

I. Для забезпечення безпечної роботи в системі «Інтернет-Клієнт-Банк» Банк рекомендує Клієнтам дотримуватись наступних правил:

- ✓ утримуватись від використання комп'ютера, з якого виконується робота в системі «Інтернет-Клієнт-Банк» для розваг та серфінгу в мережі Інтернет;
- ✓ встановити антивірусне ПЗ (наприклад KAV, KIS, NOD32 тощо), регулярно поновлювати антивірусну базу та постійно проводити перевірку системи на наявність вірусів та шпигунських програм (троянів, кейлогерів);
- ✓ обмежити доступ до комп'ютера сторонніх осіб, як фізичний, так і мережевий;
- ✓ не тримати особисті (таємні) ключі на жорстких дисках комп'ютера, а тільки на зовнішніх носіях (Smart-card, дискета, USB Flash Drive, CD, тощо) та забезпечити їх надійне зберігання;
- ✓ для унеможливлення викрадення (копіювання) таємного ключа рекомендуємо використовувати USB - токен;
- ✓ після закінчення роботи с системою «Інтернет-Клієнт-Банк» обов'язково виймати зовнішні носії (Smart-card, дискета, USB Flash Drive, CD, тощо) з таємними ключами с системного блоку комп'ютера;
- ✓ не розголошувати паролі доступу до таємних ключів, не записувати їх та не зберігати разом з носієм ключової інформації;
- ✓ встановлювати поновлення безпеки операційної системи (бажано в автоматичному режимі);
- ✓ налаштувати оглядач мережі Інтернет, а саме заборонити: автоматичне завантаження файлів з мережі Інтернет, автоматичний запуск файлів з мережі Інтернет, завантаження не підписаних елементів ActiveX;
- ✓ не працювати на комп'ютері з правами адміністратора;
- ✓ у випадку компрометації або спроби компрометації таємних ключів або комп'ютера, звільнення відповідального співробітника або ІТ спеціаліста Клієнта, який мав доступ до вказаного комп'ютера або таємних ключів необхідно терміново повідомити банківську установу для заблокування ключів ЕЦП, згенерувати та зареєструвати нові ключі ЕЦП;
- ✓ при будь-якій підозрі при роботі з «Інтернет-Клієнт-Банком» – необхідно терміново повідомити банківську установу для заблокування ключів ЕЦП та згенерувати та зареєструвати нові ключі ЕЦП;
- ✓ уважно слідкувати за повідомленнями, що виводяться на монітор комп'ютера при роботі в системі «Інтернет-Клієнт-Банк». У випадку невідповідності їх тим, які виводяться зазвичай – повідомити банківську установу. Прикладом невідповідності може слугувати: нетипове вікно з іншим логотипом, при виборі ключа не

відображається назва ключа, прохання встановити підозріле програмне забезпечення, тощо;

✓ при роботі через сайт системи звертайте увагу на адресу сайту. Вона повинна починатись на https – що свідчить про захищене з'єднання;

Застереження: Банк ніколи не здійснює розсилку електронних листів з проханням надати конфіденційну інформацію (паролі, доступ до таємних (особистих) ключів, тощо) або таких, що містять комп'ютерні програми.

II. Рекомендації по створенню надійних (стійких) паролів.

✓ При виборі пароля користувачеві необхідно керуватися запропонованими правилами:

✓ не використовувати атрибути користувача - імена і прізвища користувачів, пам'ятні дати і будь-яку іншу досягну інформацію (наприклад, номери телефонів, адреси і тому подібне);

✓ заборонено використання комбінації символів / знаків з клавішею Ctrl; паролі повинні складатися шляхом комбінації двох або більше слів;

✓ довжина пароля повинна складати не менше 8 символів;

✓ пароль повинен містити не менш 3-х з 4-х наступних символів – заголовні букви, прописні букви, цифри, спецсимволи;

✓ заборонено використовувати слова з реальних словників (наприклад, англійський, французький, японський і тому подібне) і вигаданих (наприклад, ельфійський Р. Р. Толкиена і тому подібне); пароль необхідно змінювати не рідше ніж кожні 30 календарних днів.

