УДК 004.056:336.7

АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ ЩОДО НАДМІРНОГО РОЗКРИТТЯ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ

Горохов Я. А.
e-mail: yaroslav.horokhov@nure.ua
Науковий керівник – проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В. Поповського,
м. Харків, Україна

This paper explores a privacy vulnerability within PrivatBank's digital infrastructure, specifically regarding the excessive disclosure of personal data in P2P transaction receipts. The research demonstrates how a legitimate user can exploit low-value transfers to systematically harvest sensitive information, including Full Names and Tax IDs (RNOKPP). By analyzing the structure of generated PDF receipts, the author identifies a significant vector for automated reconnaissance, which allows for the extraction of a customer's birth date and gender. The study concludes that this implementation represents a flawed architectural choice that facilitates targeted social engineering and identity theft.

У сучасному світі безпека даних клієнтів банків грає дуже важливу роль, так як їх компрометація може нести за собою серйозні наслідки як для клієнтів особисто, так і для банкової та економічної системи в цілому. Найбільші банки України несуть головну відповідальність, адже у разі втрати довіри до одного з найнадійніших гігантів люди перестануть довіряти усій банківській системі, що призведе до економічної стагнації та відсутності грошей у системі, як це було з банком "Україна" в 2001 році.

Об'єктом цього дослідження став ПриватБанк – найбільший банк України, який з 2016 року є державним. На жовтень 2025 року кількість клієнтів цього банку перевищила 18 мільйонів [1]. Використовуючи додаток можна легально отримати персональну інформацію про різних людей, яку банк надає для зручності користувачів під час переказу грошей між фізичними особами використовуючи номер картки.

Так як основну інформацію про людину можна отримати через банківську картку, то варто розуміти як формується номер клієнта. Номер цього банку складається з 16 цифр, перші 6 з яких мають назву Bank Identification Number (BIN) та визначають сам банк, а також мають інші ідентифікатори: платіжну систему (Visa або MasterCard), тип картки (дебетова чи кредитна), рівень картки (стандарт, Gold тощо). Кожен банк може мати у своєму розпорядженні кілька BIN. Наприклад, BIN 545708 означає, що це картка Приватбанку від MasterCard, яка є кредитною та має рівень Стандарт. Після BIN йдуть цифри, які ідентифікують саме клієнта, а останньою цифрою є контрольна сума за алгоритмом Луна, яка необхідна для перевірки правильності введеного номера картки. Відповідно до цього,

для ідентифікації клієнтів залишається 9 цифр, а отже мільярд можливих номерів карток лише для одного BIN.

Під час переказу коштів на картку можна отримати інформацію про отримувача перед відправленням у вигляді прізвища та ініціалів. Це необхідна міра для перевірки отримувача, але водночас є джерелом персональних даних. Таким чином, зловмисник має можливість попередньо створити словники із коректно сформованими номерами карток, після чого методом перебору сформувати власну базу даних з номерами карток, яким відповідають прізвища з ініціалами їх власників.

Наступним кроком є отримання персональних даних з квитанції після переказу коштів. У квитанції зазначені прізвище, ім'я та по-батькові (ПІБ) у повному вигляді, що доповнює вже отриману раніше інформацію. Але зловмисник також отримає реєстраційний номер облікової картки платника податків (РНОКПП), який передається у квитанції у повністю відкритому вигляді. Варто зазначити, що РНОКПП використовується у всіх сферах діяльності людини, від зміни паспорту до отримання освіти. Також важливим є те, що РНОКПП закріплюється за людиною на все життя, і замінити його майже неможливо, окрім деяких випадків, із якими більшість громадян ніколи не зіткнеться.

РНОКПП, який сам по собі є важливим ідентифікатором людини, може надати ще більше інформації, якщо розуміти метод його формування. Перші 5 цифр показують кількість днів від 1 січня 1900 року до дня народження власника номеру. Дев'ята цифра надає інформацію про стать людини, де непарні цифри (1, 3, 5, 7, 9) визначають чоловіка, а парні (2, 4, 6, 8, 0) – жінку. Остання цифра має значення контрольної суми усього ідентифікатора. Отже, аналізуючи РНОКПП, можна отримати дату народження та стать власника номера.

