Інформація про безпеку системи iFOBS

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

- обов'язкова авторизація і автентифікація користувачів;
- протоколювання усіх дій користувачів у системі;
- обмін даними лише за стандартними інтерфейсами;
- захист каналу передачі даних на підставі протоколу SSL v3.0;
- цифровий підпис документів із використанням асиметричних алгоритмів;
- цифровий підпис інформаційних запитів від клієнта із застосуванням асиметричних алгоритмів;
- контроль прав доступу користувача до об'єктів системи.

Кожен користувач системи iFOBS – є гарантом і складовою частиною системи безпеки та має дотримуватися таких правил:

- не розголошувати свої логін і паролі третім особам;
- зберігати свій особистий сертифікат і секретний ключ на зовнішньому носієві інформації (дискета, накопичувач на флеш-пам'яті тощо);
- не зберігати зовнішній носій інформації зі своїми особистим сертифікатом та ключем разом з логіном і паролями;
- не довіряти стороннім особам користуватися, наданими йому особистими сертифікатом і секретним ключем для підписання документів «від імені»;
- користуватися кнопкою «Вихід» для завершення сеансу роботи з системою;
- вилучати зовнішній носій інформації, після завершення роботи з системою iFOBS;
- застосовувати інші рекомендації Банку із забезпечення безпеки та цілісності інформації під час роботи з системою iFOBS.

Система iFOBS ідентифікує користувача за логіном, паролем на вхід в систему, секретним ключем та паролем до нього. Щоб уникнути несанкціонованого доступу до конфіденційної інформації не можна розголошувати свої реквізити на вхід в систему третім особам.

Кожному користувачеві Банк видає:

- логін - ім'я користувача;
- пароль - пароль на вхід до системи;
- пароль до секретного ключа,
- зовнішній носій інформації, що містить первинний сертифікат і секретний ключ.

Під час першого входу з цими реквізитами система iFOBS автоматично ініціює процес створення нового сертифікату та секретного ключа. Також, з метою безпеки, потрібно змінити пароль на вхід в систему.

Надалі система iFOBS періодично наполегливо рекомендує користувачеві запустити процес створення нового сертифіката та секретного ключа після закінчення терміну дії попередніх.

Система iFOBS фіксує всі спроби зміни та підбору пароля на вхід в систему.

Банк видає первинні сертифікати і ключі на зовнішньому носії інформації (дискета, накопичувачі на флеш-пам'яті тощо).

Зберігання такої інформації на зовнішніх носіях забезпечує не тільки захист конфіденційної інформації в системі iFOBS, але і збереження сертифікатів та секретних ключів під час раптових збоїв роботи комп'ютера.

Під час генерації/перегенерації робочого сертифіката й секретного ключа, необхідно указувати шлях на той носій інформації, з якого були зчитані первинні дані.

Слід пам’ятати, що у разі втрати зовнішнього носія інформації з особистим сертифікатом та ключем разом з логіном і паролями – цією інформацією можуть скористатися сторонні особи у своїх цілях.

Однією з функцій системи iFOBS під час підписання документів є функція «Підписати від імені ...». Ця функція дозволяє зменшити час на підготовку документів для надсилання до Банку. Не варто довіряти виконувати цю операцію від Вашого імені іншим користувачем системи – завжди треба самостійно вводити логін і пароль та підключати зовнішній носій з особистим сертифікатом і секретним ключем.

Після закінчення операції не залишати зовнішній носій під’єднаним до комп'ютера іншого користувача.

Відволікання від комп'ютера при активному вході в систему, без завершення сеансу роботи з програмою, може спровокувати третю особу скористатися відповідною ситуацією ...

Застосування цих та інших рекомендацій із забезпечення безпеки інформації під час роботи з системою iFOBS буде вагомим внеском щодо запобігання витоку конфіденційної інформації та крадіжки коштів.

Розробники не рекомендують користувачеві працювати з системою iFOBS:

- в інтернет-кафе та інших подібних місцях, де немає гарантії того, що за діями користувача не стежить стороння особа;
- в місцях, де встановлені пристрої відеоспостереження, за допомогою яких можна отримати інформацію про паролі користувача;
- якщо немає впевненості в безпеці використовуваного програмного забезпечення (наявність вірусів, спеціальних програм, що надсилають паролі користувача третім особам тощо).

Забезпечення безпеки при роботі через Інтернет

Безпека обміну даними під час роботи в мережі Інтернет досягається на рівні взаємної автентифікації учасників обміну даними.

Клієнтська частина для встановлення з'єднання передає на сервер запит, підписаний цифровим підписом користувача, після чого бібліотеки криптографічного захисту формують необхідні секретні параметри і ключі та підтверджують встановлення з'єднання. Таким чином, кожне з'єднання має унікальні параметри і дозволяє однозначно ідентифікувати учасників обміну даними.

Обмін даними може бути розпочатий тільки після встановлення криптографічного зв'язку між вузлами «Клієнт» і «Сервер». Весь обмін даними між клієнтом і сервером системи, включно передачу на сервер автентичних повноважень клієнта (паролі) для реєстрації та допуску до даних і операцій, виконується в зашифрованому вигляді.

Операції шифрування/розшифрування даних забезпечуються бібліотеками криптографічного захисту та виконуються на прикладному рівні, в процесі підготовки даних для передачі в Банк.

Права користувача

Залежно від режиму роботи, указаного в договорі на підключення та обслуговування клієнта системи iFOBS, користувачеві може бути наданий повний або обмежений доступ до меню системи iFOBS, рахунків, прав виконувати операції або ж лише для перегляду інформації.

Так само можуть бути обумовлені обмеження прав користувача, наприклад, користувач має право готувати документи, але не має право їх підписувати.

Для внесення змін до прав користувача необхідно звернутися до адміністратора системи iFOBS Банку.