Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В. о. завідувача кафедрою БІСТ

Мелкозьорова О. М.

_____

« » 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Дослідження та аналіз особливостей забезпечення кібербезпеки в мобільних банківських додатках»

оцінка « »

Голова ЕК

Лемешко О. В. _____

Керівник к.т.н. Єсіна М. В.

Рецензент к.т.н. Бобух В.А.

Виконавець: студентка групи КБ-41

_____ Логачова Є. О.

Харків – 2024

РЕФЕРАТ

У роботі наведено: 1 рисунок, 5 таблиць, 32 джерела, 1 додаток. Обсяг роботи становить 45 сторінки.

Темою роботи було обрано «Дослідження та аналіз особливостей забезпечення кібербезпеки в мобільних банківських додатках».

Метою роботи стало дослідження та аналіз аспектів безпеки мобільних банківських застосунків, а також, порівняння українських банківських застосунків з іноземними аналогами та сформування рекомендацій на основі дослідження. Дана робота є актуальною, адже у часи активного розвитку технологій захист даних та вкладів банківських клієнтів стає на перше місце.

Було проведено власний аналіз аспектів безпеки та зручності в популярних українських та іноземних банківських застосунках, до яких увійшли застосунки з Німеччини, Франції, Італії та Сполучених Штатів Америки. Для дослідження було використано, як літературні джерела, так і проведено власні опитування та аналіз. Дослідження показало, що українські застосунки за обраними показниками загалом не поступаються своїм іноземним аналогам. Як і серед українських застосунків, так і серед іноземних були виявлені ті, що набрали лише по одному пункту безпеки та зручності. Це показує, що як і нашим розробникам, так і іноземним варто розвивати системи безпеки та збільшувати комфорт мобільних банкінгів, зважаючи на досвід інших країн. Також було досліджено нормативно-правову базу щодо банківських мобільних застосунків в Україні та світі, та виявлено, що українська система активно намагається переймати європейський досвід, а також впроваджує власні регулювання. Подальший розвиток роботи можливий у вигляді більш глибокого дослідження систем безпеки банківських мобільних застосунків, таких як методи шифрування даних, побудова внутрішніх систем безпеки у таких застосунках та інше.

Ключові слова: БАНКІВСЬКІ СИСТЕМИ, БЕЗПЕКА ЗАГРОЗИ, ЗАСТОСУНКИ, КІБЕРБЕЗПЕКА, МОБІЛЬНІ БАНКІНГИ.

ABSTRACT

The paper contains: 1 figure, 5 tables, 32 sources, 1 application. The volume of the work is 45 pages.

The topic of the work was "Research and analysis of cybersecurity features in mobile banking applications".

The purpose of the work was to study and analyse the security aspects of mobile banking applications, as well as to compare Ukrainian banking applications with foreign analogues and to formulate recommendations based on the study. This work is relevant, as in times of active development of technologies, the protection of data and deposits of bank customers is becoming a priority.

We conducted our own analysis of the security and convenience aspects of popular Ukrainian and foreign banking applications, which included applications from Germany, France, Italy and the United States of America. The research was based on both literature and our own surveys and analysis. The study showed that Ukrainian apps are generally not inferior to their foreign counterparts in terms of the selected indicators. Both Ukrainian and foreign apps were found to have only one point of security and convenience. This shows that both our developers and foreign ones should develop security systems and increase the comfort of mobile banking, taking into account the experience of other countries. We have also studied the regulatory framework for mobile banking applications in Ukraine and globally, and found that the Ukrainian system is actively trying to adopt the European experience and is also implementing its own regulations. Further development of the work is possible in the form of a more in-depth study of the security systems of banking mobile applications, such as data encryption methods, building internal security systems in such applications, etc.

Keywords: BANKING SYSTEMS, SECURITY THREATS, APPLICATIONS, CYBERSECURITY, MOBILE BANKING.

ЗМІСТ

ВСТУП 5
ПЕРЕЛІК СКОРОЧЕНЬ 7
1 АНАЛІЗ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА СТАНДАРТИЗАЦІЙ БАНКІВСЬКИХ ЗАСТОСУНКІВ 9
1.1 Актуальні загрози банківським застосункам 9
1.2 Актуальні вразливості застосунків та можливості шахраїв 10
1.3 Стандарти кібербезпеки мобільних банкінгів у Європі та світі 14
1.4 Стандарти кібербезпеки мобільних банкінгів в Україні 19
2 ПОРІВНЯЛЬНИЙ АНАЛІЗ УКРАЇНСЬКИХ ТА ЗАКОРДОННИХ БАНКІВСЬКИХ ЗАСТОСУНКІВ 23
2.1 Еволюція мобільних банківських застосунків 23
2.2 Опис і характеристика досліджуваних банків 25
2.3 Порівняльний аналіз банківських мобільних застосунків 28
2.4 Недовіра клієнтів, огляд прикладів кібератак та практичні поради з безпеки 34
ВИСНОВКИ 40
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 42
ДОДАТОК А 46

ВСТУП

Головними аспектами успіху будь-якого застосунку є зручність та безпека. Проте більшість застосунків, які не пов’язані з персональними даними користувачів, нерідко вкладають більше зусиль саме у комфорт, щоб вижити на великому ринку, а не у параметри безпеки. Відносно нещодавно, банківська індустрія почала активно популяризувати свої застосунки – так разом із банківською карткою, клієнт отримує зручний застосунок для керування рахунком, який майже повністю або і цілковито здатен замінити фізичний офіс банку. Головною проблемою таких застосунків є саме аспект безпеки.

Безпека безпосередньо впливає на роботу банківської системи, адже клієнти будь-якого банку у першу чергу покладають відповідальність за свої рахунки та особисті дані на банки. Наразі в Україні діє 63 банки (на 01.02.2024), то ж громадяни мають широкий вибір і установи вимушені пропонувати щось, що змусить клієнтів прийти саме до них [1].

Банківські установи пропонують вигідні кредитні угоди та умови зберігання коштів, комфортний та швидкий сервіс, зручні застосунки, а головне гарантії безпеки. Проте на шляху ідеальної співпраці клієнту і банку стають шахраї, які розвиваються паралельно з новими заходами безпеки.

Фінансовий сектор є одним з найвразливіших, адже щорічно на його установи націлена більшість, як одиноких шахраїв, так і цілих шахрайських угрупувань. Так за 2022 рік кожна 10-та атака була спрямована саме на банківський сектор [2]. Шахраї вдаються до різноманітних методів і полюють за різними цілями. Їх дії варіюються від дрібної крадіжки з рахунку до вимагання викупу з самих установ за персональні дані клієнтів чи поновлення роботи серверів.

Діджиталізація внесла великі позитивні зміни у фінансову галузь, полегшуючи роботу банківських установ і клієнтів. Проте вона відкрила новий потенціал шахрайських схем. То ж боротьба за безпеку і приватність досі триває.

Експерти з інформаційної безпеки постійно оновлюють стандарти безпеки задля пошуків нових стратегій захисту.

Проблематичним є те, що попри високі стандарти, яким мають відповідати банківські мобільні застосунки, неможливо передбачити такий фактор, як людський. Будь-якими мобільними застосунками користуються саме люди, які нерідко нехтують правилами безпеки. Багато випадків шахрайських дій, проведених з мобільними банкінгами, ґрунтуються на нейролінгвістичному програмуванні і часто націлені на вразливість користувачів, а не системи.

Важливо постійно досліджувати і аналізувати аспекти безпеки у мобільних банківських застосунках, щоб при цьому лишати застосунок стандартно безпечним і цілком комфортним у використанні. Адже однією з вагомих особливостей таких застосунків є те, що вони поєднуються безпосередньо з банківськими серверами.

Предметом дослідження є забезпечення кібербезпеки при використанні мобільних банківських застосунків, а об’єктом – мобільні банківські застосунки з точки зору їх безпечності.

Мета роботи: дослідити та проаналізувати аспекти безпеки мобільних банківських застосунків, а також, порівняти українські банківські застосунки з іноземними аналогами та з’ясувати, як саме досягти гармонії між безпекою та комфортом, і сформувати рекомендації на основі дослідження.

Отримані результати будуть корисними, як для користувачів банківських застосунків, які хочуть убезпечити себе, так і для самих банківських установ, адже фінальні рекомендації допоможуть покращити рівень безпеки застосунків. Саме тому дослідження є актуальним і в подальшому може бути основою нових робіт. При виконанні роботи було поставлено наступні задачі: дослідити можливі ризики та загрози безпеці банківських мобільних застосунків; провести аналіз систем та стандартизацій українських та міжнародних банкінгів; дослідити та проаналізувати аспекти кібербезпеки та зручності українських та міжнародних застосунків, та порівняти їх; на основі виявлених відмінностей сформувати поради для покращення безпеки застосунків.

ПЕРЕЛІК СКОРОЧЕНЬ

ЗУ – закон України

ПЗ – програмне забезпечення

СЕП – система платіжних послуг

СМС – Short Message Service, служба коротких повідомлень

США – Сполучені Штати Америки

ФБР – Федеральне бюро розслідувань

ЄС – Європейський Союз

AISP – Account Information Service Provider

API – Application Programming Interface, прикладний програмний інтерфейс

COVID-19 – Коронавірусна хвороба, coronavirus disease 2019

CVV – Card Verification Value 2

DDoS – denial-of-service attack

E-ID – electronic identification

FINRA – Financial Industry Regulatory Authority

GDPR – General Data Protection Regulation

IBAN – International Bank Account Number

ISO – International Organization for Standardization

NIS – the security of network and information systems

NIS2 – the new version of security of network and information systems

NIST – National Bureau of Standards

PCI – Payment Card Industry

PCI DSS – Payment Card Industry Data Security Standard

PCTF – Pan-Canadian Trust Framework

PISP – Payment Initiation Service Provider

PSD2 – переглянута Директива про платіжні послуги

PIN – Personal Identification Number

PUSH-повідомлення – to forcibly send message

QR-код – quick response code, код швидкої відповіді

RTS – регламентні технічні стандарти

SCA – Strong Customer Authentication

SEPA – Single Euro Payments Area

SIM-карти – Subscriber Identification Module, ідентифікаційний модуль абонента

Stanford FCU – Stanford Federal Credit Union

TPP – Trans-Pacific Partnership

tProc – Transport Protection

Wi-Fi – Wireless Fidelity, бездротова правдивість відтворення

1 АНАЛІЗ ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА СТАНДАРТИЗАЦІЙ БАНКІВСЬКИХ ЗАСТОСУНКІВ

1.1 Актуальні загрози банківським застосункам

Компанія BlackBerry провела дослідження і виявила, що з березня по травень 2023 року українські структури зупинили понад 1.5 млн. атак [3]. Найбільше піддавались таким спробам сфера охорони здоров'я і фінансовий сектор. BlackBerry було зафіксовано, що більшість шахрайств було здійснено з території росії та північної кореї [3]. Такі атаки здебільшого націлені на те, щоб дестабілізувати ситуацію у країні і додатково отримати можливі прибутки.

Банківський сектор є одним з найбажаніших серед шахраїв, адже саме завдяки таким махінаціям вони можуть отримати найбільше зиску. Варто чітко усвідомлювати, що розвиток технологій призводить до нової ланки вразливостей. На прикладі банківської системи можна легко простежити, що до появи електронних рахунків злочинцям було дещо важче дістатись до клієнтських грошей, а тим паче даних. Проте це не свідчить про те, що таких шахрайств не було.

Діджиталізація банківського сектору відбувається вже десятки років, проте популярності банківські застосунки набувають тільки з 2020 року, коли пандемія COVID-19 змусила людей активно переходити на віддалений доступ. Таким чином, стало більш зручно робити більшість операцій не виходячи при цьому з дому.

Головна задача спеціалістів з кібербезпеки – забезпечити гарантії довіри банківських клієнтів і при цьому зберегти баланс комфорту. Тож мобільні банкінги пропонують певні переваги, якими може скористатись клієнт. Такими перевагами стають: можливість оформити кредит онлайн, оновлення даних через застосунок, сплата комунальних рахунків, керування підписками, аналіз витрат і доходів, поповнення мобільного рахунку, можливість оформити валютний

рахунок, витрати на благодійність тощо. Проте намагаючись догодити клієнту розробники ризикують упустити головне – належний рівень безпеки.

У сучасному світі загрози банківським застосункам виникають постійно і за роки склався парадокс, який полягає у тому, що, чим краще розвиваються системи безпеки, тим більше прогресують схеми того, як їх зламати чи обійти і ці перегони будуть продовжуватись надалі. Програми мобільного банкінгу функціонують через передачу даних між пристроєм користувача та сервером банку, то ж шахрайства можуть становити загрозу не тільки клієнту, а і самому банку. Таке сполучення застосунків із серверами відкриває можливість для вчинення шахрайств у банківській сфері за трьома основними шляхами [4]:

a) незаконний доступ до пристроїв користувачів;
b) втручання під час передачі даних;
c) незаконний доступ до серверів банку.

Використання мобільного банкінгу передбачає застосування спеціального застосунку, створеного банком, що відрізняється від онлайн-банкінгу, де користувач входить на веб-сайт банку через телефон, комп’ютер або інший пристрій. Важливо не плутати ці поняття, адже при користуванні мобільним застосунком банку, банк має набагато більше можливостей для того, щоб контролювати безпеку рахунку, ніж при використанні веб-сайту. Однак, це не гарантує того, що користування мобільним банкінгом буде повністю безпечне.

1.2 Актуальні вразливості застосунків та можливості шахраїв

У підрозділі 1.1 згадується про три можливі шляхи для шахраїв. Розглянемо детальніше вразливості та те, до чого вони можуть призвести. Перше – вразливості на пристрої клієнта. Тут існує декілька шляхів, найпростіший – пристрій було викрадено і отримано доступ до застосунку. Викрадення телефону або ще якогось пристрою, на якому використовується мобільний банкінг, може перетворитись на справжню проблему. Люди часто зберігають паролі облікових записів та інші дані, завдяки яким обійти систему безпеки банківського застосунку буде легко, прямо на пристроях і цим істотно полегшують задачу кіберзлочинцям. Іноді загрозу може становити навіть неперевірений ремонтний

сервіс, куди клієнти віддають телефон у ремонт, і як наслідок стають жертвами кіберзлочинців [4]. Рекомендується не зберігати на пристрої важливі паролі та дані, якщо телефон відправляється на ремонт. Необхідно вийти з облікових записів та видалити критично важливі застосунки, через які можна отримати доступ до чутливої інформації (у тому числі грошей).

Навіть довершений, з точки зору безпеки, застосунок може бути зламаний через необізнаність клієнта чи банківського працівника. Нерідко злочинці використовують атаки соціальної інженерії, щоб отримати необхідні дані для входу. Мішенню найчастіше стають саме клієнти і співробітники банків [4]. Шахраї видають себе за легітимну організацію, психологічно тиснуть на жертву, шокують. Наприклад, злочинці видають себе за співробітників банку і починають переконувати жертву у тому, що її рахунок знаходиться під ризиком шахрайства, і необхідно зробити переказ коштів на так званий «резервний рахунок» [4]. Після переказу жертва втрачає кошти і процес повернення є майже неможливим. Ще одним сценарієм є надсилання фішингових листів зі схожими погрозами. Фішинг має декілька стратегій.

Фішинг – одна з найпопулярніших шахрайських схем. Зловмисники надсилають лист чи повідомлення нібито з банку і просять перейти за посиланням, завантажити файл чи зробити переказ [4]. Такі листи зазвичай важко відрізнити від оригіналу. Разом із файлом з такого листа можна завантажити шкідливе програмне забезпечення. Або переходячи за посиланням на пристрій жертви потрапляє вірус. Фішингові листи можуть бути схожими не тільки на банківські, а і на звичайні листи з Netflix, служби доставки, Інтернет-магазину тощо. І тільки з часом, коли буває вже запізно, жертва дізнається, що стала мішенню кібершахраїв.

Серед можливих вірусів, які потенційна жертва може завантажити на свій пристрій є кейлогер [4]. Кейлогери – шкідливе програмне забезпечення, що зчитує інформацію, яку користувач вводить у телефон [4]. Таким чином до рук злочинців потрапляють логін, пароль та інша необхідна для входу інформація. Кейлогер

може потрапити на пристрій різними способами, наприклад, при скануванні невідомого QR-код або завантаженні підробленого банківського застосунку.

Підробити застосунок складніше, ніж сайт, проте це не є неможливим. Впродовж 2018 року у Америці було виявлено понад 60000 підроблених банківських програм і це число з кожним роком не зменшується [5]. Пошуком таких підробок займається Федеральне бюро розслідувань (ФБР, проводить постійний моніторинг застосунків у Інтернет-магазинах та слідкує за їх легітимністю. Ці фальшиві програми маскуються під легітимні, і вони виглядають майже так само, як оригінальні. Проте, після того, як користувач вводить свої облікові дані, замість входу в обліковий запис, з'являється помилка [4]. Тим часом, зловмисник отримує дані та використовує їх для доступу до справжнього застосунку. Коли користувач розуміє, що його обманули, може бути вже занадто пізно. ФБР рекомендує отримувати програми для смартфонів лише з надійних джерел, таких як офіційні магазини програм або безпосередньо з веб-сайтів банків. Окрім того компанії, що керують магазинами застосунків для смартфонів, активно перевіряють ці застосунки на шкідливий вміст. А більшість великих банків США надають посилання на свій мобільний застосунок на своєму веб-сайті [5]. Такі дії зменшують ризик потрапляння клієнта на підробку.

Вразливості у самому банку схожі на ті, що і у користувачів, адже в обох випадках з технікою працюють люди. Той же фішинг, атаки соціальної інженерії та шкідливе програмне забезпечення. Проте є і інші схеми, завдяки яким шахраї знаходять шлях до грошей клієнтів в обхід доступу до пристрою. Це перетинається із третім шляхом, коли гроші втрачаються у процесі переходу.

