РЕГЛАМЕНТ РОБОТИ СИСТЕМИ iFOBS
Інтерактивна система фронт-офісного
обслуговування клієнтів банку

Під час використання системи iFOBS Клієнт зобов`язаний суворо дотримуватися вимог цього Регламенту.

Для запобігання доступу сторонніх осіб до конфіденційної інформації клієнта через систему iFOBS, а також перегляду передачі або модифікації даних використовується багаторівнева архітектура системи безпеки, яка містить:

- обов'язкову авторизацію й аутентифікацію користувачів;
- протоколювання всіх дій користувачів у системі;
- обмін даними тільки за стандартизованими інтерфейсами;
- захист каналу передачі даних на основі SSL v3.0;
- цифровий підпис документів з використанням асиметричних алгоритмів;
- цифровий підпис інформаційних запитів від клієнта з використанням асиметричних алгоритмів;
- контроль прав доступу користувача до об'єктів системи.

1. Правила безпеки при використанні системи iFOBS.

Кожен користувач системи iFOBS є гарантом і складовою частиною системи безпеки і повинен дотримуватися таких правил:

- Не розголошуйте свій логін і паролі третім особам;
- Зберігайте Ваш особистий сертифікат і секретний ключ на зовнішньому носії інформації (дискета, накопичувачі тощо);
- Не зберігайте зовнішній носій інформації з Вашим особистим сертифікатом і ключем разом з логіном і паролями;
- Не забувайте достати зовнішній носій інформації, щойно завершите роботу з системою iFOBS;
- Встановіть антивірусне програмне забезпечення, регулярно поновлюйте антивірусну базу та регулярно здійснюйте перевірку комп'ютера на наявність вірусів та шпигунських програм.
- Обмежте доступ до комп'ютера сторонніх осіб, як фізичний, так і мережевий.
- Налаштуйте оглядач мережі Інтернет для заборони автоматичного завантаження та запуску файлів з мережі Інтернет, а також завантаження не підписаних елементів ActiveX.
- Уважно слідкуйте за повідомленнями, що виводяться на монітор комп'ютера при роботі у Системі. У випадку невідповідності їх тим, що виводяться зазвичай – повідомити Банк. Прикладом невідповідності може слугувати: нетипове вікно з іншим логотипом, прохання встановити підозріле програмне забезпечення, тощо.
- Звертати увагу на веб адресу Системи. Вона повинна починатись на „https", що свідчить про захищене з'єднання.
- Взяти до уваги, що Банк не здійснює розсилку електронних листів з проханням надати конфіденційну інформацію про паролі, тощо, або таких, що містять комп'ютерні програми.
- Змінювати Пароль не рідше ніж 1 (один) раз на 3 (три) місяці.

- Контролювати розмір залишку по своїх Рахунках та його відповідність виконаним операціям.
- Клієнт усвідомлює, що інформація надана на адресу електронної пошти, передається відкритими каналами Інтернет зв'язку та може стати відомою третім особам без відома на те Клієнта або Банку. При цьому Банк не несе відповідальності за збитки, завдані Клієнту у разі такого розголошення інформації.
- Після закінчення роботи в Системі, Користувач повинен вийти з неї, натиснувши «Вихід», та не залишати вікно Системи відкритим.
- Для роботи в Системі Користувачу бажано використовувати власний комп'ютер. Використання комп'ютера, до якого мають доступ інші особи, пов'язане із певними ризиками, описаними вище.
- На комп'ютері, із якого здійснюється доступ до Системи, рекомендується використовувати тільки ліцензійне програмне забезпечення.
- Застосовуйте інші рекомендації Банку з провадження безпеки й цілісності інформації при роботі з системою iFOBS.

Система iFOBS ідентифікує користувача по логіну, паролю на вхід у систему, секретному ключу й паролю на нього. Для запобігання несанкціонованого доступу до Вашої конфіденційної інформації не розголошуйте свої реквізити на вхід до системи третім особам.

Кожному користувачеві Банк видає:

- логін – логін користувача;
- пароль – пароль на вхід до систему;
- пароль на секретний ключ;
- зовнішній носій інформації, що містить первинний сертифікат і секретний ключ.

При першому вході з цими реквізитами система iFOBS автоматично ініціює процес створення нового сертифіката й секретного ключа. Так само, з метою безпеки, необхідно змінити пароль на вхід до системи.

Строк дії Ключів встановлюється Банком. Незважаючи на це, Клієнт має право виконувати позапланову зміну Ключів у порядку, визначеному Договором про Клієнт-Банк. Система iFOBS наполегливо рекомендує користувачеві періодично запускати процес створення нового сертифіката й секретного ключа по закінченню терміну дії попередніх.

