УДК 004.021; 004.27

Послуги мобільного банкінгу та їхній захист

Христина Омелянівна Засадна,
доцент кафедри комп'ютерних технологій
Львівського інституту банківської справи
Університету банківської справи Національного банку України (м. Київ),
кандидат фізико-математичних наук, доцент

Анотація. Описано програмне забезпечення сучасних мобільних пристроїв, можливості систем мобільного банкінгу і захист послуг мобільного банкінгу, смартфон-банкінгу, планшетного банкінгу.
Ключові слова: мобільні інтернет-пристрої, мобільний банкінг, смартфон-банкінг, планшетний банкінг, захист послуг мобільного банкінгу.

Вступ. Доступ до мережі «Інтернет» сьогодні можна отримати не лише з персонального комп'ютера, а й з мобільного телефону, смартфона, планшета. Ці мобільні інтернет-пристрої активно входять у побут, оснащуються програмним забезпеченням, їхні можливості постійно розширюються. Операційні системи для мобільних пристроїв дозволяють отримати доступ до Інтернету і використовувати всі можливості мережі, у тому числі дистанційні банківські послуги – мобільний банкінг, смартфон-банкінг, планшетний банкінг.

Метою статті є дослідження можливостей дистанційних банківських послуг, які надаються з використанням мобільних пристроїв, та їх захисту.

Постановка проблеми. Мобільний банкінг сьогодні доповнює інтернет-банкінг і поки що з ним не конкурує. Але мобільний телефон став невід'ємним побутовим пристроєм людини, він повноцінно заміняє звичайний телефон, а в багатьох випадках – персональний комп'ютер і ноутбук. У найближчі роки можливий стрімкий розвиток систем мобільного банкінгу і зменшення кількості користувачів інтернет-банкінгу.

Аналіз останніх досліджень і публікацій. Інформацію про стан використання і перспективи розвитку систем мобільного банкінгу найкраще шукати в мережі «Інтернет». Дуже цікавими є публікації В. Лейбова, деяку інформацію можна знайти на сайтах банків (вона переважно стосується реклами банківських послуг і порядку їх підключення). Інформацію про захист послуг мобільного банкінгу краще шукати на сайтах фірм – розробників програмного забезпечення для банків, наприклад, Біфіт, Сайфер, Нокк та ін.

Виклад основного матеріалу дослідження. Мобільні телефони мають процесор, оперативну пам'ять для роботи операційної системи і постійну пам'ять для зберігання телефонної книги, операційної системи та її даних. Вони використовують операційну систему виробника, яка переважно є «закритою» для сторонніх розробників. У деяких моделях телефонів (Sony Ericsson, Siemens) можливості операційної системи можна розширювати патчами – окремими програмами, які усувають проблеми у програмному забезпеченні або змінюють деякі його функції. Такі оновлення доступні лише операторові мобільного зв'язку, який виступає в ролі «системного адміністратора» операційної системи мобільного телефону. Більшість моделей мобільних телефонів мають менше функцій, аніж смартфони. Розширення функціональності телефонів можливе за рахунок Java ME-програм, які підтримуються практично всіма мобільними телефонами, смартфонами і комунікаторами. Спеціальні програмні додатки можна встановити або безпосередньо на мобільний телефон (відкривши у браузері телефона веб-сторінку), або завантажити програму і встановити її на телефон самостійно за допомогою програм для синхронізації телефона і комп'ютера. Такі програми зазвичай поставляються в комплекті з телефоном [1].

Смартфони мають більше оперативної пам'яті, ніж мобільні телефони, і власний потужний процесор. Оснащуються операційними системами Android (аналог операційної системи Linux), iOS, Windows Phone, Windows Mobile, Symbian, Bada, Aliun OS та ін., і «відкриті» для розробки програмного забезпечення сторонніми розробниками. Підтримують багато програм, написаних мовою Java та C++. Додаткові програми для смартфонів значно розширюють їхні можливості та дозволяють поліпшити функціональність. Операційні системи для смартфонів досить добре захищені й обмежують можливість налаштування системних функцій. Смартфони суміщають функціональні можливості плейєра, комунікатора й інтернет-планшета.

