

УДК342.92: 657.633.5

© К.Д. Валявская, А.И. Кормилицын, 2025

**Внутренний контроль банков по выявлению действий дропов:  
методы крупных российских банков и государственного  
регулирувания**

К.Д. Валявская

студент 4 курса специалитета НИЯУ МИФИ, Москва

Email: vkd224@yandex.ru

А.И. Кормилицын

ассистент кафедры финансового мониторинга НИЯУ МИФИ, Москва

Email: and-kormilicyn@yandex.ru

*Аннотация: Статья посвящена анализу современных методов противодействия дропперам. Рассматриваются ключевые инициативы российских банков по выявлению и блокировке подозрительных транзакций с использованием технологий искусственного интеллекта и автоматизированного мониторинга.*

*Ключевые слова: дропперы, финансовое мошенничество, Росфинмониторинг, антифрод-системы, внутренний контроль, экономическая безопасность*

**Internal control of banks for detecting drop actions: methods of major  
Russian banks and state regulation**

K.D. Valyavskaya

4th year undergraduate student, NRNU MPhI, Moscow

Email: vkd224@yandex.ru

A.I. Kormilitsyn

Assistant at the department of financial monitoring, NRNU MPhI, Moscow

Email: and-kormilicyn@yandex.ru

*Abstract: The article is devoted to the analysis of modern methods of countering droppers. The key initiatives of Russian banks to identify and block suspicious transactions using artificial intelligence and automated monitoring technologies are considered.*

*Keywords: droppers, financial fraud, Rosfinmonitoring, anti-fraud systems, internal control, economic security*

Росфинмониторинг на регулярной основе ведет работу по противодействию дропам, взаимодействуя с банковским сектором, который разрабатывает и внедряет современные системы противодействия этим

схемам. При этом финразведка намерена усилить борьбу с дропперами, используя новое право на приостановку операций клиентов банков. Росфинмониторинг рассматривает дропперство как инструмент отмывания преступных доходов и намерен системно выявлять организаторов, их финансовые связи, а также конфисковывать связанные с этой деятельностью активы. Банки, со своей стороны, будут играть ключевую роль в реализации этих мер, обеспечивая оперативное исполнение решений финразведки.

В 2024 году «Т-Банк» сообщил о блокировке около 130 тысяч подозрительных счетов, многие из которых принадлежали несовершеннолетним и безработным, ставшими жертвами или соучастниками мошеннических схем. [4] По данным регуляторов, подобные схемы с участием дропперов остаются одним из основных каналов для незаконных финансовых операций. Банки вынуждены тратить большое количество ресурсов на разработку и улучшение систем внутреннего контроля, чтобы выявлять таких участников, но преступники быстро адаптируются к новым мерам защиты.

Дропперы (или дропы) — это подставные лица, которые задействованы в нелегальных схемах, с целью обналичивания или перевода похищенных денежных средств. [1][21] Термин происходит от английского слова *drop*, что дословно переводится как «бросать, капать». На данный момент их классифицируют на «обнальщиков», «транзитников», «заливщиков». К «обнальщикам» относят тех, кто самостоятельно обналичивают денежные средства, полученные преступным путем, зачисленные на банковскую карту. «Транзитники» - промежуточное звено в мошеннической схеме, они переводят незаконно присвоенные средства дальше по цепочке на реквизиты, указанные организатором махинации. «Заливщиками» являются дропы, которые вносят наличные средства на свои банковские карты. [2][22] Также Росфинмониторинг выделил основные характеристики дроппа. Это мужчина моложе 30 лет, регулярно пользующийся интернет-ресурсами. Его кредитная история не содержит нарушений, и он не привлекался к уголовной ответственности.

Актуальность данной проблемы не вызывает сомнений, так как несмотря на принимаемые меры банков по противодействию мошенническим схемам, злоумышленникам всё же удается вовлекать граждан в незаконные операции. Многие становятся жертвами обмана из-за неосведомленности или соблазна легкого заработка. В связи с этим важно изучить, какие инструменты используют банки для минимизации рисков и защиты клиентов. В данной статье мы рассмотрим, как ведущие российские банки работают над пресечением мошенничества и какие меры позволяют снизить вероятность финансовых махинаций.

