УДК 004.056

ОБЗОР СИСТЕМ ПРОТИВОДЕЙСТВИЯ БАНКОВСКОМУ МОШЕННИЧЕСТВУ

Р. Р. ФАХРЕТДИНОВ [1], В. А. КУЛАГИН [2], А. Р. КАРИМОВ [3]

[1] rusel1362@gmail.com, [2] lander220138@gmail.com, [3] karimov.aidar111@gmail.com

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Аннотация. В статье рассматриваются существующие системы противодействия банковскому мошенничеству на мировом рынке, а также их функции и методы выявления.

Ключевые слова: антифрод; ДБО; мошенничество; кибератаки; компоненты.

ВВЕДЕНИЕ

С принятием Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств» и участившимся атаками на банковские системы возрос интерес к системам противодействия мошенничеству в банковской сфере (антифрод) и обнаружения попыток совершения мошеннических операций в системах дистанционного банковского обслуживания (ДБО). Такие системы позволяют обнаруживать и предотвращать мошеннические действия, используя технологии машинного обучения, цифровые профили устройств и пользователей и др.

С тех пор как многие банковские и платежные операции перешли в область информатизации, мошенничество в этой сфере активно развивается. Наиболее известные атаки на банковские системы за последние несколько лет были выполнены преступными группировками Cobalt, Carbanak, Lazarus и Lurk. По оценкам Сбербанка, убытки России от кибератак составляют порядка 650 млрд рублей в год. При этом только в первые две недели 2019 года Сбербанк подвергся 18 кибератакам. Злоумышленники производят атаки на системы межбанковских переводов, карточный процессинг, управление банкоматами, интернет-банкинг и платежные шлюзы.

По данным отчета Positive Technologies, злоумышленники используют простой сценарий для совершения атаки, который состоит из 5 последовательных этапов:

- Предварительная разведка и подготовительные работы.
- Проникновение во внутреннюю сеть.
- Закрепление во внутренней сети и развитие атаки.
- Компрометация банковских систем и хищение средств.
- Сокрытие следов.

Эти этапы актуальны при фишинге, заражении компьютера или смартфона жертвы известным ранее вредоносом, проведении атак типа man-in-the-middle, использовании кейлогеров и даже уязвимостей нулевого дня.

Специалисты Group-IB выделили 7 распространенных схем хищения денежных средств при атаках на системы дистанционного банковского обслуживания (ДБО):

- Социальная инженерия.
- Переводы с карты на карту.
- Переводы через онлайн-банкинг.
- Перехват доступа к мобильному банкингу.
- Поддельный мобильный банкинг.
- Покупки с помощью Apple Pay и Google Pay.

МИРОВОЙ РЫНОК СИСТЕМ ПРОТИВОДЕЙСТВИЯ БАНКОВСКОМУ МОШЕННИЧЕСТВУ

В 2018 году мировой рынок систем противодействия мошенничеству был оценен в 13,59 млрд долларов США. По прогнозам на 2024 год, масштаб должен достигнуть 31,15 млрд долларов США (CAGR = 16,42 %). Это связано с повышением возможностей мошенничества из-за увеличения количества транзакций (как денежных, так и ориентированных на информацию), технологических достижений, а также общей цифровизации финансового сектора.

По отчетам Markets and Markets, основными поставщиками систем противодействия банковскому мошенничеству по всему миру являются следующие компании:

- IBM (США);
- FICO (США);
- SAS Institute (США);
- BAE Systems (Великобритания);
- NICE Systems (Израиль);
- LexisNexis Risk solutions (США)

РЫНОК СИСТЕМ ПРОТИВОДЕЙСТВИЯ БАНКОВСКОМУ МОШЕННИЧЕСТВУ В РОССИИ

Рынок антифрод-систем в России прошел несколько характерных ступеней развития. Эволюционными прорывами были такие важные вехи, как появление Chip Liability Shift в 2007 — 2008 гг., а до этого появление стандарта мониторинга операций по банковским картам от Visa в 2003 г., которые дали толчок компонентам антифрод-систем в процессинге.

