Ольга Єсіна
ст. викладач кафедри інформаційних систем в економіці
Одеський національний економічний університет, м. Одеса

ОРГАНІЗАЦІЯ БЕЗПЕКИ ІНТЕРНЕТ-БАНКІНГУ

Обслуговування клієнтів – пріоритетний напрямок роботи будь-якого банку. Впровадження інформаційних технологій в банківську сферу призвело до того, що в Україні зараз практично немає жодного банку, в якому клієнту не пропонувалися б дистанційні форми обслуговування.

Сьогодні банки надають клієнтам наступні види дистанційних послуг: відеобанкінг; Інтернет-банкінг; PC-банкінг (система «Клиент-Банк»); мобільний банкінг; системи самообслуговування (банкомати ATM-banking, термінали) та ін. [1, с.47].

Інтернет-банкінг сьогодні є найбільш поширеною і зручною технологією для дистанційного керування рахунком і регулярних платежів через мережу Інтернет. Перевагами роботи системи Інтернет-банкінгу є те, що вона: виконує операції в режимі online; доступна з будь-якого комп'ютера, підключеного до мережі Інтернет; не потребує спеціального програмного забезпечення, лише наявність будь-якого Web-браузера; має максимально спрощену процедуру попередньої реєстрації; забезпечує економію часу – немає необхідності відвідувати банк і стояти в чергах та ін. [2, с.213].

Однак крім незаперечних переваг, Інтернет-банкінг містить в собі і чимало загроз. Основною загрозою користувачів даного сервісу є ризик шахрайського злому і несанкціонованого доступу до коштів на рахунку.

Виділяють наступні групи ризиків: злам систем захисту і адміністрування, дії від чужого імені; підробка платіжних доручень; підміна мережевих адрес; відмова в обслуговуванні; атака на рівні додатків; крадіжка секретного ключа електронного цифрового підпису; перехоплення конфіденційної інформації, яка передається через Інтернет (перехоплення логіна, пароля або sms-повідомлення); підбір паролів; фішинг; віддалене управління комп'ютером та ін.

Так як в процесі використання Інтернет-банкінгу беруть участь обидві сторони – клієнт і банк, то і ризики, пов'язані з використанням цієї послуги, експерти поділяють на 2 складові: ризики з боку клієнтів і ризики з боку банків. Відповідно, організація безпеки Інтернет-банкінгу реалізується як з боку банків, так і з боку клієнтів. Захист Інтернет-банкінгу повинен забезпечувати:

- ідентифікацію суб'єктів-користувачів послуги – клієнтів і самих банків;
- шифрування банківської інформації, що циркулює в мережі;
- безпеку каналів передачі інформації;
- захист носіїв інформації, апаратного та програмного забезпечення та ін.

Організація безпеки дистанційних послуг визначається вимогами чинного законодавства України, стандартами та нормативними документами, як Національного банку, так і встановленими всередині самого банку. Для надання якісних послуг своїм клієнтам, банки сьогодні намагаються використовувати різні системи і механізми захисту, щоб забезпечити безпеку використання Інтернет-банкінгу.

Для автоматизації робіт з обслуговування клієнтів, банки використовують велику кількість програмного забезпечення, кожне з яких має свій набір модулів, ступінь захищеності, надійність, якість обслуговування та ін. [3, с.35]. Як правило, банки працюють з системами, створеними спеціалізованими компаніями-розробниками, діяльність яких у цій галузі ліцензується державою. Питання використання та сертифікації програмного забезпечення і криптографічних засобів захисту інформації, вибору стандартів шифрування інформації та генерування цифрових підписів для платіжних банківських систем, у тому числі системи Інтернет-банкінг, регулюються Державною службою спеціального зв'язку та захисту інформації України та Національного банку України. На ринку України працює декілька компаній у галузі захисту інформації в банківських системах: БІФІТ, НОКК, Сайфер. Їх продукти функціонують у банках України в системах Інтернет-банкінг та Клієнт-банк [4, с. 225].

Для організації безпечної роботи Інтернет-банкінгу українські банки використовують різні системи і механізми. Їх різноманітність пояснюється: спектром послуг, що надаються клієнтам банку через Інтернет-банкінг; технологією реалізації дистанційних послуг; політикою банку в питаннях організації безпеки; об'ємом виділеного фінансування.

Основні механізми забезпечення безпеки Інтернет-банкінгу:

- TLS / SSL-шифрування даних – використовується для забезпечення конфіденційності переданої інформації.

- Авторизація платіжних документів – електронний цифровий підпис (ЕЦП), що забезпечує цілісність і автентичність (доказ авторства) переданої інформації та накладається за допомогою особистого ключа. Для забезпечення надійного зберігання та використання ключів ЕЦП банки використовують Usb-токени та старт-карти.

- Двофакторна аутентифікація клієнта – сувора авторизація клієнта при роботі з Інтернет-банкінгом. У більшості банків використовується в комбінації: логін / пароль і одноразовий цифровий код, який приходить на мобільний телефон клієнта для отримання доступу до системи та підтвердження фінансових операцій.

Крім перерахованих вище основних механізмів захисту, в деяких банках використовуються додаткові заходи забезпечення безпеки: обмеження часу сеансу з'єднання з сервером Інтернет-банкінгу; обмеження можливості входу в систему при певній кількості спроб введення невірних даних; обмеження переліку IP-адрес при зверненні до Інтернет-банкінгу; використання віртуальної клавіатури; використання sms-повідомлень за операціями з картою; можливість змінити пароль на вхід до системи у будь-який час; використання лімітів на платежі та ін.

Проте, статистика порушень безпеки Інтернет-банкінгу говорить про те, що більша частина проблем знаходиться на стороні клієнтів. Найчастіше причиною шахрайського доступу до рахунку клієнта є його неуважність і необережність. Тому, при роботі з Інтернет-банкінгом, клієнту необхідно

ретельно вивчати рекомендації, які розміщені на сайтах банків, а банкам при укладанні договорів проводити інформування клієнтів про існуючі ризики і вимоги до захисту інформації.

Список використаних джерел:

1. Єсіна, О. Г. Сучасний ринок дистанційних банківських послуг в Україні [Текст] / О. Г. Єсіна // Socio-economic aspects of development economics and management : Collection of scientific articles. – 2015. – Vol. 2. – P. 46-49.

2. Єсіна, О. Г. Інтернет-банкінг в Україні: сучасний стан, проблеми та перспективи [Текст] / О. Г. Єсіна // Вісник соціально-економічних досліджень. – 2013. – Вип. 48(1). – С. 209-213.

3. Гострик, О. М. Використання імітаційного моделювання для оцінки програмних засобів банківських установ [Текст] / О. М. Гострик, О. А. Клепікова // Моніторинг, моделювання та менеджмент емерджентної економіки : IY Міжнар. наук.-практ. конф., 10-12 вересня 2014 р. : матер. конф. – Одеса-Черкаси : Брама-Україна. – С. 35-38.

4. Засадна, Х. О. Про захист послуг Інтернет-банкінгу [Текст] / Х. О. Засадна // Вісник Університету банківської справи Національного банку України. – 2008. – № 3. – С. 225–229.