Проте головне, щоб технологічні новинки були затребувані споживачами, а банки окупили власні кошти. Тобто банківська інновація має бути доцільною для банку та корисною для клієнтів. Сьогодні банківська система України перебуває на етапі розвитку. Вона повільно, та все ж впроваджує в свою діяльність інноваційні продукти. Одним з позитивних прикладів розвитку банківських інновацій є відкриття відділень у вигляді кав'ярень чи вільних просторів, де клієнт може поспілкуватися з менеджером про свої потреби чи претензії за чашкою кави. Такі відділення не здійснюють банківських операцій, їхня мета – налагодження співпраці між банком та клієнтом. Отже, поглиблення взаємовідносин «клієнт – банк» має стати пріоритетним напрямом розвитку банків України [3].

Список використаної літератури:

1. Лапко О. О. Інноваційні механізми ритейлу в банківському секторі України / О. О. Лапко, А. М. Демченко // Фінансово-кредитна діяльність: проблеми теорії та практики. – 2015. – № 2. – С. 65–72.

2. POS-термінал [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/POS-термінал

3. Безготівкові розрахунки продовжують зростати [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/control/uk/publish/article?art_id=26993720

БЕЗПЕКА БАНКІВСЬКИХ ОПЕРАЦІЙ У МЕРЕЖІ ІНТЕРНЕТ

***Тищенко О. І.**, канд. екон. наук, **Конєв В. В.**, студент, Східноукраїнський національний університет імені Володимира Даля, м. Сєвєродонецьк*

Сьогодні досить актуальними залишаються питання забезпечення безпеки банківських операцій у мережі Інтернет. Кожний сучасний банк, як правило, надає своїм клієнтам можливість користування дистанційним видом обслуговування — онлайн-банкінгом, до функціоналу якого входять грошові перекази між картками та рахунками, відкриття та закриття депозитів, поповнення мобільного рахунку, можливість здійснення комунальних платежів, замовлення квитків на будь-який вид транспорту. Все більше популярності набирають також інтернет-магазини різного напрямку, де розрахунки здійснюються у формі передоплати. Значна кількість подібних операцій має міжнародний характер. Разом із тим виникає небезпека здійснення шахрайських дій або випадкових помилок під час виконання таких транзакцій.

Метою даного дослідження є визначення сучасного стану безпеки банківських операцій у мережі Інтернет та вироблення надійних механізмів її зміцнення.

Серед найбільш поширених можна виділити такі типи загроз:

1. Фішинг, що є однією з найпоширеніших кібератак. ЇЇ сутність полягає в тому, що за допомогою повідомлення електронною поштою, у соціальній мережі або SMS користувача перенаправляють на помилковий веб-

сайт, який виглядає як оригінальний ресурс банку. Користувач, не підозрюючи про підміну, вводить персональну інформацію, яка потрапляє до шахраїв. Варіантом подібної кібератаки також може бути телефонний дзвінок від шахраїв, які, представляючись працівниками банку, намагаються дізнатися таку особисту інформацію, як PIN та CVV-код банківської карти або одноразовий SMS-пароль [1;3].

2. Крадіжка бази паролів. Застосовуючи шкідливе програмне забезпечення і інші технології, хакери крадуть облікові дані користувачів для перепродажу іншим злочинцям або експлуатують їх самі для отримання доступу до чужих банківських рахунків. [2].

3. Кібератака «людина посередині». Зловмисник впроваджує власні повідомлення в трафік між комп'ютером користувача і сервером аутентифікації, для перехоплення та зміни даних платежу [1].

4. Кібератака «людина в браузері». В основі даної загрози є використання шахраями троянської програми, якою інфікується веб-браузер користувача, що дозволяє перехоплювати і модифікувати всю інформацію, що відправляється. Це дає можливість змінювати веб-сторінки і зміст операцій непомітно для користувача [2].

