Сумський державний університет
Навчально-науковий інститут бізнес-технологій «УАБС»

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ФІНАНСОВО-КРЕДИТНОЇ СИСТЕМИ УКРАЇНИ

МАТЕРІАЛИ
IV Всеукраїнської науково-практичної on-line-конференції
(Суми, 21–22 листопада 2019 року)

У двох частинах

Частина 2

Суми
Сумський державний університет
2019

УДК 303.09:336.717.1

Яровенко Ганна Миколаївна,
к.е.н., доцент,
Сумський державний університет, м. Суми
Нечепоренко Ілля Дмитрович,
Студент групи ЕК-61а
Сумський державний університет, м. Суми

СУЧАСНІ ТЕХНОЛОГІЇ КІБЕРЗАХИСТУ ЩОДО ВИЯВЛЕННЯ ШАХРАЙСТВ, ЩО ЗДІЙСНЮЮТЬСЯ ПЕРСОНАЛОМ БАНКУ

Шахрайство з грошовими засобами є розповсюдженим способом незаконного збагачення, незалежно від того, яким чином воно здійснювалося. Особливо актуальною ця проблема є для фінансово-кредитних установ, які безпосередньо мають справу з фінансовими операціями. Але шахрайські дії в банківській сфері за часту важко виявити на тлі величезної кількості автентичних транзакцій, що проводяться щодня. З іншого боку, не виявлення зловживань, фінансових махінацій, відмивання кримінальних доходів, незаконне отримання коштів з клієнтських рахунків, тощо може завдати шкоди репутації банку. Найтривожніша статистика з банківського шахрайства пов'язана саме із зловживаннями інсайдерів: у 70% випадків злочин було скоєно банківськими службовцями, а саме тими, хто має найвищий рівень доступу до банківської інформаційної системи [1]. Системні адміністратори та адміністратори баз даних мають усі можливості для здійснення або сприяння шахрайству, оскільки володіють повним доступом до банківської інформації, ключів шифрування, паролів та знищення наслідків протиправних дій. Також давні співробітники і топ-менеджери невеликих банків та філій використовують свій доступ до багатьох операцій в системі банку та можуть зловживати своїми довірчими позиціями. Схеми внутрішньобанківських шахрайств залишаються непоміченими протягом багатьох місяців завдяки тому, що фахівці ІТ-відділу

або топ-менеджери вдало скривають свої махінації. Шахрайства, скоєні банківськими службовцями, призводять до багатомільярдних втрат для банків, що також негативно впливає й на економіку країни за рахунок зниження довіри клієнтів до банківської системи та виведення коштів з країни. Саме тому ця проблема є актуальною та потребує комплексного підходу до її вирішення.

Щоб фінансова установа була на крок попереду кіберзагроз, важливо виявляти загальні попереджувальні ознаки того, що співробітник може бути залучений в будь-яке фінансове шахрайство. Як приклад, банківська система кіберзахисту повинна виявляти такі маркери [2]:

- вхід в облікові записи клієнтів у неробочий час;
- частий або надмірний доступ до акаунтів з високим прибутком;
- відмова від вихідних протягом тривалого часу;
- доступ до облікових записів тими співробітниками, які не мають відповідних прав або не є звичними для їх роботи;
- здійснення операцій по тих рахунках, які не використовувалися протягом тривалого часу;
- доступ до «чорного списку» клієнтів;
- доступ до камер спостереження у банку, тощо.

Дієвим заходом попередження шахрайств персоналом є розробка та впровадження автоматизованого рішення для моніторингу дій співробітників, яке іноді сприймається ними як акт недовіри до цінних співробітників, але дозволить виявити підозрілу поведінку. Саме на поведінковому профілюванню базуються сучасні зарубіжні системи захисту від шахрайства. Створення даної технології стало можливим завдяки використання аналітики великих даних. [3, 5] Профілювання дозволяє аналізувати дуже великі обсяги даних про історичну поведінку кожного співробітника і клієнта, щоб у результаті сформувати профіль, який описує типовий спосіб використання свого облікового запису. Потім система порівнює кожну дію співробітника у системі, яка відбувається у його профілі, з еталонним профілем, порівнює з рядом індикаторів, щоб оцінити ймовірність того, що операція або транзакція є результатом

внутрішнього або зовнішнього шахрайства. Також профілювання дозволяє визначити випадки, коли доступ до облікового запису співробітника здійснюється з незнайомої IP-адреси. Використання даної технології дозволить відслідковувати дії співробітників, які є поза межами їх посадових інструкцій. Профілювання сприяє накопиченню статистики щодо шахрайств та включенню цих випадків, як продуційних правил системи кіберзахисту, що в подальшому сприятиме блокуванню підозрілих транзакцій і запобіганню втрат.

Потужною технологією для систем захисту від шахрайства є машинне навчання, яке набуває поширення у закордонних системах захисту, але не є розповсюдженою в українських банках. Машинне навчання, засноване на статичних елементах управління і поведінковому профілювання, надає більш точний і чутливий набір інструментів для виявлення шахрайства. Застосування машинного навчання в системах протидії шахрайству передбачає використання великих обсягів історичних даних для навчання алгоритмів, щоб вони поступово вчилися виявляти аномалії серед маси законних транзакцій. Прикладом технології машинного навчання для протидії шахрайству є програмне забезпечення NetGuardians. Було встановлено, що його застосування NetGuardians дозволяє скоротити число помилкових спрацьовувань на 80 відсотків [4].

На нашу думку, є велика потреба у створенні потужного продукту для виявлення внутрішніх шахрайств – експертної системи, яка б поєднала технологію профілювання та машинного навчання. Це можливо завдяки реалізації алгоритмів, які базуються на побудові нейронних мереж та нечітких множин, у поєднанні із сучасними мовами програмування. Шахраї стають все більш витонченими, швидко реагують на появу нових технологій, що дозволяє змінювати і адаптувати свої підходи до шахрайства. Тому банки повинні також бути гнучкими, щоб реагувати на нові загрози. Для боротьби із шахрайством банкам слід використовувати нові підходи, що дозволить зберегти репутацію та підвищити довіру населення.

Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України».

Список використаних джерел:

1. Тарасюк Я. Основні способи скоєння шахрайств в банківсько-кредитній сфері та протидія їм [Електронний ресурс] / Я. Тарасюк. – Режим доступу до ресурсу: https://blogdocentyarynatara.io.ua/s2304419/osnovni_sposobi_skonnya_shahraystv_v_bankivsko-kreditniy_sferi_ta_protidiya_em.

2. 6 Indicators of Employee Fraud for Financial Institutions [Електронний ресурс] // Verafin. – 2019. – Режим доступу до ресурсу: https://verafin.com/2019/08/6-indicators-of-employee-fraud-for-financial-institutions/.

3. Bharadwaj R. AI for Cybersecurity in Finance – Current Applications [Електронний ресурс] / R. Bharadwaj // EMERJ. – 2019. – Режим доступу до ресурсу: https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/.

4. Digital banking fraud: Best practice for technology-based prevention [Електронний ресурс] // NetGuardians. – Режим доступу до ресурсу: https://netguardians.ch/digital-banking-fraud/.

5. Mossa B. Internal Fraud in Banks - Recognizing Red Flags [Електронний ресурс] / B. Mossa // LinkedIn. – 2018. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/internal-fraud-banks-recognizing-red-flags-bahru-mossa-cm.