В 2011-2012 гг. произошла массовая серия атак на ДБО, поначалу затронувших преимущественно юридических лиц и впоследствии распространившихся на граждан.

В 2014-2015 гг. банковский троян Lurk и другие вредоносные программы дали толчок к появлению российских решений от компаний Group-IB и «Лаборатории Касперского».

В 2018 г. принятый Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств» [1] вновь накалил вопрос об антифрод-системах, особенно для тех представителей кредитно-финансового сектора, для которых акты реализации транзакционного мошенничества были невелики и по факту измерялись ниже стоимости самих антифрод-решений.

По данным Сбербанка, за 2018 год с помощью внедренной антифрод-системы удалось сохранить более 32 млрд рублей, принадлежащих вкладчикам.

ФУНКЦИИ СИСТЕМ ПРОТИВОДЕЙСТВИЯ БАНКОВСКОМУ МОШЕННИЧЕСТВУ

Процесс обнаружения и предотвращения мошенничества не имеет начальной или конечной стадии, он должен выполняться непрерывно и включать в себя следующие подпроцессы:

- Мониторинг;
- Обнаружение;
- Принятие решений;
- Обучение.

Системы противодействия мошенничеству могут иметь в своем арсенале следующие технологии и возможности: Текстовая аналитика, которая выполняется с помощью технологий поиска, категоризации контента и извлечения сущностей. Расчет статистических параметров, который используется для выявления отклонений, которые могли бы указать на мошенничество. Сетевая аналитика, которая используется для идентификации соединений, выявления закономерностей. Gap-тестирование подразумевает обнаружение любых недостающих элементов в последовательных данных там, где их не должно быть. Подтверждение даты входа используется для оценки неподходящего или подозрительного времени для размещения или ввода информации. Контролируемое машинное обучение, которое производится на основе исторических данных, что позволяет выявлять определенные шаблоны. Обучение без учителя,

что подразумевает анализ и оценку данных, которые не содержат сведений о выявленном мошенничестве. Используется для выявления новых аномалий.

Функция у всех антифрод-систем едина — выявлять и предотвращать мошенничество. Однако они могут по-разному решать данную задачу и сравнивать антифрод-системы без проведения дополнительной классификации является неверным решением. Так, например, есть так называемые core-системы — мощные аналитические платформы, позволяющие реализовывать логику в отдельных сегментах (ДБО или процессинг банковских карт), также существуют специализированные системы, контролирующие параметры устройств и риски на их стороне. И в то же время разрабатываются отдельные системы, заточенные под распознавание фото, видео, речи. Многие из систем не конкурируют, а, наоборот, дополняют функции друг друга. Например, конкретное узкоспециализированное решение не может само по себе закрывать требования Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств» [1] и существовать как независимая платформа.

Исходя из этого мы разделили существующие системы противодействия банковскому мошенничеству на 3 класса:

1 класс. Решения данного класса направлены на выявление и идентификацию следов мошенничества и выявление аномалий.

2 класс. Решения данного классы направлены на идентификацию инструментов мошенничества, причины или риска (например, наличие вредоносных программ, компонентов удаленного управления, компонентов фишинга).

3 класс. Решения данного класса решают узкоспециализированные задачи. В частности, они могут быть предназначены для распознавания изображений для выявления мошенничества, могут быть оснащены системой распознавания речи.

КРАТКИЙ ОБЗОР СИСТЕМ ПРОТИВОДЕЙСТВИЯ БАНКОВСКОМУ МОШЕННИЧЕСТВУ

Далее будет рассмотрено 4 вида систем противодействия банковскому мошенничеству:

1). Комплексные системы обнаружения банковского мошенничества и выявления аномалий;

2). Системы идентификации инструментов банковского мошенничества;

3). Узкоспециализированные системы обнаружения признаков банковского мошенничества;

4). Смешанные системы противодействия банковскому мошенничеству.

