СПЕЦПРОЕКТ

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ

Незалежна асоціація банків України

www.nabu.com.ua

Дистанційне банківське обслуговування

РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕЧНОГО КОРИСТУВАННЯ

Для забезпечення належної якості послуг та безпеки систем дистанційного банківського обслуговування банки рекомендують:

1. Використовувати лише ліцензійне програмне забезпечення на робочих місцях.
2. Використовувати ліцензійне антивірусне програмне забезпечення та своєчасно виконувати оновлення антивірусних баз.
3. За жодних обставин не зберігати таємні ключі на жорсткому диску комп'ютера. Використовувати для їх зберігання лише зовнішні носії (токени і т.п.).
4. Після закінчення роботи із системою дистанційного обслуговування та під час перерв необхідно від'єднувати носій із секретним ключем від комп'ютера.
5. Після закінчення роботи із системою дистанційного обслуговування обов'язково здійснювати вихід із системи для недопущення використання системи сторонніми особами.
6. Не використовувати будь-який віддалений доступ до робочого комп'ютера, на якому встановлено систему дистанційного обслуговування.
7. У разі будь-якої підозри на компрометацію ключів системи дистанційного банківського обслуговування необхідно негайно сповіщати про це Банк.

8. Контролювати стан Вашого поточного рахунку.
9. Не використовувати комп'ютер із встановленою системою дистанційного обслуговування для перегляду сумнівних інтернет-ресурсів та не пов'язаних з роботою, які найчастіше є джерелом поширення шкідливих програм (непомітного втручання кібершахраїв).
10. Не завантажувати та не зберігати на комп'ютері із встановленою системою дистанційного обслуговування підозрілі файли, отримані з невідомих/підозрілих джерел, надіслані електронною поштою від невідомих адресантів і т.п. Такі файли необхідно видаляти або — у разі необхідності завантаження — перевіряти антивірусною програмою.
11. Зберігати зовнішні носії ключової інформації (токени і т.п.) у сейфі.
12. Не передавати стороннім особам носії ключової інформації та не повідомляти їм паролі доступу до системи дистанційного обслуговування.
13. При виявленні/підозрі про факти доступу сторонніх осіб до ключової інформації негайно ініціювати блокування та зміну ключової інформації.
14. Не зберігати та не записувати паролі таємних ключів разом із носіями ключів (токени, usb flesh і т.п.).
15. Уникати використання для роботи із системою дистанційного обслуговування комп'ютерів, встановлених у публічних місцях, чужих ноутбуків та комп'ютерів, смартфонів та ін.
16. Не відповідати на підозрілі листи з проханням надіслати секретний ключ електронного цифрового підпису, пароль та інші конфіденційні дані!

ДОДАТКОВІ ЗАСОБИ ЗАХИСТУ

Для підвищення безпеки використання систем дистанційного обслуговування замовляйте у своєму Банку додаткові засоби захисту.

Додатковий засіб захисту	Результат від використання
Прив'язка робочого місця, на якому встановлено систему дистанційного обслуговування, за IP-адресою Клієнта на стороні Банку.	Унеможливлює доступ до використання системи з будь-якої IP-адреси, крім вказаної клієнтом.
Використання засобів для забезпечення безпечного зберігання таємних ключів — USB-токенів, SMART-карток тощо.	Унеможливлює компрометацію таємного ключа.
Використання SMS-підтвердження проведення операції.	Унеможливлює проведення операції без уведення одноразового паролю, який надходить у SMS-повідомленні.
Використання електронних пристроїв ідентифікації користувача.	Унеможливлює вхід до системі без уведення одноразового паролю, який генерується спеціальним пристроєм.

Індикатори несанкціонованого втручання в роботу комп'ютера, на якому встановлено систему дистанційного обслуговування.

1. Перебій у роботі комп'ютера, раптове перезавантаження системи.

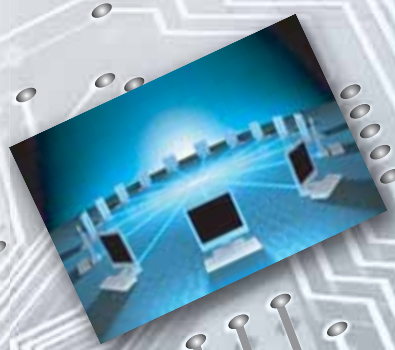
2. Неможливість або ускладнення запуску програм та додатків.

3. Наявність невідомих записів в історії входів до системи та проведення операцій.

4. Поява незрозумілих вікон, незрозуміле уповільнення дії, самостійна активність (наприклад, самостійний рух курсора комп'ютерної миші з відкриттям вікон, запуском програм та ін.).

5. Сповіщення антивірусного програмного забезпечення про виявлений вірус.

6. Підвищений трафік мережевого обміну (для адміністраторів ctrl+shift+Esc, закладка «Networking»).



Порядок дій у разі виявлення випадку несанкціонованого доступу до рахунку або підозри на компрометацію логіну, паролю чи ключа.

У разі виявлення несанкціонованого переказу коштів у системі ДБО Клієнту (потерпілому) — юридичній особі, приватному підприємцю чи іншому суб'єкту господарювання необхідно:

1. Негайно звернутися до підрозділу свого Банку, відповідального за обслуговування рахунку (до свого обслуговуючого менеджера, на Контакт-Центр, до співробітника служби банківської безпеки (за необхідності) тощо), по телефону або іншим доступним засобом зв'язку та:

   1.1. сповістити банківського працівника про факт несанкціонованого переказу коштів;

   1.2. обов'язково встановити та занотувати ПІБ, посаду банківського працівника, до якого Клієнт звертався у зв'язку з фактом несанкціонованого переказу коштів у системі ДБО;

   1.3. вимагати термінового блокування доступу будь-яких користувачів до свого рахунку через систему ДБО;

   1.4. вимагати призупинення виконання платежу;

   1.5. вимагати повернення коштів (якщо вони ще не зараховані на рахунок отримувача).

За неможливості оперативного зв'язку з Банком та за наявності технічної можливості відкликати переказ коштів з використанням іншого комп'ютера, після чого вжити заходів із блокування системи ДБО (пп 1.1 – 1.5).

2. Вимкнути комп'ютер із системою ДБО, знеструмивши його (примусово відключити електроживлення в обхід штатної процедури завершення роботи, витягти всі акумуляторні батареї з ноутбука, від'єднати шнур живлення). Якщо робота з ДБО виконується через віддалений доступ, необхідно завершити сесію.

   За відсутності можливості знеструмлення комп'ютера здійснити відключення відповідно до штатної процедури і записати зазначений факт.

   Негайно сповістити IT-підрозділ та внутрішню службу безпеки своєї компанії або директора про інцидент.

Ваша уважність є найкращим захистом!

www.anticyber.com.ua

НЕЗАЛЕЖНА АСОЦІАЦІЯ БАНКІВ УКРАЇНИ

НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

УКРАЇНА