автоперевізники мають використовувати тахографи [Електронний ресурс] / Урядовий портал. Єдиний веб-портал органів виконавчої влади України – Режим доступу: http://old.kmu.gov.ua/kmu/control/uk/publish/article?art_id =244865811& cat_id= 248446163 (дата звернення 28.10.2018). – Назва з екрана.

4. Укртрансінспекція: Більшість автомобільних перевізників не використовують тахографи [Електронний ресурс] / Урядовий портал. Єдиний веб-портал органів виконавчої влади України – Режим доступу: https://www.kmu.gov.ua/ua/news/247394736 (дата звернення 28.10.2018). – Назва з екрана.

5. Цифровий тахограф - безпека водія [Електронний ресурс] / Сайт фірми RENAMAX TIR service, м.Рівне – Режим доступу: http://stenck.com/?p=tahografy (дата звернення 30.09.2018). – Назва з екрана.

6. Тахографи цифрові та аналогові [Електронний ресурс] / Сайт фірми RENAMAX TIR service, м.Рівне – Режим доступу: http://goldenpages.rv.ua/svitaho (дата звернення 30.09.2018). – Назва з екрана.

7. Цифровий тахограф Smartach [Електронний ресурс] / Сайт фірми "КАМ"– Режим доступу: http://kam.com.ua/takhografy/digital-tahograf.html (дата звернення 25.10.2018). – Назва з екрана. Фирма

8. Лемешонок С. Все о тахографах [Електронний ресурс] / Веб сайт Лемешонка С – Режим доступу: http://tachograph.su/content/actia-smartach (дата звернення 28.10.2018). – Назва з екрана.

9. Тахограф Flextach [Електронний ресурс] / Сайт фірми RENAMAX TIR service, м.Рівне – Режим доступу: https://svitaho.business-guide.com.ua/ products/unit?pid=182421 (дата звернення 30.09.2018). – Назва з екрана.

10. Цифровой тахограф SmarTach Actia [Електронний ресурс] / Сайт фірми Allbiz, м.Львів – Режим доступу: https://ua.all.biz/cifrovoj-tahograf-smartach-actia-g13313414 (дата звернення 25.10.2018). – Назва з екрана.

11. Міжнародні перевезення: особливості організації [Електронний ресурс] / Веб-портал golovbukh.ua – Режим доступу: https://www.golovbukh.ua/article/6113-qqq-17-m3-03-03-2017-organzatsya-mjnarodnih-perevezen (дата звернення 4.11.2018). – Назва з екрана.

Організація додаткового захисту в компоненті "рс-банкінг" системи ibank 2 ua

Грицаюк Є. С., Тітова В.Ю., Чешун В. М.
Хмельницький національний університет

РС-Банкінг являє собою компоненту системи iBank 2 UA і призначений для обслуговування в режимі офлайн клієнтів – юридичних і фізичних осіб. Дана компонента реалізована у вигляді додатку, що запускається локально на машині клієнта. Модуль РС-Банкінг повністю

аналогічний Internet-Банкінг - різниця в тому, що клієнт працює з фінансовими клієнтами локально, а обмін інформацією між клієнтом і банком відбувається в ході короткочасних сеансів зв'язку по Інтернету – синхронізація. Частота проведення синхронізації обирається клієнтом.

Загалом, синхронізація є обміном інформацією між клієнтом і сервером банку в ході короткочасного з'єднання через Інтернет або модемне з'єднання. В процесі синхронізації відбувається відправка створених і відредагованих клієнтом документів, оновлення статусів документів, довідників системи і отримання виписок по рахунках клієнта, а також оновлення версії РС-банкінг (за наявності такого).