Трояни або троянські віруси є одним із типів шкідливих програм, які можуть становити серйозну загрозу для безпеки користувачів. Cleafy LABS нещодавно виявила трояна під назвою SharkBot, який може обманом змусити вас надіслати гроші шахраям із вашого власного банківського застосунку та навіть перехопити законні повідомлення від вашого банку, щоб обійти двофакторну автентифікацію [6]. SharkBot здатен ініціювати грошові перекази зі зламаних пристроїв за допомогою технології автоматичних систем переказу в обхід

механізмів багатофакторної автентифікації. Ці механізми використовуються для примусової перевірки особи користувачів і автентифікації, вони зазвичай поєднуються з методами поведінкового виявлення для виявлення підозрілих грошових переказів. Після того, як SharkBot успішно встановлено на пристрої жертви, зловмисники можуть отримати конфіденційну банківську інформацію (шляхом зловживання службами доступності), таку як облікові дані, особиста інформація, поточний баланс тощо [6]. Також трояни можуть використовуватися для розповсюдження інших видів шкідливого програмного забезпечення, таких як віруси або черви, що можуть завдати значних збитків для системи або мережі банку.

Зловмисники також можуть спробувати використовувати методи обману заміни SIM-карти через мобільного оператора для того, щоб отримати доступ до мобільного банкінгу.

Процедура заміни SIM-карти відбувається тоді, коли шахраї видають себе за клієнта або ж є у змові з працівником компанії оператора, а потім переміщають обліковий запис на свій пристрій. Після отримання номеру телефону вони можуть перехоплювати повідомлення, дзвінки та інші дані жертви. Цього зазвичай достатньо шахраям, щоб отримати доступ до облікового запису в банківській програмі та обійти двофакторну автентифікацію [6]. За даними ФБР, у 2021 році заміна SIM-карт призвела до втрат жертв на суму понад 68 мільйонів доларів [3].

Злом Wi-Fi або атаки типу «людина посередині» також є доволі розповсюдженими. Суть атаки полягає в тому, що зловмисник видає себе за проміжний вузол між двома легітимними сторонами комунікації, наприклад, між мобільним пристроєм користувача та сервером банку [4]. Це може статися, наприклад, коли зловмисник успішно отримує контроль над мережею Wi-Fi, до якої підключений користувач.

У контексті мобільних банківських застосунків, атаки «людина посередині» можуть мати серйозні наслідки. Зловмисник може перехоплювати та переглядати комунікацію між мобільним пристроєм користувача і сервером банку, включаючи надсилання конфіденційної інформації, такої як паролі або дані банківських

карток. Він також може втручатися у цю комунікацію, змінюючи дані або надсилаючи фальшиві запити до сервера банку, що може призвести до крадіжки коштів або доступу до особистої інформації користувача.

Враховуючи потенційну загрозу атак «людина посередині», важливо вживати заходи безпеки, такі як використання шифрування трафіку, двофакторна автентифікація та захищені мережі Wi-Fi, для захисту користувачів мобільних банківських застосунків від цих видів атак. До схожих атак належать: атака на одноразові паролі та атака на зв'язок. Щоб забезпечити безпеку, часто використовують одноразові паролі. Проте зловмисники можуть намагатися отримати доступ до цих паролів на мобільних пристроях користувачів для власних цілей. У таких атаках, як атака на зв'язок, зловмисники використовують шкідливе ПЗ для перехоплення комунікації між мобільним застосунком і банківським сервером [7].

Незашифровані дані можуть становити значну загрозу для фінансових установ будь-якого розміру. Якщо зловмисники отримають доступ до ваших незашифрованих даних, вони зможуть негайно використовувати їх, що призведе до серйозних проблем для вашої організації. Усі дані повинні бути зашифровані, щоб навіть у разі крадіжки зловмисниками, вони зіткнулися з перешкодою у спробах розшифрувати їх [7].

1.3 Стандарти кібербезпеки мобільних банкінгів у Європі та світі

Фінансові установи борються за клієнта, який в свою чергу шукає гарантовано надійну установу для співпраці. З появою мобільного банкінгу рівень ризиків шахрайства підвищився. Проте кожна країна намагається убезпечити фінансовий сектор по-своєму.

Особливість фінансового сектору країн Європейського Союзу (ЄС) полягає у тому, що стандарти, яким має відповідати мобільний банкінг визначаються не самими банками. Вирішення усіх питань стосовно кібербезпеки мобільних застосунків банку визначаються на рівні усього ЄС і поширюється на кожну банківську установу, яка хоче створити застосунок. Країни ЄС не стали виключенням і також зазнали кризи, що була пов'язана з пандемією COVID-19,

проте інтерес користувачів до мобільних банкінгів значно виріс. Для порівняння, у 2014 році 61% користувачів користувались застосунками банків [8]. А у 2020 банківський сектор має найвищу частку цифрових користувачів у Європі, збільшившись ще на 23% користувачів цифрових технологій, уперше з початку пандемії [8]. За останній час Європейською комісією було прийнято декілька рішень для покращення рівня безпеки.

PSD2 – директива про платіжні послуги, була прийнята комісією 25 листопада 2015 року [9]. Однією з ключових вимог і нововведень цієї директиви є впровадження обов'язкової двофакторної автентифікації для клієнтів банків. Банки мають забезпечувати використання принаймні двох складових для автентифікації, що забезпечує високий рівень захисту [9]. З особливостей такої системи є те, що обрані компоненти автентифікації можуть існувати незалежно один від одного. Таким чином дане нововведення істотно зменшує ризик виконання злочину. Компоненти поділено на категорії: «щось, що ви знаєте», наприклад, пароль та логін, «щось, що ви маєте», наприклад, фізичні документи, що позначають особу, та «щось, що схоже на користувача», наприклад, біометричні дані [9].

Директива PSD2 перекладає значну відповідальність за можливі інциденти на банки, примушуючи їх активно працювати над удосконаленням систем безпеки. Однак вона також полегшує відповідальність клієнтів за можливі інциденти, роблячи банківські застосунки більш надійними та безпечними.

Додатковою зміною стало те, що Фінансові установи мають надавати інформацію про рахунки третім сторонам за згодою своїх клієнтів, щоб забезпечити автоматизацію стандартних банківських операцій та усунути посередників. Це передбачає розробку стандартизованих API для забезпечення доступу до даних рахунків та реєстру [10]. Ці API розрізняють дві категорії сторонніх постачальників платіжних послуг (TPP). Для того, щоб компанія могла отримати статус TPP, необхідно оформити одну з ліцензій наступних видів [10]:

- AISP – ліцензія постачальника інформації про облікові записи, даний вид дозволяє тільки перегляд клієнтських даних. Даний вид ліцензії може бути

корисний для обміну даними клієнта з певними установами, наприклад, іншими банками чи кредиторами;

- PISP – ліцензія постачальника послуг з ініціювання платежів, цей вид ліцензії розширює можливості третьої сторони і дозволяє проводити платежі з рахунку за згодою клієнта. Наприклад, такі дії можуть сприяти заощадженню, переводячи фіксовану суму до «скарбнички».

Доповненням до PSD2 став RTS – делегований регламент комісії ЄС 2018/389. RTS розширює область застосування Директиви (ЄС) 2015/2366 Європейського Парламенту та Ради, щодо регулювання технічних стандартів для надійної автентифікації клієнтів та встановлення загальних і безпечних стандартів зв'язку [11]. У серпні 2022 року Європейська Комісія оприлюднила Делегований Регламент Комісії (ЄС) від 3 серпня 2022 року, який запровадив зміни до регулятивних технічних стандартів (RTS), що викладені у Делегованому Регламенті 2018/389, згаданому вище. Ці зміни стосувалися 90-денного терміну для доступу до рахунків.

Чинна форма RTS внесла певні зміни, якими від 2021 року стали [11]:

- Введення обов'язкового винятку від посиленої автентифікації клієнта (SCA) для конкретного сценарію, коли доступ здійснюється через AISP лише за умови виконання певних умов.

- Обмеження сфери застосування виключення від SCA тільки у випадках, коли клієнт отримує безпосередній доступ до облікового запису.

- Збільшення інтервалу оновлення SCA з 90 до 180 днів для випадків, коли доступ до інформації здійснюється через AISP або безпосередньо клієнтом.

Наступною регулюючою директивою стала NIS, яку було прийнято ще у 2016 році. Вона служить широким регулюванням кібербезпеки. NIS вимагає від членів ЄС створювати групи співпраці. Що має сприяти чіткій комунікації у разі кібератаки та заохочувати готовність до інцидентів [12]. Щоб впоратися з нещодавніми сплесками кіберзлочинів у всьому світі, попередню Директиву було оновлено до Директиви NIS2 [13]. Директива NIS2 зосереджена на підвищенні безпеки мереж та інформаційних систем по всій Європі та містить вимоги до

компаній щодо впровадження відповідних технічних заходів і заходів для запобігання, виявлення та реагування на інциденти безпеки. Про ці інциденти також необхідно повідомляти їх національні компетентні органи. Дана Директива зосереджена на оцінці можливих ризиків та запобіганні їм і почне активно діяти з осені 2024 року [13]. Додатково дані громадян ЄС захищені загальним регламентом захисту даних (GDPR), що був прийнятий у 2018 році [9].

Банки, які надають електронні банківські послуги, мають здійснювати заходи для зменшення ризиків різних видів атак, таких як соціальна інженерія, фішинг та інші. Важливу роль в цьому відіграють токени, які використовуються для забезпечення безпеки автентифікації. Ці токени можуть бути апаратними або мобільними. Прикладами таких токенів є tProc ECC та tPro Mobile [9].

Comarch tPro ECC відповідає високим вимогам клієнтів, які очікують певний хороший рівень швидкості, ефективності та зручності у сфері безпеки онлайн-банкінгу [14]. Цей компактний та легкий USB-токен не потребує установки драйверів. Здебільшого його створено для авторизації документів, підтвердження особи за допомогою електронного підпису та онлайн-транзакцій. У такому випадку підписання відбувається за допомогою кнопки на самому пристрої. Таке рішення підвищує захист від різноманітних видів зовнішніх атак і убезпечує інструкції від втручання третьої сторони.

У свою чергу tPro Mobile – це мобільна платформа, яка забезпечує надійну автентифікацію користувачів і авторизацію транзакцій відповідно до вимог директиви PSD2. Ця платформа складається з мобільного застосунку та набору бібліотек розробника, які можна інтегрувати з існуючими продуктами [15].

На відміну від європейських країн, США мають трохи іншу систему регулювання фінансової кібербезпеки, оскільки юрисдикцію мають як штати, так і федеральний уряд. Норми США стосуються боротьби з шахрайством та відмиванням коштів. У 2018 році набув чинності Закон про мобільні зв’язки, який є частиною нового Закону про економічне зростання, регуляторні заходи та захист прав споживачів [9]. Цей новий закон скасовує попередні обмеження, накладені законом Додда-Френка. Закон про мобільні пристрої дозволяє банкам залучати

клієнтів за допомогою легшого процесу онлайн-підтвердження [9]. Наприклад, потенційні клієнти можуть відсканувати документ, що посвідчує особу, такі як паспорт, і використати для підтвердження електронний підпис.

Також керівними у сфері кібербезпеки, як мобільних банкінгів, так і загалом застосунків, є Національний інститут стандартів і технологій (NIST). NIST особливо виділив правила для сфери охорони здоров'я, фінансів і роздрібної торгівлі. Фінансові установи звітують перед Органом регулювання фінансової індустрії (FINRA) [9]. Рекомендації NIST йдуть рука об руку з вимогами Управління регулювання фінансової індустрії щодо процесів і засобів контролю, необхідних для управління та пом'якшення кіберризиків. Розглянуті теми включають засоби контролю автентифікації, внутрішні оцінки ризиків і розкриття вразливостей. Наприклад, положення Нью-Йорка про кібербезпеку 23 NYCRR 500 вимагає, щоб порушення кібербезпеки розкривалися протягом 72 годин [9].

Станом на 2022 рік виникли деякі нові тенденції забезпечення кібербезпеки мобільних банківських застосунків. Тенденції розділяють на дві групи: вимоги щодо покращення ідентифікації та вимоги щодо захисту користувацьких даних.

До першої групи увійшли зміни у Японії та Швейцарії [16]:

- у Швейцарії був ухвалений Закон про захист даних, який зобов'язує компанії негайно повідомляти про серйозні порушення даних федеральному комісару із захисту даних та інформації;

- з квітня 2022 року, в Японії запровадили правила, що стосуються використання Закону про захист персональних даних. Ці правила передбачають обов'язок суб'єктів повідомляти про будь-які порушення даних до комісії із захисту персональних даних і вживати заходів щодо суб'єктів, які порушують цей закон.

До другої групи увійшли зміни запроваджені у Канаді, США, Данії та інших країнах [16]:

- Комісія ЄС працює над завершенням інструментарію для країн-членів, який буде включати перелік конкретних архітектур, найкращих практик, стандартів, посилань та рекомендацій з питань створення цифрових гаманців;

- NIST випускає у США проєкт Керівництва з цифровою ідентифікацією для протидії фішинговим атакам за допомогою фішингово-стійких автентифікаторів;

- Данія впроваджує покращений MitID як заміну системі NemID для затвердження платежів та авторизації входу;

- Уряд Федеральної ради Швейцарії розробляє державну інфраструктуру E-ID для використання постачальниками ідентифікаційних даних, агентами, довіреними особами або постачальниками ідентифікаційних гаманців;

- Канада створює програму Voila Verified Trustmark, яка видає знаки довіри організаціям, що відповідають вимогам PCTF.

1.4 Стандарти кібербезпеки мобільних банкінгів в Україні

В Україні фактично не існує єдиної системи, за якою регулювалась би розробка мобільних банківських застосунків. Відповідальність за безпеку здебільшого покладається на самі банки. Проте це не значить, що не існує регулювань з боку законодавства та стандартизації. Україна активно впроваджує також європейські стандартизації у сфері кібербезпеки і деякий відповідний досвід уже запроваджено у банківській сфері.

Одним з найважливіших Законів України у банківській сфері, у тому числі і для банківських мобільних застосунків, є Закон про банки і банківську діяльність. Даний Закон повинен забезпечувати захист інтересів вкладників та інших клієнтів банку, сталий розвиток і стабільність банківської системи. Цей Закон визначає структуру банківської системи, економічні, організаційні і правові засади створення, діяльності, реорганізації і ліквідації банків [17].

Ще одним Законом України, який регулює в тому числі і банківські мобільні додатки є ЗУ «Про платіжні послуги», прийнятий Верховною Радою у 2023 році. Даний Закон визначає поняття та загальний порядок виконання платіжних операцій в Україні. Визначає перелік платіжних послуг, порядок їх надання та список надавачів. Регулює засади регулювання електронних та цифрових грошей. Також визначає перелік прав, обов’язків та відповідальностей учасників платіжного ринку в Україні [18].

ЗУ «Про платіжні послуги» також регулює порядок надання доступу до банківської інформації, такої як особистий рахунок користувача, особиста інформація користувача та інше [18].

Однією з впроваджених нещодавно змін банківської діяльності є документ ISO 20022. ISO 20022 – це нормативний документ, який сприяє розширенню функціоналу Системи електронних платежів (СЕП) та його адаптації до стандартів Європейського Союзу [19]. Цей стандарт застосовується для платежів між рахунками IBAN-IBAN і не охоплює операції з цінними паперами, банківськими картками, торговими та валютними операціями. Даний стандарт впроваджується Національним банком України задля виконання умов, що були поставлені Україні для набуття статусу кандидата на вступ до ЄС.

З 1 квітня 2023 року Українські банки почали використовувати ISO 20022 у своїх розробках. Такий перехід передбачав перехід на нове покоління електронних платежів СЕП-4.0. Дана зміна передбачала можливість здійснення [19]:

- управління функціоналом миттєвих переказів, що має запровадиться з наступною версією СЕП-4.1, тестування якої проводилось у 2023 році. Дане покращення дасть змогу клієнтам таке важливе покращення швидкості оброблення платіжних інструкцій в електронній формі, при цьому, даючи можливість виконати негайне зарахування коштів на рахунок отримувача;
- сприятливих умов для приєднання України до Єдиної зони платежів у євро – SEPA. SEPA дозволяє здійснювати транскордонні перекази в євро з країнами ЄС;
- реалізації мультивалютності, трекінг-сервісу для платежів та інше.

ISO 20022 сприяє уніфікації обміну фінансовою інформацією, спрощуючи взаємодію між різними фінансовими установами та підвищуючи ефективність операцій. Впровадження цього стандарту спрямоване на покращення якості та надійності фінансових послуг [19].

Наступною важливою сертифікацією для безпеки українських банківських застосунків є PCI DSS. Сертифікація PCI DSS в Україні – це набір стандартів

безпеки, призначених для того, щоб усі організації, які приймають, обробляють, зберігають або передають інформацію про кредитні картки, підтримували безпечне середовище [20]. Сертифікація індустрії безпеки платіжних карток є радою для керування поточною оцінкою стандартів безпеки PCI з акцентом на покращенні безпеки суми платежу протягом усього процесу транзакції. Дана стандартизація передбачає виконання дванадцяти головних умов [21]:

a) захист систем, що обробляють платіжні дані у тому числі і фізичний;

b) захист даних про власників карток від стороннього доступу;

c) захист мережі, що обробляє дані від несанкціонованого доступу;

d) захист від шкідливих програм;

e) обмеження доступу, тобто доступ повинен надаватись лише авторизованим користувачам;

f) тестування і розвиток безпеки систем;

g) запровадження та підтримка діяльності ефективних політик безпеки;

h) обмеження фізичного доступу до приміщень, у яких знаходиться обладнання для обробки платіжних даних;

i) моніторинг можливого виникнення інцидентів;

j) захист від зовнішніх видів атак;

k) управління підтримкою та обслуговуванням;

l) впровадження політики та процедури безпеки пропонує розробку та впровадження політик та процедур безпеки для забезпечення відповідності стандарту.

