ЗАТВЕРЖЕНО
Голова Правління АТ «МетаБанк»

_____ Нужний С.П.
10.03.2014р.

ПРАВИЛА НАДАННЯ КОМПЛЕКСНИХ ПОСЛУГ ТА ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ КЛІЄНТІВ – ФІЗИЧНИХ ОСІБ В СИСТЕМІ ІНТЕРНЕТ-БАНКІНГ «METABANK ONLINE»

ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА “МЕТАБАНК”

Запоріжжя 2014р.

Зміст

1. Терміни

Автентифікація	процедура ідентифікації Клієнта шляхом перевірки Банком пред'явлених Автентифікаційних даних на предмет їх належності Клієнту з метою надання доступу до Системи та/або надання комплексних банківських послуг в Системі.
Атентифікаційні дані (Клієнта)	всі разом або окремі дані, що використовується для Автентифікації Клієнта, а саме: Логін, код скретч-картці, Пароль для входу та Одноразовий пароль.
Договір	Договір на здійснення договірного списання та надання інформаційних послуг в системі «MetBank Online».
Доручення (Клієнта) на договірне списання (далі - Доручення)	правочин, вчинений Сторонами у формі електронного документа відповідно до умов цього Договору, що містить інформацію, необхідну для здійснення Договірного списання: номер Рахунку, та/або реквізитів Рахунку Клієнта, найменування, код та рахунок отримувача, найменування та код банку отримувача, сума та призначення платежу. Доручення не є розрахунковим документом. Доручення є невід'ємною частиною цього Договору.
Рахунки	всі поточні та вкладні рахунки Клієнта в Банку, які відкриті станом на дату укладання цього Договору та будуть відкриті в майбутньому, реквізити яких Банк визначить самостійно. До Рахунків належать, в тому числі, поточні рахунки, операції за якими можуть здійснюватися з використанням спеціальних платіжних засобів (далі Рахунки). Перелік Рахунків відображається в Системі. Розрахунково-касове обслуговування Рахунків здійснюється відповідно до договорів про відкриття та ведення Рахунків з урахуванням особливостей визначених цим Договором.
Логін	умовне позначення Клієнта, що визначається Клієнтом і використовується разом з паролем на скетч-картці Клієнта
Операційний день	частина робочого дня Банку, протягом якої приймаються документи на переказ і документи на відкликання та можна, за наявності технічної можливості, здійснити їх обробку, передачу та виконання. Інформація про тривалість Операційного дня розміщується на сайті Банку http://www.mbank.com.ua/
Пароль для входу	таємна послідовність символів, що визначається Клієнтом і використовується разом з Логіном.
Правила	встановлені Банком Правила користуванням системою дистанційного обслуговування Клієнтів «MetaBank Online»Правила розміщуються на сайті Банку http://www.mbank.com.ua/, та є невід'ємною частиною Договору
Таємний пароль Скретч-картки	це випадково сгенерована послідовність символів, яка дійсна тільки для одного сеансу аутентифікації.
Скретч-Картка Клієнта	паперова,пластикова тощо - картка із захисним шаром, який скриває пароль для першої Автентифікації Клієнта. При наданні Клієнту скретч-картки, захисний шар має бути непошкодженим.

Система «MetaBank Online» (Система)	система дистанційного обслуговування клієнтів та надання комплексних послуг «MetaBank Online», доступ до якої здійснюється через мережу Інтернет, та яка забезпечує створення, передачу та обробку Доручень, а також надання інформаційних послуг.
Тимчасовий пароль для входу	таємна послідовність символів, що визначається Клієнтом і використовується разом з Логіном.
Тарифи	затверджені Банком Тарифи для приватних клієнтів, що визначають розмір комісійної винагороди (плати) за обслуговування у Системі.

Інші терміни, що використовуються у тексті цих Правил, мають значення, визначене Договором.

2. Правила користування Системою

2.1. Режими роботи Системи

В Системі передбачено два режими роботи – інформаційний режим (пасивний) та Активний режим.
2.1.1. Інформаційний режим дозволяє Клієнту виконувати наступні дії:

- Переглядати перелік власних рахунків/продуктів;
- переглядати архів власних операцій за рахунками;

2.1.2. Активний режим дозволяє Клієнту виконувати наступні дії:

- переглядати перелік власних рахунків/продуктів;
- переглядати архів власних операцій за рахунками;
- ініціювати Договірне списання, тобто подавати Доручення на договірне списання з власних рахунків Клієнта в Банку.

