осіб. 4.4. Забороняється передавати БПК для використання стороннім особам. Забороняється розголошувати та повідомляти персональні дані або інформацію про БПК на вимогу будь-яких сторонніх осіб, у тому числі і працівників Банку, крім екстрених випадків (звернення у Контакт-центр для здійснення операцій по БПК). 4.5. БПК необхідно зберігати у місці, недоступному для сторонніх осіб та віддаленому від джерел температурного та електромагнітного випромінювання. 4.6. З метою запобігання незаконним операціям з використанням Вашої БПК рекомендуємо Вам підключити Послугу Мобінформ (СМС-інформування) з метою направлення СМС-повідомлень/ PUSH-повідомлень про проведені операції з використанням Вашої БПК на номер мобільного телефону, вказаного Вами при здійсненні оформлення/перевипуску/заміни останньої БПК. Ви можете відмовитись від підключення Послуги Мобінформ (СМС-інформування) зазначивши про це у договорі банківського рахунку, укладеного з Банком за формою діючою в Банку. 4.7. Ви також маєте можливість самостійно змінювати Добові авторизаційні ліміти в Системі або шляхом здійснення дзвінка в Контакт-центр в автоматичному телефонному меню.	4. General rules for using BPC and PIN code 4.1. BPC is used at any point of sale and cash withdrawal point where the logo of the relevant IPS is located. 4.2. You must not disclose the PIN code to third parties (family members, acquaintances, Bank employees, persons trying to help when using the BPC). 4.3. The PIN code must be remembered or written down and stored separately from the BPC in a place inaccessible to third parties. 4.4. It is prohibited to transfer the BPC for use by third parties. It is prohibited to disclose and report personal data or information about the BPC at the request of any third parties, including Bank employees, except in emergency cases (applying to the Contact Center to perform BPC operations). 4.5. BPC must be stored in a place inaccessible to unauthorized persons and away from sources of temperature and electromagnetic radiation. 4.6. In order to prevent illegal operations using your BPC, we recommend that you activate the Mobinform Service (SMS-informing) in order to send SMS notifications/PUSH notifications about operations performed using your BPC to the mobile phone number specified by you when issuing/reissuing/replacing the last BPC. You may refuse to activate the Mobinform Service (SMS-informing) by noting this in the bank account agreement concluded with the Bank in the form valid at the Bank. 4.7. You also have the opportunity to independently change the Daily Authorization Limits in the System or by calling the Contact Center in the automatic telephone menu.

4.8. У випадку неможливості самостійно змінити Добові авторизаційні ліміти, Ви можете це здійснити шляхом здійснення телефонного дзвінка до служби Контакт-центру та проходження Вами процедури Автентифікації як Держателя БПК.

4.9. Підключення послуги СМС-інформування здійснюється у Системі або шляхом зверненням у будь-яке відділення Банку/ телефонного звернення у Контакт-центр з проходженням процедури Автентифікації згідно вимог Банку.

4.10. Якщо БПК втрачено чи викрадено (в т. ч. за кордоном), Вам необхідно для цілей Блокування БПК негайно повідомити АТ «КРЕДОБАНК», зателефонувавши в Контакт-центр (0-800-500-850 - безкоштовно по Україні. +38-032-297-6470 - з-за кордону. Також Ви маєте можливість самостійно тимчасово заблокувати таку БПК в Системі або зателефонувавши в Контакт-центр в автоматичному телефонному меню.

4.11. Ви можете розблокувати тимчасово заблоковану БПК самостійно в Системі або зателефонувавши в Контакт-центр в автоматичному телефонному меню.

4.12. Для здійснення перевипуску БПК, Вам необхідно звернутись у Контакт-центр.

4.13. Якщо БПК пошкоджена або з іншої причини стала непридатною для використання, Вам необхідно звернутись у будь-яке відділення Банку із відповідною заявою на заміну БПК або зателефонувати у Контакт-центр.