PCI DSS передбачає рівень захисту компанії відповідно до кількості оброблюваних транзакцій. Таким чином компанії з найбільшою кількістю транзакцій потребують найвищий рівень сертифікації. Відповідна градація виглядає наступним чином [22]:

- рівень 1 – компанії, що обробляють понад 6 млн. транзакцій;
- рівень 2 – компанії, що обробляють від 1 до 6 млн. транзакцій;
- рівень 3 – компанії, що обробляють від 20 тис. до 1 млн. транзакцій;
- рівень 4 – компанії, що обробляють до 20 тис. транзакцій.

Апаратний маркер tProc ECC, що був згаданий раніше, нині вже доступний і в Україні. Цей маркер відомий своєю стійкістю до віддалених атак, завдяки застосуванню криптографії еліптичних кривих. Українська версія токена розроблялась у співпраці з місцевим дистриб’ютором Comarch IT Park і відповідає українському стандарту електронного підпису, також вона підтримує геш-функцію «Купина». Це робить tProc ECC добре пристосованим до українських стандартів та легко інтегрованим в інфраструктуру будь-якого банку в Україні [23].

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ УКРАЇНСЬКИХ ТА ЗАКОРДОННИХ БАНКІВСЬКИХ ЗАСТОСУНКІВ

2.1 Еволюція мобільних банківських застосунків

Банківські мобільні застосунки починають своє зародження ще у 1980-х роках, коли Citibank, Chase Manhattan, Chemical and Manufacturers Hanover запровадили нову послугу для своїх клієнтів – домашній банкінг. Домашній банкінг ґрунтувався на використанні системи Videotex. Videotex – це загальний термін для систем, які передають текст і графіку діловому або домашньому користувачу за допомогою сигналів, що передаються по телефонній лінії, кабелю або будь-якому з каналів телевізійного або радіомовлення [24].

Ще одним провідним новатором у сфері фінансового обслуговування є Stanford Federal Credit Union. Ще у 1970-ті роки цей банк надав клієнтам можливість користуватись чековими рахунками та кредитними картками. Наступним кроком було широке впровадження банкоматів та обслуговування по телефону. А вже у 1994 році Stanford Federal Credit Union вперше в історії запропонували своїм клієнтам послуги онлайн-банкінгу [25].

Проте першим офіційним мобільним банківським застосунком вважається розроблений у 2007 році банкінг від Bank of Scotland. Цей інноваційний застосунок відкрив нові горизонти в області фінансових послуг, забезпечуючи клієнтам зручний та мобільний доступ до своїх банківських рахунків. У 2011 році банк випустив повнофункціональний застосунок, доступний на пристроях Apple, що ще більше розширило можливості користувачів. Пізніше застосунок було адаптовано і для пристроїв BlackBerry та Android, що дозволило ще більшій аудиторії користувачів зручно користуватися ним [24]. Основні функції застосунка включали можливість отримання виписки з рахунку, перевірку останніх транзакцій та балансу, що значно полегшувало керування фінансами прямо зі смартфонів. Цей крок був важливим у розвитку мобільного банкінгу та

встановленні нових стандартів у забезпеченні клієнтам більш зручних та доступних фінансових послуг.

Український фінансовий ринок також поступово застосовував розвиток технологій для розширення можливостей та конкурентоспроможності. Так у 2001 році почались розробки першого українського мобільного банківського застосунку від банку Приват Банку. До початкового функціоналу входила авторизація клієнтів та здійснення платежів за допомогою одноразових SMS-паролів. Проте ця розробка ще була далекою від звичного сьогодні поняття мобільного-банкінгу.

Вже починаючи з 2008 року Приват Банк презентував свою розробку повноцінного банківського застосунку, щоправда на той час можливість користуватись такою розробкою мали тільки власники iOS. У 2010 році Приват24 проходить оновлення, на ринку з'явилася версія застосунку для Android, розширивши доступність сервісу на різних платформах. У вересні 2019 року вийшла оновлена версія Приват24 з новим дизайном та більшими можливостями, включаючи меню для підприємців, технологію FacePay24, і можливість користувачам інших банків здійснювати операції через цей застосунок. Ці постійні вдосконалення демонструють бажання банку надати клієнтам найзручніші та інноваційні фінансові послуги [24].

Для створення Приват24 необхідна була сучасна технологічна інфраструктура, що забезпечувала обробку та збереження фінансової інформації користувачів, а також гарантувала безпеку та зручність користування. Одним з ключових аспектів було впровадження найвищих стандартів безпеки, таких як PCI DSS, для захисту фінансових даних користувачів від несанкціонованого доступу [24].

Після створення Приват24 в Україні з'явилось чимало інших банківських застосунків, таких як Monobank, Raiffeisen Online, Ощад24, Альфа-Мобайл та інші. Кожен з цих застосунків пропонують клієнтам зручний доступ до банківських послуг через мобільні пристрої та має свої певні особливості щодо безпеки та програмного інтерфейсу [26].

Український ринок мобільних банківських застосунків активно розвивається, і наразі можна гордитись досягненнями в цій сфері. На сучасному фінансовому ринку почали з’являтись онлайн-банки, такі як Monobank, які дозволяють клієнтам користуватися фінансовими послугами суто через мобільні застосунки. Це кардинально змінює спосіб взаємодії з банківськими послугами, забезпечуючи максимальний комфорт для клієнтів. Також більшість українських банківських організацій, таких як ПриватБанк, Raiffeisen Bank, Oschadbank, OTP Bank, також приєдналися до світу онлайн-банкінгу, пропонуючи широкий спектр послуг своїм клієнтам.

Україна виходить на передові позиції, впроваджуючи QR-коди для безготівкових платежів та стаючи однією з перших країн, що використовує цю технологію. Це революціонізує оплату рахунків і покупок, зменшуючи ризик помилкових транзакцій та скорочуючи черги в банківських відділеннях. Проте, українська сфера мобільних банківських застосунків зіштовхується також і з проблемами, такими як недовіра клієнтів, відсутність стандартів та єдиних правил безпеки, а також недостатня кількість точок доступу до якісного Інтернету та недостатнє регулювання з боку держави [26].

Проте ці проблеми не є перешкодою для постійно зростаючої кількості осіб, які користуються банківськими послугами. За останні роки кількість користувачів мобільного банкінгу різко зросла; воно зросло з 4,7 мільйона людей у 2018 році до 8,9 мільйона людей у 2022 році – майже вдвічі більше, ніж попередні цифри. Ці цифри красномовно говорять про величезну прихильність цих програм серед користувачів, а також є хорошим провісником їх майбутньої еволюції [26].

2.2 Опис і характеристика досліджуваних банків

З часів першої розробки, мобільні банківські застосунки стали невід’ємною частиною нашого життя. Основою хорошої взаємодії клієнта з банківською установою є довіра. Саме тому банки усіляко намагаються довести своїм клієнтам, що використання саме їх застосунку є безпечним.

Та не безпекою єдиною можна завоювати користувача. Конкурентоспроможність застосунків також підвищує їх простота у використанні.

Через велику варіативність застосунків користувачі прискіпливо відносяться до таких аспектів, як функціональність, легкість використання, привабливість візуального дизайну та інше.

Для дослідження було обрано десять крупних банків, як тих, що мають свої фізичні філії, так і ті, що існують для користувача тільки у віртуальному просторі. У дослідженні порівнюються українські та закордонні банківські застосунки. Серед країн, що розглядаються, окрім України є Німеччина, Франція, Італія та Америка. Через особливості і різноманітні погляди на безпеку та зручність, були обрані саме ці країни. Як було згадано раніше, американська система дещо відрізняється від європейської, яка поширюється на усі країни союзниці. Українські ж установи намагаються вводити стандартизації та інновації, які також зможуть полегшити інтеграцію державних систем до загальноєвропейських.

Перший банк, який досліджується, згаданий раніше, – Stanford FCU, який був створений і використовується в США. Оновлений застосунок Stanford FCU було випущено у вересні 2016 року та було завантажено більше 10000 разів. Stanford FCU Bank пропонує клієнтам два способи завантаження – з сайту банку та PlayMarket [24].

Італійський банківський застосунок Fideuram – наступний банк, який було досліджено. Він з’явився на ринку застосунків в лютому 2015 року. Застосунок завантажено понад 100000 разів і розроблено для пристроїв iPhone.

N26 позиціонується як європейський мобільний банк із головним офісом у Берліні. Застосунок доступний для користувачів у країнах-членах Європейського Союзу, Великобританії та США. N26 був запущений у січні 2015 року і з тих пір зібрав понад 8000000 користувачів [24].

Наступним іноземним банківським застосунком для дослідження став французький мобільний-банкінг Banque populaire, який було презентовано банком Banque populaire du nord у 2010 році. З цього часу кількість завантажень перевищує 1000000. Ця програма використовується виключно у Франції. На сайті банку QR-коди надаються для завантаження програм, відсканувавши їх, можна легко завантажувати програму з різних платформ [24].

Останнім іноземним банківським застосунком є Sparkasse, німецький банк, який отримав понад 10000000 завантажень з моменту розробки свого застосунку в 2014 році. Застосунок – «S-pushTAN – sichere Freigaben» також додатково завантажується і використовується для підвищення надійності автентифікації, але не рекомендується встановлювати його на тому ж пристрої, що і основний банківський застосунок, оскільки це може полегшити проникнення шахраїв у разі злому [24].

Серед українських банків було також обрано повністю віртуальний банк, що фактично існує тільки в мобільному застосунку. Monobank-перший в Україні повноцінний мобільний банк без фізичного відділення, тобто відділення банку Monobank працює з 2017 року і пропонує своїм клієнтам широкий спектр послуг без необхідності відвідувати фізичне відділення. Monobank не поступається своїм конкурентам, а його застосунок завантажили понад 10000000 разів [24].

Наступний досліджуваний і один з найпопулярніших застосунків в Україні вже згадувався раніше. Приват24 був першим мобільним банківським застосунком в Україні, створеним у 2001 році, а застосунок, який використовується сьогодні, був випущений у 2011 році, і його завантажили понад 10000000 користувачів [24].

Ще одним досліджуваним застосунком став Укрсиб-онлайн. Він є менш популярним за Приват24, але також використовується багатьма українцями. Застосунок був розроблений у 2017 році і має понад мільйон користувачів. Укрсиббанк надає посилання для завантаження на своєму сайті, що є плюсом для безпеки користувачів [24].

ПУМБ – український банківський застосунок, що з’явився на ринку у 2018 році. Застосунок сумісний з усіма пристроями, включно зі смартфонами, комп’ютерами та планшетами. На сьогодні застосунок ПУМБ пропонує своїм користувачам великий спектр послуг і має доволі привабливий та комфортний інтерфейс, чим і приваблює своїх користувачів. Наразі кількість завантажень застосунку ПУМБ перевищує 1000000 [24].

Останнім з досліджуваних українських банківських застосунків є застосунок Ощадбанку. Оновлений і більш популярний застосунок з’явився не так і давно, вже після початку пандемії – у 2021 році. Розробники запевняють, що нова версія включає автентифікацію за допомогою PIN-коду картки, тому застосунок має надійний захист. Застосунок Ощадбанк можна завантажити за авторизованим посиланням на сайті Ощадбанку. За цей короткий термін, застосунок завантажили понад 1000000 разів [24].

Перелічені застосунки можна завантажити з офіційних джерел, таких, як легітимний сайт банку. Такий захід допомагає зменшити ризик завантаження користувачем фальшивого застосунку.

Також на сайті банків розміщено багато інформації, що може бути корисною для клієнтів. До такої входять статті про можливі види шахрайств, запобіжні заходи, контакти банку. Також інформація про те, які питання ніколи не поставить представник банку. Таким чином банк проводить певні заходи із підвищення обізнаності своїх клієнтів у сфері кібергігієни.

2.3 Порівняльний аналіз банківських мобільних застосунків

Банківські мобільні застосунки стали одним з найзручніших методів управління фінансами. Кількість користувачів такими мобільними застосунками щорічно збільшується. Разом з тим підвищується ризик виникнення атак у фінансовому секторі, що будуть націлені саме на мобільні банкінги.

У розробці банківських мобільних застосунків важливо звертати особливу увагу на аспекти безпеки. Мобільні банкінги мають прямий зв’язок із серверами банку та взаємодіють з фінансами клієнта. Враховуючи нинішнє законодавче та документальне положення більшість відповідальності за виникнення кіберінцидентів лягає саме на банківські організації.

Проте самим користувачам варто не забувати про важливість безпеки і не нехтувати правилами лише заради миттєвої зручності. Саме тому такі застосунки потребують особливої уваги щодо безпеки. До того ж, розробники намагаються ненав’язливо і непомітно забезпечити своїх клієнтів усіма необхідними заходами безпеки.

Аналіз було проведено за п’ятьма дібраними аспектами безпеки. Аналіз аспектів безпеки закордонних та українських застосунків наведено у табл. 2.1 та табл. 2.2 [24].

Таблиця 2.1 – Аналіз безпеки закордонних банківських застосунків

Безпека	Наявність двофакторної автентифікації	Наявність PUSH-повідомлень	Зміна PIN у застосунку	Вимикати посилену автентифікацію	Вибір власного CVV
Stanford FCU	+	-	-	-	-
Fideuram	+	-	+	-	-
N26	+	+	+	-	-
Banque populaire du nord	+	+	-	+	-
Sparkasse	+	+	+	-	-

Таблиця 2.2 – Аналіз безпеки українських банківських застосунків

Безпека	Наявність двофакторної автентифікації	Наявність PUSH-повідомлень	Зміна PIN у застосунку	Вимикати посилену автентифікацію	Вибір власного CVV
Monobank	+	+	+	-	+
Приват24	+	+	+	-	-
Укрсиб-онлайн	+	+	+	-	-
Ощадбанк	+	-	-	-	-
ПУМБ	+	+	-	-	-

Наявність двофакторної автентифікації сьогодні скоріше є необхідністю, ніж додатковим запобіжним заходом. Двофакторна автентифікація є основою захисту конфіденційності даних клієнта та цілісності його рахунку. Даний захід дозволяє пом’якшити насліди, які можуть виникнути при розкритті зловмисником паролю та логіну для входу. Як правило цього буде не достатньо для нанесення невиправної шкоди. То ж двофакторна автентифікація просить користувача надавати два незалежних підтвердження своєї ідентичності для успішного проведення входу, платежу та інших функцій застосунку.

Наявність PUSH-повідомлень дозволяє банку ефективно та швидко надсилати сповіщення користувачу про виконання важливих дій, таких як проведення та отримання переказу, вхід до застосунку з інших пристроїв, дозволи на проведення транзакцій. Також PUSH-повідомлення допомагають попередити користувачів про виникнення підозрілих або несанкціонованих дій у застосунку та допомагають запобігти та швидше відреагувати на можливі кіберінциденти.

Додатковою перевагою використання PUSH-повідомлень є те, що вони можуть використовуватись в якості додаткової необхідної перевірки для здійснення входу чи проведення інших дій у застосунку. І навіть в разі успішного входу у застосунок зловмисник не зможе проводити ніякі дії без PUSH-повідомлення.

Зміна PIN у застосунку є важливим аспектом безпеки мобільних банкінгів. Рекомендовано періодично змінювати пароль банківського застосунку. Зміна PIN допомагає запобігти використанню зловмисником перехоплених паролів та є профілактичним заходом для запобігання інших видів атак. То ж така дія зменшує ризик несанкціонованого доступу до застосунку. Раніше зміна PIN не була доступною функцією у застосунку, проте зараз допомагає швидко реагувати на можливі загрози та вчасно запобігти несанкціонованому доступу.

Вимкнення посиленої автентифікації за Законом України «Про платіжні послуги» не розглядається, як безпечна дія, адже банки зобов'язані забезпечити своїм клієнтам посилену автентифікацію для виконання певних наборів операцій [18]. Проте вибір вмикати чи вимикати посилену автентифікацію на певних операціях має лишатись правом самого клієнта. Тут аспект безпеки безпосередньо перетинається із аспектами комфорту, адже користувачі прагнуть легкості та швидкості при використанні застосунку, а додаткові перевірки можуть подовжувати час виконання певних операцій.

Вибір власного CVV є ще одним доволі важливим, проте не надто поширеним аспектом безпеки мобільних банківських застосунків. CVV, як правило складається з трьох або ж чотирьох чисел, які розміщуються на зворотній стороні картки. Таким чином даний код використовується для перевірки чи дійсно володіє і є власником картки особа, що хоче здійснити певні дії за допомогою застосунку. Можливість вибору власного CVV допомагає запобігти маніпуляціям шахраїв за допомогою викраденої картки у разі розкриття старого CVV.

За даними з табл. 2.1 та 2.2 можна побачити, що лідерами за шкалою безпеки є N26, Sparkasse, Banque populaire du nord, Monobank, Приват24 та Укрсиб-онлайн. Зважаючи на отримані результати помітно, що українські банки

намагаються не поступатись міжнародним. Більше того, за розглянутими пунктами, лідером є український Monobank, який набрав чотири пункти з п’яти.

Єдиним банківським мобільним застосунком, який все ж дозволяє своїм користувачам керувати посиленою автентифікацією виявилась французька розробка – Banque populaire du nord. Найнижчий результат за безпекою показав застосунок, який є одним з найстаріших розробок – Stanford FCU, набравши всього один пункт.

Також з даних табл. 2.1 та 2.2 можна помітити, що українські мобільні банкінги трохи лідирують за показниками безпеки в порівнянні з закордонними застосунками. Проте розглянуті аспекти безпеки не свідчать про точний загальний рівень безпеки програм, а відповідають рівню безпеки на який може вплинути і користувач. Серед аспектів безпеки недоступних при взаємодії користувача із застосунком є також спосіб шифрування даних, використання криптографічних шифрів, рівень стійкості застосунку до відмов та багато іншого.

