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 функціоналу 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 ґенези 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-

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-

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

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].

Процес підписання передбачає автентифікацію користувача за допомогою кнопки, вбудованої в пристрій. Це забезпечує захист транзакцій від віддалених атак, гарантуючи, що жодна третя сторона не матиме доступу до інструкцій без відома користувача.

tPro Mobile – це мобільна платформа, яка підтримує надійну автентифікацію користувачів і авторизацію транзакцій відповідно до директиви *PSD2*. Вона складається із зовнішньої програми та бібліотек розробки, які інтегруються з існуючими продуктами [6].

Більшість банків також використовують *PUSH*-повідомлення та біометричні методи для надання додаткових гарантій безпеки в процесі використання мобільного банкінгу.

Варто також зазначити кілька нових вимог до мобільного банкінгу, які були опубліковані в період з 2021 по 2022 рік у різних країнах світу. Такі нові вимоги можна поділити на дві категорії: вимоги про покращення цифрової ідентифікації та вимоги щодо захисту персональних даних. Про покращення захисту цифрової ідентифікації [8]:

- Данія замінює *NemID* на вдосконалений *MitID* для схвалення платежів і входів;
- Канада запускає програму *Voila Verified Trustmark*, яка видає знаки довіри організаціям, що демонструють відповідність компонентам *PCTF*;
- Європейська комісія завершує роботу над інструментарієм для країн-членів, який міститиме перелік конкретних архітектур, найкращих практик, стандартів, посилань та рекомендацій щодо створення цифрових гаманців;
- уряд Федеральної ради Швейцарії розробляє державну інфраструктуру *E-ID*. Вона буде використовуватися постачальниками ідентифікаційних даних, агентами, довіреними особами або постачальниками ідентифікаційних гаманців;
- Національний інститут стандартів і технологій США випускає для громадського обговорення проект Керівництва з цифрової ідентичності для протидії фішинговим атакам з використанням фіш-стійких автентифікаторів.

Вимоги щодо захисту персональних даних [8]:

- в Японії 1 квітня 2022 року набули чинності правила застосування Закону про захист персональних даних, які зобов'язують суб'єктів повідомляти про порушення даних до комісії із захисту персональних даних та застосовувати норми щодо суб'єктів, які їх порушують;
- Швейцарія ухвалила Закон про захист даних, який зобов'язує компанії негайно повідомляти про серйозні порушення даних федеральному комісару із захисту даних та інформації.

4. Стандартизація кібербезпеки банківських застосунків в Україні

Основним документом для регулювання банківської діяльності в Україні є Закон про банки і банківську діяльність. Цей закон визначає організаційну структуру банківської системи, а також економічні та правові основи для створення, функціонування, реорганізації та ліквідації банків. Основною метою цього законодавства є юридичне забезпечення захисту законних інтересів вкладників та інших клієнтів банків. Також, воно спрямоване на забезпечення стійкого розвитку та стабільності банківської системи. Крім того, його ціль – створення сприятливих умов для економічного розвитку України та встановлення належного конкурентного середовища на фінансовому ринку. За допомогою цього закону створюються необхідні рамки для підтримки ефективності функціонування фінансових інститутів, що сприяє загальному економічному добробуту країни [9].

Вітчизняні системи мобільних банкінгів поки не регулюються повністю відповідно до стандартизацій ЄС, проте вже не перший рік проходить ряд змін. Так, з 1 квітня 2023 року, Україна почала використовувати міжнародний стандарт ISO 20022. Він дозволяє стандарти-

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;

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	-	+	-	-	-	-

За даними табл. 1, помітно, що такі додатки, як Monobank, Sense bank, А-банк, Приват-Банк 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.

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

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.*