5. Недостатня безпека мобільних операційних систем. Проблема полягає в тому, що для кожної мобільної операційної системи (Android, iOS, Windows Phone) характерні свої вразливості, що присутні і в додатках для мобільного банкінгу. Це вразливості, що ведуть до некоректної роботи протоколу шифрування даних, що означає можливість викрадення інформації про платежі та їх перехоплення [2].

6. Випадкові помилки під час виконання транзакцій. Навіть сучасні розвинені системи інтернет-банкінгу та обробки даних не застраховані від технічних та програмних збоїв, що впливають на коректність виконання банківських операцій [3].

Для посилення захисту банківської інформації слід використовувати наступні механізми, що було розташовано за ступенем зниження ефективності їхнього впливу на безпеку банківських онлайн-операцій:

1. Стандарти PCI DSS (Payment Card Industry Data Security Standard). Це стандарти захисту інформації, розроблені міжнародними платіжними системами, що захищають дані банківських карт. Стандарти визначають такі вимоги, як: побудова і супровід захищеної мережі, захист даних власників карток, підтримка програми управління вразливостями, реалізація заходів щодо суворого контролю доступу, регулярний моніторинг і тестування мережі, підтримка політики інформаційної безпеки. Будь-яка компанія, яка збирається здійснювати інтернет-платежі, повинна відповідати стандартам PCI DSS. [4].

2. Антифрод-системи. Являють собою платформи, які аналізують фінансові операції онлайн і дозволяють виявляти серед них сумнівні. У разі виникнення підозри у шахрайських діях, система заблокує списання коштів. Система оцінює операції і виявляє аномальні й підозрілі. Антифрод-системи можуть працювати за різними параметрами: ліміти на здійснення операцій з однієї IP-адреси, обмеження за сумою, часом або кількістю покупок, оцінка

поведінки покупця в процесі платежу, транзакції на основі статистики. Для тих операцій, що були визначені довіреними, механізм дозволяє не проводити додаткову авторизацію платежу за SMS, що, безумовно, підвищує зручність для покупця і сприяє просуванню покупок в інтернет-магазинах [2].

3. Шифрування даних. Сайти інтернет-банкінгу мають використовувати протокол шифрування даних SSL - Secure Socked Layer, який дозволяє безпечно передавати зашифровану інформацію від користувача до сервера. Сайти, що використовують SSL, передають зашифровані дані протоколом HTTPS (Hypertext Transfer Protocol Secure), розшифрувати які можна лише за допомогою спеціального секретного ключа. [1;3].

4. Електронний цифровий підпис (ЕЦП). Цей механізм захисту інформації використовується при обслуговуванні банками юридичних осіб та окремих індивідуальних клієнтів. Переваги ЕЦП в тому, що він дозволяє однозначно ідентифікувати користувача. За правовим статусом він прирівнюється до власноручного підпису або печатки. За умови правильного зберігання власником секретного (особистого) ключа його підробка неможлива. Але ЕЦП також буде вразливий для шахраїв, які зможуть дістатися до ключа, заразивши комп'ютер клієнта шкідливим програмним забезпеченням [1].

5. Зовнішні електронні пристрої, такі як генератор одноразових паролів та зовнішній електронний ключ. Ці системи є спрощеною версією ЕЦП. Проте, вони також мають і певні недоліки, пов’язані з тим, що клієнт не може отримати доступ до свого рахунку, не маючи поряд спеціального пристрою [1].

6. Антивірусні програми. Використання клієнтом банку ефективних ліцензійних антивірусних програм від перевірених виробників та їх своєчасне оновлення дає можливість забезпечити захист операційних систем персональних комп’ютерів та смартфонів від ураження шкідливим програмним забезпеченням [2].

7. Одноразові SMS-паролі (система 3D-Secure). Це захисна технологія, що підключена до більшості банківських карт. Система підвищує безпеку платежу і знижує ризик несанкціонованих операцій. Щоразу, при оплаті онлайн на мобільний телефон клієнта висилається одноразовий SMS-пароль для підтвердження платежу [4].