4.14. Якщо Ваш ПІН-код став відомий сторонній особі, Вам необхідно здійснити операцію «Зміна ПІН-коду» в банкоматі Банку або операцію «Перевипуск ПІН-коду» одним із способів, вказаних в п. п. 3.3- 3.6. цих Правил.

4.15. У випадку, якщо Ви забули ПІН-код Вашої БПК, Вам необхідно здійснити операцію «Перевипуск ПІН-коду» одним із способів, вказаних в п. п. 3.3- 3.6. цих Правил.

4.16. В системі моніторингу Банку діють обмеження по транзакціях за участю БПК Банку, в т. ч. і по транзакціях, що відбуваються за кордоном. В ході моніторингу транзакцій 4/12 Банк може заблокувати операцію по БПК, по якій виникла підозра на шахрайські дії з боку третіх осіб.

4.17. Якщо Ви плануєте подорож до однієї із перелічених країн та плануєте користуватись БПК, Вам необхідно зателефонувати у Контакт-центр з метою скасування встановлених обмежень.

4.18. Перелік країн, що належать до списку високоризикових, наведений на Інтернет-сторінці Банку за <https://kredobank.com.ua/private/kartky/bezpekavy/korystannya/vysokoryzykovani-krayiny/>

4.19. Особливості користування БПК при використанні Сервісу мобільних платежів визначено Правилами та умовами користування Сервісом мобільних платежів, що розміщені на Сайті Банку та є доповненнями до Правил надання комплексних банківських послуг фізичним особам у Акціонерному

4.8. If You are unable to change the Daily Authorization Limits yourself, you can do this by making a phone call to the Contact Center service and going through the Authentication procedure as a BPC Holder.

4.9. SMS notification service is connected in the System or by contacting any branch of the Bank/by calling the Contact Center and going through the Authentication procedure in accordance with the Bank's requirements.

4.10. If the BPC is lost or stolen (including abroad), you must immediately notify JSC «KREDOBANK» for the purposes of BPC Blocking by calling the Contact Center (0-800-500-850 - free of charge within Ukraine. +38-032-297-6470 - from abroad. You also have the opportunity to temporarily block such BPC in the System yourself or by calling the Contact Center in the automatic telephone menu.

4.11. You can unblock a temporarily blocked BPC yourself in the System or by calling the Contact Center in the automatic telephone menu.

4.12. To reissue the BPC, You must contact the Contact Center.

4.13. If the BOD is damaged or for some other reason has become unusable, You should contact any branch of the Bank with a corresponding application for replacement of the BPC or call the Contact Center.

4.14. If Your PIN code has become known to a third party, you must perform the operation «Change PIN code» at the Bank's ATM or the operation «Reissue PIN code» in one of the ways specified in clauses 3.3-3.6. of the Rules.

4.15. If You have forgotten the PIN code of your BPC, you should perform the operation «Reissue PIN code» in one of the ways specified in clauses 3.3-3.6. of the Rules.

4.16. The Bank's monitoring system has restrictions on transactions involving the Bank's BPC, including transactions taking place abroad. During transaction monitoring, The Bank may block a BPC transaction for which there is a suspicion of fraudulent actions by third parties.

4.17. If you are planning a trip to one of the listed countries and plan to use BPC, you need to call the Contact Center to cancel the established restrictions.