К комплексным системам обнаружения банковского мошенничества и выявления аномалий можно отнести следующие:

FICO Application Fraud Manager [8]. Система FICO Application Fraud Manager от компании FICO относится к общеаналитическим платформам и осуществляет идентификацию попыток мошенничества в режиме реального времени за счет аналитической системы, которая использует технологии машинного обучения и адаптивного анализа. Решение может быть установлено как локально, так и использоваться по технологии SaaS. Система позволяет предотвращать попытки мошенничества со стороны третьих лиц, а также попытки преднамеренного злоупотребления привилегиями учетных записей, направленные на мошенничество с кредитными и дебетовыми платежными картами, электронными платежами, депозитными счетами.

FraudWall [9]. Систему FraudWall от компании «Фродекс» можно отнести к классу общеаналитических платформ. Она предназначена для предотвращения кражи средств клиента в системах дистанционного банковского обслуживания (ДБО), борьбы с внутренним мошенничеством (например, несанкционированные платежи в АБС), предотвращения кражи средств банка через АРМ КБР. Когда система выявила подозрительный платеж, она совершает звонок клиенту и ведет с ним живое общение, распознавая ответы клиента. По завершению звонка FraudWall принимает решение об исполнении платежа или остановке операции.

IBM Safer Payments [11]. Решение IBM Safer Payments от компании IBM относится к общеаналитическим платформам. Оно разработано на основе платформы IRIS после приобретения компанией IBM компании IRIS Analytics. Система предназначена для обнаружения попыток мошенничества в реальном времени. При этом обеспечивается безопасность как при проведении безналичных платежей во многих системах (автоматизированные расчетные палаты, банки-эквайеры, Единая зона платежей в евро, Chip & Pin и других), так и через торговые терминалы, банкоматы, онлайн- и мобильные банки.

К системам идентификации инструментов банковского мошенничества можно отнести следующие:

F5 WebSafe [18]. Решение по защите от мошенничества от компании F5 называется F5 WebSafe и предназначено для борьбы с кражей учетных записей, обнаружения признаков заражения вредоносными программами, кейлоггинга, фишинга, троянов удаленного доступа (RATs), а также атак типа MITM (Man in the Middle), MITB (Man in the Browser) и MITP (Man in the Phone — взлом мобильных устройств). При этом F5 WebSafe применяет различные методы идентификации мошеннических действий, например, попытки автоматического перевода, особенности внедрения вредоносных программ, таких как Zeus, Citadel, Carberp. При этом система выполняет анализ цифровых профилей устройств и пользователей.

IBM Trusteer Rapport [19]. Антифрод-система от компании IBM предназначена для защиты пользователей от перехвата учетных данных, захвата экрана, вредоносных программ и фишинговых атак, в том числе атак типа MITM и MITB. Для этого в IBM Trusteer Rapport применяются технологии машинного обучения, что позволяет автоматически обнаружить и удалить вредоносные программы с конечного устройства, обеспечив безопасность сеанса работы в режиме онлайн.

Kaspersky Fraud Prevention [20]. Решение Kaspersky Fraud Prevention от «Лаборатории Касперского» предназначено для решения проблемы цифрового мошенничества в онлайн-банкинге, ритейле, государственных сервисах, онлайн-играх и других отраслях, использующих веб-сайты и мобильные приложения для предоставления своих услуг.

WEB ANTIFRAUD [23]. Система направлена на предотвращение кражи пользовательских аккаунтов в онлайн-сервисах. Для этого используется формирование отпечатка и анализ устройства пользователя, анализ поведения на сайте, поиск присутствия троянов в браузерах (в том числе автоматический перевод средств и MITB атаки), поиск принадлежащих одному владельцу аккаунтов (в целях реализации мер по предотвращению отмывания денег, AML), а также другие технические инструменты, препятствующие деятельности мошенников на сайте онлайн-сервиса. Антифрод решение WEB ANTIFRAUD работает автоматически без участия человека, но при необходимости предоставляет подробную аналитику по произошедшим инцидентам. WEB ANTIFRAUD помогает принять решение о необходимости двухфакторной аутентификации в каждом конкретном случае, а также сообщает об инцидентах безопасности и признаках кражи аккаунтов.

