УДК 004.78:336.717

БЕЗПЕКА БАНКІВСЬКИХ ТРАНЗАКЦІЙ У ВІДКРИТИХ МЕРЕЖАХ

Чебурахін М.І.
Науковий керівник - доцент Балагура Д.С.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
тел. +38(067) 113-52-42

These theses are dedicated to the security of banking transactions at the banks. The stench hoots complex pidhid to improve the security of bank transactions, including zastosuvannya modern methods of identification and authentication, protection against cyber attacks, backup of data and encryption of information. Efficient protocols for securing banking transactions, such as SSL / TLS, IPSec and SSH, as well as international security standards, are also considered. These theses will be relevant for cyber security facilitation, banking services and other affected parties, as they will increase the level of security of banking transactions at different banks.

В умовах все більшої цифрової трансформації та зростаючої популярності онлайн-банкінгу, безпека банківських транзакцій у відкритих мережах стає надзвичайно важливим питанням для банківських установ та їх клієнтів. Необхідність захисту від кіберзлочинців, які шукають можливості для зламування системи та крадіжки конфіденційної інформації, вимагає від банківських інститутів використовувати нові технології та стратегії для забезпечення безпеки банківських транзакцій у відкритих мережах. Основні принципи роботи сьогоденної системи безпеки банківських транзакцій у відкритих мережах полягають у використанні шифрування, аутентифікації та контролю доступу. Шифрування даних забезпечує конфіденційність та цілісність інформації, що передається від клієнта до банку та назад. Аутентифікація забезпечує перевірку ідентичності клієнта та банку перед здійсненням транзакції. Контроль доступу забезпечує обмеження доступу до ресурсів тільки авторизованим користувачам та пристроям. Для досягнення максимального рівня безпеки використовуються різноманітні технології, такі як цифровий підпис, мультифакторна аутентифікація, вірусні сканери та інші. Найкращими протоколами для захисту банківських транзакцій у відкритих мережах є SSL/TLS, IPSec та SSH. Вони забезпечують ефективний захист від кіберзлочинців та забезпечують конфіденційність та цілісність даних, передаваних від клієнтів до банку та назад. Крім того, ці протоколи дозволяють встановлювати безпечне з'єднання між банківським сервером та клієнтськими пристроями, що забезпечує надійність та захищеність банківських транзакцій.

SSL/TLS, IPSec та SSH - це протоколи, які забезпечують криптографічний захист даних, що передаються через відкриті мережі. SSL/TLS

використовуються для захисту веб-трафіку, IPSec - для захисту трафіку між мережами та пристроями, а SSH - для захисту трафіку, що передається між комп'ютерами по протоколу SSH. Крім того, ці протоколи мають вбудовані механізми аутентифікації та ідентифікації користувачів, що дозволяє перевіряти, що клієнт та сервер, між якими відбувається комунікація, є дійсною стороною. Використання цих протоколів допомагає підвищити рівень безпеки банківських транзакцій у відкритих мережах та захистити важливу інформацію від кібератак. Для забезпечення міжнародної безпеки банківських транзакцій у відкритих мережах використовуються міжнародні стандарти, такі як PCI DSS, ISO 27001, SWIFT CSP та інші. Ці стандарти містять вимоги до захисту інформації та персональних даних клієнтів, вимоги до захисту від кібератак, вимоги до керування ризиками та безпекою в цілому. Використання цих стандартів дозволяє забезпечити високий рівень безпеки банківських транзакцій та забезпечити довіру клієнтів до банківської установи. Однак, для досягнення повного захисту від кіберзагроз необхідно використовувати комплексний підхід, що включає не лише використання стандартів, а й регулярне оновлення програмного та апаратного забезпечення, навчання персоналу та впровадження нових технологій захисту.

Недоліками сучасної системи забезпечення безпеки у банківських транзакцій у відкритих мережах є наявність вразливостей у програмному забезпеченні та можливість злому через соціальну інженерію, недостатня увага до кібербезпеки з боку користувачів, а також ризик злому технічних засобів захисту. Також важливим недоліком є нестача регуляторних норм, які б встановлювали стандарти безпеки та відповідні вимоги для банківських інституцій та їх клієнтів. Крім того, існує загроза кібератак, які можуть призвести до втрати конфіденційної інформації та коштів.

Для підвищення рівня безпеки банківських транзакцій у відкритих мережах необхідно використовувати комплексний підхід, який включає застосування сучасних методів індентифікації та аутентифікації, захисту від кібератак, резервне копіювання даних та шифрування інформації. Крім того, важливо постійно оновлювати програмне забезпечення та апаратне забезпечення, використовувати мережеві протоколи з високим рівнем безпеки та навчати персонал заходам кібербезпеки.

Щоб ефективно підвищити безпеку банківських транзакцій у відкритих мережах, також необхідно проводити регулярний аналіз ризиків та оцінювати потенційні загрози. Крім того, важливо розробляти та впроваджувати стратегії дій у випадку кібератаки або інших небажаних ситуацій, щоб мінімізувати можливі втрати. До інших шляхів підвищення ефективності системи безпеки можна віднести впровадження двофакторної аутентифікації та використання біометричних технологій, які дозволяють підтверджувати ідентифікацію користувача з високою точністю.