Кишенькові комп'ютери, доповнені функціями мобільного телефону, – комунікатори – проіснували недовго і були витіснені смартфонами. У даний час не існує чіткого розмежування між смартфонами і комунікаторами, оскільки функціональність обох класів пристроїв приблизно однакова [2].

Інтернет-планшет (веб-планшет) – тип планшетних комп'ютерів, які поєднують можливості ноутбука і смартфона. Інтернет-планшети можуть бути постійно підключені до мережі «Інтернет» через безпровідникові канали Wi-Fi або 3G/4G. Інтернет-планшети зручно використовувати для перегляду веб-сайтів і веб-сторінок, роботи з веб-додатками і використання веб-сервісів. Інтернет-планшети несумісні апаратно з IBM-комп'ютерами, тому на них встановлюються такі ж операційні системи, як і в смартфонах (Android, iOS, Open webOS, Windows RT та ін.). Ці «мобільні» операційні системи не дозволяють використовувати про-

грамне забезпечення, доступне для звичайних і планшетних персональних комп'ютерів, але мають більше функцій, аніж електронні книги – дозволяють переглядати веб-сайти, мультимедіа-файли, працювати з електронною поштою тощо.

Планшетний персональний комп'ютер (планшетний ноутбук) – це різновид ноутбука, який обладнаний сенсорним екраном. Основна його перевага – апаратна сумісність із сучасними персональними комп'ютерами і можливість встановлення повноцінних операційних систем (Microsoft Windows NT, Windows XP, WindowsVista, Windows 7, Linux та ін.), що дозволяє використовувати будь-яке програмне забезпечення, доступне для звичайного офісного чи домашнього персонального комп'ютера [3].

Мобільний банкінг – це система, що дає можливість отримання інформації та управління коштами на банківському рахунку за допомогою мобільного телефону, смартфона або планшетного комп'ютера. Перші та найпростіші системи мобільного банкінгу – це SMS-банкінг та управління платежами з банківського рахунку за допомогою вказівок фахівців колцентру банку. Для підключення до системи мобільного банкінгу потрібно стати клієнтом банку, зайти в будь-яке відділення з паспортом, підключити систему «Інтернет-банк», а через неї завантажити і підключити додаток для мобільного інтернет-пристрою. Додатки час від часу оновлюються і клієнтам стає доступною для завантаження та встановлення нова версія програми. Підключитись до системи можна також при відкритті карткового рахунку, через Інтернет, банкомат або за дзвінком в інформаційний центр банку (з уведенням коду з клавіатури телефона). Додаток для телефона або планшета завантажується із сайта банку або з офіційного магазину додатків [4; 5].

За допомогою мобільного банкінгу можливе здійснення двох основних типів операцій – отримання (передавання) інформації та проведення платежів: внутрішньобанківські перекази коштів у різних валютах, погашення кредитів, купівля-продаж валюти, платежі до податкових і бюджетних організацій, оплата за користування мобільними і стаціонарними телефонами, Інтернетом, комерційним телебаченням, комунальними послугами та інші. Тобто мобільний банкінг є аналогом пластикової смарт-картки.

Мобільний банкінг, що використовує мобільний телефон, має кілька різновидів.