2.2. Умови користування Інформаційним режимом

2.2.1. Користування Інформаційним режимом можливе за умови:

- наявності скретч-картки Клієнта;
- наявності укладеного Договору;
- зазначення в Договорі актуального Номеру мобільного телефону Клієнта, на який будуть надходити Одноразові паролі;
- логіну;
- тимчасовий пароль для входу.
- активації доступу до Системи Банку у порядку, визначеному в п 2.4 цих Правил.

2.3. Умови користування Активним режимом

2.3.1. Користування Активним режимом можливе за умови:

- наявності скретч-картки Клієнта;
- наявності укладеного Договору;
- зазначення в Договорі актуального Номеру мобільного телефону Клієнта, на який будуть надходити Одноразові паролі та Тимчасовий пароль для входу;
- логіну;
- активації доступу до Системи Банку у порядку, визначеному в п 2.4 цих Правил.

2.4. Процедура активації доступу до Системи Банку

2.4.1. З метою отримання можливості користування Системою в Інформаційному та Активному режимі Клієнту необхідно здійснити процедуру активації доступу до Системи Банку.

2.4.2. Для активації доступу до Системи необхідно пройти процедуру Автентифікації в Системі по коду зі скретч-картки Клієнта;

2.4.3. Після виконання активації доступу до Системи у порядку, визначеному п. 2.4.2. цих Правил та в разі виконання всіх необхідних умов, визначених пп. 2.3.1. п. 2.3. цих Правил, Клієнт може користуватись Системою в Інформаційному та Активному режимі.

2.5. Процедура Автентифікації в Системі

2.5.1. Для першого входу в Систему Клієнту необхідно:

- зайти на сайт Системи https://MetaBankOnline.com.ua;

При здійсненні першого входу необхідно в обов'язковому порядку встановити постійний Пароль для входу.

- ввести Логін та Пароль для входу(свій власний пароль, який Клієнт встановлює самостійно), підтвердити пароль для входу;
- ввести номер Договору;
- ввести Таємний пароль зі скретч-картки, що вказаний на зворотньому боці Картці;
- ввести Одноразовий пароль, що надійде у вигляді SMS-повідомлення.

Термін дії Одноразового паролю для підтвердження має обмежений термін дії і становить 3 хвилини. В разі, якщо Клієнт не встиг скористатись наданим у SMS -повідомленні Одноразовим паролем для підтвердженні при першому вході, необхідно натиснути кнопку «Вислати СМС вдруге» та ввести Одноразовий пароль знову.

Пароль для входу повинен відповідати вимогам, зазначеним в пп. 4.3.2. п. 4.3. цих Правил. 2.5.2. Для наступних входів в Систему Клієнту необхідно:

- Ввести Логін;
- Ввести Пароль для входу (постійний пароль, який Клієнт встановив при першому вході).

2.5.3. В разі, якщо Клієнт тричі ввів некоректно Логін або Пароль для входу, Клієнту блокується доступ до Системи.

У цьому випадку Клієнту необхідно здійснити дії, зазначені в п.п. 2.6. та п.п. 2.8.

2.6. Поновлення Паролю або Логіну для входу в разі, якщо Клієнт забув пароль або Логін:

2.6.1. У випадку, якщо Клієнт забув Пароль або Логін для входу до Системи, необхідно здійснити наступні дії:

Розблокування доступу до Системи, який раніше було заблоковано, можливе тільки після звернення Клієнта до відділення Банку із відповідною Заявою на внесення змін до умов обслуговування за Договором та пред'явлення співробітнику Банку паспорту або документу, що його замінює.

2.6.2. В разі успішної ідентифікації Клієнта, Клієнт отримує в касі нову скретч-картку з Таємним паролем.

2.6.3. Після цього Клієнту необхідно зайти в Систему та здійснити процедуру першого входу, а саме:
- ввести Логін та Пароль для входу(свій власний пароль, який Клієнт встановлює самостійно), підтвердити пароль для входу;
- ввести номер Договору;
- ввести Таємний пароль зі скретч-картки, що вказаний на зворотньому боці Картці;
- ввести Одноразовий пароль, що надійде у вигляді SMS-повідомлення.