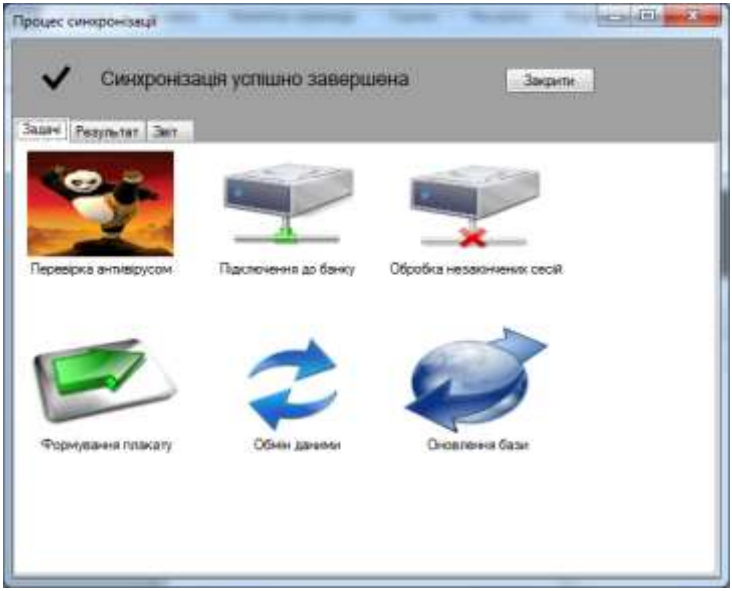
У процесі синхронізації зовнішній носій з секретним ключем ЕЦП повинен знаходитися в комп'ютері користувача.

Для проведення синхронізації слід натиснути кнопку Синхронізація на панелі інструментів. На екрані з’явиться вікно Синхронізація з банком. Зовнішній вигляд АРМа РС-банкінг для корпоративних клієнтів представлений на рисунку 1. Для початку обміну даними у вікні Синхронізація з банком натисніть кнопку Синхронізація. На екрані відкриється вікно Процес синхронізації, в якому відображається процес синхронізації з банком, яке складається з трьох вкладок (рис. 2-3).

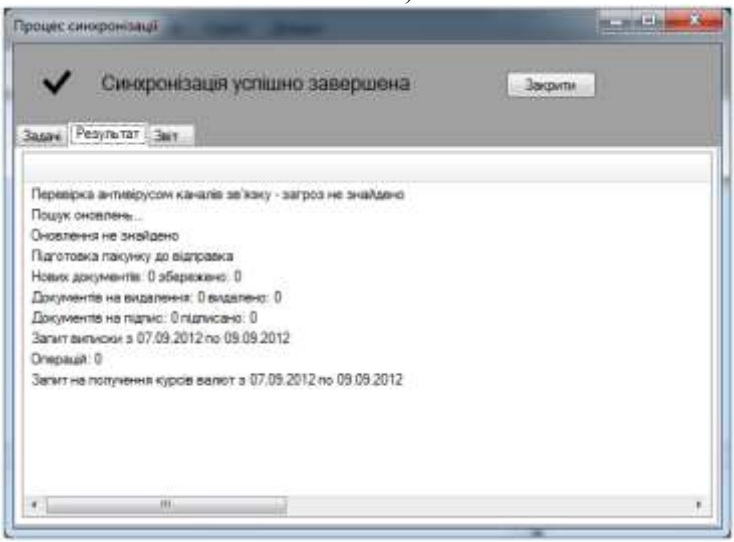
Рисунок 1 - АРМ РС-Банкінг для корпоративних клієнтів

Після завершення обміну даних у вікні Процес синхронізації слід натиснути кнопку Закрити.

Для того, щоб захистити свій комп’ютер від несанкціонованого доступу до ваших даних під час синхронізації потрібно натиснути кнопку Режим посиленої безпеки синхронізації. В результаті цього з’явиться діалогове вікно, в якому ви можете обрати або скасувати Режим посиленої безпеки синхронізації, як показано на рисунку 4.