Як було згадано раніше, нерідко користувачі надають більшу перевагу зручним і привабливим застосункам, а вже з годом замислюються про їх безпеку. З часів перших мобільних банкінгів пройшла значна еволюція можливостей, які можуть бути запропоновані користувачу. Перші застосунки могли запропонувати своїм користувачам лише перевірку балансу та виконання простих транзакцій, таких як переказ коштів. Проте на сьогодні через банківські застосунки можна виконувати різні види операцій.

Запропоновані операції можна поділити на декілька умовних категорій:

- операції, що дозволяють отримати та керувати даними облікового запису. До цієї категорії відносяться: перевірка балансу, перегляд звітностей про витрати та доходи, перевірка історії транзакцій та інше;
- операції, що дозволяють проводити транзакції, такими є здійснення переказів, сплата рахунків та інше;
- операції, що відносяться до служби підтримки, за їх допомогою користувач може знаходити найближчі банкомати, користуватись технічною підтримкою банку та інше;

- операції, що дозволяють стежити за новинами, така функція у застосунках дозволяє дізнатись актуальні новини з фінансового сектору або ж самої банківської установи.

Для проведення порівняльного аналізу зручності українських та закордонних банківських мобільних застосунків було обрано п’ять критеріїв, які дозволяють оцінити загальний стан зручності застосунків. Порівняльний аналіз наведено у табл. 2.1 – 2.4 [24].

Таблиця 2.3 – Аналіз зручності закордонних банківських застосунків

Зручність	Сплата будь-якого рахунку	Кредитна лінія у застосунку	Відкриття валютного депозиту	Аналіз витрат і доходів	Наявність страхування
Stanford FCU	-	-	-	-	-
Fideuram	+	-	-	+	-
N26	+	-	-	+	+
Banque populaire du nord	+	+	-	+	+
Sparkasse	+	-	-	+	-

Таблиця 2.4 – Аналіз зручності українських банківських застосунків

Зручність	Сплата будь-якого рахунку	Кредитна лінія у застосунку	Відкриття валютного депозиту	Аналіз витрат і доходів	Наявність страхування
Monobank	-	+	+	+	+
Приват24	+	+	+	+	+
Укрсиб-онлайн	-	-	-	+	-
Ощадбанк	-	-	-	+	+
ПУМБ	-	+	+	+	+

Сплата будь-якого рахунку із застосунку є зручною функцією банківського застосунку, адже користувач зможе сплатити будь-які рахунки, починаючи від комунальних послуг і продовжуючи благодійними внесками.

Кредитна лінія у застосунку – хороше доповнення, яке істотно полегшує життя клієнтам банку. Раніше для оформлення кредиту чи зміни кредитного ліміту, клієнту необхідно було прийти до банку. Проте зараз ці операції займають декілька хвилин. Враховуючи, що гроші можуть терміново і не заплановано знадобитись, така функція робить використання застосунку ще зручнішим і комфортнішим.

Можливість відкриття валютного депозиту у застосунку позитивно впливає на прихильність користувачів до банківського мобільного застосунку. Така функція стала широко популярною відносно нещодавно. За допомогою застосунку клієнти можуть відкрити ще один депозит, який може містити будь-яку валюту. При цьому не обов'язково звертатись до фізичного відділення банку, як це було раніше. У цього рахунку будуть доступні такі ж функції, як і у звичайного. Можливість перевірити баланс, здійснення переказів, а також доступ до іншої важливої інформації пов'язаної з валютним рахунком.

Аналіз витрат і доходів є базовою функцією мобільних банківських застосунків. Така функція дозволяє слідкувати за витратами та надходженнями, відслідковувати історію транзакцій. Якщо раніше для цього було необхідно отримувати виписку з рахунку у фізичному банку, зараз такі дії виконуються за секунду і істотно полегшують взаємодію між банком та клієнтом.

Наявність страхування у застосунку є зручним доповненням до інших функцій. Таке страхування може включати у себе, як страхування фізичної особи, так і страхування особистого рахунку клієнта. Зручним є те, що за допомогою застосунку клієнт може з легкістю не тільки оформити страхування, а і керувати його умовами. Це робить процес оформлення страхування більш комфортним, адже тепер клієнту не потрібно відвідувати банк.

За даними з табл. 2.3 та 2.4 найкраще у аспектах зручності проявили себе такі банківські мобільні застосунки, як Monobank, ПУМБ, N26, Banque populaire du nord. Найбільше відповідностей було помічено у застосунку Приват24.

Найгірші результати було виявлено у одного закордонного застосунку, а саме Stanford FCU. Stanford FCU не отримав позитивної відмітки за жодним з показників.

Серед українських банкінгів найгіршим за аспектами зручності виявився Укрсиб-онлайн, набравши всього один пункт – «Аналіз витрат і доходів». Проте безпекова складова частково компенсує дані недоліки застосунку.

Також аналізуючи дані таблиць 2.3 та 2.4 стає помітно, що українські банківські застосунки в загальному вигляді мають вищі показники зручності, ніж

закордонні, що є певною перевагою. Проте розробники українських банківських застосунків мають звернути більшу увагу на аспекти безпеки, які можуть підвищити рівень довіри клієнтів до такого виду технологій. Ввести більший контроль з боку держави та загальні стандартизації для державних банківських установ. А також покращити інфраструктуру для більшого розповсюдження точок доступу до Інтернету.

Проте іноземним спеціалістам також є чому повчитись на нашому досвіді. Українські банківські застосунки є більш комфортними для користувачів, працюють швидше і зрозуміліше для звичайного користувача. Поліпшений інтерфейс, не нав'язливе введення обов'язкових процедур безпеки та введення миттєвих переказів може істотно підвищити рівень конкурентоспроможності банківського застосунку на ринку застосунків.

Хоч зберегти баланс між безпекою та зручністю це складна задача, деяким досліджуваним банківським застосункам це вдалось і вони показали гарний результат за досліджуваними параметрами. Серед іноземних застосунків найкращий результат за обома показниками було виявлено у застосунках N26 та Banque populaire du nord, також застосунок Sparkasse показав негірший результат за безпекою, але дещо гірший за показниками зручності.

Серед українських мобільних банківських застосунків можна виділити Monobank та Приват24. Непоганий результат, як і Sparkasse показав застосунок ПУМБ. Який має більшість показників зручності, проте безпековими аспектами поступається своїм конкурентам.

2.4 Недовіра клієнтів, огляд прикладів кібератак та практичні поради з безпеки

Не дивлячись на доволі успішні показники за аспектами зручності та безпеки, за статистикою наведеною у статті Гасій О.В., Скорба О.А. та Рошко Н.Б. [27], все ж українці користуються мобільними банківськими застосунками менше, ніж громадяни країн Європейського Союзу – рис. 2.1 [27].

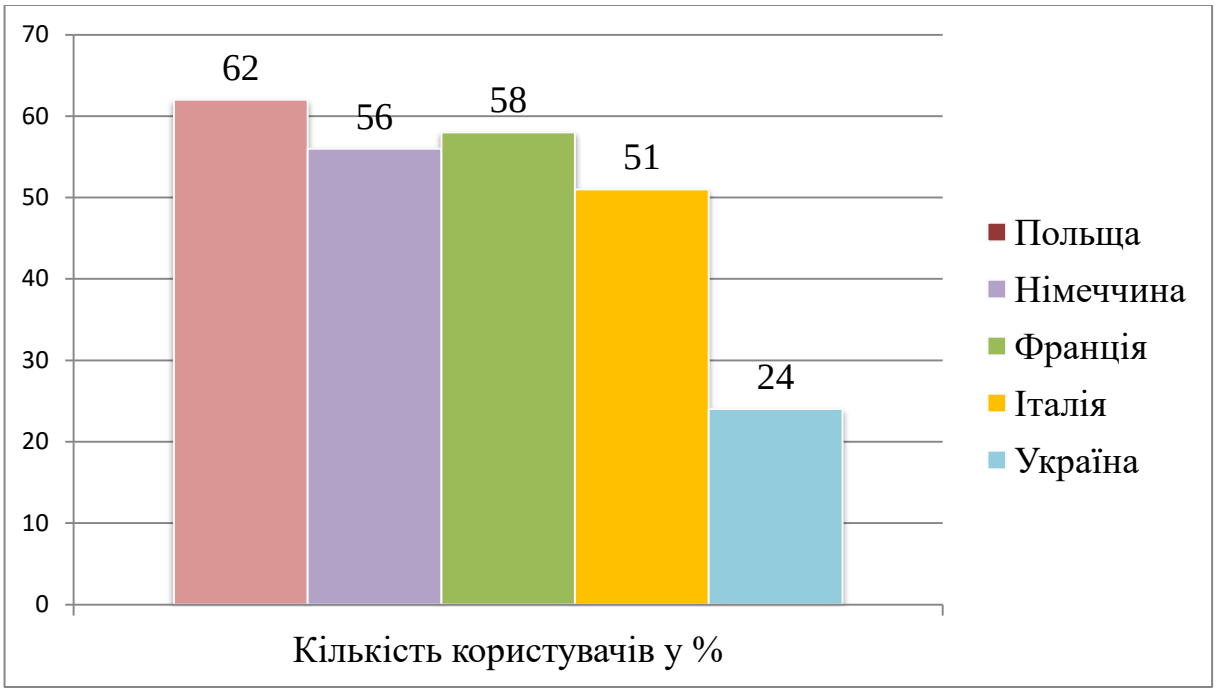


Рисунок 2.1 – Статистика поширення використання мобільних банкінгів у країнах ЄС та Україні за кінець 2023 р. – початок 2024 р.

Така статистика може бути пов’язана з певним рівнем недовіри клієнтів до вітчизняних банківських систем. Що в свою чергу викликана збільшеннями кількості кібератак з початку повномасштабного вторгнення.

То ж початок повномасштабного вторгнення мав свій вплив також і на банківську сферу, виникла висока потреба у швидкій діджиталізації [28]. Постала необхідність у віддаленій та швидкій сплаті, переказі, звіті. При чому, завдяки високому рівню можливостей, які надають українські мобільні банкінги, громадяни могли користуватись ним і за кордоном. Адже для отримання фінансової допомоги необхідно було надати звідності з банків про стан рахунку та баланс. То ж для проведення цих операцій не потрібно було відвідувати філіал, що звісно привернуло увагу нової кількості клієнтів до використання мобільних банкінгів.

Проте не можна сказати, що це призвело до збільшення довіри до мобільних банкінгів, для користувача все ще лишаються певні переваги та недоліки за якими він віддає або не віддає перевагу використанню банківських застосунків. То ж можна виділити такі переваги та недоліки, що впливають на прихильність користувачів до мобільних банківських застосунків – табл. 2.5 [27].

Таблиця 2.5 – Переваги та недоліки мобільного банкінгу, що впливають на прихильність користувачів

Переваги	***Недоліки***
Швидкість доступу до банківських послуг	Високий рівень залежності від мережі Інтернет
Цілодобова доступність	Можливість втратити кошти
Спрощеність системи надання банківських онлайн послуг	Можливість втратити конфіденційну інформацію
Мала часова витратність	

Ще з часів появи перших мобільних банкінгів, шахраї почали вигадувати різноманітні способи для отримання власної вигоди, себто для незаконного отримання інформації чи збагачення. Мобільні банківські застосунки працюють в якості посередника між банком та клієнтом – це стало додатковою ланкою можливостей для злодіїв.

Будь-який розвиток технологій безпеки не тільки покращує захист, а і призводить до розвитку злочинців. При цьому, нові шахрайські схеми також надихають представників інформаційної безпеки для покращення старих заходів безпеки. У першому розділі у загальному вигляді було розглянуто види загроз та вразливостей у банківських мобільних застосунках. У цьому підрозділі пропонується розглянути конкретні випадки кібератак, які були здійснені на українські мобільні банкінги.

Наразі українські банківські застосунки доволі часто стають жертвами спроб здійснення різних видів кібератак, раніше згадувалось, що більшість атак здійснюється з території росії. Одним з найскладніших періодів для кіберсектору в Україні став початок 2022 року, коли кожна десята кібератака була спрямована саме на фінансовий сектор [26].

Одним з прикладів таких масових атак є 15 лютого 2022 року. За даними розслідувань, цього дня російські спецслужби вчинили масштабні кібератаки на різні сфери функціонування України. Одними з жертв стали застосунки великих банківських корпорацій. Атаки зазнали мобільні застосунки таких банків: ПриватБанк, Ощадбанк, АльфаБанк, Monobank та інші. Ворог використав DDoS-

атаки для дестабілізації застосунків. Таким чином вони занадто навантажували трафік, що в порівнянні було значно більше за звичайний потік користувачів [26].

Це призвело до того, що легітимні користувачі не мали можливості користуватись застосунком у звичайному режимі, виконувати фінансові операції і навіть просто авторизуватись у застосунку. Атака продовжувалась цілий день і припинилась приблизно опівночі. На щастя до серйозних втрат це не призвело, проте порушило роботу застосунків ще на деякий час після відбиття атаки.

Ще одна DDoS-атака націлена на електронні системи ПриватБанку сталась у 2023 році, і тривала з 13:45 до 17:00 з обсягом трафіку 600 Гбіт/с [29]. Ця атака є прикладом одної з чисельних атак, які довелось відбити з початку повномасштабного вторгнення, українським спеціалістам з кібербезпеки.

У грудні 2023 року сталась атака на мережу «Київстар». Вона не була напряму пов’язана із банківською системою, проте навела безладу у деяких банківських мережах. Окрім збою роботи у певних відділеннях та банкоматах, перебої мережі також призвели до погіршення роботи деяких банківських застосунків. Так, наприклад, Ощад24, який при проведенні транзакцій просить проходження подвійної автентифікації не міг провести автентифікацію за СМС кодом належним чином. Адже через проблеми мережі повідомлення просто не могло надійти до користувачів мережі «Київстар». Причиною атаки став комп’ютерний черв’як, який потрапив до корпорації. То ж мобільні банкінги залежать не тільки від очевидних умов, а і можуть не працювати належним чином, наприклад, через проблеми оператора мережі та зв’язку. Тут у нагоді стала б функція управління двофакторною автентифікацією з боку користувача. Проте такий вид переказів все ж можна було б назвати не однозначно безпечними. У той же день DDoS-атаки зазнав і Monobank, проте фахівці змогли вдало її відбити і дані клієнтів жодним чином не постраждали [26].

Ще одна атака на Monobank сталась 2 травня 2024 року. Ця атака також відноситься до DDoS-атак. Користувачі віртуального банку не могли зайти у застосунок, адже той видавав помилку. На щастя, на цю атаку теж було успішно прореаговано та відбито, і дані та вклади користувачів не постраждали [30].

Іноземні банківські застосунки та й загалом банківські електронні системи також під загрозою виникнення кібератак. Так 18 жовтня 2012 року HSBC Holdings – британський транснаціональний банк став жертвою кібератаки. Тоді важливі дані клієнтів не постраждали, проте витік такої інформації, як електронні пошти, імена та інше, міг спричинити масштабну кібератаку [31].

У 2019 році виявили кібератаку на мобільний застосунок Bank of America. Хакери використали LockBit, щоб викрасти конфіденційні дані користувачів, такі як ім’я, адреса та фінансові дані. LockBit відноситься до програм вимагачів. Від цієї атаки постраждало близько 57000 клієнтів [32].

Фатальні помилки при захисті застосунку можуть допускати, як працівники банку, так і його клієнти. Помилки в дизайні, що супроводжуються слабкою безпекою, реалізованою під час розробки програми, часто призводять до зломів. До таких недоліків відносять [26]:

- недостатня перевірка вхідних даних може дозволити зловмисникам впровадити шкідливий код у застосунок;
- слабке управління сеансами призводить до несанкціонованого доступу до облікових записів користувачів;
- недостатня обробка помилок дає можливість розкриття конфіденційної інформації потенційним зловмисникам;
- погано реалізований контроль доступу може призвести до несанкціонованих дій у застосунку;
- відсутність безпечних методів кодування робить застосунок вразливим до різних атак.

Є також інші помилки, яких варто уникати. Помилки в кодуванні можуть порушити роботу мобільного застосунку, іноді спричиняючи непередбачені наслідки. Ці вразливості можуть виникати через такі проблеми, як переповнення буфера, помилки рядка форматування та умови конкуренції. Щоб захистити програму від таких проблем, дуже важливо мати надійний метод тестування безпеки мобільного банкінгу. Цей метод допомагає помітити та зупинити ці

помилки кодування, перш ніж вони стануть проблемами, забезпечуючи безперебійну та безпечну роботу програми [26].

Застосунки мобільного банкінгу часто потребують підключення до зовнішніх джерел, щоб працювати в повному обсязі. Однак зовнішні джерела – більше точок входу для кіберзлочинців, щоб отримати доступ до конфіденційної інформації в програмі мобільного банкінгу. Ось чому ретельне тестування банківських застосунків є надважливим для їх захисту [26].

Якщо клієнти не планують установку програми належним чином і не знайомі з комп'ютерними системами, це може призвести до помилок. Наприклад, вони можуть забути видалити облікові записи налагодження або паролі. Чи можуть зіткнутися з проблемами з керуванням версіями. Тому важливо налагоджувати увесь процес таким чином, щоб користувач однозначно міг пройти процес встановлення та налагодження правильно і безпечно. Наприклад, у 2018 році в основних магазинах застосунків службами США було виявлено майже 65000 підроблених програм. Тому США проводять контроль банківських застосунків у онлайн-маркетах, тобто постійно перевіряють мережу на наявність шахрайських підробок популярних банківських застосунків. До того ж більшість великих банків США надають посилання на свій мобільний застосунок на своєму веб-сайті [26].

