УДК

БЕЗПЕКА СИСТЕМИ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ ТА НАПРЯМИ ЇЇ ЗАБЕЗПЕЧЕННЯ

Захарченко О.М., асистент кафедри фінансової політики, грошового обігу і кредиту
ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі»

Система дистанційного банківського обслуговування (ДБО) давно є нормою життя в економічно розвинених країнах. В Україні за останні роки вона перетворилася з додаткового на основний інструмент надання банківських послуг. Такий результат спричинили кілька процесів: це і загальне поширення онлайн-технологій, що надають користувачам максимальну мобільність та зручність, і переведення всіх доступних операцій «в мережу», що дозволяє суттєво знизити витрати на надання послуг у відділеннях банку. Позитивний як для клієнта, так і для банку сценарій закономірно привів до того, що дистанційне банківське обслуговування сьогодні у банків в пріоритеті.

Однак, віддалений банкінг є не тільки затребуваним, а й уразливим сервісом. Поряд з очевидною привабливістю такого способу здійснення банківських операцій як у банківської установи, так і в її клієнтів виникає чимало додаткових джерел банківських ризиків, основними причинами виникнення яких є:

1) віртуальний характер дистанційних банківських операцій;
2) загальнодоступність відкритих телекомунікаційних систем;
3) гранично висока швидкість виконання транзакцій;
4) глобальні масштаби міжмережевої операційної взаємодії;
5) активна участь компаній-провайдерів послуг у проведенні операцій [3].

Дистанційне обслуговування – важлива функціональна складова сучасної банківської системи. Тому, однією з найважливіших задач банків при наданні дистанційних послуг є забезпечення найвищого рівня безпеки систем електронного

банкінгу, що забезпечує мінімальні ризики відносно несанкціонованого доступу до інформації та рахунків клієнтів.

Значення безпеки і необхідність захисту інформації при дистанційному банківському обслуговуванні перебільшити складно. Безпека здійснення розрахунків була і залишається найважливішим аспектом дистанційної взаємодії клієнта з банком. Проблеми забезпечення безпеки та захисту інформації актуальні для всіх каналів ДБО.

Для забезпечення необхідного рівня безпеки систем ДБО банки співпрацюють не тільки з розробниками систем дистанційного обслуговування, але і з компаніями, що займаються питаннями інформаційної безпеки і захисту інформації. Проблеми безпеки віддалених сервісів актуальні не тільки для банків, але і для їх клієнтів. Відповідним чином має бути захищена не тільки банківська частина системи, що забезпечує дистанційні послуги, а й технічні та програмні засоби клієнта, за допомогою яких клієнт здійснює доступ до послуг.

Найважливішу роль у забезпеченні безпеки дистанційних платежів відіграє організація процесу віддаленого обслуговування: ніж вона слабкіше – тим вище ризики порушення безпеки. Фахівці в галузі забезпечення безпеки вважають, що в банківському бізнесі у зв'язку з високим рівнем організації процесів, наявністю жорсткого контролю з боку регулятора банківської діяльності – центрального банку рівень безпеки набагато вище, ніж у небанківській установі. Тому, можна припустити, що можливе залучення інших суб'єктів ринку до дистанційного здійснення платежів призведе до збільшення проблем, пов'язаних із забезпеченням безпеки і захистом інформації при розрахунках, які здійснюються віддаленим способом [5].

Досвід робіт із забезпечення безпеки систем дистанційного обслуговування показує, що стійкий стан системи, при якому відображаються всі можливі атаки зловмисників, реалізувати дуже важко. Виходом може бути вироблення додаткових і дієвих вимог щодо забезпечення безпеки дистанційних розрахунків і правильна реалізація цих вимог.

У рамках концепції безпеки систем дистанційного обслуговування рекомендується реалізувати, як мінімум, такі процедури:

- розмежувати права користувачів і контролю доступу;
- провести контроль парольної політики, використання криптографії та поводження з криптографічними ключами;
- антивірусний захист;
- забезпечення безпеки корпоративної мережі;
- аналіз захищеності і внутрішнього аудиту;
- резервне копіювання та аварійне відновлення;
- забезпечення безперервності;
- забезпечення фізичного захисту;
- забезпечення безпеки прикладного та системного програмного забезпечення;
- моніторинг подій та реагування на інциденти інформаційної безпеки;
- підвищення обізнаності клієнтів та співробітників з питань інформаційної безпеки;
- внесення змін та оновлення програмних засобів [1].