2.7. Блокування доступу до Системи

2.7.1. Блокування доступу до Системи може бути здійснено за ініціативою Клієнта, в разі якщо:

- Клієнт не бажає користуватись Системою;
- Клієнт втратив скретч-картку Клієнта з Таємним паролем;
- Скретч-картку Клієнта з Таємним паролем було викрадено;
- Скретч-картку Клієнта з Таємним паролем скомпрометовано (тобто, є підстави вважати, що Таємний код став відомий сторонній особі);
- Логін та пароль для входу скомпрометовано (тобто, є підстави вважати, що Логін та Пароль для входу став відомий сторонній особі);

2.7.2. Для блокування доступу до Системи, в разі настання причин, перелічених в пп. 2.7.1. п.2.7. Правил, Клієнту необхідно звернутись у відділення Банку.

2.7.3. Блокування доступу до Системи може бути здійснено за ініціативою Банку з метою попередження можливого шахрайства, будь-яких незаконних або непогоджених дій, що можуть призвести до фінансових збитків Клієнта або Банку або до погіршення іміджу Банку.

2.8. Розблокування доступу до Системи

2.8.1. Розблокування доступу до Системи, який раніше було заблоковано з ініціативи Клієнта, можливе тільки після звернення Клієнта до відділення Банку із відповідною Заявою на внесення змін до умов обслуговування за Договором та пред'явлення співробітнику Банку паспорту або документу, що його замінює.

3. Правила виконання банківських операцій в Системі

3.1. Здійснення комунальних платежів на користь ПАТ «Запоріжгаз» (платежі)

3.1.1. В Системі передбачена можливість здійснювати платежі за використаний природний газ. Для виконання платежу необхідно здійснити наступні дії:
- Натиснути кнопку «Сплата послуг»;
- Вибрати регіон, в якому здійснюється оплата;
- Вибрати тип платежу;
- Вибрати із списку отримувачів «Запоріжгаз»;
- Здійснити пошук за номером особового рахунку;
- Перевірити дані з Системи на співпадіння особовому рахунку клієнта, якщо дані не співпадають треба натиснути кнопку «Відміна»;
- Перевірити суму нарахувань, якщо Клієнт бажає сплатити іншу суму, необхідно в полі «сума» ввести необхідну суму;
- Якщо в клієнта є дані показників лічильників, то треба заповнити поле «Показники лічильника»;
- В разі заповнення всіх необхідних полів натиснути кнопку «Сплатити».

.3.1.2. В Системі передбачена можливість здійснювати платежі за послуги надані працівниками ПАТ «Запоріжгаз». Для оплати послуг необхідний унікальний код роботи і номер цеху, ця інформація зазначена в квитанції на оплату. Для виконання платежу необхідно здійснити наступні дії:
- Натиснути кнопку «Сплата послуг»;
- Вибрати регіон, в якому здійснюється оплата;
- Вибрати тип платежу;
- Вибрати із списку отримувачів «Запоріжгаз»;
- Здійснити пошук за номером особового рахунку;
- Вибрати вкладку «Сплата за послуги Запоріжгазу»;
- Із списку послуг треба вибрати відповідну послугу;
- Із списку цехів треба вибрати відповідний цех;
- Треба зазначити дату послуги;
- Треба зазначити «Унікальний код работи»;
- Перевірити дані з Системи на співпадіння особовому рахунку клієнта, якщо дані не співпадають треба натиснути кнопку «Відміна»;
- В полі «сума» ввести необхідну суму;
- В разі заповнення всіх необхідних полів натиснути кнопку «Сплатити».

3.2. Здійснення комунальних платежів на користь ПАТ «Укртелеком» (платежі)

3.2.1. В Системі передбачена можливість здійснювати платежі за телекомунікаційні послуги на користь ПАТ «Укртелеком». Для виконання платежу необхідно здійснити наступні дії:

- Натиснути кнопку «Сплата послуг»;
- Вибрати регіон, в якому здійснюється оплата;
- Вибрати тип платежу;
- Вибрати із списку отримувачів «Укртелеком»;
- Здійснити пошук за номером телефону або за номером особового рахунку(зазначеному у квитанції на сплату);
- Перевірити дані з Системи на співпадіння особовому рахунку клієнта, якщо дані не співпадають треба натиснути кнопку «Відміна»;
- Перевірити суму нарахувань, якщо Клієнт бажає сплатити іншу суму, необхідно в полі «сума» ввести необхідну суму, але ні в якому разі менш ніж нарахованої;
- В разі заповнення всіх необхідних полів натиснути кнопку «Сплатити».