Система iFOBS фіксує всі спроби зміни й підбору пароля на вхід до системи.

При генерації/перегенерації робочого сертифіката й секретного ключа, необхідно вказувати шлях на той носій інформації, з якого були прочитані первинні дані.

Не довіряйте стороннім особам користуватися Вашим особистим сертифікатом і секретним ключем для підписання документів за допомогою функції «від імені».

Однією з функцій системи iFOBS під час підписання документів є: «Підписати від імені…». Дана функція системи дозволяє скоротити час на підготовку документів для відправлення в Банк. Не довіряйте виконувати цю операцію від Вашого імені іншим користувачем системи – завжди самостійно вводьте логін і пароль, а також самостійно підключайте зовнішній носій з Вашим особистим сертифікатом і секретним ключем. Після завершенню виконання операції не забувайте Ваш зовнішній носій на комп'ютері іншого користувача.

Не рекомендується користувачеві працювати із системою iFOBS:

- в інтернет-кафе й інших подібних місцях, де немає гарантії того, що за діями користувача не стежить стороння людина;

- у місцях, де встановлені пристрої відео спостереження, за допомогою яких можна одержати інформацію про паролі користувача;
- якщо немає впевненості в безпеці використовуваного програмного забезпечення (наявність вірусів, спеціальних програм, що надсилають паролі користувача третім особам і т.п.).

У випадку виявлення Вами несанкціонованого Електронного документу або спроби несанкціонованого доступу до Системи, **негайно повідомте про це Банк, зателефонувавши за тел.: (044) 291-60-96 з вимогою блокування облікового запису або персонального ключа ЕЦП, що були скомпрометовані. Для виконання зазначеної дії Клієнт має вказати кодове слово (зазначається у заяві на підключення до системи, додаток 1).** Блокування облікового запису або персонального ключа ЕЦП здійснюється до 10-00 наступного банківського дня.

До 10-00 наступного банківського дня Клієнт має надати до Банку у письмовому вигляді лист-повідомлення про несанкціонований переказ коштів та лист-згоду на взаємодію із правоохоронними органами з метою реагування на протиправні дії. У разі не надання Клієнтом відповідних листів у письмовому вигляді, обліковий запис та ключ ЕЦП будуть автоматично розблоковані.

2. Блокування електронних ключів

Банк може виконати блокування електронних ключів або облікових записів Клієнта у разі виявлення таких фактів:

- Користування системою iFOBS осіб, які не мають право користуватися або не уповноважені директором організації.
- Підозра у несанкціонованому доступі або несанкціонованому списанні коштів.
- Ненадійне зберігання клієнтом ключів або ключової дискети.
- Ненадання до Банку інформації щодо змін в установчих документах Клієнта, що зберігаються в справі з юридичного оформлення рахунку, зміни свого місцезнаходження, змін у складі керівництва (осіб, включених до карток із зразками підписів), змін власників Клієнта, зміни номера телефону організації.
- Закінчення строку (припинення) дії ключа.
- Втрати чинності чи визнання недійсними поданих документів.
- За дзвінком клієнта.
- Клієнт розірвав «Договір про розрахункове обслуговування шляхом здійснення електронних платежів».
- Банк не одержав від Клієнта плату за надані послуги з розрахункового обслуговування за допомогою системи «Клієнт-Банк» за тарифами, що встановлюються Банком.

Після тричі невірно введеного пароля на вхід до системи відбувається автоматичне блокування доступу до системи iFOBS.

3. Дії, які повинен виконати Клієнт для забезпечення роботи в системи iFOBS

3.1. Для підключення до системи iFOBS Клієнт повинен:

3.1.1. Підписати Додаткову угоду на банківське обслуговування по каналах зв'язку „Клієнт-Банк" (iFOBS) до Договору банківського рахунку та здійснення розрахунково-касового обслуговування (далі – Додаткова угода).

3.1.2. Клієнт, посадові особи якого мають право підпису на розрахункових документах, сформованих щодо Рахунків Клієнта, відкритих в Банку (вид підпису "перший" або "другий", тобто Підписувач), та які зазначені у відповідній картці із

зразками підписів та відбитком печатки та/або кожний працівник Клієнта, якому Клієнт надає доступ до Комплексу та право здійснювати певні дії, спрямовані на отримання Клієнтом послуг, передбачених Додатковою угодою, подає заяву встановленого зразку (додаток 1) на підключення до системи КБ.

3.1.3. Після підписання Додаткової угоди та подання заяв отримати від Банку на підставі Акту введення системи в експлуатацію:

- логін користувача;
- пароль на вхід до системи;
- пароль на секретний ключ;
- зовнішній носій інформації, що містить первинний сертифікат і секретний ключ;
- інсталяційний файл для встановлення системи з документацією.