Дуже складною проблемою в процесі дистанційного обслуговування є регулювання великої кількості користувачів-клієнтів банку. Дії, які повинен вживати клієнт для забезпечення достатнього рівня безпеки при здійсненні платежів з використанням віддалених сервісів банк може тільки зафіксувати у відповідному договорі, змусити і контролювати клієнта в питаннях дотримання потрібних вимог банк не має можливості. Тому виникає необхідність пошуку механізмів впливу на кожного користувача дистанційних послуг, залучення його уваги до питань дотримання безпеки, а також відповідного навчання користувачів.

Банки мають звертати увагу на необхідність поширення попереджувальної інформації для своїх клієнтів, у тому числі з використанням представництв в мережі Інтернет (web-сайтів), про можливі випадки неправомірного отримання персональної інформації користувачів систем ДБО. До складу такої інформації доцільно включати опис офіційно використовуваних способів і засобів інформаційної взаємодії з клієнтами, а також описи прийомів неправомірного отримання кодів персональної

ідентифікації клієнтів, інформації про банківські карти та запобіжних заходів, яких необхідно дотримуватися клієнтам, що користуються системами ДБО.

В якості запобіжних заходів, яких мають дотримуватися клієнти, що користуються системами ДБО, банки могли б, наприклад, рекомендувати клієнтам:

- виключити можливість неправомірного отримання персональної інформації користувачів систем ДБО – не передавати неуповноваженим особам;
- здійснювати операції з використанням банкоматів, встановлених у безпечних місцях (в державних установах, підрозділах банків, великих торгових комплексах, готелях, аеропортах і т.п.);
- не використовувати банківські карти в організаціях торгівлі та обслуговування, що не викликають довіри;
- при здійсненні операцій з банківською картою без використання банкоматів не випускати її з поля зору;
- не користуватися пристроями, що потребують введення ПІН-коду для доступу в приміщення, де розташований банкомат;
- не використовувати ПІН-код при замовленні товарів або послуг по телефону / факсу або через мережу Інтернет;
- користуватися послугою SMS-оповіщення про проведені операції із застосуванням ДБО (у разі можливості отримання такої послуги);
- здійснювати інформаційну взаємодію з банком тільки з використанням засобів зв'язку (мобільні та стаціонарні телефони, факси, інтерактивні web-сайти / портали, звичайна та електронна пошта та ін.), реквізити яких обумовлені в документах, одержуваних безпосередньо в банківській установі [4].

І наостанок, для того, щоб ефективно протистояти діям шахраїв при використанні дистанційних сервісів, необхідно не тільки мати систему безпеки, але ще й налаштувати цю систему на можливі атаки зловмисників. Необхідно враховувати, що різні уразливості системи призводять до різних наслідків. Вкрай важливо проводити роботи по максимальному виявленню уразливостей систем дистанційного обслуговування і

максимальним чином протидіяти порушенню безпечного функціонування цих систем.

Усі зазначені рекомендації спрямовані на те, щоб схильність банків та їх клієнтів до неминучих ризиків виявилася мінімальною. При впровадженні системи дистанційного банківського обслуговування необхідно опрацьовувати питання створення системи безпеки та підтримання цієї системи на потрібному рівні. Це складний і довгий шлях, який вимагає системного підходу, але тільки завдяки цьому можна домогтися гарних результатів.

Список використаних джерел

1. Бабенко А. Безопасность систем дистанционного банковского обслуживания [Електронний ресурс] / А. Бабенко. – Режим доступу: http://bankir.ru/publikacii/s/bezopasnost-sistem-distantsionnogo-bankovskogo-obsluzhivaniya-10001328/
2. Володин А. Защитить удаленные финансовые услуги / А. Володин // Банковское обозрение. – 2009. – № 10. – С. 98-99.
3. Воронін А. Електронний банкінг та ризики його використання / А. Воронін // Фінансовий ринок України. – 2009. – № 1 (63). – С. 8-9.
4. Поспелов А. Интернет-банкинг: вопросы обеспечения безопасности / А. Поспелов // Деньги и кредит. – 2009. – № 4. – С. 61-63.
5. Современные проблемы безопасности при реализации дистанционных платежей [Електронний ресурс] / Режим доступу: http://www.bankdbo.ru/sovremennye-problemy-bezopasnosti-pri-realizacii-distancionnyx-platezhej