3.3. Здійснення комунальних платежів на користь ПрАТ «Запоріжзв'язоксервіс» (платежі)

3.3.1. В Системі передбачена можливість здійснювати комунальні платежі з використанням бази нарахувань ПрАТ «Запоріжзв'язоксервіс». Для виконання платежу необхідно здійснити наступні дії:

- Натиснути кнопку «Сплата послуг»;
- Вибрати регіон, в якому здійснюється оплата;
- Вибрати тип платежу;
- Вибрати із списку отримувачів «Запоріжзв'язоксервіс»;
- Вибрати тип платежу;
- Здійснити пошук за номером особового рахунку;
- Вибрати підприємство на користь, якого буде здійснено платіж;
- Перевірити дані з Системи на співпадіння особовому рахунку клієнта, якщо дані не співпадають треба натиснути кнопку «Відміна»;
- Перевірити суму нарахувань, якщо Клієнт бажає сплатити іншу суму, необхідно в полі «сума» ввести необхідну суму;
- Якщо в клієнта є дані показників лічильників, то треба заповнити поле «Показники лічильника»;
- В разі заповнення всіх необхідних полів натиснути кнопку «Сплатити».

3.4. Здійснення комунальних платежів на користь КП «Основаніє» (платежі)

3.4.1. В Системі передбачена можливість здійснювати комунальні платежі з використанням бази нарахувань КП «Основаніє». Для виконання платежу необхідно здійснити наступні дії:

- Натиснути кнопку «Сплата послуг»;
- Вибрати регіон, в якому здійснюється оплата;
- Вибрати тип платежу;
- Вибрати із списку отримувачів «КП Основаніє»;
- Вибрати тип платежу;
- Здійснити пошук за номером особового рахунку;
- Перевірити дані з Системи на співпадіння особовому рахунку клієнта, якщо дані не співпадають треба натиснути кнопку «Відміна»;
- Перевірити суму нарахувань, якщо Клієнт бажає сплатити іншу суму, необхідно в полі «сума» ввести необхідну суму;
- Якщо в клієнта є дані показників лічильників, то треба заповнити поле «Показники лічильника»;
- В разі заповнення всіх необхідних полів натиснути кнопку «Сплатити».

4. Заходи безпеки при користуванні Системою.

4.1. Вимоги інформаційної безпеки до персонального комп'ютера (іншого пристрою), з якого здійснюється доступ до Системи

4.1.1. Для отримання доступу до Системи Клієнт зобов'язаний використовувати персональний комп'ютер або інший пристрій, що забезпечує доступ до мережі Інтернет та на якому встановлено:

- операційну систему (наприклад, Microsoft Windows, Unix тощо) з останніми оновленнями;
- останню доступну версію веб-браузера (Mozilla, Opera, Chrome);
- ліцензійне антивірусне програмне забезпечення (наприклад, Kaspersky Anti-Virus, Dr. Web тощо) з останніми оновленнями баз вірусних сигнатур;
- антишпигунське програмне забезпечення (antispyware) та програмний персональний мережевий екран (firewall) (наприклад, Kaspersky Internet Security, Norton Internet Security, McAfee Internet Security тощо) з останніми оновленнями.

4.1.2. Рекомендується регулярно (не рідше, ніж раз на тиждень) здійснювати повне сканування персонального комп'ютера (іншого пристрою) для виявлення вірусів та зловмисного програмного забезпечення.

4.1.3 Не рекомендується встановлювати на персональний комп'ютер (інший пристрій) програмне забезпечення із ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо).

4.2. Вимоги безпеки до Автентифікаційних даних Клієнта

4.2.1. Автентифікаційні дані повинні зберігатися в таємниці, а мобільний телефон (SIM-карта, що відповідає Номеру мобільного телефону Клієнта) – під постійним особистим контролем Клієнта.
4.2.2. При використанні Автентифікаційних даних необхідно Логін та Пароль для входу до Системи Банку Клієнта зберігати окремо.

