УДК 004.056.5

*Д. В. Загута*

**ИССЛЕДОВАНИЕ проблем обеспечения информационной безопасности в сфере банковской деятельности на примере УСЛУГ дистанционного банковского обслуживания**

Балтийский государственный технический университет «Военмех» имени Д. Ф. Устинова

В настоящее время дистанционное банковское обслуживание (далее — ДБО) является неотъемлемой частью банковских услуг, востребованных клиентами и удобных для кредитных организаций. Количество пользователей систем ДБО неуклонно растёт, увеличивается число и объем операций. Одновременно возрастает и риск от мошеннических действий злоумышленников, пытающихся на волне роста популярности дистанционного банкинга похищать денежные средства в системах ДБО.

Киберпреступники хорошо оснащены и организованы, в таких группах есть ролевое распределение – координаторы, дропперы и прочие специализации. Технологии хищения также развиваются и представляют полноценный технологический процесс - от стадии выявления уязвимостей до готовых инструментов и методов хищения

Атаки, при этом, могут вестись на информационные системы и самих банков и их клиентов, включая АРМ КБР (Автоматизированное рабочее место клиента Банка России), С[ДБО](http://www.tadviser.ru/index.php/%D0%94%D0%91%D0%9E) (система дистанционного банковского обслуживания), АБС (Автоматизированная банковская система) и прочие. Основная цель киберпреступников – максимизация прибыли от хищения при минимизации рисков, реже – причинение репутационного ущерба.

Как показывает практика, решение проблемы обеспечения безопасного дистанционного банковского обслуживания клиентов заключается в комплексном подходе, в сочетании организационных и технических средств защиты, как на стороне клиента, так и на стороне банка. В качестве распространённых и хорошо зарекомендовавших себя методов можно назвать использование на стороне клиента средств аутентификации (токены, считыватель смарт-карт Safe Touch, носители и генераторы сеансовых ключей), ограничение доступа (IP/MAC фильтрация), а на стороне банка — внедрение системы уведомления о событиях, автоматическое завершение по таймауту сессии пользователя, установка лимитов платежей, и т. п.

При этом полностью проблему мошенничества в системах ДБО невозможно решить исключительно техническими и организационными мерами — на каждую доработку систем защиты, на каждое организационное ограничение свободы работы клиента в системе ДБО всегда найдётся новое вредоносное программное обеспечение, новая техническая возможность мошенничества. Не секрет, что по-прежнему самой распространённой предпосылкой успешных атак является невыполнение пользователями основных рекомендаций по обеспечению безопасности при использовании операционной системы и, в частности, при работе в системе ДБО. Любые технические и программные средства будут бесполезны без соблюдения элементарных правил безопасности, без организационных мер. Хороший тому пример – рост числа хищений с помощью методов социального инжиниринга, когда человеческий фактор становится самым слабым звеном в цепи, против которых иногда бессильны самые продвинутые организационные и технические средства. С помощью этого метода происходит более 90% хищений денежных средств[[1]](#footnote-1).

Поэтому в дополнение к перечисленным выше мерам активно развиваются и в настоящее время даже выходят на первый план системы защиты, основанные на экспертном анализе поведения клиента — так называемые антифрод-системы[[2]](#footnote-2), с помощью которых фиксируются аномалии в поведении клиента и выявляются операции, имеющие признаки выполнения их не клиентами банка, а злоумышленниками.

Простейшие антифрод-решения используют обычные фильтры, аналогичные фильтрам в АБС (по сумме платежа, черным спискам и пр.), более сложные обучаются на накапливаемых данных о поведении клиентов, истории платежей и используют хорошо зарекомендовавшие себя методы машинного обучения, такие как поиск аномалий (отклонений от обычного поведения).

Все эти решения помимо их предназначения объединяет одно – они получают данные для анализа из некоторого источника и на основе определенных критериев делают свое заключение, считать ли платеж правомочным или мошенническим. Основным источником данных для анализа является система ДБО, т.к. именно через нее идет общение клиента с банком и именно в ней формируются платежные документы и другие события, анализом которых и занимается антифрод-система. Часть этих данных антифрод может получить и из АБС, но информация о многих событиях системы [ДБО](http://www.tadviser.ru/index.php/%D0%94%D0%91%D0%9E) до [АБС](http://www.tadviser.ru/index.php/%D0%90%D0%91%D0%A1) не доходит, т.к. в АБС она просто не нужна.