Як згадувалось вище, користувачі не менше відповідальні за безпеку своїх рахунків, ніж банки. Тому рекомендовано щомісяця оновлювати паролі застосунків, оновлювати програмне забезпечення, уникати загроз не тільки мобільним банкінгам, а і усьому мобільному пристрою, при виявленні підозрілої активності повідомляти відповідні служби [26].

Навчання користувачів та персоналу банку є не менш важливими заходами безпеки, адже нерідко саме ці змінні в системі безпеки є найвразливішими. Зловмисники часто використовують методи соціальної інженерії, які націлені на велику масу людей. У такому випадку, помилка співробітника чи самого користувача застосунку може призвести до втрат даних та накопичувань.

ВИСНОВКИ

Активний розвиток технологій вплинув і на розвиток фінансового сектору в усьому світі. За останні роки банківські мобільні застосунки стають все більше популярними. Проте сама технологія мобільного банкінгу починала своє зародження з минулого сторіччя.

Не дивлячись на великий та активний розвиток, користувачі все ще сумніваються чи довіряти цим технологіям свої особисті дані, а тим паче надавати доступ до рахунків. Та все ж банківські застосунки привертають до себе все більшу кількість людей, пропонуючи різноманітні послуги.

Якщо перші мобільні банківські застосунки мали обмежений перелік функцій, які надавали лише можливість сплати, а потім і слідкування за транзакціями, то зараз спектр надаваних послуг значно розширився, користувачі можуть сплачувати більшість рахунків, таких як плата комунальних рахунків, отримувати виписки про витрати і надходження, брати кредити через застосунок, отримувати послуги страхування, керувати підписками, відкривати рахунок та ще багато іншого.

Проте зручність часом не здатна компенсувати безпекові ризики. Починаючи з виникнення перших мобільних банківських застосунків, кіберзлочинці намагаються знайти можливість обійти системи безпеки задля наживи. Види загроз поділяють на три можливі види: незаконний доступ до пристроїв користувачів; втручання під час передачі даних; незаконний доступ до серверів банку. До конкретних прикладів найпоширеніших загроз відносять: фішинг, такі види шкідливого програмного забезпечення, як кейлогери, підроблені банківські застосунки, погано реалізовані системи безпеки, а також атаки на злам Wi-Fi та атаки виду «людина посередині».

Стандарти та закони в США, країнах ЄС та Україні дещо відрізняються між собою. У країнах ЄС регулювання кібербезпеки мобільних банкінгів та й загалом банків відбувається на рівні рішень Європейського Союзу. Діючими стандартами

та регуляторними рішеннями є PSD2, RTS, NIS2, а також дані клієнтів підлягають захисту загальним регламентом захисту даних (GDPR).

Система регулювання кібербезпеки мобільних банкінгів у США дещо відрізняється, адже рішення щодо безпеки банківських застосунків приймаються не тільки на рівні держави, а і окремо на рівні кожного штату. Також більшість норм США націлені на боротьбу з шахрайством та відмиванням коштів. Одним з показових законів є Закон про мобільні зв'язки, що увійшов в дію з 2018 року. Найбільшими організаторами стандартів та норм у США є організація NIST.

Українська система безпеки банківських мобільних застосунків намагається наблизитись до європейської, проте рішення щодо безпеки все ще можуть прийматись окремими банківськими установами. В Україні також було введено в дію ISO 20022 та мобільні і апаратні токени. Також новим введенням стала сертифікація PCI DSS. Основними регулюючими законами є Закон «Про банки і банківську діяльність» та Закон «Про платіжні послуги».

Проводячи порівняльний аналіз українських та закордонних банківських застосунків за аспектами безпеки та зручності було визначено, що українські мобільні банкінги можуть конкурувати з іноземними банкінгами, і за деякими показниками мають кращі результати. Проте системи безпеки вітчизняних застосунків ще потребують розвитку систем безпеки, а також розвитку супутньої інфраструктури для отримання більшої прихильності користувачів.

Натомість іноземні банківські застосунки часом потребують більшої уваги щодо аспектів зручності, задля конкурентоспроможності на великому ринку мобільних банківських застосунків.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Головні тенденції банківського ринку за 12 місяців війни. [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/columns/2023/03/13/697976/.

2. Броня фінтеху за сотні тисяч доларів. [Електронний ресурс]. – Режим доступу: https://forbes.ua/money/bronya-fintekhu-za-sotni-tisyach-dolariv-pid-chas-viyni-kiberataki-na-finansoviy-biznes-pochastishali-v-razi-yak-kompanii-zakhishchayutsya-vid-napadiv-04052023-13434.

3. Digital fraud in Ukraine grows by 13% compared to last year. [Електронний ресурс]. – Режим доступу: https://www.taslink.ua/en/didzhytal-shakhraystvo-v-ukrayini-zroslo-na-13-u-porivnyanni-z-mynulym-rokom/.

4. The Risks of Mobile Banking Apps: Keep Your Money Safe. [Електронний ресурс]. – Режим доступу: https://www.identityguard.com/news/risks-of-using-mobile-banking-apps.

5. Increased Use of Mobile Banking Apps Could Lead to Exploitation. 10 June 2020. [Електронний ресурс]. – Режим доступу: https://www.ic3.gov/Media/Y2020/PSA200610.

6. SharkBot: a new generation of Android Trojans is targeting banks in Europe [Електронний ресурс]. – Режим доступу: https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe.

7. The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them. [Електронний ресурс]. – Режим доступу: https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/.

8. Are banks Cyber-proof in the digital world. [Електронний ресурс]. – Режим доступу: https://www.bankingsupervision.europa.eu/press/speeches/date/2020/html/ssm.sp201022~a0b3fd5947.en.html.

9. Comarch Financial Services. [Електронний ресурс]. – Режим доступу: https://www.comarch.com/finance/articles/.

10. PSD2 та відкритий банкінг. [Електронний ресурс]. – Режим доступу: https://itomychstudio.com/ua/blog/psd2-open-banking.

11. Commission Delegated Regulation amending the RTS as regards the 90-day exemption for account access. [Електронний ресурс]. – Режим доступу: https://www.regulationtomorrow.com/eu/commission-delegated-regulation-amending-the-rts-as-regards-the-90-day-exemption-for-account-access/.

12. Cyber regulations for banking in Europe vs. America. [Електронний ресурс]. – Режим доступу: https://blog.rsisecurity.com/cyber-regulations-for-banking-in-europe-vs-america/.

13. NIS2 Directive: New EU cybersecurity and compliance requirements. [Електронний ресурс]. – Режим доступу: https://build38.com/nis2-directive/.

14. Comarch tPro ECC. USB token used mainly for authorization of documents and online transactions. [Електронний ресурс]. – Режим доступу: https://www.comarch.com/cyber-security/adaptive-authentication-suite/tpro/tpro-ecc/.

15. Comarch tPro ECC. tPro Mobile for mobile banking security. [Електронний ресурс]. – Режим доступу: https://www.comarch.com/cyber-security/adaptive-authentication suite/tpro/tpro-mobile/.

16. Mobile Banking Compliance Requirements: Does Your Product Comply with Latest Trends. [Електронний ресурс]. – Режим доступу: https://binariks.com/blog/mobile-banking-compliance-requirements/.

17. Закон України Про банки і банківську діяльність (Відомості Верховної Ради України (ВВР), 2001, № 5-6, ст.30). [Електронний ресурс]. – Режим доступу: https://www.comarch.com/finance/articles/.

18. Закон України Про платіжні послуги (Відомості Верховної Ради України (ВВР), 2023, № 10-11, ст.26) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1591-20#Text.

19. Національний банк України. Упровадження стандарту ISO 20022. [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/ua/payments/project-iso20022.

20. Сертифікація PCI DSS в Україні. [Електронний ресурс]. – Режим доступу: https://www.certvalue.com/pci-dss-certification-in-ukraine/.

21. Payment Card Industry Data Security Standard. Version 4.0. – Режим доступу: https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf.

22. Що таке сертифікація PCI DSS, і навіщо вона потрібна для приймання платежів. [Електронний ресурс]. – Режим доступу: https://interkassa.com/blog/shcho-take-sertyfikatsiia-pci-dss.

23. Comarch tPro gets certified in Ukraine. [Електронний ресурс]. – Режим доступу: https://www.comarch.com/finance/news/comarch-tpro-gets-certified-in-ukraine/.

24. Логачова Є. О. Порівняльний аналіз українських та закордонних банківських застосунків / Є. О. Логачова, М. В. Єсіна // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2024. – Випуск 216. – С. 57-61.

25.“Stanford Federal Credit Union Transforms Member Experience with Digital Banking Innovations”. [Електронний ресурс]. – Режим доступу: https://www.q2.com/blog/stanford-federal-credit-union-transforms-member-experience-with-digital-banking-innovations.

26. Єлизавета Логачова Аналіз особливостей забезпечення кібербезпеки у банківських мобільних додатках / Єлизавета Логачова, Марина Єсіна, Всеволод Бобух//. Computer science and cybersecurity. – Харківський національний університет імені В. Н. Каразіна, 2023, Випуск 1(23) – С. 63–73. – Режим доступу: https://periodicals.karazin.ua/cscs/article/view/23094/21104.

27. Гасій О. Вплив Інтернет-банкінгу та мобільних додатків на зручність та доступність банківських послуг для клієнтів в Україні / О. Гасій, О. Скорба, Н. Рошко //. Економіка та суспільство, 2024. [Електронний ресурс]. – Режим доступу: https://economyandsociety.in.ua/index.php/journal/article/view/3466.

28. Ірина Химич Діджиталізація банкінгу в Україні: переваги та виклики для клієнтів та фінансових установ / Ірина Химич, Юрій Петручок //. – Тернопільський національний технічний університет імені Івана Пулюя

м. Тернопіль, Україна. – Режим доступу: https://elartu.tntu.edu.ua/bitstream/lib/40873/2/MNPK_2023_Petruchok_Y-Digitalization_of_banking_67-69.pdf.

29. Найбільша кібератака в Україні була здійснена на «ПриватБанк» та тривала понад 3 години. 2023 – [Електронний ресурс]. – Режим доступу: https://mvs.gov.ua/news/naibilsa-kiberataka-v-ukrayini-bula-zdiisnena-na-privatbank-ta-trivala-ponad-3-godini.

30. На monobank здійснюється потужна DDoS-атака – Гороховський, Юрій Тарасовський. 2024. [Електронний ресурс]. – Режим доступу: https://forbes.ua/news/na-monobank-zdiysnyuetsya-potuzhna-ddos-ataka-gorokhovskiy-02052024-20938.

31. HSBC Is the Latest Attack Victim Tenth Bank Affected by DDoS in Recent Weeks. [Електронний ресурс]. – Режим доступу: https://www.bankinfosecurity.com/hsbc-latest-ddos-victim-a-5213.

32. Bank of America Customers Left In The Dark About Data Breach For 90 Days. [Електронний ресурс]. – Режим доступу: https://www.forbes.com/advisor/personal-finance/data-breach-affects-bank-of-america-customers/.

ДОДАТОК А

ПЕРЕЛІК ПУБЛІКАЦІЙ

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

УДК 004.056.5

АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У БАНКІВСЬКИХ МОБІЛЬНИХ ДОДАТКАХ

Єлизавета Логачова[1], Марина Єсіна[1,2], Всеволод Бобух[2]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
lohachova2020kb11@student.karazin.ua, m.v.yesina@karazin.ua

[2] АТ «ІІТ», вул. Коломенська, 15, Харків, 61166, Україна
jsciitua@gmail.com

Надійшла: листопад 2023. Прийнята: грудень 2023.

***Анотація**: В даній статті розглядаються важливі аспекти забезпечення кібербезпеки в мобільних банківських додатках. В роботі аналізуються потенційні загрози безпеки та ефективні стратегії, щодо їх запобігання та протидії. У зв'язку зі стрімким розвитком цифрових технологій у банківській галузі, мобільні застосунки та онлайн сервіси стали необхідною складовою фінансового взаємодії клієнтів, забезпечуючи зручні та ефективні фінансові операції. Однак, розвиток функціонату таких застосунків породжує нові виклики у сфері кібербезпеки, на які активно відповідають фахівці з інформаційної безпеки. Стаття присвячена оглядовому аналізу міжнародних та вітчизняних стандартів кібербезпеки в банківському секторі, а також містить аналіз мобільних додатків відомих українських банків. На основі цього аналізу формулюються конкретні рекомендації, стосовно можливостей подальшого вдосконалення кібербезпеки в таких застосунках. Розглядається вплив комфорту клієнтів на рівень безпеки. Крім того, в роботі розглядається вплив рівня безпеки в банківському секторі на загальну діджиталізацію фінансової галузі. Автори роблять акцент на тому, як підвищення рівня безпеки може стимулювати та підтримувати процеси діджиталізації, забезпечуючи довіру клієнтів та оптимальне використання мобільних банківських застосунків. Комплексний підхід до оцінки рівня безпеки, порівняння різних додатків і стандартів (як українських, так і міжнародних), а також розгляд взаємозв'язку питань безпеки та інновацій в банкінгу, роблять цю роботу корисною для розуміння тенези кібербезпеки у сфері мобільного банкінгу.*

***Ключові слова:** банківська система, безпека, загрози, кібербезпека, банкінг, мобільні додатки.*

1. Вступ

З приходом діджиталізації більшість сфер побутового життя значно полегшились. Банківська сфера також зазнала змін – на ринку з'явились мобільні банкінги – застосунки банківських установ, за допомогою яких з легкістю можна виконати більшість банківських операцій фізично не відвідуючи саму установу. Заради приваблювання клієнтів розробники вимушені йти на поступки і зменшувати потужність захисту задля зручності, бо навряд когось із користувачів привабить довге і незручне проходження автентифікації, коли легше буде піти у найближче відділення. То ж переважна більшість користувачів вимагають від банківських застосунків більшого комфорту, не замислюючись при цьому про ризики безпеки.

Фінансовий сектор був і залишається привабливим для кіберзлочинців, зі збільшенням розвитку технологій, збільшується кількість атак. У контексті України з 2022 року кількість кібератак зросла на 2.8%, де кожна 10-та атака була здійснена на фінансовий сектор. На жаль, країна-агресор продовжує потуги розбити фінансову систему нашої країни, таким чином наносячи велику шкоду роботі держави [1]. Банківські застосунки мають низку особливостей з точки зору кібербезпеки, адже, на відмінну від більшості додатків, зберігають особисту інформацію клієнта і поєднуються безпосередньо із самою банківською установою.

2. Актуальні загрози та вразливості банківських додатків

Важливо усвідомлювати, що розвиток технологій та стратегій захисту будь-яких додатків, у тому числі і банківських, призводить до росту і розвитку іншої сторони – кіберзлочинності. Починаючи з 2020 року діджиталізація (цифровізація) різних сфер життя набула попу-

 © Логачова Є., Єсіна М., Бобух В., 2023

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

лярності і досі є одним з важливих аспектів ведення бізнесу чи іншої діяльності. Задля підвищення рівня конкурентоспроможності, банки додають все більше функцій та часом нехтують безпекою заради зручності.

Банкінги, як і інші програмні застосунки, що можуть надавати доступ до грошей, є привабливою мішенню для злочинців. То ж сьогодні клієнти банків мають турбуватись не тільки про те, як вберегти свою фізичну банківську картку й особисті дані, а і як убезпечити себе від мобільних-шахраїв, які мають у своєму розпорядженні «вагомий» арсенал різних злочинних схем та методик проведення атак для здобуття доступу до їх грошей.

Мобільний банкінг означає використання спеціального програмного застосунку, розробленого банком. Це відрізняється від банкінгу онлайн, який передбачає вхід на веб-сайт банку на телефоні та/чи через комп'ютер. Як не дивно, але це має певне значення при розгляді питань безпеки.

Банки мають більше контролю над безпекою рахунку при користуванні застосунком, ніж при використанні веб-сайту. Наприклад, шахраї можуть створювати фішингові сайти, схожі на сторінку входу банку, або перехоплювати користувацьку мережу *Wi-Fi*. Але злочинцям набагато важче вдатися до шахрайства у випадку програмного застосунку. Однак це не означає, що у такому випадку використання банкінгу є цілком безпечним [2].

Програми мобільного банку передають дані між пристроєм клієнта та сервером банку. З цього виділяється три основні можливості здійснення шахрайств пов'язаних з банкінгами:

1. Доступ на пристрої користувача;
2. Під час передачі даних;
3. Доступ на сервері самого банку.

Тож усі дії шахраїв будуть засновані на цих трьох аспектах. Варто також пам'ятати, що кіберзлочинці несуть загрозу не тільки клієнтам, а і самому банку для якого найголовнішим пріоритетом є довіра клієнтів [2].

Атаки соціальної інженерії. Атаки соціальної інженерії використовують психологію та «терміновість», щоб обманом змусити жертв піти на розкриття облікових даних, які пропонують шахраям доступ до фінансових рахунків. Такі дії можуть включати у себе повідомлення та дзвінки, що надходять нібито з банку. Насправді ж, злочинці змушують повірити клієнта, що його рахунок якимось чином під загрозою і усе, що необхідно зробити – надати необхідні секретні дані.

Також поширеним є погроза «зламу» картки і маніпуляція про необхідність здійснення переказу на інший рахунок. Якщо клієнт погоджується, то фактично власноруч здійснює переказ, який неможливо скасувати, на реквізити зловмисника [2].

Фішинг. Фішинг є однією з найулюбленіших стратегій шахраїв для викрадення інформації або компрометацію пристроїв потенційних жертв. Фішинг-лист, що надходить під виглядом звичайного і містить у собі посилання, файли і так далі, у випадку завантаження активізує свої зловмисні наміри. Ці електронні листи можуть виглядати так само, як листи, які клієнти звикли отримувати від свого банку, і відправник може навіть підробити ім'я «від» для того, щоб виглядати легітимним [2]. Найгіршим у такий спосіб є той факт, що посилання у фішингових електронних листах можуть завантажити на пристрій жертви зловмисне програмне забезпечення (ПЗ), яке в наступному надасть хакерам доступ до мобільної банківської програми. Фішингові електронні листи також не обов'язково надходять від банку, наприклад можна отримати зловмисний електронний лист від шахраїв, які видають себе за *Netflix*, кур'єрську службу тощо [2].