К узкоспециализированным системам обнаружения признаков банковского мошенничества можно отнести следующие:

FPS.Bio. Система противодействия банковскому мошенничеству FPS.Bio от компании «ВижнЛабс» относится к классу узкоспециализированных платформ. Система разработана на базе решения по биометрической верификации и идентификации физических лиц. Ядром FPS.Bio является нейронная сеть, которая, по словам разработчиков, использует уникальные алгоритмы. К функциям системы относится формирование биометрического портрета клиента, сравнение его с миллионами аналогичных портретов и предоставление результатов для принятия решений.

SmartTracker.FRAUD. Программно-аппаратный комплекс фотобиометрический идентификации SmartTracker.FRAUD позволяет заменить проверку подлинности документов и предоставленной клиентами банка информации на совершено другой метод, основанный на контроле идентификации внешности (той информации, которую человек не может подделать).

К смешанным системам противодействия банковскому мошенничеству можно отнести следующие:

RSA Adaptive Authentication and Transaction Monitoring. Данная система от компании RSA относится к классу общеаналитических платформ 1 класса, но включает в себя возможности и 2 класса. Система позволяет выявлять попытки мошенничества в режиме реального времени и производит мониторинг транзакций после входа пользователя в систему, что позволяет защититься от атак типа MITM и MITB. При этом RSA Transaction Monitoring and Adaptive Authentication может быть внедрена как на серверах организации, так и использоваться в качестве облачного сервиса.

ЗАКЛЮЧЕНИЕ

Мошенничество в банковской сфере продолжает прогрессировать с каждым годом. А потому растет рынок систем противодействия банковскому мошенничеству. Лидерами в данной сфере являются США. Однако обеспечение безопасности от фрода актуально и для российских финансовых организаций. При выборе системы противодействия мошенничеству необходимо в первую очередь определиться с тем, какие задачи ей следует выполнять. В большинстве случаев для того чтобы защитить банк от мошенничества, потребуется использование антифрод-систем нескольких классов. При этом, при выборе общеаналитических платформ следует обращать внимание на сложность внедрения и удобство использования, а при выборе систем, которые мы отнесли ко 2 классу, стоит обратить внимание на применяемые методы (например, схемы выявления вредоносных программ, возможности удаленного управления и т. д.). Продукты 3 класса могут дополнить систему защиты, т. к. каждый продукт решает узкоспециализированную задачу (распознает изображение, речь и т. д.).

СПИСОК ЛИТЕРАТУРЫ

1. Отчет “Атаки на банки” от компании Positive Technologies [Электронный ресурс] / – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Banks-attacks-2018-rus.pdf

2. ARIC White Label [Электронный ресурс] / – Режим доступа: https://www.featurespace.com/.

3. FRAUD-Анализ [Электронный ресурс] / – Режим доступа: http://www.bssys.com/

ОБ АВТОРАХ

ФАХРЕТДИНОВ Руслан Равилевич, магистрант 2-го курса ФИРТ.

КУЛАГИН Вячеслав Александрович, магистрант 2-го курса ФИРТ.

КАРИМОВ Айдар Радикович, магистрант 2-го курса ФИРТ.

METADATA

Title: Review of anti-fraud systems.

Authors: R. R. Fakhretdinov [1], V. A. Kulagin [2], A. R. Karimov [3]

Affiliation: Ufa State Aviation Technical University (UGATU), Russia.

Email: [1] rusel1362@gmail.com, [2] lander220138@gmail.com, [3] karimov.aidar111@gmail.com

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), no. 2 (25), pp. 92-96, 2021. ISSN 2225-9309 (Print).

Abstract: This article discusses the existing systems of countering bank fraud on the world market, as well as their functions and methods of detection.

Key words: antifraud, RBS, fraud, cyberattacks, components.

About authors:

FAKHRETDINOV, Ruslan Ravilevich, postgraduate student 1 year, Ufa state aviation technical University.

KULAGIN, Vyacheslav Alexandrovich, postgraduate student 1 year, Ufa state aviation technical University.

KARIMOV, Aydar Radikovich, postgraduate student 1 year, Ufa state aviation technical University.