- SMS-банкінг – один із видів дистанційного банківського обслуговування, що забезпечує доступ до рахунків та операцій на рахунках; послуга забезпечується з використанням номера мобільного телефону клієнта, що зареєстрований у банку. Для виконання операцій використовуються SMS-повідомлення, укладені за допомогою типових шаблонів. Використовуючи послугу, можна отримати SMS-інформування про операції з банківськими картками, перевірити залишок на банківському рахунку або рахунку банківської картки, отримати інформацію про залишок заборгованості за кредитом, переглянути курси валют, виконати пошук найближчого відділення банку, отримати нагадування про закінчення терміну дії картки, про обов'язкові платежі й інші подібні послуги. Для отримання послуги слід надіслати до процесингового центру на визначений номер SMS-запит із власного мобільного телефону; власник картки отримає звіт про виконану операцію відповідно до наданої команди. Цей тип послуг – SMS-інформування про проведені операції – банкінгом не вважають, оскільки він не дозволяє здійснювати платежі та грошові перекази.
- SMS-банкінг розширений (advance) – при підключенні до цієї послуги клієнт може робити низку нескладних операцій, наприклад, заплатити за мобільний телефон, відправивши SMS-повідомлення із сумою платежу.
- WAP-банкінг – клієнт отримує доступ до банківських рахунків із мобільного телефону через WAP-сайти – за протоколом безпровідникових додатків. Цей вид банкінгу є інформаційним: він забезпечує оперативний доступ до інформації про банківські операції на рахунках, про банки і курси валют, але не дозволяє виконувати операції, пов'язані з рухом коштів на рахунках.
- JAVA-банкінг – на мобільний телефон клієнта встановлюється Java-додаток (додаткове програмне забезпечення, написане мовою Java). Система для телефонів із підтримкою Java володіє такими можливостями: переказ коштів між рахунками клієнта, переказ між рахунками в різних валютах; поповнення балансу мобільного телефону; оплата послуг Інтернет-провайдерів; здійснення платежів (у тому числі комунальних) із використанням шаблонів, створених в інтернет-банку; перевірка балансу за всіма банківськими продуктами (рахунками, депозитами, кредитними продуктами); перегляд витягу за рахунком, перегляд списку останніх операцій, отримання інформації про кредити і погашення кредиту. Технологія Java реалізує повноцінний мобільний банкінг, бо дозволяє клієнтам виконувати різноманітні операції зі своїм рахунком. Java-додаток можна коригувати в режимі on-line.
- Операційні системи і платформи для мобільних телефонів (Windows Phone, Android, Symbian) передбачають можливість відкриття, створення і редагування документів. Уже розроблені програми, здатні за допомогою камери телефона сканувати надіслане повідомлення на сплату податку і автоматично підготувати платіж за потрібними реквізитами, після чого залишиться їх тільки перевірити і ввести суму платежу. Розробляються і програми для здійснення платежів за шаблонами з керуванням голосу власника телефону [5].

Вид надаваних послуг залежить від технології, що використовується для комунікації між клієнтом, банком і оператором мобільного зв'язку.

Мобільний банкінг, що використовує смартфон, має такі функції: оплата за використання мобільного телефону і послуг інтернет-провайдерів; перекази між рахунками клієнта; перекази іншому клієнтові банку або в інший банк; оплата комунальних послуг, комерційного телебачення і т. п. (за допомогою шаблонів інтернет-банку); перегляд доступного балансу рахунку та отримання детальної інформації за рахунками. А також пошук найближчих банкоматів, відділень, місць погашення кредиту, перегляд детальної інформації стосовно обраного об'єкта (адреси, режим роботи, можливі сервіси), перегляд актуальних курсів валют тощо. Для підключення системи потрібно стати клієнтом банку, зайти в будь-яке його відділення з паспортом, підключити систему «Інтернет-банк», а через неї завантажити і підключити додаток Android.

Приблизно таку ж функціональність мають додатки для iPhone (мультимедійний смартфон корпорації Apple, працює під керуванням операційної системи iOS) та iPad (інтернет-планшет корпорації Apple). Самі додатки періодично оновлюються і клієнтам банку стає доступною для завантаження та встановлення нова версія програми.

Однією з проблем при використанні мобільного банкінгу вважається зростання випадків шахрайства. Системи мобільного банкінгу можна реалізувати з дуже надійними засобами захисту, які є стійкими до дій шахраїв. Але ці засоби захисту є незручними в експлуатації для звичайного користувача. Вони передбачають вивчення довгих інструкцій і проходження багаторівневих процедур ідентифікації, а це може зайняти більше часу, ніж дорога до найближчого банківського відділення [6].

Найбільшою перевагою сьогодні вважають відносну захищеність мобільних пристроїв від вірусів та атак хакерів.

До основних загроз мобільного банкінгу ІТ-фахівці відносять можливість несанкціонованого доступу до даних за допомогою вірусних програм і збиток при фізичній втраті пристрою. Кількість вірусів для мобільних пристроїв набагато менша, ніж для персональних комп'ютерів. Невелика також імовірність попадання вірусу до програмного забезпечення мобільного пристрою. У системах мобільного банкінгу можлива поява нових видів зловживань, про це свідчить публікація [7]. У ній описано схему крадіжки грошей із картрахунків волонтерів – клієнтів ПриватБанку та користувачів Київстару.