Фізична крадіжка пристрою. Мабуть, один з найпримітивніших способів, проте також небезпечний – викрадення пристрою. У деяких випадках, пристрій навіть не потрібно викра-

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

дати, клієнт сам віддає його у руки, наприклад, відносячи телефон до ремонту у неперевірені сервіси. Хакери з відносною легкість зможуть знайти доступ до такого пристрою і до банківських додатків, використовуючи надалі пристрій клієнта для своїх дій [2].

Підробка банківських додатків. Якщо шахраї не зможуть отримати доступ до вашої мобільної банківської програми, вони спробують обманом змусити вас використовувати шахрайську програму. Так, наприклад, за 2020 рік ФБР (*Федеральне Бюро Розслідувань*) повідомило, що було виявлено майже 65000 підроблених банківських програм [3]. Ці підроблені програми виглядають, як цілком законні, але після вводу облікових даних, замість входу, користувач отримує повідомлення про помилку. У той же час шахрай отримав облікову інформацію жертви буде намагатися увійти у обліковий запис у справжньому додатку, а коли ж користувач зрозуміє, що його вже ошукали, то може бути вже пізно [2].

Зловмисне програмне забезпечення – кейлогери

Хакери використовують тип зловмисного ПЗ, яке записує всю інформацію, яка вводиться власником гаджету з якого відбувається сеанс банкінгу, зокрема банківські рахунки і паролі. При завантаженні додатків під контролем кейлогерів, злочинці зможуть легко зайти у відповідну банківську програму. Навіть гірше, можна випадково завантажити зловмисне ПЗ на свій пристрій, просто від сканувавши відповідний *QR*-код у відкритому доступі [2]. Тож навіть, якщо не завантажувати шахрайську банківську програму, шахраї все одно можуть отримати доступ до рахунків через інші заражені шкідливим ПЗ, програмні додатки.

Інші види шахрайств. Окрім вже перерахованих видів є ще багато зловмисних дій направлених на викрадення клієнтських статків, які варті не меншої уваги.

- *Трояни Android, такі, як SharkBot*. Основна мета *SharkBot* – ініціювати грошові перекази зі зламаних пристроїв за допомогою технології автоматичних систем переказу (*ATS*) в обхід механізмів багатофакторної автентифікації [4].
- *Атаки за допомогою програм вимагачів* – при виконанні атаки шахраї викрадають і шифрують важливі фінансові документи, блокують клієнтів у системах, паралізують банківські системи і за спокій вимагають викуп [5].
- *Незашифровані дані* – здебільшого уся важлива інформація шифрується, проте деякі дані лишаються незашифрованими на банківському сервері, зловмисники націлені знайти ці дані про клієнтів [5].
- *Атаки на одноразові паролі* – часто елементом безпеки є використання одноразових паролів, зловмисники можуть намагатись перехопити паролі з мобільних пристроїв користувачів, щоб використати їх на свою користь [5].
- *Атаки на зв'язок* – у даній атаці кіберзлочинці використовують шкідливе ПЗ для перехоплення комунікації між мобільним застосунком і банківським сервером, та інші [5].

Враховуючи все вищезазначене слід підкреслити, що загрозу мобільним банкінгам несуть не тільки кіберзлочинці, а і необізнаність працівників та користувачів гаджетів та послуг відповідних сервісів, з питань ІБ.

3. Стандарти кібербезпеки мобільних банкінгів у Європі та світі

Довіра є основою функціонування банківської системи, руйнування іміджу банку призводить до стрімкого спадання клієнтського потоку та негативно впливає на усю подальшу роботу організації. Саме тому банківські установи не шкодують витрат на розвиток кібербезпеки і постійно оновлюють свої системи згідно нових стандартизацій.

Сфера банківських мобільних застосунків не стала виключенням, а навпаки потребує все більшої уваги. Зважаючи на європейський досвід, можна помітити, що через важливість

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

кібербезпеки у банківському секторі, самі банки не можуть визначати, які стандарти безпеки їм використовувати. У країнах Європейського Союзу (ЄС) право приймати такі рішення не надається окремій країні чи організації, а безпосередньо відбувається на рівні ЄС і є чинними та однаковими для всіх країн учасників. Прикладами таких рішень є *PSD2* – директива про платіжні послуги. А також *RTS* – делегований регламент комісії ЄС 2018/389, який називають доповненням до *PSD2* [6].

RTS доповнює Директиву (ЄС) 2015/2366 Європейського Парламенту та Ради стосовно нормативних технічних стандартів для надійної автентифікації клієнта та загальних і безпечних відкритих стандартів зв'язку. 16 серпня 2022 року Європейська Комісія опублікувала Делегований Регламент Комісії (ЄС) від 3.8.2022, який вносить зміни до регуляторних технічних стандартів (РТС), викладених у Делегованому Регламенті 2018/389, зазначеному вище. Зміни стосувались 90-денного звільнення для доступу до рахунку [7].

Однією з ключових ініціатив в напрямку безпеки є Директива *PSD2*. Одним з основних положень цієї директиви стало введення двофакторної автентифікації для клієнтів банків. Тепер банки повинні вимагати від своїх клієнтів використання принаймні двох компонентів для автентифікації, забезпечуючи високий рівень захисту [6].

Ці компоненти можуть належати до трьох основних категорій: - *«щось, що ви знаєте»*, наприклад, пароль; - *«щось, що ви маєте»*, наприклад, документи, які знаходяться у вас; - та *«щось, що ви є»*, наприклад, біометричні дані. Унікальність цього підходу полягає в тому, що ці компоненти можуть діяти незалежно один від одного, таким чином зменшуючи вразливість системи до порушень [6].

Директива *PSD2* покладає велику частку відповідальності за інциденти на банки, змушуючи їх активно турбуватись про покращення систем безпеки. Однак вона також полегшує відповідальність клієнтів за можливі інциденти, роблячи банківські застосунки більш надійними та безпечними [6].

Поточний *RTS* для надійної автентифікації клієнта та спільного і безпечного зв'язку (*SCA*) дозволяє не вимагати виконувати надійну автентифікацію клієнтів за умови, що: доступ обмежений лише до балансу рахунку та/або недавньої історії транзакцій, конфіденційні платіжні дані не розкриваються, а також *SCA* застосовується, коли доступ до інформації здійснюється вперше та принаймні кожні 90 днів після цього. У 2021 році було запропоновано ввести певні правки до директиви, а саме [7]:

- запровадження обов'язкового винятку для *SCA* для конкретного випадку, коли доступ здійснюється через AISP і лише за умови виконання певних умов;
- обмеження сфери дії добровільного виключення випадками, коли клієнт безпосередньо отримує доступ до інформації про обліковий запис;
- подовжувати терміни оновлення *SCA* від кожні 90 днів до кожні 180 днів, коли доступ до інформації здійснюється через *AISP* або безпосередньо клієнтом.

Додатково, банки, що пропонують електронні банківські послуги, вживають заходів для мінімізації ризиків використання різноманітних атак, таких як фішинг та інших. Тут важливою стає роль токенів, які використовуються для забезпечення безпеки автентифікації. Ці токени можуть бути апаратними або мобільними, прикладами є *tProc ECC* та *tPro Mobile* [6].

Comarch tPro ECC ідеально відповідає вимогам клієнтів, які висувають високі стандарти щодо швидкості, ефективності та комфорту в сфері безпеки онлайн банкінгу. Цей невеликий та легкий *USB*-токен, який не вимагає встановлення драйверів, призначений переважно для авторизації документів та онлайн-транзакцій, а також для підтвердження особи за допомогою електронного підпису [6].

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

зувати обмін фінансовою інформацією, спрощуючи комунікацію між різними фінансовими установами та підвищуючи ефективність операцій. Його впровадження має на меті поліпшити якість та надійність фінансових послуг [10].

tProc ECC апаратний маркер (згаданий вище) віднедавна доступний і в Україні. Даний апаратний маркер є стійким до віддалених атак, адже використовує криптографію еліптичної кривої. Вітчизняна версія токену була розроблена в співпраці з локальним дистриб'ютором *Comarch IT Park* і відповідає державному стандарту електронного підпису. Крім того, вона підтримує геш-функцію «Купина». Це робить *tProc ECC* добре адаптованим до державних стандартів та легко інтегрованим в інфраструктуру будь-якого вітчизняного банку [6].

PCI DSS – ще один стандарт впроваджений в Україні. Загалом його створення ініціювали міжнародні платіжні системи *American Express, Visa, Mastercard, JCB* та *Discover*. Стандарт *PCI DSS* визначає 12 вимог, які складають комплекс заходів, обов'язкових для досягнення максимального рівня безпеки інформації про власників платіжних карток. Ці вимоги стосуються усіх етапів обробки даних – від їх передачі до зберігання та обробки в інформаційно-технологічних структурах організацій. Ці вимоги включають у себе [11]:

- захист системи включає у себе забезпечення безпеки систем, що обробляють платіжні дані;
- захист власницьких даних описує захист від доступу до даних власників платіжних карток;
- захист мережі для запобігання несанкціонованому доступу до мережі, що обробляє платіжні дані;
- захист від шкідливих програм;
- захист доступу описує обмеження доступу до даних лише авторизованим користувачам;
- розвиток та тестування системи безпеки;
- підтримка політик безпеки включає запровадження та підтримка ефективних політик безпеки;
- захист фізичного доступу вимагає обмеження фізичного доступу до приміщень, що містять обладнання для обробки платіжних даних;
- моніторинг та виявлення інцидентів;
- захист від зовнішніх атак;
- управління підтримкою та обслуговуванням;
- політики та процедури безпеки пропонують розробку та впровадження політик та процедур безпеки для забезпечення відповідності стандарту.

5. Мобільні банківські застосунки: огляд функцій та ризиків

У процесі розвитку банківські операції у мобільних застосунках постійно розширювали свій спектр і вже зараз користувачі мають змогу не тільки здійснювати прості транзакції та відслідкувати стан рахунку, а і оформити кредит, переглянути наявні комунальні платежі, оновити документи, що пов’язані з карткою, поповнити мобільний та ще багато іншого.

Можна сказати, що історія мобільних банкінгів бере свій початок з *«Bank of America»*, який впровадив систему під назвою *«Electronic Recording Machine, Accounting and Credit»* (*ERMA*) у 1950-х роках. *ERMA* була призначена для автоматизації банківських операцій, включаючи обробку чеків та інші транзакції. *ERMA* була революційною технологією, система визначалася, як комп'ютеризований облік чеків та банківських транзакцій, і вона використовувалася для автоматизації та полегшення роботи банківських операцій. Основні можливості *ERMA* включали: - читаючий пристрій для чеків; збереження інформації про транзакції;

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

передачу даних, тобто ця система дозволяла передавати інформацію між різними банківськими підрозділами та об'єктами [12].

Першим банкінгом в Україні став «Приват24». Приват24, як мобільний застосунок, був вперше представлений у 2011 році ПриватБанком, який вже на той момент був лідером вітчизняного банкінгового сектору. Цей мобільний застосунок став важливим інструментом для клієнтів банку, що дозволяє їм здійснювати різноманітні банківські операції саме через мобільні пристрої. Для створення Приват24 потрібна була сучасна технологічна інфраструктура для обробки та збереження фінансової інформації користувачів, забезпечення безпеки та зручності користування. З урахуванням чутливості фінансової інформації, важливим етапом було впровадження найвищих стандартів безпеки, таких як *PCI DSS*, щоб захистити дані користувачів від несанкціонованого доступу [11].

З часів створення Приват24 в Україні з'явилось багато банківських застосунків, таких як Monobank, Raiffeisen Online, Ощад24, Альфа-Мобайл та інші. Кожен з цих додатків надає клієнтам зручний доступ до банківських послуг за допомогою мобільного пристрою та має певні особливості безпеки та користувацького інтерфейсу. Асоціація ЄМА провела дослідження у якому було розглянуто дані аспекти. (табл.1-2) [14].

Таблиця 1 – Аспекти зручності

Table 1 – Convenience aspects

Банк	Кредитна лінія у застосунку	Підв'язка карток інших банків	Оплата будь-якого рахунку з застосунку	Відображення різних рахунків клієнта	Вимкнення подвійної конвертації	Відкриття валютного депозиту
Monobank	+	+	-	+	+	+
Sense bank	+	+	-	+	+	+
А-банк	+	+	-	+	+	+
Приват-Банк	+	+	+	+	+	+
ПУМБ	+	+	-	-	-	+
Укргазбанк	-	+	-	-	-	+
Укрсиббанк	-	+	-	-	-	-
Otpbank	-	+	-	-	-	-
Райффайзен банк	-	-	-	-	-	-
Ощадбанк	-	-	-	-	-	-

Таблиця 2 – Аспекти безпеки

Table 2 – Security Aspects

Банк	Зміна *PIN* у застосунку	*3D*-secure можливість вимкнути посилену автентифікацію	Керування перевіркою геолокації клієнта і отримувача платежу	Вибір власного *CVV* у додатку	Управління токенізованими застосунками	Керування підписками на ресурси застосунку
Monobank	+	+	+	+	+	+
Sense bank	+	-	+	-	+	+
А-банк	+	+	-	-	-	+
Приват-Банк	+	-	-	-	-	+
ПУМБ	+	-	+	-	-	-
Укргазбанк	+	-	-	-	-	-
Укрсиббанк	+	+	-	-	-	-
Otpbank	+	-	-	-	-	-
Райффайзен банк	+	-	-	-	-	-
Ощадбанк	-	+	-	-	-	-

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

За даними табл. 1, помітно, що такі додатки, як Monobank, Sense bank, А-банк, ПриватБанк є помітними лідерами за зручністю.

Спостерігається достатня увага до *аспектів зручності* у більшості найпопулярніших банківських додатків. Що ж стосується *аспектів безпеки (див. табл.2)*, то варто відмітити, що більшість банків не мають повного комплекту усіх аспектів. Єдиний банк, що містить у собі всі аспекти, це Monobank, який при цьому не має фізичної установи банку. Слід зазначити, що в усіх додатках присутні: - цифрова картка, онлайн підтримка та можливість відкриття депозиту. Також можна спостерігати те, що банки здебільшого не мають ніяких аспектів, окрім зміни *PIN* у застосунку, та при цьому включають у себе більше аспектів зручності, орієнтуючись при цьому на користувацькі побажання, але це не заважає більшості додатків працювати коректно і надійно та все ж викликає певні вразливості у їх системах.

Варто зазначити, що вітчизняний ринок мобільних банківських застосунків продовжує успішно розвиватись і вже на сьогодні є досягнення якими можна пишатись. На сучасному фінансовому ринку з'явилася значна кількість онлайн-банків, включаючи Monobank, які надають клієнтам можливість користуватися фінансовими послугами шляхом використання мобільних застосунків. Це докорінно змінює взаємодію з банківськими послугами, надаючи максимальний комфорт власним клієнтам. Крім того, інші впливові банки держави, такі як ПриватБанк, Raiffeisen Bank, Oschadbank, OTP Bank, також вирішили приєднатися до можливостей онлайн-банкінгу, надаючи своїм клієнтам широкий спектр можливостей. Цей вибір фінансових мобільних програм відкриває нові можливості для клієнтів, дозволяючи їм обирати оптимальний сервіс, який відповідає їхнім користувальницьким потребам [15].

Україна вийшла на лідируючі позиції, впроваджуючи QR-коди для безготівкових платежів та стаючи однією з перших країн у світі, що використовує цю технологію. Це механізм оплати рахунків й здійснення покупок помітно зменшує ризик помилкових транзакцій та скорочує черги в банківських відділеннях. Прогрес у цьому напрямі став можливим завдяки технологічним інноваціям, таким як мобільні платежі та електронні гаманці, що сприяють зручності та ефективності фінансових операцій.

Проте вітчизняна сфера мобільних банківських застосунків продовжує зіштовхуватись з проблемами, які затримують її розвиток, наприклад: - недовіра клієнтів; відсутність стандартів і єдиних правил, щодо безпеки мобільних банківських додатків; мала кількість точок доступу до якісного інтернет; недостатність необхідного регулювання з боку держави та ін. Але ці проблеми не заважають активному збільшенню кількості користувачів банківськими сервісами. Так, кількість користувачів мобільними банкінгами у 2018 році становила 4,7 млн. осіб, а вже у 2022 році зросла до 8,9 млн. осіб, що є майже вдвічі більше попереднього значення. Ця статистика свідчить про велику популярність таких застосунків та «обіцяє» і надалі помітний розвиток їх можливостей [15].

6. Приклади кібератак, основні помилки та практичні рекомендації

Зусілля кіберзлочинців проникнути у банківську систему та викрасти клієнтські гроші чи дані відбуваються постійно. Проте більшість банків успішно справляються з такими атаками. Нерідко, особливо у старшого покоління, мобільні банківські застосунки викликають недовіру, адже вони звикли користуватись фізичними картками чи готівкою. Тому розробники намагаються довести клієнтській аудиторії, що їм можна довіряти. На жаль, рівень безпеки залежить не тільки від того, наскільки надійно побудована система відповідного мобільного додатку, а і від того, наскільки люди, що працюють з цією програмою є обізнаними у сфері ІБ. Саме тому банківські корпорації не шкодують грошей для проведення тренінгів, щодо питань безпеки серед своїх клієнтів та працівників.