8. Обмеження тривалості сесії. У разі неактивності користувача, сесія в системі інтернет-банкінгу через певний час (зазвичай 10-15 хвилин) буде закрита. Після цього для відновлення роботи буде потрібно заново пройти аутентифікацію. Даний механізм є особливо ефективним при здійсненні клієнтом доступу до рахунку з комп'ютеру, що знаходиться у публічному доступі [1].

Зростання обсягів банківських операцій в мережі Інтернет обумовлює також і зростання шахрайських дій. Типовими загрозами безпеці банківських операцій у Інтернеті є кібератаки, серед яких найнебезпечнішими є фішинг, зараження персональних комп’ютерів шкідливим програмним забезпеченням та недостатня безпека мобільних операційних систем. Для протидії цим загрозам буде ефективним використання таких превентивних механізмів, як стандарти PCI DSS, шифрування даних, антивірусні програми для персональних комп’ютерів

та мобільних пристроїв, електронний цифровий підпис, система 3D-Secure і таких фактичних дієвих систем, як антифрод-системи.

Список використаних джерел:

1. Резніченко Є. Безпека Інтернет банкінгу: практичні аспекти [Електронний ресурс]: [сайт] // Bankchart.com.ua. – 2017. – 30 трав. – Режим доступу: http://www.bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_praktichni_aspekti (дата звернення 23.10.2018). – Назва з екрану.
2. Зарицький В. Сім кроків до безпеки інтернет-банкінгу [Електронний ресурс]: [сайт] // Itbiz.ua. – 2015. – 13 жовт. – Режим доступу: https://itbiz.ua/sem-shagov-k-bezopasnosti-internet-bankinga (дата звернення 23.10.2018). – Назва з екрану.
3. Безпека в інтернеті. Як правильно розраховуватися банківською карткою [Електронний ресурс]: [сайт] // Uteka.ua. – 2016. – 28 груд. – Режим доступу: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-bezopasnost-v-internete-kak-pravilno-rasschityvatsya-bankovskoj-kartoj (дата звернення 24.10.2018).- Назва з екрану.
4. 9 правил безпечних інтернет-платежів [Електронний ресурс]: [сайт] // Finance.ua.- 2018.- Режим доступу: https://easypay.finance.ua/9-pravyl-bezpechyh-internet-platezhiv (дата звернення 24.10.2018). – Назва з екрану.

ФІНАНСОВА БЕЗПЕКА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

***Тищенко О. І.**, канд. екон. наук, доцент, **Філоненко Ж. В.,** студ., Східноукраїнський національний університет імені В. Даля, м. Сєвєродонецьк*

Безпека банківської діяльності є частиною національної фінансової безпеки, так як банківська система є найважливішою складовою фінансово-кредитної сфери держави. Саме стан банківського сектора і визначає рівень фінансово-кредитної безпеки, а отже, і рівень фінансової безпеки держави.

Фінансову безпеку банку визначають по-різному:

1) як сукупність умов, при яких потенційно небезпечні для фінансового стану банківської установи дії або обставини ліквідовані або зведені до такого рівня, при якому вони не можуть завдавати збитків при функціонуванні банку, збереженню і відтворенню його майна, інфраструктури, а також перешкоджати досягненню банком статутних цілей;

2) як стан захищеності фінансових інтересів комерційного банку, його фінансової стійкості, а також середовища, в якому він функціонує [1].

Побудова системи безпеки банківської діяльності має на меті:

– захист прав банківських установ, їх структурних підрозділів та співробітників;

– збереження та ефективне використання фінансових, матеріальних, інформаційних ресурсів;

– підвищення конкурентоспроможності та зростання прибутковості за рахунок забезпечення якості банківських послуг і безпеки для клієнтської бази [2].