УДК 004.056

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ШАХРАЙСТВА В БАНКІВСЬКИХ ПЛАТІЖНИХ СИСТЕМАХ

Жмуровська Катерина Романівна
Чукалов Кирило Едуардович
Товстик Вадим Олександрович
курсанти факультету № 4
Харківського національного університету внутрішніх справ
Заводний Олександр Олександрович
студент факультету № 6
Харківського національного університету внутрішніх справ
Онищенко Юрій Миколайович
заступник декана з навчально-методичної роботи факультету № 4
Харківського національного університету внутрішніх справ
кандидат наук з державного управління, доцент

Визначення актуальності проблеми шахрайства в банківських системах включає в себе докладний огляд та обґрунтування важливості вивчення цього явища. Розглянемо, наскільки проблема шахрайства є актуальною у сучасному банківському секторі. Важливо визначити, чому саме ця тема є значущою для держави та бізнесу. Сьогодні існує три основні схеми, через які виводяться кошти. Наведемо ключові аспекти цього аналізу:

1) Виведення коштів через розміщення їх на кореспондентських рахунках в іноземних банках.

2) На другому місці за популярністю серед схем виведення активів банку за кордон – відчуження активів банку за заниженою ціною. Оцінювачі, вступаючи у змову із співробітниками банку, оцінюють майно, значно занижуючи його реальну вартість. Після цього вказане майно реалізується серед довірених осіб та партнерських організацій.

3) Виведення майна з-під застави. Мова йде про майно, що належить проблемному банку та на яке накладається обмеження щодо можливості його відчуження, оскільки воно виступає у якості майнового забезпечення. Як

правило, у такій схемі приймають участь, крім посадових осіб банку, ще й зацікавлені особи з числа державних виконавців виконавчої служби, які незаконно знімають заборону на відчуження, вилучаючи відповідний запис з Державного реєстру речових прав на нерухоме майно [1].

Аналіз цих аспектів дозволяє встановити реальний обсяг проблеми та її вплив на банківську сферу, що, в свою чергу, обґрунтовує необхідність подальших досліджень та розробки ефективних заходів протидії шахрайству в цій галузі.

Безпека платіжних операцій в сучасному світі стала ключовим питанням для обох сторін платіжного процесу – як для клієнтів, так і для фінансових установ. Для клієнтів – це не лише технічна гарантія, але й ключовий елемент їхньої фінансової стабільності. Можливість здійснювати безпечні та захищені транзакції додає впевненості користувачам, що їхні фінансові активи належним чином захищені від можливих загроз. Для фінансових установ забезпечення безпеки платіжних операцій є стратегічним завданням, що не тільки спрямовано на захист інтересів клієнтів, а й сприяє підтримці довіри до самого фінансового сектору в цілому.

Впровадження сучасних технологій, які гарантують шифрування та виявлення шахрайських атак, дозволяє фінансовим установам створювати безпечне електронне середовище для проведення транзакцій. Важливість безпеки платіжних операцій визначається необхідністю відповідності законодавчим вимогам та відповідним стандартам. Фінансові установи повинні забезпечувати дотримання найвищих стандартів безпеки, щоб уникнути ризиків та зберегти довіру клієнтів.

В сучасному світі, коли банківські платіжні системи відіграють ключову роль у фінансових взаємодіях, загрози їхній безпеці стають все більш виразними та вдосконаленими. Ретельний аналіз популярних видів атак в цій області розкриває важливі аспекти, які потрібно враховувати для забезпечення надійності та захищеності банківських систем.

1) Фішинг – це спосіб виманити в людини дані банківської картки за

допомогою інтернет-ресурсів. Для цього шахраї створюють копії сайтів банків, інтернет-магазинів чи платіжних систем. Проводячи на таких сайтах оплату, жертва вносить туди свої платіжні реквізити, після чого шахраї отримують доступ до її банківського рахунку [2].

2) Malware – це зловмисне програмне забезпечення, яке може негативно впливати на пристрої користувачів чи банківські системи. Ефективний захист від Malware вимагає постійного оновлення антивірусного програмного забезпечення, використання брандмауерів та ретельного моніторингу активності.

3) Соціальний інжиніринг – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів; зловмисники намагаються зробити так, аби жертва добровільно переказала їм кошти або назвала конфіденційну банківську інформацію, нічого при цьому не запідозривши. Для цього шахраї можуть втертися в довіру до цієї людини, зокрема видавши себе за знайомого чи родича жертви [2].

Банківські системи стають об'єктом постійних кібератак та спроб злому програмного забезпечення, що ставить під загрозу безпеку фінансових даних та конфіденційність клієнтів. Для отримання та використання конфіденційної інформації зловмисники використовують різноманітні техніки, програми-вимаганки та експлойти для отримання несанкціонованого доступу до інформаційних систем банківських установ.

Кібератаки можуть включати в себе розповсюдження шкідливих програм, таких як віруси, трояни та рансомвіруси, спрямованих на шифрування інформації з метою вимагання викупу. Фішингові атаки та соціальна інженерія використовуються для обману користувачів та отримання їхніх облікових даних. У контексті програмного забезпечення зловмисники активно використовують нуль-денні вразливості та експлуатують їх до тих пір, поки виробники не виправлять ці дефекти. Крадіжка автентифікаційних даних також є серйозною загрозою, коли зловмисники отримують доступ до паролів та інших ідентифікаційних даних користувачів. Атаки типу SQL-ін'єкцій

застосовуються для отримання доступу до баз даних через вразливості у програмному забезпеченні. Деніал-оф-сервіс (DDoS) атаки спрямовані на перевантаження мережевих ресурсів та призводять до зниження доступності банківських систем для легітимних користувачів.