Безпека операцій із банківським рахунком з боку банку полягає: у використанні різних схем автентифікації клієнта (запити логічного імені та пароля, динамічно згенерованих ключів, статистичного кодового слова); блокування додатка на мобільному пристрої за спроби підбору пароля доступу до нього; застосуванні електронного цифрового підпису клієнта при здійсненні операцій; авторизації всіх операцій у процесинговому центрі банку, під час якої проводиться ідентифікація клієнта і перевірка його електронного підпису; використанні захищеного GSM-каналу для доставки повідомлень; використанні криптографічних протоколів WTLS і SSL для шифрування даних і автентифікації банку; співучасті операторів мобільного зв'язку при виконанні банківських операцій; доступ до банківського додатка за PIN-калькулятором. Смартфон-банкінг має вбудовану функцію генерації одноразових паролів (альтернатива апаратним пристроям OTP-токенам), усі надіслані документи підписуються електронним цифровим підписом – для цього використовуються бібліотеки криптографічних перетворень, які здійснюють накладання електронного цифрового підпису на повідомлення та їх шифрування [8; 9].

Безпека операцій із банківським рахунком з боку клієнта полягає: у введенні пароля доступу при підключенні до послуги (його можна дізнатись, зателефонувавши до інформаційного центру банку) або PIN-коду; використанні окремої SIM-карти з інтегрованим платіжним додатком (STK-модель банкінгу); ідентифікації за ID-картками та підтвердженні операцій контрольними PIN-1 і PIN-2 кодами. Очевидно, усі ці засоби ідентифікації клієнт банку повинен зберігати в суворій таємниці.

Зазвичай фахівці банку рекомендують використовувати мобільний пристрій із ліцензійною операційною системою, антивірусну програму, наголошують на обережності при встановленні на телефон програм із сумнівних джерел, акуратному зберіганні паролів у недоступних (для сторонніх осіб) місцях [6].

Правил безпеки потрібно також дотримуватися під час роботи з мобільного пристрою в мережі «Інтернет», виконуючи аналіз адрес посилань, які приходять з електронними листами і SMS-повідомленнями від невідомих відправників. Віддаючи телефон у ремонт, треба стерти банківський додаток або заблокувати роботу з ним через кол-центр банку. Іноді фахівці з комп'ютерної безпеки радять виділити для мобільного банку окремий пристрій, але незручно використовувати лише для цього окремий телефон або планшет. Зрозуміло, що підключати до системи мобільного банкінгу всі банківські рахунки (особливо з великими постійними залишками коштів на них) без крайньої потреби не варто. Для постійних платежів логічно виділити окремі рахунки, залишки на яких були б невеликими. Якщо при використанні мобільного банкінгу виникла загроза доступу зловмисників до рахунків або був загублений мобільний пристрій, фахівці з банківської безпеки радять якнайшвидше зателефонувати в банк для блокування доступу до мобільного банкінгу.

Клієнти ПриватБанку можуть зайти зі смартфона або мобільного телефону в систему «Приват24» і отримати доступ до системи мобільного банкінгу не лише за своїми логічними іменами та паролями (які банк надсилає на мобільний телефон), а й за допомогою QR-кодів. Для цього слід піднести до екрана персонального комп'ютера смартфон (мобільний телефон) і зчитати QR-код. Аккаунт клієнта у Приват24 (переважно це логічне ім'я і пароль) завантажиться сам, цей спосіб ідентифікації безпечніший і швидший, аніж уведення логічного імені та пароля клієнта з клавіатури. Система розпізнавання QR-кодів використовує принцип зв'язку аккаунта клієнта з його смартфоном (телефо-

ном). Клієнти смартфон-версії електронного банкінгу можуть здійснювати також безконтактні операції зняття готівкових коштів у банкоматах ПриватБанку за допомогою QR-коду [10].

Наприклад, щоб оплатити рахунок, слід відкрити відповідний додаток і сфотографувати телефоном QR-код на банкоматі або код оплати товару. Програма проведе авторизацію клієнта і запропонує обрати платіжну картку, з якої списуються кошти. Користувач повинен підтвердити платіж паролем або SMS-кодом. Крім безконтактних платежів, без використання картки в системі Приват24 власники смартфонів і планшетів можуть переглядати витяги за рахунками, поповнювати рахунки мобільних телефонів, оплачувати комунальні послуги, керувати кредитами і депозитами, придбавати автобусні, залізничні та авіаквитки на всі напрямки як в Україні, так і за кордон [10].