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

Нещодавня кібератака на оператора мобільного зв'язку «Київстар» не була напряму пов'язана із банківською системою, проте «навела безладу» у деяких мережах. Так, окрім збою у роботи деяких відділень та банкоматів, перебої мережі зв'язку також призвели до погіршення роботи деяких банківських застосунків. Наприклад, Ощад24, який при проведенні транзакцій вимагає проходження подвійної автентифікації не міг провести автентифікацію за sms-кодом належним чином, бо через проблеми зв'язку повідомлення не могло надійти до абонентів «Київстар». У той же день DDoS-атаки зазнав і Monobank, проте фахівці змогли її відбити [16]. Одним за умовно «найгірших» періодів у кібербезпеці банківських додатків в Україні можна вважати початок 2022 року. 15 лютого відбулись наймасовіші атаки на різні сфери функціонування держави, у тому числі і у банківському секторі. Атакуючі намагалися здійснити DDoS-атаки, навантажуючи трафік банківських додатків у значущу кількість разів більше, ніж звичайні користувачі. Атаки зазнали мобільні застосунки ведучих вітчизняних банків таких як: - ПриватБанк, Ощадбанк, АльфаБанк, Monobank та інші. Ця атака припинилась приблизно опівночі та до серйозних втрат вона не призвела, проте було порушено штатну роботу додатків ще на деякий час після її відбиття [17].

Важливо підкреслити, що фатальні (тобто такі, що мають серозні наслідки) помилки при захисті мобільного банківського додатку можуть допускати, як самі працівники банку, так і його клієнти. Помилки в дизайні, що супроводжуються «слабкою» безпекою, реалізованою під час розробки відповідного ПЗ, потенційно можуть призвести до компрометації (зломів) додатку. До таких недоліків насамперед відносять [18]:

- *недостатню перевірку вхідних даних* – це може дозволити зловмисникам впровадити шкідливий код у застосунок;
- *слабке управління сеансами* – призводить до несанкціонованого доступу до облікових записів користувачів;
- *недостатню обробку помилок* – дає можливість розкриття конфіденційної інформації потенційними зловмисниками;
- *погано реалізований контроль доступу* – може призвести до несанкціонованих дій у застосунку;
- *відсутність безпечних методів кодування* – робить мобільний застосунок вразливим до різних типів атак.

Також є інші помилки, яких варто всіляко уникати, наприклад помилки в кодуванні можуть порушити роботу мобільного застосунку, іноді спричиняючи непередбачені наслідки. Ці вразливості ПЗ можуть виникати через такі проблеми, як: - переповнення буферу та/чи помилки рядка форматування тощо. Щоб захистити програмний додаток від подібних проблем, дуже важливо коректне проведення етапу тестування відповідного ПЗ та мати надійний метод тестування безпеки мобільного банкінгу. Цей метод допомагає помітити та локалізувати можливі помилки кодування, перш ніж вони стануть джерелом проблем безпеки, забезпечуючи неперервну та безпечну роботу відповідного додатку [18].

Застосунки мобільного банкінгу часто потребують підключення до зовнішніх джерел, щоб працювати в повному обсязі. Однак, використання зовнішніх джерел потенційно забезпечує більше точок входу для кіберзлочинців, щоб отримати доступ до конфіденційної інформації в програмі мобільного банкінгу користувачів. Ось чому ретельне тестування банківських застосунків є найважливішим чинником для їх подальшої безпечної роботи [18].

Якщо клієнти не планують установку програми мобільного банкінгу належним чином та не знайомі з комп'ютерними системами, то це може в купі може призвести до помилок. Так наприклад, вони можуть забути видалити облікові записи налагодження або паролі. Чи можуть зіткнутися з проблемами управління різними версіями. Тому важливо налагоджувати

ISSN 2519-2310 CS&CS, Issue 1(23) 2023

увесь весь процес таким чином, щоб користувач однозначно міг пройти процес встановлення та налагодження додатку правильно і безпечно. Наприклад, у 2018 році в основних магазинах програмних застосунків, службами США було виявлено майже 65000 підроблених програм. Тому США проводять ретельний контроль банківських застосунків у відповідних онлайн-маркетах, тобто постійно перевіряють мережу на наявність шахрайських підробок популярних мобільних банківських застосунків. До того ж більшість великих банків США надають посилання на свій мобільний додаток безпосередньо на своєму власному веб-сайті [3].

Як згадувалось вище, користувачі не менше відповідальні за безпеку своїх рахунків, ніж банки. Тому рекомендовано щомісяця оновлювати паролі застосунків, оновлювати програмне забезпечення, уникати загроз не тільки мобільним банкінгам, а і усьому мобільному пристрою, при виявленні підозрілої активності повідомляти відповідні служби.

4. Висновки

1. Останні роки на фінансовому ринку спостерігається велика потреба у діджиталізації, одним з таких рішень стало широке поширення мобільних банківських застосунків, які у свою чергу вирішили багато проблем, що виникли у процесі пандемії, а потім війни.

2. Чим більше розвивається індустрія мобільного банкінгу, в тим більшої мірі кіберзлочинці намагаються знайти шлях до отримання «легких» грошей. Вони так само, як і спеціалісти з ІБ, досліджують шляхи доступу до застосунку, проте мають зовсім інші наміри. Онлайн шахраї постійно розробляють нові комплексні сценарії проведення атак, до складу яких залучають: - трояни, кейлогери, методи соціальної інженерії, експлуатацію вразливостей цільових систем, необачність користувачів й працівників банку та ін..

3. Вітчизняна сфера мобільного банкінгу потребує певних довершень з точки зору забезпечуваного рівня безпеки. Такими можуть стати: - єдина обов'язкова стандартизація для всіх банків, встановлення більш стійких точок доступу до мережі інтернет, впровадження контролю над поширенням нелегітимних (в т.ч. невідомих) програмних застосунків, розповсюдження онлайн тренінгів з безпеки серед працівників та клієнтів банківських установ.

Список літератури

[1] Бегаль І. (2023). Броня фінтеху за сотні тисяч доларів. Під час війни кібератаки на фінансовий бізнес почастішали в рази. Як компанії захищаються від нападів. (http://surl.li/pgzrw)

[2] The Risks of Mobile Banking Apps: Keep Your Money Safe. (2023). (https://www.identityguard.com/news/risks-of-using-mobile-banking-apps)

[3] Increased Use of Mobile Banking Apps Could Lead to Exploitation. (2020). (https://www.ic3.gov/Media/Y2020/PSA200610)

[4] SharkBot: a new generation of Android Trojans is targeting banks in Europe. (2021). (https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe)

[5] The Top 10 Cybersecurity Threats to Digital Banking and How to Guard Against Them. (2023).(https://www.guardrails.io/blog/the-top-ten-cyber-security-threats-to-digital-banking-and-how-to-guard-against-them/)

[6] Comarch Financial Services. (https://www.comarch.com/finance/articles/)

[7] Albert Weatherill. Commission Delegated Regulation amending the RTS as regards the 90-day exemption for account access. (2022). (https://www.regulationtomorrow.com/eu/commission-delegated-regulation-amending-the-rts-as-regards-the-90-day-exemption-for-account-access/)

[8] Mobile Banking Compliance Requirements: Does Your Product Comply with Latest Trends. (2022). (https://binariks.com/blog/mobile-banking-compliance-requirements/)

[9] Відомості Верховної Ради України. Закон України Про банки і банківську діяльність. № 5-6, ст.30. (2001). (https://zakon.rada.gov.ua/laws/show/2121-14#Text)

[10] Міжнародний стандарт ISO 20022 - з 01 квітня 2023 року в Україні. (2023) (https://dn.tax.gov.ua/media-ark/news-ark/667242.html)

[11] PCI DSS Certification (https://getpci.com/)

[12] Our Heritage: Bank of America revolutionizes banking industry. (2020) (https://about.bankofamerica.com/en/our-company)

[13] ПриватБанк. (https://privatbank.ua/)

[14] ЄМА. (2023). (https://www.ema.com.ua/)

[15] Мірошник, Р., Кухта, І. (2023). ДІДЖИТАЛІЗАЦІЯ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ В СУЧАСНИХ УМОВАХ. Економіка та Суспільство, (49).
[16] Як кібератака на «Київстар» вплинула на роботу НБУ та банківської інфраструктури. (2023). (https://minfin.com.ua/ua/2023/12/14/117801942/)
[17] ПриватБанк, Ощадбанк, monobank, Альфа-Банк, урядові сайти та портал «Дія» зазнали кібератаки. (2022). (https://forbes.ua/news/dzherela-v-nbu-privatbank-ta-oshchadbank-zaznali-kiberataki-servisi-vzhe-vidnovlyuyut-robotu-15022022-3691)
[18] Enhancing Mobile Banking App Security: Top Threats and Solutions. (2023). (https://cybersecurity.asee.co/blog/mobile-security/enhancing-mobile-banking-app-security-top-threats-and-solutions/)

Received: on November 2023. **Accepted:** on December 2023.

Authors:
Yelyzaveta Lohachova, CSD Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: lohachova2020kb11@student.karazin.ua
Maryna Yesina, Ph.D., Associate Professor, Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
ORCID: https://orcid.org/0000-0002-1252-7606
E-mail: m.v.yesina@karazin.ua
Vsevolod Bobukh, Ph.D., head of the information protection hardware department of JSC "IIT", Kharkiv, Ukraine.
E-mail: jsciitua@gmail.com

Analysis of cybersecurity features in banking mobile applications.

Abstract. This article discusses important aspects of cybersecurity in mobile banking applications. The article analyses in detail potential threats and effective strategies for their prevention and counteraction. Due to the rapid development of digital technologies in the banking industry, mobile applications and online services have become a necessary component of financial interaction between customers, providing convenient and efficient financial transactions. However, the development of the functionality of such applications gives rise to new cybersecurity challenges that information security professionals are actively addressing. The article is devoted to a comprehensive review of international and Ukrainian cybersecurity standards in the banking sector, and also contains quick review of mobile applications of well-known Ukrainian banks. Based on this review basic recommendations for improving cybersecurity in such applications are formulated. The article considers the impact of customer comfort on the level of security. In addition, the article considers the impact of the level of security in the banking sector on the overall digitalisation of the financial industry. It is noted that improving the level of security can stimulate and support digitalisation processes, ensuring customer trust and optimal use of mobile banking applications. A comprehensive approach to assessing the level of security, comparing various applications and standards (both Ukrainian and international), as well as considering the relationship between security issues and innovations in banking, make this work useful for understanding the genesis of cyber security in mobile banking.

Keywords: *Banking System, Security, Threats, Cybersecurity, Banking, Mobile Apps.*

УДК 004.065.5 DOI:10.30837/rt.2024.1.216.04

Є.О. ЛОГАЧОВА, М. В.ЄСІНА, канд. техн. наук

ПОРІВНЯЛЬНИЙ АНАЛІЗ УКРАЇНСЬКИХ ТА ЗАКОРДОННИХ БАНКІВСЬКИХ ЗАСТОСУНКІВ

Вступ

Банківські мобільні застосунки вже не перший рік спрощують життя клієнтам банківських установ. З кожним роком кількість користувачів збільшується, як і кількість операцій, які можна виконувати за допомогою застосунків. Проте банківські мобільні застосунки мають бути не тільки комфортними, а й убезпечувати своїх користувачів від різних видів шахрайств. Саме тому кібербезпека посідає важливе місце у розробці таких застосунків.

1. Розвиток мобільних банківських застосунків та загроз

Мобільні банківські застосунки можуть здаватись достатньо новою розробкою, проте насправді вони беруть свій початок з кінця минулого сторіччя. Початком зародження мобільних банківських застосунків можна вважати появу онлайн-банкінгів. У 1981 році вперше з'являються послуги домашнього, себто онлайн банкінгу. Чотири найбільші міські банки, а саме Citibank, Chase Manhattan, Chemical and Manufacturers Hanover запропонували своїм клієнтам можливість використання системи Videotex [1]. Videotex – це загальний термін для систем, які передають текст і графіку діловому або домашньому користувачу за допомогою сигналів, що передаються по телефонній лінії, кабелю або будь-якому з каналів телевізійного або радіомовлення [2]. Наступним важливим кроком у розвитку онлайн-банкінгів стало те, що Stanford Federal Credit Union вперше надав усім своїм клієнтам можливість користуватись онлайн банкінгом [3].

Першим офіційним мобільним банківським застосунком вважається розробка The Bank of Scotland 2007 року. Пізніше у 2011 банк випустив повнофункціональний застосунок, доступний на пристроях Apple, пізніше застосунок адаптували і для BlackBerry та Android. Застосунок дозволяв отримати виписку з рахунку, перевірити останні транзакції та баланс [4].

Першим мобільним банківським застосунком в Україні став Приват24, який почав зароджуватись у 2001 році. Клієнти банку могли здійснювати авторизацію та проводити платежі за допомогою одноразових SMS-паролів. У 2008 році була випущена перша версія повного мобільного застосунку Приват24 для iOS. А вже у 2010 році, була представлена версія застосунку для Android. У вересні 2019 року було випущено оновлену версію Приват24 з оновленим дизайном та функціоналом, включаючи меню для підприємців, технологію FacePay24 та доступ для клієнтів інших банків до банківських операцій [5].

Разом із розвитком технологій, що з кожним разом все більше полегшувало користування фінансовими операціями, еволюціонували і можливості кіберзлочинів. Адже перші банківські застосунки не дозволяли виконувати настільки багато фінансових операцій, як сучасні. Це відбувається за рахунок роботи між пристроєм користувача та банківським сервером. І це відкриває більше можливостей для шахраїв, щоб незворотньо викрасти гроші або ж дані користувачів. До основних загроз належать [7]:

- атаки соціальної інженерії;
- фішинг;
- підробка банківських додатків;
- кейлогери;
- зловмисне програмне забезпечення;
- віруси трояни;
- фізична крадіжка пристрою;
- злам Wi-Fi;

- атаки на зв'язок;
- атаки на одноразові паролі та інше.

2. Характеристика досліджуваних застосунків

Для порівняльного аналізу було обрано п'ять українських застосунків та п'ять застосунків з різних країн. Перший досліджуваний банк згадувався раніше – Stanford FCU, який створили та використовують в США. Оновлений застосунок Stanford FCU випущено у вересні 2016 року, за цей час його завантажили понад 10 000 разів. Банк Stanford FCU пропонує своїм клієнтам два способи завантаження – з сайту банку та через PlayMarket [6].

Наступним досліджуваним банком є Fideuram – італійський банківський додаток. Fideuram з'явився у лютому 2015 року. Додаток налічує більше 100000 завантажень. Застосунок створено для пристроїв iPhone [8].

N26 – європейський мобільний банк, головний офіс якого розташований у Берліні. Додаток доступний для використання у країнах Європейського Союзу (ЄС), Великої Британії та США. N26 випустили у січні 2015 року, з того часу кількість клієнтів налічує понад 8000000 [9].

Banque populaire – французький банк, який презентував свій застосунок – Banque populaire du nord ще у 2010 році. Кількість завантажень перевищує 1000000. Застосунок використовують на території Франції. Для завантаження застосунку надано QR-коди, відсканувавши які можна легко завантажити застосунок з різних платформ [10].

Останній досліджуваний закордонний банківський застосунок – Sparkasse. Sparkasse – німецький банк, який розробив свій додаток у 2014 році, з того часу кількість завантажень перевищує 10000000. Як правило додатково завантажується і S-pushTAN – sichere Freigaben, який в подальшому буде використовуватись для покращення надійності автентифікації, проте його не рекомендують ставити на один пристрій із застосунком, адже у випадку зламу це може полегшити вхід шахраям [11].

Серед українських банків було обрано Monobank – перший український повноцінний мобільний банк, який не має фізичного відповідника, тобто банківського філіалу. Monobank існує з 2017 року і надає своїм клієнтам широкий спектр послуг, завдяки якому у них не виникає необхідності звертатись до фізичної філії. Monobank не поступається своїм конкурентам, застосунок завантажили більше 10 мільйонів разів [12].

Приват24 – перший український мобільний банківський застосунок, який зароджувався ще у 2001 році, а у 2011 році випустив застосунок який використовується нині і налічує понад 10000000 завантажень [5].

Укрсиб-онлайн є менш популярним, проте його також використовує багато українців, застосунок розроблено у 2017 році, його використовує понад 1 мільйон користувачів. Укрсиббанк надає посилання для завантаження на своєму сайті [13].

Наступним для розгляду було обрано Ощадбанк. Оновлений застосунок випустили відносно нещодавно – у 2021 році, а він вже завантажений більше одного мільйону разів. Розробники стверджують, що застосунок має надійну безпеку, адже до нової версії додано верифікацію по PIN-коду картки. Завантажити застосунок можна за допомогою перевірених посилань на сайті Ощадбанк [14].

Банківський застосунок від ПУМБ було випущено у 2018 році, застосунок пропонує велику кількість послуг та вигідних пропозицій, наразі налічує понад 1000000 завантажень. Також застосунок підтримується на всіх пристроях, телефоні, комп'ютері чи планшеті [15].

Кожен з розглянутих банків надає посилання для завантаження на своєму сайті адже однією з потенційних шахрайських дій є саме підробка застосунків. Додатковою перевагою є те, що банки турбуючись про безпеку свої клієнтів нагадують користувачам правила безпеки при використанні мобільного банківського застосунку, розглядають потенційні загрози та надають необхідні контакти, до яких можна звернутись у разі виникнення загрози.

3. Порівняльний аналіз застосунків

У контексті сучасного фінансового рину одними з найважливіших аспектів при виборі клієнтом банку є безпека та зручність. Банківські застосунки напряму пов'язані з персональними даними клієнтів, їх банківськими рахунками та серверами банку. Такі застосунки потребують особливих заходів безпеки, наприклад, наявності обов'язкової двофакторної автентифікації чи наявності можливості заміни паролю у застосунку. У таблицях 1 та 2 наведено порівняльний аналіз досліджуваних банків за аспектами безпеки.