Варто зазначити, що квитанція з ПІБ та РНОКПП формується незалежно від суми переказу. Це означає, що отримати дані людини можливо витративши лише 1 копійку на переказ. Зловмисник, попередньо визначивши робочі номери карток витратить лише 100 гривень, отримавши при цьому інформацію про 10000 людей.

Отже, використовуючи прозорість системи цього банку зловмисник може сформувати базу даних у якій будуть зберігатися номера карток, ПІБ, РНОКПП, дата народження та стать клієнтів. Цієї інформації буде достатньо аби максимально підвищити довіру людини до зловмисника, коли той представиться від імені банка або іншої державної структури, яка володіє цими даними.

З юридичної точки зору така деанонімізація клієнтів один для одного є сірою зоною із-за розмитості законів та власного трактування їх банком. Згідно з інструкцією НБУ №163 “Про безготівкові розрахунки”, п. 37, “Платіжна інструкція має містити обов’язкові реквізити: код платника та код отримувача... (РНОКПП для фізичних осіб)” [2]. ПриватБанк прирівнює платіжну інструкцію до клієнтської квитанції, тим самим додаючи до неї

персональні дані платника та отримувача. НБУ потребує наявність РНОКПП тільки на документах, які знаходяться всередині банку, про клієнтські квитанції уточнень немає. Відповідно до закону «Про захист персональних даних», ст. 6, “Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки” [3]. Сам термін “Ненадмірні дані” є неточним, тому ПриватБанк може вважати передачу РНОКПП необхідністю для підтвердження платежу. Також, враховуючи те, що клієнт погодився з умовами договору про користування послугами цим банком, він автоматично дав згоду на передачу його персональних даних іншим клієнтам, які відправляють або отримують кошти.

Порівнюючи з іншими банками, наприклад, Monobank, стає зрозумілим, що не використовувати РНОКПП можливо, якщо використовувати інший ідентифікатор – International Bank Account Number (IBAN). За цим ідентифікатором за необхідності можна відправити запит до банку та підтвердити особу, яка була учасником процесу переказу грошей. Таким чином, персональні дані клієнта банку буде розглянуто лише за необхідності відповідними структурами, наприклад, судом, та РНОКПП не буде надаватися кожному, хто відправив або отримав гроші на картку.

Отже, дане дослідження показало, що зловмисник може отримати персональну інформацію клієнта ПриватБанку, ціна якої складає 1 копійка. З розкриттям банком ПІБ клієнтів можна погодитися задля ідентифікації отримувача та зручності при переказі коштів, але розкриття РНОКПП є надмірним використанням персональної інформації клієнтів, яку не потрібно знати суб’єктам операції переказу грошей. Задля збереження ідентифікації суб’єкта операції можна використовувати IBAN, як це робить Monobank, зберігаючи персональні дані в безпеці. Наразі головною проблемою залишається різне трактування законів та постанов державних установ, і допоки це не буде змінено, персональні дані будуть надаватися ПриватБанком при кожному переказі, а зловмисники матимуть легальний канал отримання чутливої інформації про клієнтів.

Список використаних джерел:

1. Кількість клієнтів ПриватБанку перевищила 18 млн. Редактор. 2025. 23 жовт. URL: https://redaktor.com.ua/2025/10/23/kilkist-kliyentiv-pryvatbanku-perevyshhyla-18-mln/ (дата звернення: 24.02.2026).

2. Про затвердження Положення про організацію кіберзахисту в банківській системі України : Постанова Правління Національного банку України від 29.12.2022 № 163. URL: https://zakon.rada.gov.ua/laws/show/v0163500-22 (дата звернення: 24.02.2026).

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 24.02.2026).