Несмотря на то, что технологии мониторинга финансовых операций развиваются быстро, проблема дропперов остается одной из ключевых

угроз для банковской системы. Крупные банки, такие как «Сбербанк», «Т-Банк», «ВТБ» и «Альфа-Банк», работают над тем, чтобы выявлять и предотвращать такие схемы. Они разрабатывают системы дроп-мониторинга, предназначенные для обнаружения подозрительных транзакций и блокировки счетов дропов. При этом каждая компания старается разработать наиболее продуктивные методы, позволяющие эффективно выявлять и верифицировать такие аккаунты. Ключевая задача банка – отслеживать деятельность клиентов, предотвращать проникновение мошеннических схем в финансовую сферу и контролировать их операции. Также банки должны осуществлять обмен данных с уполномоченными органами. Но в наши дни требования к работе банков изменились, и теперь необходимо учитывать интересы клиентов, помимо соблюдения требований и законов.

Банки активно разрабатывают системы дроп-мониторинга и иные инструменты для выявления операций с дропами. Одним из ярких примеров является система «Т-Банка». Они создали механизм, основанный на анализе большого количества операций клиентов, среди которых были и те, кто пользовался картой с целью участия в мошеннических схемах. После качественного анализа они также выявили основные признаки, демонстрирующие, что клиент, вероятно, оформил карту, чтобы в дальнейшем передать или продать её третьим лицам. Далее следует проверка на совпадения с полученными признаками, и при необходимости проводят расследование или блокируют счет. Проверка осуществляется путем сравнения полученных признаков с поведением клиента в режиме реального времени с помощью искусственного интеллекта, который формирует реакцию на возможное совпадение. Также «Т-Банк» на регулярной основе осуществляет выявляет и блокирует группы и сообщества, которые мошенники создают для распространения методов обхода банковских защитных систем. Вследствие работы алгоритмов удалось снизить количество подставных лиц в 2 раза в течение года. Таким образом, «Т-Банк» показывает хорошие результаты по выявлению и сокращению подозрительных операций.

В свое время Альфа-Банк создал антифрод-систему, которая моментально проверяет каждую транзакцию, выявляет признаки подозрительных операции и автоматически блокирует подозрительные счета до момента вывода средств. Особенностью системы является возможность возврата похищенных средств непосредственно со счетов злоумышленников. [9] Данное решение демонстрирует комплексный подход к противодействию финансовому мошенничеству, сочетая оперативное выявление подозрительных операций с механизмом восстановления клиентских средств. Система интегрирована в банковские процессы и работает автоматически, минимизируя человеческий фактор в принятии решений о блокировке.

В отличие от Т-Банка и Альфа-Банка, Газпромбанк применяет более гибкий подход к обработке подозрительных операций. Банк не блокирует автоматически счета клиентов, помеченные как "потенциальные дропы". Вместо мгновенной блокировки специалисты Газпромбанка проводят детальный анализ каждого подозрительного счета и его операций. Это позволяет выявлять характерные признаки дроппинга, которые в дальнейшем используются для маркировки потенциально рискованных счетов. Такой подход дает возможность более точно идентифицировать подозрительную активность, минимизируя ложные срабатывания. [4]

В условиях постоянного усложнения мошеннических схем российские банки продолжают развивать системы противодействия, внедряя инновационные решения. Примером такой работы выступает ВТБ, где специалисты разработали механизм выявления новых видов финансовых преступлений. Банком была обнаружена схема, заключающаяся в том, злоумышленники стали брать карты дропов в аренду вместо покупки, перекладывая ответственность на их владельцев. Такие карты используются как "безопасные счета" для перевода похищенных средств. Для противодействия этой схеме ВТБ разработал систему дроп-мониторинга, способную выявлять подозрительную активность еще до поступления денег на счета. В 2023 году система доказала свою эффективность - было заблокировано более 1 млрд рублей на счетах дропов, включая как клиентов ВТБ, так и других банков. [23]