4.18 The list of countries included in the list of high-risk countries is provided on the Bank's website at the link <https://kredobank.com.ua/private/kartky/bezpekavy/korystannya/vysokoryzykovani-krayiny/>

4.19. The features of using the BPC when using the Mobile Payment Service are determined by the Terms and Conditions for Using the Mobile Payment Service, which are posted on the Bank's Website and are supplements to Terms and Conditions for Provision of Comprehensive Banking Services to Individuals at JSC «KREDOBANK» and to Terms and

Товаристві «КРЕДОБАНК» і до Правил надання комплексних банківських послуг юридичним особам та фізичним особам-підприємцям в АТ «КРЕДОБАНК».	Conditions for Provision of Comprehensive Banking Services to Services to Legal Entities and Sole Proprietors at JSC «KREDOBANK».
5. Правила користування банкоматом 5.1. Перед використанням банкомата Ви повинні оглянути його щодо наявності підозрілих пристроїв що розташовані в місці набору ПІН-коду або в місці, призначеному для прийому БПК (наприклад, наявність нерівно встановленої клавіатури для набору ПІН-коду). 5.2. У випадку їх наявності, не використовуйте даний банкомат для здійснення операцій з використанням БПК та повідомте про це Банк за номером телефону, який зазначено на банкоматі. 5.3. ПІН-код необхідно набирати таким чином, щоб особи, які перебувають поруч, не змогли його побачити. Під час набору ПІН-коду прикривайте клавіатуру рукою. Якщо банкомат працює некоректно (наприклад, довгий час перебуває в режимі очікування, перезавантажується), Вам необхідно відмовитись від послуг такого банкомата та відмінити поточну операцію, натиснувши на клавіатурі кнопку «Відміна» («Отмена» чи «CANCEL») і дочекатись повернення БПК. 5.4. Перед здійсненням операції в банкоматі, на екрані банкомату відображається інформація щодо комісії за здійснення такої операції і Ви маєте можливість відмовитись від такої операції після ознайомлення з комісією. 5.5. Після отримання готівки в банкоматі необхідно її перерахувати та переконатись у тому, що БПК була повернена банкоматом, дочекатись видачі чеку в разі його запиту і тільки після цього відходити від банкомату. Роздруковані банкоматом чеки потрібно зберігати для звірки зазначених у них сум з випискою про рух коштів по Поточному рахунку. 5.6. Під час проведення операції через банкомат може виникнути ситуація, коли банкомат не повертає БПК. Причинами цього може бути: а) збій в роботі банкомата (БПК не видана протягом 1,5- 2 хв.); б) закінчення ліміту часу, відведеного для того, щоб забрати БПК (БПК не забрана Клієнтом протягом 30-35 сек.); в) інше. 5.7. У даному випадку Вам необхідно звернутись у Контакт-центр, повідомити про факт затримання банкоматом БПК та тимчасово заблокувати БПК. 5.8. Для отримання інформації щодо Відділення, в якому Ви можете отримати вилучену банкоматом БПК, Вам необхідно звернутися у Контакт-центр не раніше 5 робочих днів з моменту повідомлення про затримання банкоматом Вашої БПК. 5.9. Також Ви можете здійснити постійне Блокування та перевипуск даної БПК шляхом звернення у Контакт-центр	5. Rules for using an ATM 5.1. Before using an ATM, You must inspect it for any suspicious devices installed near the PIN code keypad or the BPC insertion slot (for example, an unevenly fitted PIN code keypad). 5.2. If any such devices are detected, do not use the ATM to perform Transactions using the BPC and notify the Bank thereof by calling the telephone number indicated on the ATM. 5.3. PIN code should be entered in such a manner that it cannot be seen by any persons nearby. When entering the PIN code, cover the keypad with your hand. If the ATM is not operating properly (for example, it remains in standby mode for an extended period or restarts), you must discontinue using such ATM and cancel the current Transaction by pressing the «Cancel» («Відміна», «Отмена» or «CANCEL») button on the keypad and wait for the BPC to be returned. 5.4. Before a Transaction is performed at an ATM, information on the fee charged for such transaction shall be displayed on the ATM screen, and you may decline to proceed with the transaction after reviewing the applicable fee. 5.5. After receiving cash from an ATM, You should count it, ensure that the ATM has returned the BPC and, if a receipt has been requested, wait for the receipt to be issued. You should leave the ATM only after completing all these steps. Receipts printed by the ATM must be retained for the purpose of reconciling the amounts specified therein against the statement of transactions in the Current Account. 5.6. When performing a transaction at an ATM, the ATM may retain the BPC. This may occur due to: a) an ATM malfunction (the BPC is not returned within 1.5–2 minutes); б) expiry of the time allowed for retrieving the BPC (the Client fails to retrieve the BPC within 30–35 seconds); в) other reasons. 5.7. In such a case, you must contact the Contact Centre, report that the BPC has been retained by the ATM and temporarily block the BPC. 5.8. To obtain information about the branch from which you may collect the BPC retained by the ATM, you must contact the Contact Centre no earlier than five business days after reporting that your BPC has been retained by the ATM. 5.9. You may also permanently block and have the BPC reissued by contacting the Contact Centre.