Компанія може впровадити розробку додаткових елементів захисту інженерами безпеки. Вони вже на етапі розробки аналізуватимуть моделі загроз, екстрені випадки тощо, та визначатимуть вимоги, які будуть використовувати розробники. Після цього платформу захисту можна також перевірити, виставивши її на публічний хакінг, для тестування на вразливість незалежними експертами. Для того щоб максимально захистити компанію від кіберзагроз, варто на постійній основі займатись питаннями інформаційної безпеки. Для цього можна найняти відповідного співробітника, створити власні відділи/департаменти з кібербезпеки або ж доручити цей напрямок спеціалізованій компанії, яка проведе аудит інформаційної безпеки компанії та на основі отриманих даних збудує стратегію кіберзахисту, відповідну даному бізнесу [3].

Вдосконалення методів автентифікації та авторизації користувачів є критично важливим завданням у контексті зростаючих кіберзагроз та забезпечення надійного захисту інформації. Однією з ключових стратегій є впровадження більш сучасних та безпечних методів, які забезпечують високий рівень ідентифікації та авторизації. По-перше, використання двофакторної автентифікації є ефективним засобом забезпечення безпеки даних. Крім традиційного пароля, система вимагає додаткового підтвердження, такого як код, отриманий на мобільний пристрій або за допомогою біометричних даних. Це робить значно складнішими спроби несанкціонованого доступу. Для покращення захисту, біометричні методи, такі як сканування відбитків пальців, розпізнавання обличчя чи сканування сітківки ока, використовуються для ідентифікації користувачів. Ці унікальні біологічні характеристики надають високий рівень достовірності та важко підробляються.

Аналіз поведінки користувача може стати важливим елементом

вдосконалення систем автентифікації. Системи можуть вивчати та аналізувати звички та стиль роботи користувача, використовуючи це для створення унікального «цифрового відбитка» і виявлення аномальної активності. Заходи по вдосконаленню авторизації та автентифікації включають у себе строгі політики доступу, які обмежують права користувачів відповідно до їхніх ролей та необхідності доступу.

Правильно налаштована автентифікація та авторизація є ключовими складовими захисту даних користувачів. Це дозволяє уникнути несанкціонованого доступу до особистої інформації, фінансових даних та інших конфіденційних даних. У підсумку, автентифікація та авторизація є фундаментальними процесами для забезпечення безпеки даних користувачів. Захист особистої інформації в мережі стає все важливішим, і правильне його забезпечення сприяє підвищенню довіри користувачів до онлайн-сервісів та додатків [4].

Не менш важливим є розвиток та впровадження антивірусного програмного забезпечення. Ці заходи мають на меті ефективний захист від широкого спектру кіберзагроз, включаючи віруси, троянські програми, шкідливе програмне забезпечення тощо. Розробка антивірусного програмного забезпечення включає в себе створення алгоритмів та методів, спрямованих на виявлення та нейтралізацію нових та еволюційних загроз. Врахування останніх тенденцій у сфері кібербезпеки, аналіз підписів вірусів, а також використання технологій машинного навчання та штучного інтелекту дозволяють антивірусному програмному забезпеченню ефективно розпізнавати й блокувати нові загрози. Впровадження антивірусного програмного забезпечення включає в себе інтеграцію з іншими компонентами системи безпеки та мережевою інфраструктурою.

Забезпечення регулярних сканувань файлів, підключених пристроїв та мережевого трафіку дозволяє вчасно виявляти та ізолювати можливі загрози. Крім того, ефективне використання антивірусного програмного забезпечення вимагає свідомості та підготовки персоналу користувачів. Тренінги з

кібербезпеки допомагають уникнути недбалого використання, сприяючи оптимальному функціонуванню захисних механізмів.

Отже, аналіз сучасних методів шахрайства в банківських платіжних системах демонструє високий рівень технологічної складності та винахідливості кіберзлочинців у їхніх спробах незаконного отримання доступу до фінансових ресурсів. Фактори, такі як фішинг, кібератаки, соціальна інженерія та зловживання автентифікаційними даними, визначають тривалість та масштаб кіберзагроз у банківському секторі**.**

Важливо відзначити, що такі атаки стають більш витонченими та цілеспрямованими, викликаючи необхідність постійного удосконалення заходів безпеки. Виробники програмного забезпечення та фінансові установи повинні активно впроваджувати передові технології та аналітичні засоби для виявлення та запобігання нових типів та видів загроз.

Зростаюча роль інформаційної грамотності користувачів та їхнє активне залучення до процесів безпеки також стають ключовими компонентами боротьби з шахрайствами. Висновок полягає у необхідності невпинного моніторингу та адаптації стратегій безпеки, а також у формуванні відповідальної культури безпеки серед усіх учасників банківських платіжних систем. Тільки комплексний та постійно оновлюваний підхід може гарантувати ефективний захист від постійно зростаючих загроз в цифровому фінансовому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні проблеми банківської системи України: причини виникнення та шляхи розв'язання. URL: https://jfub.donnu.edu.ua/article/view/2835/2874 (дата звернення: 25.05.2024).

2. Шахрайство в інтернеті: найбільш поширені схеми. URL: https://www.epravda.com.ua/publications/2023/12/18/707794/ (дата звернення: 25.05.2024).

3. Основні види кібератак і як від них захиститися. Експлейнер від «Кіберакселератора» URL: https://speka.media/kiberbezpeka/osnovni-vidi-kiberatak-i-yak-vid-nix-zaxistitisya-kvz5wv (дата звернення: 25.05.2024).

4. Автентифікація та авторизація: Захист даних користувачів. URL: https://it-rating.ua/autentifikatsiya-ta-avtorizatsiya-zahist-danih-koristuvachiv (дата звернення: 25.05.2024).