Сбербанк, будучи одним из ведущих банков с обширной клиентской базой, предпринимает активные меры по борьбе с дропперами. Ещё в 2022 году банк запустил специальную программу по их обнаружению, и за это время количество таких злоумышленников, использующих его инструменты, уменьшилось в 10–12 раз. [5][6] Однако из-за масштабов операций Сбер столкнулся с технической сложностью: существующие системы управления базами данных (СУБД) не справлялись с обработкой огромного количества транзакций, что замедляло анализ подозрительных операций. Чтобы решить эту проблему, банк разработал собственную СУБД, которая значительно ускорила процесс проверки транзакций. Это позволило оперативно выявлять подозрительные действия и моментально принимать решения по блокировке. Эффективность всей системы подтвердилась, когда Сбер в тестовом режиме заблокировал несколько тысяч карт дропперов — ни одной жалобы от клиентов не поступило. Это означает, что алгоритмы работают точно, и блокировки затрагивают только мошенников [20].

Центральный банк совместно с Росфинмониторингом приступили к разработке единой информационной платформы, которая будет собирать данные о дропперах и предоставлять соответствующие сведения всем кредитным организациям. По информации, предоставленной Центральным банком, в настоящее время данные о таких клиентах передаются только в

те кредитные организации, в которых у них открыты счета. Однако, учитывая, что злоумышленники открывают счета в различных финансовых учреждениях, возникла необходимость в создании централизованной системы. Данное решение позволит кредитным организациям своевременно принимать защитные меры в отношении указанных лиц. При этом следует отметить, что конкретные критерии включения в реестр пока окончательно не определены. На текущий момент база формируется на основании запросов правоохранительных органов и содержит паспортные данные, ИНН и реквизиты счетов. В перспективе планируется расширить перечень идентификационных признаков, включив в него номера банковских карт и расчетных счетов. [25]

Из-за большого числа участников схемы возникает сложность в выявлении связей между ними. Банк России работает над улучшением системы анализа подозрительных операций, чтобы точнее определять уровни вовлеченности. Особое внимание уделяется дропперам «второго уровня», основным субъектам мошеннических операций, на счета которых поступают средства, полученные незаконным путём от жертв. Также существуют дропперы первого уровня, к ним относятся те, кто получает средства напрямую от своих жертв. Затем эти средства либо обналичиваются, либо переводятся дропперам более высокого уровня, что затрудняет отслеживание цепочки. [8] По информации Центрального банка, в декабре 2024 года в дропперскую деятельность было вовлечено около 700 тысяч человек. [3] По оценкам МВД, эта цифра составляет более 2 миллионов человек. За девять месяцев прошлого года объём незаконного обналичивания через карты физических лиц составил 39 миллиардов рублей. [7]

Росфинмониторинг играет ключевую роль в противодействии дропперам. Согласно данным ведомства, только за 2024 год объём подозрительных операций с участием дропперов составил десятки миллиардов рублей, а вовлечение несовершеннолетних в такие схемы выросло в шесть раз. Для борьбы с этим явлением Росфинмониторинг использует комплекс мер. С 1 июня 2024 года ведомство получило инструмент воздействия в виде приостановки до десяти дней операции с денежными средствами в случае обнаружения признаков их использования с целью легализации преступных доходов. Эта мера позволит оперативно блокировать подозрительные транзакции. «Массовой блокировки не будет — решения будут взвешенными», — подчеркивает Олег Крылов, первый заместитель директора Росфинмониторинга. [10] Особое внимание уделяется противодействию деятельности организаторов преступных схем. Как заявил статс-секретарь — заместитель директора Росфинмониторинга Герман Негляд: «Речь о том, чтобы выявить в первую очередь организаторов преступной сети, их финансовые связи и заблокировать соответствующие активы». [7] Ведомство также поддерживает

ужесточение уголовной ответственности для дропперов, особенно тех, кто осознанно участвует в мошеннических операциях. Росфинмониторинг усиливает меры, направленные на противодействие иностранным дропперам, чья активность выросла в десять раз, а также на пресечение схем с использованием доверенностей. Взаимодействие с банками, правоохранительными органами и зарубежными финансовыми разведками позволяет эффективнее выявлять и пресекать незаконные операции. Эти меры создают основу для более эффективного противодействия дропперству, формируя правовые предпосылки для дальнейшего ужесточения ответственности за организацию и участие в подобных преступных схемах.