6. Правила здійснення безготівкових розрахунків з використанням БПК 6.1. Ви не повинні використовувати БПК в торговельній мережі для оплати товарів або послуг, якщо торговець/продавець/касир викликав у вас недовіру. 6.2. Розрахунки з використанням БПК повинні здійснюватися лише у Вашій присутності. Це забезпечить зниження ризику неправомірного отримання Ваших персональних даних, зазначених на БПК. 6.3. Під час використання БПК для оплати товарів або послуг продавець/касир може вимагати від Вас надати паспорт, підписати квитанцію або ввести ПІН-код. Перед набором ПІН-коду Ви повинні переконатися, що треті особи, які перебувають у безпосередній близькості від Вас, не зможуть його побачити. Перед тим, як підписати квитанцію, Вам необхідно в обов'язковому порядку перевірити суму, що зазначена на ній.	6. Rules for making cashless payments using a BPC 6.1. You should not use the BPC to pay for goods or services at a merchant outlet if the merchant/seller/ cashier causes you to have any doubts as to their trustworthiness. 6.2. Payments using the BPC must be made only in Your presence. This will reduce the risk of unauthorised access to your personal data indicated on the BPC. 6.3. When you use the BPC to pay for goods or services, the seller/ cashier may require You to present your passport, sign the transaction confirmation slip or enter your PIN. Before entering the PIN, You must ensure that no third persons in your immediate vicinity can see it. Before signing the transaction confirmation slip, you must check the amount indicated thereon.
7. Правила здійснення операцій через мережу Інтернет 7.1. Використання ПІН-коду під час замовлення товарів або послуг через мережу Інтернет, а також за телефоном/факсом, не передбачене правилами платіжних систем і свідчить про шахрайський характер операції. В жодному випадку Ви не повинні здійснювати таких операцій. 7.2. Для придбання товарів та послуг в мережі Інтернет користуйтеся тільки відомими та перевіреними платіжними сайтами! 7.3. Не потрібно робити повторних спроб оплатити рахунок безліч разів. Це може призвести до блокування Банком можливості провести платіж, так як може спрацювати система безпеки Банку від підбору параметрів БПК. 7.4. Якщо оплата товару (послуги) здійснюється через чужий комп'ютер, після завершення всіх розрахунків, Вам необхідно переконатися, що реквізити БПК та інша конфіденційна інформація не збереглися на даному комп'ютері. Для цього необхідно знову відкрити сторінку продавця, на якій здійснювалась оплата товару, та переконатись, що відповідні поля бланку-замовлення перебувають у незаповненому стані. 7.5. На комп'ютер, з якого регулярно здійснюються операції з використанням БПК, необхідно встановити антивірусне програмне забезпечення і вчасно здійснювати його оновлення, а також оновлення інших програмних продуктів (операційної системи, прикладних програм). Це зменшить ризик «зараження» Вашого комп'ютера вірусними програмами, які здійснюють викрадення персональних даних. 7.6. При здійсненні операцій оплати товарів та послуг з використанням БПК у мережі Інтернет, в т. ч. засобами інтернет-банкінгу, на Інтернет-сайтах, що	7. Rules for performing transactions Online 7.1. The rules of the Payment Systems do not provide for the use of the PIN code when ordering goods or services online or by telephone/fax, and any request to use the PIN code for such purposes indicates that the transaction is fraudulent. Under no circumstances should You perform such transactions. 7.2. When purchasing goods and services online, use only well-known and trusted payment websites! 7.3. Do not make repeated attempts to pay the same bill. This may result in the Bank blocking the payment, as the Bank's security system designed to prevent attempts to guess BPC details may be triggered. 7.4. If payment for goods (services) is made using another person's computer, after completing all payments you must ensure that the BPC Details and other confidential information have not been saved on that computer. To do so, reopen the merchant's webpage on which the payment was made and ensure that the relevant fields of the order form are blank. 7.5. Anti-virus software must be installed and regularly updated on any computer routinely used to perform Transactions using the BPC. Other software, including the operating system and applications, must also be kept up to date. This will reduce the risk of your computer being «infected» with malicious software designed to steal personal data. 7.6. When transactions for the payment of goods and services are performed using the BPC online, including through online banking facilities, on websites supporting 3D Secure, the Bank