3.1.4. Запустити інсталяційний файл та здійснити встановлення системи. При першому вході система iFOBS автоматично ініціює процес створення нового сертифіката й секретного ключа. Ідентично система запропонує змінити пароль на вхід до системи.

3.1.5. Для активації роботи системи надати Банку підписаний та завірений печаткою організації СЕРТИФІКАТ ВІДКРИТОГО КЛЮЧА ЕЦП КЛІЄНТА (додаток 3) кожної посадової особи Клієнта, згідно з заявою на підключення до системи.

3.2. Зміна Ключів

3.2.1. У разі зміни підписів посадових осіб у картках зі зразками підписів та відбитком печатки Клієнт у день надання до Банку нової картки зі зразками підписів та відбитком печатки зобов'язаний:

3.2.1.1. Надати в Банк заяву встановленого зразку (додаток 2) на підключення до системи КБ.

3.2.1.2. На підставі Акту введення системи в експлуатацію отримати від Банку: логін користувача, пароль на вхід до системи, пароль на секретний ключ, зовнішній носій інформації, що містить первинний сертифікат і секретний ключ, а також інсталяційний файл для встановлення системи з документацією. Сертифікат та секретний ключ формується та засвідчується у порядку, визначеному п.п.3.1.4-3.1.5 цього регламенту.

Після отримання Сертифікатів на Ключі нових посадових осіб Клієнта, Банк блокує Ключі осіб, які не входять в перелік посадових осіб, визначених в новій картці із зразками підписів та відбитком печатки.

3.2.2. Зміна Ключів посадових осіб Клієнта з інших підстав здійснюється у порядку, визначеному п.п.3.2.1.1 та 3.2.1.2 цього регламенту.

3.3. Втрата паролю на систему

Після тричі невірно введеного пароля доступ до системи автоматично блокується.

У випадку втрати паролю або блокування доступу до системи Клієнту необхідно надати до Банку підписаний керівником та завірений печаткою організації лист з проханням перегенерувати пароль для вказаного користувача та розблокування системи КБ.

В листі обов’язково вказати П.І.П/б користувача, контактний телефон користувача.

Додаток 1

Начальнику ОПЕРУ/
Начальнику відділення
ПАТ «ВЕРНУМ БАНК» /
Начальнику Управління ІТ
ПАТ «ВЕРНУМ БАНК»

__._____. 20___р.

ЗАЯВКА

Просимо надати послуги з інсталяції та налаштування ПЗ “iFOBS”

Найменування клієнта		
Контрагент №		
Дата подачі заявки		
Контактна особа (П.І.П/б, телефон)		
Кодове слово		
Право першого підпису	Посада	П.І.П/б
Право другого підпису	Посада	П.І.П/б

Надання прав доступу до рахунків:

Номер рахунку	**Валюта**	**Перегляд**	**Дебетування**	**Прийом документів за наступну дату**

М.П. _____ Керівник

Відмітка Банка про отримання: _____ _____ _____
(П.І.П/б) (Підпис) (Дата)

Відмітка Банка про виконання _____ _____ _____
(П.І.П/б) (Підпис) (Дата)

Додаток №2

Начальнику ОПЕРУ/
Начальнику відділення
ПАТ «ВЕРНУМ БАНК» /
Начальнику Управління ІТ
ПАТ «ВЕРНУМ БАНК»

„___” _____ 20___ р.

ЗАЯВКА

Просимо змінити права доступу до рахунків:

Найменування клієнта		
Контрагент №		
Дата подачі заявки		
Контактна персона (П.І.П/б, телефон)		
Кодове слово		
Право першого підпису	Посада	П.І.П/б
Право другого підпису	Посада	П.І.П/б

Надання прав доступу до рахунків:

Номер рахунку	**Валюта**	**Перегляд**	**Дебетування**	**Прийом документів за наступну дату**

_____ Керівник

М.П.

Відмітка Банка про отримання: _____ _____ _____
(П.І.П/б) (Підпис) (Дата)

Відмітка Банка про виконання _____ _____ _____
(П.І.П/б) (Підпис) (Дата)

Додаток 3

Інформація про відкриті ключі користувача (сертифікат)

Клієнт:

№ сертифіката: _____

Найменування: _____

Ідентифікатор клієнта: _____

Адреса:

Телефон:

Користувач: **ТИП ПІДПИСУ**

П.І.Б. _____

Ідентифікатор користувача: _____

EMAIL:

Телефон:

Хеш відкритого ключа RSA

_____

Керівник організації _____ (підпис, дата, відбиток печатки)	Уповноважений представник банку _____ (підпис, дата, відбиток печатки)