Также источниками информации могут служить «черные списки», распространяемые анти-дроп клубом, [ЦБ РФ](http://www.tadviser.ru/index.php/%D0%A6%D0%91_%D0%A0%D0%A4) ([FinCERT](http://www.tadviser.ru/index.php/FinCERT" \o "FinCERT)), базы проверки контрагентов, сформированные по открытым и закрытым источникам (например, от компании «Интегрум»).

Среди анализируемых антифрод-системой параметров и событий могут быть как данные о получателе платежа, банке получателя, назначении и сумме платежа, времени и периодичности платежей, остатке по счету, так и характеристики рабочего места отправителя платежа. Эти данные включают, в том числе, информацию о IP и MAC адресе, ошибках входа и изменения логина/пароля, изменении устройства, провайдера или домена в ходе сессии работы пользователя, наличии возможности для удаленного доступа, наличии обращений к зловредным доменам, файлах cookie, геоданных и прочие. В реально работающих системах фрод-анализа таких параметров десятки.

Как отмечалось выше, в развитых антифрод-системах данные анализируются в динамике, с учетом накапливаемой истории платежей по каждому клиенту и при каждом платеже или другом событии производится поиск аномалий, т.е. отклонений от стандартных паттернов поведения, присущих определенному клиенту.

Основными метриками эффективности антифрод-систем является процент ложных срабатываний – положительных (правомочный платеж признан фродом) и отрицательных (пропущен фродовый платеж). Обе метрики должны быть минимизированы, т.к. в случае положительного ложного срабатывания потребуется ручная проверка платежа (нагрузка на сотрудников банка) и до получателя деньги дойдут позже, а в случае отрицательного деньги будут украдены киберпреступниками. Эти две метрики взаимосвязаны и зависят от настройки чувствительности системы или, по-другому, от порога срабатывания. Развитые антифрод-системы при соответствующей настройке и опытном фрод-аналитике позволяют снизить положительные ложные срабатывания до менее 1%, а отрицательные свести практически к 0.

В заключение хотелось бы отметить, что на момент написания статьи Министерством финансов РФ в Государственную Думу РФ внесен законопроект федерального закона "О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия хищению денежных средств)".[[3]](#footnote-3) Предлагается дополнить Федеральный закон от 27 июня 2011 г. №161-ФЗ "О национальной платежной системе" новой статьей — "Признаки совершения перевода денежных средств без согласия клиента и порядок действий оператора по переводу денежных средств при их выявлении". В частности, была внесена принципиальная правка — если банкам раньше предоставлялось право блокировать подозрительные переводы, тогда как сейчас это вменяется им в обязанность. Таким образом, Банки будут обязаны блокировать операции по переводу денег на срок до двух дней, если транзакция покажется им подозрительной, т.е. сработает система обнаружения мошеннических операций. Однако, не смотря на то, что решение проблем обеспечения информационной безопасности Банки берут на себя, главная задача — это научить самих пользователей систем ДБО управлять рисками, которые сопровождают развитие цифровых финансовых услуг.

**Список использованных источников**

1. Атаки на системы ДБО [Электронный ресурс]. URL: <https://www.securitylab.ru/analytics/485467.php>
2. Анти-фрод системы и как они работают [Электронный ресурс]. URL: <https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/339929.php>
3. Безопасность ДБО [Электронный ресурс]. URL: <http://bankir.ru/publikacii/20120604/bezopasnost-dbo-zavisit-i-ot-banka-i-ot-klienta-10001755/>
4. Безопасность систем дистанционного банковского обслуживания [Электронный ресурс]. URL: <http://bankir.ru/publikacii/20120305/bezopasnost-sistem-distantsionnogo-bankovskogo-obsluzhivaniya-10001328/>
5. Безопасность [Электронный ресурс]. URL: <http://www.bankdbo.ru/bezopasnost>
6. Что умеет ANTI-FRAUD в ДБО? [Электронный ресурс]. URL:  
   <http://www.bssys.com/about/press-center/articles/chto-umeet-anti-fraud-v-dbo/>
7. FRAUD-Анализ [Электронный ресурс]. URL: <http://www.bssys.com/solutions/financial-institutions/fraud/>
8. Как выбрать антифрод-систему для банка? [Электронный ресурс]. URL: <http://www.tadviser.ru/index.php/Статья:Как_выбрать_антифрод-систему_для_банка>

1. По данным издания «[Российская газета» - Федеральный выпуск №7122 (254)](https://rg.ru/gazeta/rg/2016/11/10.html) от 10 ноября 2016 г. [↑](#footnote-ref-1)
2. Термин «фрод» произошел от английского слова «fraud», что переводится как «мошенничество» [↑](#footnote-ref-2)
3. По данным интернет-издания ComNews от 10.10.2017 [↑](#footnote-ref-3)