а)



б)

Рисунок 2 - Вікна процесу синхронізації: а) задачі – перевірка антивірусом каналів зв'язку успішно). б) результат – відображається результат синхронізації окремих документів та звітів;

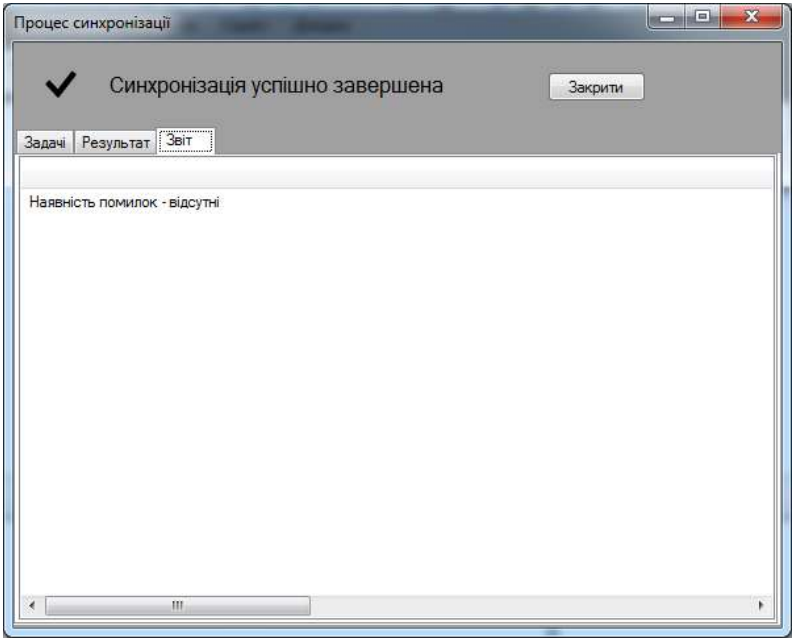


Рисунок 3 - Вікна процесу синхронізації: звіт – відображається інформація про помилки, вхідні листи, відкинуті документи.

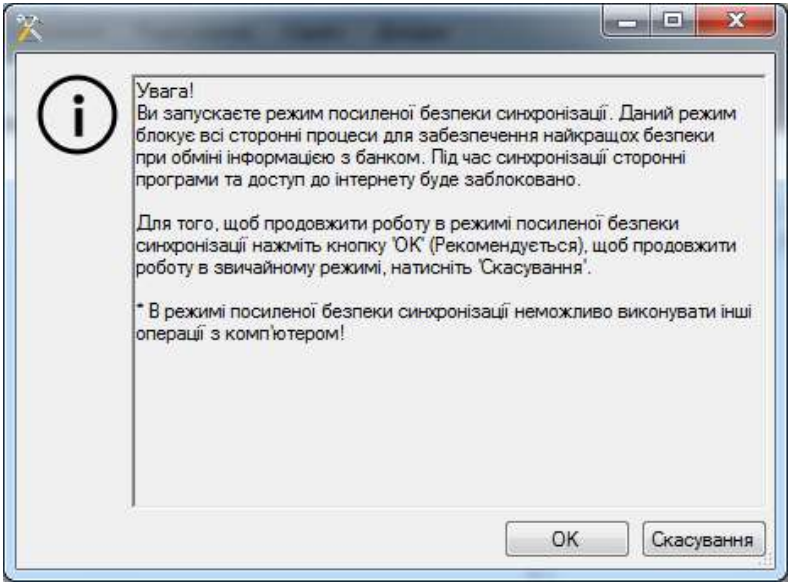


Рисунок 4 - Режим посиленої безпеки синхронізації

Основною відмінністю РС-Банкінгу від Internet-Банкінгу є відсутність необхідності підтримувати постійне з'єднання з сервером банку в процесі роботи і, як наслідок, більш низькі вимоги до каналів зв'язку. Вибір клієнтом моменту синхронізації також дозволяє працювати з iBank 2 UA при низькій або нестійкій якості зв'язку.

Для роботи з модулем РС-Банкінг корпоративні клієнти банку використовують автоматизоване робоче місце (АРМ) РС-Банкінг для корпоративних клієнтів. В АРМі РС-Банкінг для корпоративних клієнтів, що реалізований у вигляді додатку, що локально запускається, здійснюється реєстрація клієнта, адміністрування ключів ЕЦП клієнта і поточна робота клієнтів банку. Крім того, реєстрацію та адміністрування ключів ЕЦП клієнта РС-Банкінгау можна здійснювати за допомогою АРМ Реєстратора, реалізованого у вигляді java-аплету.