Таблиця 1

Аспекти безпеки закордонних застосунків

Безпека	Наявність двофакторної автентифікації	Наявність PUSH-повідомлень	Зміна PIN у застосунку	Вимикати посилену автентифікацію	Вибір власного CVV
Stanford FCU	+	-	-	-	-
Fideuram	+	-	+	-	-
N26	+	+	+	-	-
Banque populaire du nord	+	+	-	+	-
Sparkasse	+	+		-	-

Таблиця 2

Аспекти безпеки українських застосунків

Безпека	Наявність двофакторної автентифікації	Наявність PUSH-повідомлень	Зміна PIN у застосунку	Вимикати посилену автентифікацію	Вибір власного CVV
Monobank	+	+	+	-	+
Приват24	+	+	+	-	-
Укрсиб-онлайн	+	+	+	-	-
Ощадбанк	+	-	-	-	-
ПУМБ	+	+	-	-	-

За даними таблиць 1 та 2 помітно, що лідерами за шкалою безпеки є N26, Banque populaire du nord, Monobank, Приват24 та Укрсиб-онлайн. Виходячи з результатів можна помітити, що українські банки загалом намагаються не поступатись міжнародним.

Проте для того, щоб клієнт обрав певний застосунок, надійності може бути не достатньо. Адже стандарти зручності у користувачів підвищуються, а це значить, що розробники вимушені знаходити баланс між зручністю та безпекою. Так, наприклад, подовжена перевірка легітимності користувача чи відсутність миттєвих переказів може змусити клієнта обрати інший більш швидкий та зручний застосунок. Порівняльний аналіз аспектів зручності досліджуваних банків наведено у таблицях 3 та 4.

Таблиця 3

Аспекти зручності закордонних застосунків

Зручність	Сплата будь-якого рахунку	Кредитна лінія у застосунку	Відкриття валютного депозиту	Аналіз витрат і доходів	Наявність страхування
Stanford FCU	-	-	-	-	-
Fideuram	+	-	-	+	-
N26	+	-	-	+	+
Banque populaire du nord	+	+	-	+	+
Sparkasse	+	-	-	+	-

Таблиця 4

Аспекти зручності українських застосунків

Зручність	Сплата будь-якого рахунку	Кредитна лінія у застосунку	Відкриття валютного депозиту	Аналіз витрат і доходів	Наявність страхування
Monobank	-	+	+	+	+
Приват24	+	+	+	+	+
Укрсиб-онлайн	-	-	-	+	-
Ощадбанк	-	-	-	+	+
ПУМБ	-	+	+	+	+

За даними з таблиць 3 та 4 лідируючі позиції за зручністю займають такі банки, як N26, Banque populaire du nord, Monobank, ПУМБ, найбільше відповідностей помічено у Приват24.

Банківські застосунки закордонного походження мають низку значних переваг над українською системою: структуровані вимоги до безпеки банківських мобільних застосунків, відповідність міжнародним нормам, більша увага безпеці, аніж зручності. Проте українські застосунки, хоч і зіштовхуються з певними проблемами – відсутність стандартів та єдиних правил в Україні щодо безпеки мобільних банківських застосунків; мала кількість точок доступу до якісного Інтернету, недостатність необхідного регулювання з боку держави, бажання догодити клієнтам новими покращеннями швидкості та зручності, все ж розвиваються і покращуються у плані кібербезпеки в тому числі. За останні роки було впроваджено нові норми та стандартизації, які наближають рівень безпеки українських мобільних банкінгів до Європейських і тим самим допомагають Україні більше інтегруватись до ЄС [7].

Висновки

1. Враховуючи темп сучасного життя, мобільні банківські застосунки стають необхідністю для повноцінного комфорту. Кількість користувачів таких застосунків щорічно збільшується, а разом із тим прогресують можливості, які надають застосунки.

2. Рівень безпеки за обраними критеріями в українських банківських застосунках знаходиться на тому ж рівні, що і у міжнародних застосунках. При цьому Monobank показав навіть кращий результат, охопивши чотири пункти з п'яти. Проте оглядаючи загальну картину відповідності міжнародним нормам стає помітно, що українським системам ще необхідно розвиватись.

3. За обраними критеріями зручності найкращі результати отримав Приват24, серед міжнародних банківських застосунків найкраще показав себе Banque populaire du nord, натомість найгіршим виявився Stanford FCU. За отриманими результатами найкраще поєднання безпеки та зручності вдається N26, Banque populaire du nord, Monobank та Приват24.

Список літератури:

1. Dr. Yellaswamy Ambati, "International Journal of Research in Management, Economics and Commerce", ISSN 2250-057X, Impact Factor: 6.384, Volume 07 Issue 12, Dec.2017, Page 68-73. [Електронний ресурс]. – Режим доступу: https://indusedu.org/pdfs/IJRMEC/IJRMEC_1468_22786.pdf

2. "VI Deotex Systems and Services", L.R. Bloom, A.G. Hanson, R. F. Linfield, D.R. Wortendyke, u.s. Department of Commerce, Oct.1980. [Електронний ресурс]. – Режим доступу: https://its.ntia.gov/umbraco/surface/download/publication?reportNumber=80-50_ocr.pdf

3. "Stanford Federal Credit Union Transforms Member Experience with Digital Banking Innovations" [Електронний ресурс]. – Режим доступу: https://www.q2.com/blog/stanford-federal-credit-union-transforms-member-experience-with-digital-banking-innovations

4. "Banking app, 2011" [Електронний ресурс]. – Режим доступу: https://www.natwestgroup.com/heritage/history-100/objects-by-theme/going-the-extra-mile/banking-app-2011.html

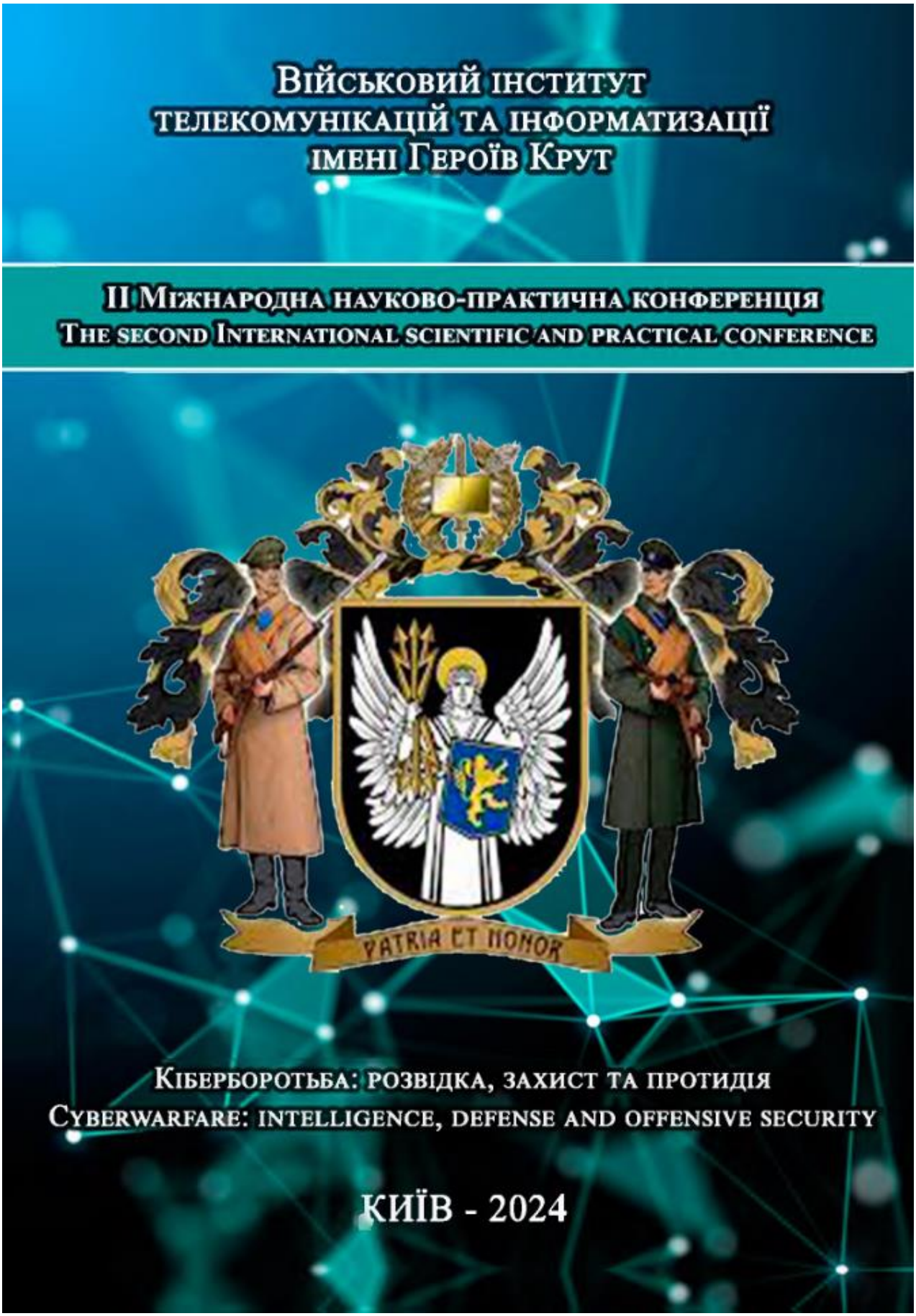
5. "Приват24 включив рейтинг діджитальності користувачів" [Електронний ресурс]. – Режим доступу: https://privatbank.ua/news/2021/3/26/1401

6. "Mobile app and Online Banking" [Електронний ресурс]. – Режим доступу: https://www.sfcu.org/online-banking/

7. “Аналіз особливостей забезпечення кібербезпеки у банківських мобільних додатках”, Єлизавета Логачова, Марина Єсіна, Всеволод Бобух, Computer science and cybersecurity. – Харківський національний університет імені В. Н. Каразіна, 2023, Випуск 1(23) – С. 63–73. – [Електронний ресурс]. – Режим доступу: https://periodicals.karazin.ua/cscs/article/view/23094/21104.
8. “Fideuram Online” [Електронний ресурс]. – Режим доступу: https://www.fideuram.it/prodotti-e-soluzioni-personalizzate/servizi-online/fideuram-online/
9. “Open a bank account online in minutes” [Електронний ресурс]. – Режим доступу: https://n26.com/en-eu/open-bank-account-online
10. “Banque populaire du nord” [Електронний ресурс]. – Режим доступу: https://www.banquepopulaire.fr/nord/votre-banque/choisir-une-region/?source_id=3494&wording=region
11. Онлайн-банкінг від шпаркаси App „Sparkasse“ [Електронний ресурс]. – Режим доступу: https://www.berliner-sparkasse.de/content/dam/myif/berliner-sk/work/dokumente/pdf/allgemein/PushTan-und-OnlineBanking-UKR.pdf?stref=imagetextbox
12. “Monobank” [Електронний ресурс]. – Режим доступу: https://www.monobank.ua/cpa?lang=uk
13. “UKRSIB online” [Електронний ресурс]. – Режим доступу: https://online.ukrsibbank.com/ibank/
14. “Мобільний додаток Ощад 24/7” [Електронний ресурс]. – Режим доступу: https://www.oschadbank.ua/mobilnij-dodatok
15. “ПУМБ Online - це моє!” - ПУМБ [Електронний ресурс]. – Режим доступу: https://www.pumb.ua/pumbonline

Надійшла до редколегії 00.00.2024

Відомості про авторів:
Логачова Єлизавета Олегівна – Харківський національний університет імені В. Н. Каразіна, студентка факультету комп’ютерних наук; Україна; e-mail: lohachova2020kb11@student.karazin.ua; ORCID: https://orcid.org/0000-0002-9815-466X
Єсіна Марина Віталіївна – канд. техн. наук, доцент, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, АТ «Інститут Інформаційних Технологій», науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606


Військовий інститут
телекомунікацій та інформатизації
імені Героїв Крут
II Міжнародна науково-практична конференція
The second International scientific and practical conference
PATRIA ET HONOR
Кіберборотьба: розвідка, захист та протидія
Cyberwarfare: intelligence, defense and offensive security
КИЇВ - 2024

Y. Lohachova (V. N. Karazin Kharkiv National University)
PhD **M. Yesina** (V. N. Karazin Kharkiv National University)

ANALYSIS OF THE CYBERCRIMINAL'S PERSONALITY

Introduction

In the age of digitalisation, professionals from various industries and ordinary citizens are facing the problem of cybercrime. As technology has expanded into most areas of life, such as medicine, the legal sector, banking, education and many others. In the era of large-scale digitalisation, the need to protect personal data has not only increased, but fraudsters' schemes and strategies have also evolved since the first cybercrime. An important aspect of preventing and combating cybercrime is to be aware of the psychology of criminals and which categories of people may pose the greatest threat. The main task is to analyse the personality of the cybercriminal and explore how such techniques help in practice.

1. Classification of cybercriminals

Almost everyone uses a computer every day for work, study, and entertainment, but some people are beginning to use their devices to commit cybercrime. The fact is that, depending on certain traits and characteristics, people tend to behave differently in the same situations. Thus, cybercriminals, due to a set of certain characteristics and peculiarities, are more prone to criminal activity in the technical space than ordinary users [1].

Cybercriminals can be classified in several ways. They can be divided according to their personal qualities [2]: people who commit a crime by accident; people who commit a crime for mercenary purposes; hackers; computer hooligans. The second classification includes more features of the offender and divides them into three groups [2]: professionals; fanatics; mentally ill. These classifications overlap in one way or another and cannot be assessed without each other. The most common motivation of cybercriminals is selfishness, but they can also be motivated by a desire for revenge, self-assertion, power, chaos and other feelings that have arisen as a result of certain circumstances. An example of such behaviour is the UBS Paine-Webber attack - the attacker was an employee of the company who planted a "logic bomb" that took down about 2,000 servers across the country and caused the company to be unable to conduct operations for several weeks in some of its offices [3].

Sometimes, cybercrime can be committed not by a single person, but by a group. Such groups can attack various institutions: financial institutions, hospitals, state-owned enterprises, corporations, and so on. The group always has a leader in the centre, who coordinates the attack and controls the entire branched structure of the group.

2. Psychological and personal characteristics of cybercriminals

There are many stereotypes about hackers and other criminals in the virtual space. Most people, if asked to describe such a person, will provide the same set of qualities. These stereotypes are that a cybercriminal is a person alienated from society, addicted to computers and having outstanding mental abilities, belonging to a young age group and mostly male. In order to understand what the real personal and psychological characteristics are, it is worth looking at statistics. The following conclusions can be drawn from the statistics presented in the study [2].

The majority of cybercrime offenders are indeed men, with 87.5% of them in the statistics, while women make up only 12.5%. The next characteristic is age: most cybercrime is committed by people in the 30-50 age group, with 36.2% of the total. Young people aged 18 to 25 are also one of the most common age groups, with a 34.3% participation rate. The majority of people who commit crimes using technology are single, accounting for 70% of the total number of offenders. This is largely due not only to the fact that cybercriminals are quite young, but also to the fact that married people are less likely to commit any type of crime because they are afraid of harming their family. Another remarkable feature of cybercriminals is that they are most often people with higher education or incomplete higher education. This type of criminal is characterised by good mental abilities, as they need to be on a par with those responsible for security systems when committing a

cybercrime. Approximately half of those who commit cybercrime are unemployed. Among those who do work permanently, managers are most likely to commit technical crime, while programmers are less common in statistics. Another important feature worth paying attention to is the presence of any kind of addiction. After all, people who are addicted to gambling, alcohol, drugs, etc. can get under the influence and then deliberately cause harm by committing a cybercrime. Some hackers carry out cyberattacks that they believe are beneficial to society. Such cybercriminals are mainly aimed at helping society. Such actions may be motivated by religious, political or social beliefs.

3. Using profiling in the investigation of cybercrime

Cybercrime is a crime just like physical theft or damage, but committed in the technological space. Therefore, the methods used to identify conventional criminals can also be used for cybercriminals. Criminal profiling is one of the methods actively used to identify a potential criminal (or to prevent such a person from entering an institution or enterprise under the guise of an employee or client). Profiling consists of analysing behavioural patterns that can help predict certain things about a person who has committed a crime [4]. Such analysis is aimed not only at identifying and understanding the perpetrator, but also at enabling appropriate measures to be taken. The analysis includes the study of the offender's personality traits, modus operandi, motivation and potential future steps.

It is important to understand the motive of the cybercriminal, which can vary significantly. If a hacker is motivated by the desire to get pleasure or the possibility of being recognised by the hacker community, he or she may be subject to legal measures and exposure, which can significantly complicate his or her future attempts to gain the approval of "colleagues" or close this path forever. The motives may also be the desire to have fun, excitement, obtaining benefits in the form of money, etc. [4]. Cybercriminals are human beings like everyone else, and therefore they are also driven by inherent characteristics. Humans are often prone to habits, so cybercriminals often become recognisable by the "signature" of their crimes, making them easier to detect and find. Another clue is the ultimate goal achieved by the hacker. It is important to determine what they have achieved - obtaining customer data, money, locking down a system, searching for intellectual property or installing malware, etc.

Conclusions

Cybercrime is committed by people who expect to be uncertain and unpunished, but, as with other criminals, they can be identified and exposed. An important aspect of the work of cybersecurity professionals is knowledge of the personal and psychological characteristics of cybercriminals, such as motivation, purpose, habits, etc. With this knowledge, it is possible not only to identify the offender after the crime has been committed, but also to identify potential cybercriminals and prevent cyber incidents.

REFERENCES

1. Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets / Marleen Weulen Kranenbarg, Jean-Louis van Gelder, Ard J. Barends, Reinout E. de Vries: Computers in Human Behavior, 2023.

2. Науковий вісник Міжнародного гуманітарного університету № 26, Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі / М. Ю. Піцик, 2017.

3. Logic Bomb' Dropped On Brokerage / CBS News, 2002.

4. Inside the Mind of the Enemy. A Guide to Profiling Cyber Criminals. / Richard Barrell and the team at CounterCraft.