У майбутньому з метою підвищення безпеки в системі мобільного банкінгу можливе використання систем розпізнавання власника за голосом, зображенням камери телефона або сервісів GPS-позиціонування.

Дистанційне банківське обслуговування розвивається досить швидкими темпами і розширюватиме спектр послуг. Слід очікувати вдосконалення цих систем з одночасним спрощенням інтерфейсу. Програмне забезпечення для мобільних пристроїв розвивається у напрямі здійснення невеликих масових платежів (оплата послуг транспорту, розрахунки в торговельних мережах, закладах харчування, автозаправках, використання платіжних систем тощо) за допомогою безконтактних чипів. Уже сьогодні технології зв'язку невеликого радіуса дії (NFC і Bluetooth) інтегровані в мобільні телефони. Банки тісно співпрацюватимуть з операторами мобільного зв'язку, які обслуговують багато абонентів із невеликими залишками коштів на рахунках.

Українські банки використовують такі системи мобільних платежів: М-банкінг, Мобільний банкінг, «ПлатиМО!», Portmone.Mobile, Mobile Banking, StarMobile.

Компанія Google розробляє технологію, яка буде використовуватися у смартфонах із програмним забезпеченням Android. Вона перетворить мобільний телефон в електронний гаманець. Проект стартуватиме в Нью-Йорку, Сан-Франциско та інших містах США, у ньому візьмуть участь роздрібні торговельні точки і мережа кафе швидкого харчування. Вони оновлять термінали в точках продажу для того, щоб синхронізувати касові апарати з мобільними пристроями відвідувачів [11].

Висновки. Сьогодні мобільний банкінг зі всіма його недоліками вважається безпечнішим, аніж інтернет-банкінг, доступ до якого забезпечений зі службового комп'ютера або з комп'ютера в інтернет-салоні чи готелі. Банки намагаються забезпечити належний ступінь захисту послуг мобільного банкінгу в поєднанні з максимально зручним інтерфейсом системи для її користувачів. При дотриманні простих правил, про які банки повідомляють на своїх сайтах, небезпека використання мобільного банкінгу – мінімальна.

Список використаних джерел

1. Електронний ресурс [сайт]. – Режим доступу: http://uk.wikipedia.org/wiki/мобільний_телефон.
2. Електронний ресурс [сайт]. – Режим доступу: http://uk.wikipedia.org/wiki/смартфон.
3. Електронний ресурс [сайт]. – Режим доступу: http://uk.wikipedia.org/wiki/планшетний комп'ютер.
4. Електронний ресурс [сайт]. – Режим доступу: http://www.scritube.com/limba/ucraineana/35849.php.
5. Електронний ресурс [сайт]. – Режим доступу: http://20minut.ua/Novyny-Ternopolya/Groshi/Сам-собі-банкір-зі-смартфоном-10270580.html.
6. Лейбов В. Можливості та перспективи мобільного банкінгу [Електронний ресурс] [сайт]. – Режим доступу: http://www.ufin.com.ua/analit_mat/gkr/160.htm.
7. Електронний ресурс [сайт]. – Режим доступу: http://www.ua-reporter.com/novosti/132737.
8. Електронний ресурс [сайт]. – Режим доступу: http://www.bifit.ua/decisions/sms-banking/index.html.
9. Електронний ресурс [сайт]. – Режим доступу: http://www.bifit.ua/decisions/smartfone-banking/index.html.
10. Електронний ресурс [сайт]. – Режим доступу: https://www.privatbank.ua/news/privatbank-otkryl-vkhod-v-privat24-cherez-qr-kod//.
11. Електронний ресурс [сайт]. – Режим доступу: http://news.rambler.ru/10007991//.

Summary. This work describes the software for modern mobile appliances, the capabilities of mobile banking systems, as well as protection of mobile banking, smartphone banking, and tablet banking services.

Keywords: mobile Internet devices, mobile banking, smartphone banking, tablet banking, protection of mobile banking services.