надають можливість використання 3D Secure, Банк надсилає Вам СМС-повідомленням/ PUSH-повідомлення з одноразовим паролем на номер мобільного телефону, вказаного Вами при здійсненні оформлення/перевипуску/заміни останньої БПК для підтвердження проведення операції з БПК шляхом введення даного одноразового паролю у відповідне поле веб-сторінки у мережі Інтернет або поле засобу інтернет-банкінгу. 7.7. Згідно з Правилами МПС MasterCard Worldwide на інтернет - сайтах, які підтримують 3D Secure, обов'язково має зазначатись логотип MasterCard SecureCode	shall send you an SMS/Push Notification containing a one-time password to the mobile telephone number specified by you when applying for, reissuing or replacing the most recently issued BPC. To confirm the BPC transaction, you must enter the one-time password in the relevant field on the webpage or in the relevant online banking facility. 7.7. In accordance with the rules of the MasterCard Worldwide International Payment System, websites supporting 3D Secure must display the MasterCard SecureCode logo
8. Термін дії БПК та видача нової БПК 8.1. Термін дії БПК вказано на її лицьовій стороні. БПК дійсна до останнього дня місяця, вказаного на ній, включно. 8.2. Банк здійснює повідомлення про закінчення терміну дії Вашої БПК не пізніше ніж за десять календарних днів до закінчення терміну її шляхом надсилання відповідного СМС-повідомлення на Ваш Фінансовий номер мобільного телефону. 8.3. Якщо протягом останніх трьох місяців терміну дії БПК відбувались транзакції по БПК (безготівкові операції з БПК, зняття готівки з БПК, переказ коштів з БПК, зарахування коштів на БПК та інші операції, що за своїм характером належать до зазначених категорій операцій) , то така БПК перевипускається автоматично, якщо БПК даного типу не заблокована та не знята з продажу на момент закінчення її терміну дії 8.4. Для отримання перевипущеної БПК Вам необхідно звернутись у відділення Банку, де відкритий Ваш Поточний рахунок, протягом останнього місяця терміну дії БПК. 8.5. У випадку відсутності активності по БПК протягом останніх трьох місяців терміну дії БПК, вона не буде перевипущена. Для випуску нової БПК до Вашого Поточного рахунку Вам необхідно звернутись у відділення Банку, де відкритий Ваш Поточний рахунок.	8. BPC validity period and issuance of a new BPC 8.1. BPC validity period is indicated on the front side of BPC. BPC shall remain valid through the last day of the month indicated thereon. 8.2. The Bank shall notify You of the expiry of Your BPC no later than ten calendar days before its expiry by sending a relevant SMS message to your Financial Phone Number. 8.3. If BPC transactions were performed during the last three months of the BPC validity period—including cashless BPC transactions, cash withdrawals using the BPC, funds transfers from the BPC, crediting of funds to the BPC, and other transactions that by their nature fall within the above categories—the BPC shall be reissued automatically, provided that, as of its expiry date, BPCs of the relevant type have not been blocked or withdrawn from sale. 8.4. To collect the reissued BPC, you must visit the Bank's branch at which your Current Account was opened during the last month of the BPC validity period. 8.5. If no BPC transactions were performed during the last three months of the BPC validity period, the BPC shall not be reissued. To have a new BPC issued for your Current Account, you must visit the Bank's branch at which your Current Account was opened.
9. Збійні операції в термінальній мережі Банку 9.1. Під час здійснення операції в банкоматах, ПТКС або POS-терміналах Банку може відбутись збій операції, викликаний технічними несправностями комунікаційних мереж, самого терміналу, помилки програмного забезпечення або з будь-яких інших технічних причин. 9.2. У випадку наявності такої збійної операції, що не була в повному обсязі проведена, Ви повинні звернутись у будь-яке відділення Банку для складання відповідної заяви на проведення розслідування або зателефонувати у Контакт-центр. 9.3. Термін проведення розслідування - до 45 днів від моменту Вашого звернення у Відділення/ Контакт-центр.	9. Failed transactions within the Bank's terminal network 9.1. When performing a Transaction at an ATM, SHSC or POS Terminal of the Bank, the transaction may fail due to technical malfunctions of communication networks or the terminal itself, software errors or any other technical reasons. 9.2. If a failed transaction has not been completed in full, you must contact any branch of the Bank to submit the relevant application for an investigation or call the Contact Centre. 9.3. The investigation shall be completed within 45 days from the date of Your request to the branch/Contact Centre.