4.3. Парольна політика

4.3.1. Пароль для входу в Систему не повинен містити словарне слово або ім'я, пов'язане з користувачем (ім'я, прізвище, ім'я дружини, дітей тощо), не містити послідовності знаків, що повторюються (наприклад, «access»), очевидних послідовностей та узорів, які створюються символами, нанесеними на клавіші клавіатури (наприклад, asdfghjkl или erdfcv).
4.3.2. Пароль для входу в Систему повинен відповідати наступним вимогам: мінімум 8 символів; максимум 20 символів; мінімум 1 маленька літера; мінімум 1 велика літера; мінімум 1 цифра;
4.3.3. Пароль для входу в Систему не має містити символи, які можна сплутати, наприклад: 1, L, 0, i, 0,O і т.д.

4.4. Базові правила безпеки при використанні Системи

4.4.1. При використанні Системи Клієнт повинен:

4.4.1.1. Здійснювати підключення до Системи тільки з надійних робочих станцій, уникати підключення з публічних місць (Інтернет-кафе, готелів, бібліотек тощо).
4.4.1.2. Впевнитись при вході в Систему, що в адресному полі веб-браузера знаходиться адреса саме Системи «MetaBank Online».
4.4.1.3. При підключенні до Системи перевіряти, чи ввімкнено шифрування. Про ввімкнене шифрування свідчить наявність значка «Замок» у вікні браузера.
4.4.1.4. Перевіряти надійність надавача сертифікату, дійсність сертифікату та термін його дії. Підтвердженням того, що між веб-браузером Клієнта та веб-сервером Банку встановлено безпечне з'єднання, є наявність цифрового (електронного) сертифікату Банку.
4.4.1.5. Після відкриття сесії перевіряти дату останнього входу до Системи.
4.4.1.6. Не залишати персональний комп'ютер (інший пристрій, з якого здійснюється доступ до Системи) без нагляду.
4.4.1.7 Закінчувати поточну сесію (тобто, закінчувати роботу з Системою) через посилання «Вихід» та закривати вікно веб-браузера.
4.4.1.8. Якщо вхід у Систему здійснюється в публічних місцях, перед закриттям вікна браузера очистити буфер браузера та видалити тимчасові файли та cookies.
4.4.1.9. Не переглядати інші сайти в тому ж веб-браузері, коли Клієнт працює в Системі.
4.4.1.10. Стежити за тривалістю веб-сесії (тривалості знаходження в Системі без будь-яких дій з боку Клієнта), яка задля безпеки обмежена п'ятьма хвилинами.
4.4.1.11. Для навігації в Системі використовувати виключно посилання і кнопки Системи та не використовувати кнопки навігації браузера (наприклад «Вперед» / «Назад»).
4.4.1.12. Звертати увагу на повідомлення веб-браузера про небезпеку.

4.4.2. При використанні Системи Клієнт забороняється:

- Для входу в Систему підключатися за банерним посиланням або посиланнями, отриманими електронною поштою.

- Відповідати на запити (найчастіше розсилаються електронною поштою), які містять вимогу надати або перевірити Логін, Пароль для входу та/або інші Автентифікаційні дані.

Банк за жодних обставин не здійснює:
- Розсилку електронних листів із вимогою надіслати Пароль для входу, Логін та/або інші Автентифікаційні дані або перейти за вказаною електронною адресою.
- Розповсюдження електронною поштою комп'ютерних програм.

4.4.3. Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *.exe, *.pif, *.vbs та інші файли.
4.4.4. У разі виявлення будь-якого зловмисного програмного забезпечення (віруси, троянські програми тощо) на робочій станції, необхідно здійснити вхід в Систему із гарантовано незараженої робочої станції та замінити пароль доступу до Системи.
4.4.5. При виявленні спроби несанкціонованого доступу до Системи необхідно терміново змінити Пароль для входу до

Системи та звернутися до Інформаційного центру за телефоном 0 800 30 10 38 для отримання рекомендацій щодо подальших дій. Рекомендується також провести сканування робочої станції на виявлення вірусів та іншого зловмисного програмного забезпечення.