Один з можливих варіантів (прикладів) вибору пароля: складіть список простих слів, наприклад, квітка, аркуш, ручка і так далі виберіть перші три букви і загальна кількість букв в словах; об'єднаєте отримані результати, додайте одну цифру і один із спеціальних символів ("&'{[-_@]]}\$*% !:/ ;, ?+)=) і зробіть одну з букв заголовної; при зміні пароля використовуйте приведені рекомендації з іншим набором слів. Приклад: яблуко, груша і наберіть їх в латинському регістрі.

Увага! Не використовуйте як пароль наведені приклади! Безумовно, для створення пароля можуть використовуватися інші методи створення надійного пароля, але вибраний пароль не має бути слабкіше запропонованій мірі стійкості.

Увага! Пам'ятаєте, що ні за яких обставин Ваш пароль не має бути відомий третім особам, ніхто не має права вимагати від Вас розкриття пароля, навіть співробітники Банку.

III. Використання пристрою «USB-токен» в системі «Інтернет-Клієнт-Банк».

Рекомендовано Клієнту використовувати Usb-токен для генерації особистих ключів ЕЦП.

Usb-токен генерує особисті ключі усередині себе, забезпечує їх захищене зберігання і формує ЕЦП під електронними документами усередині пристрою згідно ДСТУ 4145.

Підтримка Usb-токенів забезпечена для всього спектру настільних платформ –

Windows, Linux і Mac OS X. Робота Usb-токенів підтримується за основними каналами обслуговування корпоративних клієнтів системи «іbank 2 UA».

У одному Usb-токені може зберігатися до 64-х особистих ключів. Можливе зберігання особистих ключів ЕЦП відповідальних співробітників різних корпоративних клієнтів. Забезпечується одночасна робота відразу з декількома підключеними до комп'ютера Usb-токенами.

IV. Використання сервісу IP – фільтрація

3.4.1. Підключення, відключення сервісу IP – фільтрація.

У Систему вбудований механізм обмеження доступу клієнтів заданими ір-адресами. Для посилення заходів безпеки в разі постійної роботи з одних робочих місць рекомендується підключити сервіс "ір-фільтрація" в системі «Інтернет-Клієнт-Банк». Даний механізм обмеження доступу по ір-адресах є індивідуальним для кожного Клієнта і налаштовується співробітником Банку за письмовою заявою клієнта з зазначенням переліку ір-адрес комп'ютерів клієнта, з яких здійснюватиметься підключення до Системи. Якщо спроба входу в АРМ здійснюється із забороненої ір-адреси, видається повідомлення про помилку «Доступ заборонений», вхід в АРМ неможливий.

Існує можливість налаштування обмеження входу в Систему, використовуючи наступні ір-фільтри:

✓ Вхід лише з ір-адрес українських провайдерів. Застосовується для обмеження доступу до Системи з ір-адрес зарубіжних провайдерів, оскільки досить часто з цих ір-адрес здійснюється несанкціонований вхід в Систему.

✓ Вхід лише через модемний пул. Застосовується технологія Dial-up зв'язку для підключення до АРМ «PC-banking» Системи за допомогою модему через телефонну лінію.

✓ Вхід лише із заданих ір-адрес (індивідуальний список ір-адрес, з яких дозволено працювати вказаному клієнтові). Перелік ір-адрес надає клієнт.

Якщо Клієнт використовує для доступу до Системи ір-адреси іноземних провайдерів (буває за кордоном, де використовує для доступу до Системи місцеві інтернет - мережі), то необхідно надати в Банк заяву на відключення сервісу "ір-фільтрація", за встановленою типовою формою.

Увага! Рекомендується уточнювати і погоджувати перелік ір-адрес із службою технічної підтримки. Якщо використовується великий перелік ір-адрес або ір-адреса постійно міняється в рамках діапазону, то рекомендуємо вказувати діапазон ір-адрес за допомогою маски мережі. Заява для активації сервісу підписується особами, уповноваженими на підписання договорів з боку клієнта.

Увага! Клієнт зобов'язаний ознайомити всіх своїх співробітників, що мають право на роботу в системі «Інтернет-Клієнт-Банк», з умовами обмеженого доступу з вказаних робочих станцій (комп'ютерів) і несе повну відповідальність за це.