9.4. По результатах проведеного розслідування, у разі підтвердження збійної операції, суми усіх виявлених збійних операцій, що відбулись в термінальній мережі Банку зараховуються/повертаються на відповідні рахунки в залежності від типу збійної операції.	9.4. Based on the investigation results, where a failed transaction is confirmed, the amounts of all identified failed transactions that occurred within the Bank's terminal network shall be credited/refunded to the relevant accounts, depending on the type of failed transaction.
10. Рекомендації щодо використання БПК 10.1. Під час використання БПК Вам слід дотримуватись наступних рекомендацій з метою забезпечення нормального функціонування БПК впродовж терміну її дії: не допускати пошкодження поверхні БПК твердими предметами – можлива втрата функціональності магнітної стрічки та чіп модуля, також може привести до зовнішніх пошкоджень, тріщин, подряпин на панелі для підпису, голограми; не допускати будь-якого агресивного чи фізичного впливу навколишнього середовища на БПК - можлива втрата функціональності магнітної стрічки, чіп модуля і захисних елементів; не допускати деформації (короблення) БПК – можлива втрата функціональності БПК, можливе відшаровування оверлей. не піддавати БПК температурним впливам, більше 60° - можлива зміна розмірів і короблення; не навантажувати БПК зверху, в області чіп-модуля більше 8Н – можлива втрата функціональності	10. Recommendation for the use of BPCs 10.1. When using the BPC, You should comply with the following recommendations to ensure the proper functioning of the BPC throughout its validity term: do not allow the surface of the BPC to be damaged by hard objects – as this may result in loss of functionality of the magnetic stripe and chip module and may also cause external damage, cracks or scratches to the signature panel or hologram; do not expose the BPC to any aggressive environmental or physical impact as this may result in loss of functionality of the magnetic stripe, chip module and security features; prevent deformation (warping) of the BPC – as this may result in loss of functionality of the BPC or delamination of the overlay. do not expose the BPC to temperatures exceeding 60°C, as this may cause dimensional changes or warping; do not apply a load exceeding 8 N to the BPC in the area above the chip module, as this may result in loss of functionality