Механізми захисту інформації в "iBank 2 UA"

Базові механізми

Система "iBank 2 UA" відноситься до систем захищеного електронного документообігу між банком і клієнтом. Електронні документи, що передаються клієнтами в банк, підписуються електронним аналогом власноручного підпису і шифруються - це гарантує надійний захист документів від підробки. Електронний документ з ЕЦП є підставою для здійснення банком фінансових операцій і, більш того, виступає доказовою базою при вирішенні конфліктної ситуації.

Для доказу авторства і підтвердження цілісності електронних документів використовуються механізми електронного цифрового підпису, які забезпечені вбудованою в систему "iBank 2 UA" криптобібліотека "Гепард 2.0". Криптобібліотека "Гепард 2.0" має експертний висновок ДСТСЗІ України і підтримує повний спектр національних стандартів ЕЦП, шифрування та інших криптоалгоритмів.

Для вирішення конфліктних ситуацій в системі "iBank 2 UA" ведуться контрольні архіви, в яких зберігаються усі електронні документи з електронними підписами клієнтів. Контрольні архіви зберігаються в банку на Сервері БД системи "iBank 2 UA".

Для забезпечення конфіденційності в системі реалізовані шифрування і контроль цілісності каналу зв'язку за допомогою SSL або GSL (SSL подібний протокол, з шифруванням ГОСТ 28147). Головні переваги захищеного мережевого протоколу - надзвичайно низький обсяг службових даних, переданих в процедурі узгодження сеансових ключів, а також невелике навантаження на процесори банківського сервера.

Для запобігання несанкціонованого доступу зловмисників до рахунків клієнтів реалізовані механізми:

- ✓ багатофакторної аутентифікації клієнтів (у вигляді додаткового підтвердження входу одноразовим паролем, отриманим по SMS, згенерованим OTP-токеном або в додатку "Google Authenticator")
- ✓ підтвердження перед відправкою в банк документів (документи підтверджуються одноразовими паролями, отриманими по SMS, згенерованими OTP-токеном або в додатку "Google Authenticator")

Для виключення випадків шахрайства при віддаленому доступі до рахунків клієнтів вбудована підтримка апаратних сховищ закритих ключів ЕЦП, спеціально створених для безпечного зберігання клієнтських даних і забезпечення високого рівня захисту електронних сервісів. У систему "iBank 2 UA" вбудована підтримка наступних видів апаратних сховищ:

- ✓ USB-токени "iBank 2 Key", "iToken" і смарт-карта "Інтегра 1.0" (розробки компанії "ДБО Софт")
- ✓ USB-токен "SecureToken318" і смарт-карта "CryptoCard 318" (розробки компанії "Автор")
- ✓ USB-токен "Кристал-1" (розробки компанії "ІІТ")
- ✓

Також для організації безпечної роботи в модулях системи використовуються штатні засоби захисту Web-браузерів, віртуальної Java-машини і вбудовані в систему додаткові механізми захисту інформації.

Додаткові механізми

В системі "iBank 2 UA" реалізовані наступні додаткові механізми безпеки:

Для додаткового захисту електронного документообігу реалізована IP-фільтрація по клієнтам. Вхід в систему "iBank 2 UA" може бути здійснений тільки в разі збігу IP-адреси (діапазону адрес) комп'ютера, що передає дані, з IP-адресою клієнта, що зберігається в списку банку. Підтримуються 2 варіанти заповнення списку дозволених IP-адрес для клієнтів:

- ✓ ручне формування списку відповідальним співробітником банку в індивідуальних

налаштуваннях для кожного клієнта
- ✓ автоматичне формування списку за допомогою запуску спеціальної утиліти, яка аналізує журнали Сервера Додатків "iBank 2 UA" і виділяє найчастіше використовувані IP-адреси для кожного клієнта

Додатково ведеться протоколювання спроб доступу з заборонених IP-адрес.

Для виявлення підозрілих документів, відправлених клієнтами через систему "iBank 2 UA", реалізований додатковий сервіс, який проводить автоматичний аналіз усіх документів за наступним алгоритмом:

- ✓ реквізити отримувача платежу порівнюються з заданими банком «чорним» і «білим» списками, в «чорному» списку можуть бути задані як конкретні реквізити (наприклад, рахунки одержувачів, раніше фігурували в інцидентах), так і їх маски (наприклад, маска рахунку 2625 – картковий рахунок фіз.особи)
- ✓ якщо реквізити отримувача відповідають записам в «чорному» списку і не вказані в «білому» списку, то платіж позначається як підозрілий і не вивантажується в систему банку, в іншому випадку - платіж успішно вивантажується в систему банку

Підозрілі документи знаходяться в статусі «Підозрілий» і вимагають ручної обробки співробітниками банку в системі "iBank 2 UA".

Для оперативного інформування відповідальних співробітників банку про появу підозрілих документів рекомендується використовувати серверний модуль "Тікер для операціоністів".

Для додаткового контролю клієнтами руху грошових коштів компанії реалізовано оперативне SMS-інформування про наступні події:

- ✓ вхід в систему "iBank 2 UA"
- ✓ списання коштів з рахунків компанії
- ✓ зарахування коштів на рахунки компанії

Отримання SMS дозволить клієнтам своєчасно дізнатися про несанкціонований доступ та оперативно вжити необхідних заходів.

Для виявлення шкідливих програм, таких як трояни і віруси, на робочих станціях клієнтів в системі "iBank 2 UA" реалізований додатковий механізм "Trojan-detector".

Для виявлення шахрайських операцій в системі "iBank 2 UA" реалізований додатковий механізм контролю робочого середовища клієнта "Device FingerPrint". Механізм заснований на зборі інформації про робоче середовище клієнта і збереженні інформації в системі у вигляді набору хеш-функцій. Це дозволяє банку відстежувати зміни робочого середовища клієнтів за допомогою зовнішньої системи Fraud-моніторингу електронних платежів, і, в результаті, виявляти розкрадання, що проходять за типовими сценаріями (наприклад, копіювання файлу з персональними ключами ЕЦП, віддалений доступ шкідливої програми до робочого місця клієнта по RDP і т.д.).

Дані механізми є допоміжними і повинні використовуватися на додаток до вище перерахованих технологій безпеки.

Комплексне застосування додаткових механізмів безпеки дозволяє істотно знизити ймовірність успішного викрадення коштів клієнта