УДК 004.6:004.77

А. В. КОЗИКОВ, ст.викладач, А. Є. НЕХАЄВА, студентка
Криворізький національний університет

ПИТАННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ В СИСТЕМАХ МОБІЛЬНИХ ПЛАТЕЖІВ

Мобільні платежі стали невід'ємною складовою сучасного життя завдяки впровадженню сучасних мобільних пристроїв та швидкому розвитку технологій бездротового зв'язку. Процес переказу грошей між користувачами за допомогою мобільних пристроїв відомий як мобільні платежі. Ця технологія використовує бездротову мережу, що потенційно може спричинити певні проблеми з безпекою та конфіденційністю.

Мобільні інтернет-браузери, цифрові гаманці, мобільні грошові перекази, покупки в додатках, а тепер і безконтактні альтернативи, такі як оплата дотиком (tap-to-pay), а також системи касових терміналів (POS) у стаціонарних закладах – все це вважається "мобільними платежами".

Near-Field Communication (комунікація ближнього радіусу дії), часто відома як NFC, – це передова технологія, що використовується в більшості мобільних платежів, яка дозволяє клієнтам і продавцям надсилати та отримувати безконтактні платежі [1].

Оскільки споживачі через мобільні пристрої передають конфіденційну інформацію, таку як номери карток, імена користувачів та паролі, питання безпеки та конфіденційності стають все більш важливими. Таким чином, користувачі наражаються на небезпеку втручання з боку зловмисників, які можуть викрасти ці дані та використати їх для шахрайства.

Як це не парадоксально, але мобільні платежі можуть бути безпечнішими, ніж звичайні платежі, за умови, що впроваджені інші ключові заходи безпеки. Завдяки таким засобам захисту, як токенізація та шифрування, що застосовуються на більшості мобільних пристроїв і в платіжних компаніях, мобільні платежі за замовчуванням мають більше заходів безпеки [1].

Щоб гарантувати безпеку та конфіденційність у системах мобільних платежів, розробники додатків повинні дотримуватися суворих правил безпеки. Це включає в себе використання шифрування для захисту даних користувачів і постійне оновлення програмного забезпечення, щоб уникнути вразливостей.

Безпечні методи оплати, такі як Apple Pay або Google Pay, повинні використовуватися клієнтами, які бажають гарантувати найбільший ступінь безпеки та конфіденційності в мобільних платіжних системах. Небезпека втрати інформації про картку зменшується завдяки таким підходам, які замінюють номер картки технологією безпеки, наприклад, токенами.

За допомогою технології, яка називається токенізація, можна ефективно просувати мобільні платежі, одночасно захищаючи конфіденційні дані споживачів від кібератак та інших ризиків безпеки. Злодії можуть отримати доступ до токенізованих даних лише в тому випадку, якщо систему продавця буде зламано кібератакою. Оскільки дані клієнта шифруються за допомогою токену, який генерується випадковим чином, токенізовані дані нічого не варті для кіберзлочинців. На відміну від використання кредитної картки для здійснення платежу, мобільні гаманці не передають основний номер рахунку (PAN) картки. Токен надсилається на POS-термінал під час мобільної платіжної транзакції, захищаючи дані під час передачі [2].

Отже, питання конфіденційності та безпеки мобільних платіжних систем є надзвичайно важливими. Користувачі та розробники мобільних додатків повинні бути обережними і використовувати всі можливі заходи безпеки, щоб гарантувати безпеку і конфіденційність своїх даних. Використання безпечних методів оплати, надійних паролів і багатофакторної автентифікації – все це рекомендовані найкращі практики безпеки та захисту даних.

Список літератури

1. Ху Дж. Mobile payment security threats and challenges. Virtual Cards That Protect Your Payments | Online Payment Security. URL: https://privacy.com/blog/mobile-payment-security-threats-and-challenges (дата звернення: 07.04.2023).

2. How to solve mobile payment security concerns | cardconnect. CardConnect. URL: https://cardconnect.com/launchpointe/payment-security/mobile-payment-security (дата звернення: 07.04.2023).