Скретч-карти і OTP-токени – засоби додаткової авторизації операцій в Системі «Клієнт-Банк». Вони містять шестизначні одноразові коди, що підтверджують Ваші витратні операції.

При підключенні послуги сервер Системи «Клієнт-Банк» буде підраховувати суму всіх видаткових операцій за Вашим розрахунковому рахунку з моменту останнього введення коду. При перевищенні порогової суми, визначеної Вами в Банку заздалегідь, сервер запросить у Вас в інтерфейсі Системи додатковий одноразовий код (рис. 5).

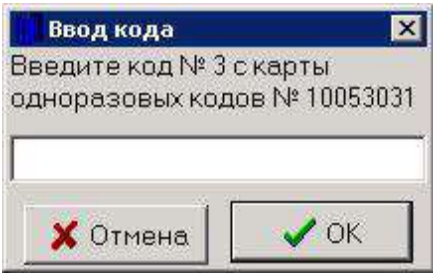


Рисунок 5 – Вікно для введення коду

Кожен код використовується тільки один раз.

Скретч-карта – пластикова картка розміру 8х5 см з 114 кодами, закритими типографічною плівкою (видаються за Вашою заявою безкоштовно), показана на рисунку 6.

При запиті чергового коду Вам необхідно стерти захисний шар з не обхідного коду будь-яким підходящим предметом і ввести його в вікно «Введення коду» в програмі.

Після закінчення 114 кодів необхідно отримати наступну карту.

Рисунок 6 - Скретч-картка

Якщо Ви здійснюєте багато операцій по списанню грошових коштів, Ви можете отримати кілька скретч-карт відразу. У цьому випадку для активації подальшої карти, необхідно буде на діючій карті стерти захисний шар над «Кодом активації наступної карти» і ввести його у вікно програми.

OTP-токен (модель – Aladdin eToken PASS) дозволяє не піклуватися про кількість одноразових кодів авторизації. Це брелок з екраном, що формує чер-гові одноразові коди без обмежень по кількості на основі унікального ключа, розміщеного в його мікропроцесорі. Після натискання на кнопку черговий код відображається протягом 20 секунд на екрані, після чого екран вимикається, приклад точену показаний на рисунку 7.

Рисунок 7 - OTP-токен

Для захисту від випадкових натиснень Система зможе прийняти від Вас не тільки поточний код, але і декілька наступних. Брелок видається за додатко-ву плату.

Порогове значення ліміту списань встановлюється за Вашою письмовою заявою і дозволяє гнучко налаштовувати цю перевірку. Якщо Ви залишите по-рогове значення по замовчуванню – 0 руб. – то черговий код буде запитуватися в кожному сеансі з видатковими операціями по Вашому рахунку. Якщо ж Ви направляєте багато доручень на списання невеликих грошових сум окремими сеансами, то Вам, можливо, буде зручно встановити деяке ненульове порогове значення – черговий код Система буде запитувати тільки після того, як сума списань досягне цього порога.

Передбачено два режими роботи модуля РС-Банкінгу для

корпоративних клієнтів – мережевий і звичайний. Робота в мережевому режимі аналогічна роботі в звичайному режимі, головна відмінність – в рамках одного примірника модуля підтримується одночасна робота декількох співробітників корпоратив-ного клієнта.

Механізми безпеки iBank 2 UA наступні.

Для забезпечення інформаційної безпеки в iBank 2 UA використовуються наступні механізми:

1. Електронний цифровий підпис під електронними документами – для забезпечення цілісності та автентичності інформації.

2. Механізм криптографічної аутентифікації сторін – для забезпечення захищеної взаємодії через Інтернет.

3. Шифрування даних – для забезпечення конфіденційності переданої через Інтернет інформації.

Для установки PC-Банкінгу скачайте з сайту банку дистрибутив, в якому вмонтований безкоштовний антивірус Panda. Наступним кроком потрібно запустити файл PC-Banking.exe, він вам встановлює клієнт та безкоштовний хмарний антивірус.

Для запобігання несанкціонованого доступу до Вашого комп'ютера ми пропонуємо скористатися спеціальною послугою і підписатися на антивірусні продукти Panda, які дозволять надійно захистити Ваші комп'ютери від всіх типів загроз з мінімальним впливом на швидкість роботи ПК. Проект реалізова-ний спільно з компанією Panda Security, одним зі світових лідерів в області антивірусного захисту і забезпечення інформаційної безпеки.

Щодо антивірусного ПЗ одним з найкращих варіантів, який можна використати це хмарний антивірус Panda Antivirus Pro 2013. "Хмарна" технологія Panda Security пропонує нову модель захисту, засновану на співтоваристві користувачів, де кожен робить свій внесок. Ваш комп'ютер завжди буде оновлений і захищений. Крім того, Ваш комп'ютер не буде обмежувати можливості виявлення, так як величезна база даних Panda для виявлення вірусів розташована в Інтернеті (в "хмарі").

Як наслідок, отримується покращений всебічний захист:

1. Захист від шпигунів, фішингу (онлайн-шахрайства), руткітів (прихованих технік зараження) і банківських троянів.

2. Захист в режимі реального часу.

3. Новий веб-фільтр для безпечної подорожі в Інтернеті.

4. Повний захист від відомих і невідомих вірусних атак.

5. Захист Ваших USB-пристроїв ("флешок") від інфекцій.

6. Файєрвол. Блокує вторгнення хакерів навіть в бездротовій мережі.

7. Режим посиленої безпеки синхронізації.

Література
1. Модуль РС - Банкинг системы iBank 2 UA: полное руководство (Версия 2.14) / М.: ООО Бифит, 2012. - 93с.
2. Особенности функционирования модуля "РС-Банкинг для корпоративных клиентов в сетевом режиме / М.: ООО Бифит, 2012. - 12с.
3. Общая информация о системе iBank 2 UA / М.: ООО Бифит, 2012. - 18с.
4. РС-Банкинг / електронний ресурс http://www.bifit.ua/decisions/pc-banking/index.html
5. Системи ELECTRONIC-BANKING / електронний ресурс http://pidruchniki.ws/13290305/bankivska_sprava/sistemi_electronic-banking

Кореляційний метод зниження похибки вимірювання потужності сигналів

Гурман І.В.
Хмельницький національний університет

Суть запропонованого підходу полягає у використанні інформації, яка міститься в фазі прийнятих сигналів, для уточнення оцінки різницю часу надходження сигналів з невідомими параметрами і на цій основі уточнення потужності прийнятих сигналів в розподілених точках прийому. У методі вимірювання сигналів [1], за обвідною сигналу або обвідною взаємокореляційної функції, запропоновано момент формування часового інтервалу, внаслідок перевищення сигналом заданого порогу, використовувати в якості попереднього наближення оцінки параметру з наступним уточненням по фазі сигналу. При цьому одночасно на інтервалі автокореляційної функції сигналу вимірюється значення несучої частоти. Подальшим розвитком даного метода є використання отриманого уточнення параметра різниці часу прийому сигналів для уточнення параметра потужності прийнятих сигналів в розподілених точках. При здійсненні попередньої оцінки різниці часу надходження імпульсного радіосигналу по його обвідній, або по максимальному значенню взаємнокореляційної функції з подальшим уточненням результату за даними вимірювання фази в точці попереднього наближення, в умовах апріорної невизначеності несучої частоти сигналу. Одночасно з вимірюванням фази сигналу додатково проводять оцінку середнього значення частоти спектру сигналу шляхом лінійного передбачення на інтервалі автокореляції сигналу [1; 2] і в подальшому визначають потужність сигналу, що відповідає уточненому значенню різниці часу.

Розвинутий метод, з врахуванням даних [1], реалізується наступним чином. Імпульсні радіосигнали, які поступають на входи вимірювача різниці часу прийому сигналу в розподілених точках прийому $U_{\grave{a}}(t)$ і $U_b(t-\tau)$,