На фоне усиления мер по борьбе с деятельностью дропов, ключевой задачей остается установление уголовной ответственности для таких субъектов за осуществляемую ими противоправную деятельность. На данный момент отсутствует статья, которая могла бы в полной мере определить ответственность за такое преступление, так как зачастую, подставные лица не осознают, с какой целью будет использоваться их платежное средство. В связи с этим на практике применяются статьи 159 УК РФ или 159.3 [15] при условии, если будет доказано, что дроп знал о преступном использовании своей карты. В случаях, когда дроп стал жертвой мошеннической схемы по незнанию, но действовал из корыстных побуждений, может применяться статья 187 УК РФ. [17][18] Также если дроп участвовал в схеме отмыwania денежных средств, то к нему может быть применена статья 174 УК РФ [13], однако сложность заключается в том, что необходимо доказать, что дроп понимал преступное происхождение средств. В более серьезных случаях, при организации целой сети дроппов, к организаторам может применяться статья 210 УК РФ. [16] В исключительных ситуациях, когда средства направлены через дропа на финансирование терроризма, возможно применение статьи 205.1 УК РФ. [11] В связи с тем, что большинство дропов не осознают преступного характера своих действий, их сложно привлечь к строгой ответственности. В следствие этого в Госдуму внесен законопроект, предусматривающий ответственность за передачу из корыстной заинтересованности электронного средства платежа или доступа к нему для осуществления неправомерных действий. За такие действия предполагается наказание вплоть до шести лет лишения свободы со штрафом от трехсот тысяч рублей до одного миллиона рублей. [12][19] Эти изменения позволят более эффективно привлекать к ответственности лиц, сознательно участвующих в мошеннических схемах, даже если они не знали всех деталей преступного замысла.

Принцип, согласно которому незнание закона не освобождает от ответственности, особенно важен в финансовой сфере. Помимо мер безопасности, которые применяют банки, важно повышать правовую и

финансовую грамотность населения, особенно подростков и студентов. Для этого необходимо расширить программу образовательных программ для учащихся, а также проводить разъяснительную работу с родителями, которые несут ответственность за действия своих несовершеннолетних детей. Особое внимание следует уделить социальной рекламе, которая должна воздействовать на две ключевые группы: тех, кто осознаёт противоправность своих действий, но идёт на риск ради быстрой прибыли, и тех, кто становится жертвой методов социальной инженерии. Подобные меры позволяют косвенно снизить активность дропперов - посредников в незаконных финансовых операциях. Важным инструментом работы с молодёжью является Международная Олимпиада по финансовой безопасности, одним из организаторов которой выступает Росфинмониторинг. Это мероприятие направлено на формирование современного финансового мышления и новых подходов деятельности, а также на развитие ключевых компетенций в сфере экономической безопасности. Она способствует профессиональной ориентации школьников и студентов, помогая подготовить квалифицированные кадры для системы финансовой безопасности. Кроме того, олимпиада создает основу для формирования единого образовательного, научно-исследовательского и будущего информационного пространства, что позволит системно укреплять знания и практические навыки в области экономической и финансовой безопасности. Также следует отметить, что проблема часто рассматривается исключительно в правовом аспекте, тогда как угрозы экономической безопасности имеют гораздо более широкий спектр. Если оставить ситуацию без контроля, это может привести к дестабилизации экономического сектора и подрыву национальной безопасности. Поэтому, помимо совершенствования законодательной базы, необходимо развивать систему контроля и модернизировать технические средства мониторинга. Особую роль играет международное сотрудничество, которое включает активное участие в глобальных системах финансового контроля, транснациональное отслеживание денежных потоков и реализацию международных конвенций. Ключевыми аспектами является оперативная правовая помощь, механизмы ареста преступных активов на основе иностранных данных, экстрадиция преступников и отказ в убежище. [24] Только комплексный подход, сочетающий образовательные, законодательные и технические меры при активном международном воздействии, позволит эффективно противостоять финансовым преступлениям и обеспечить экономическую безопасность страны.

Таким образом, проблема дроппов требует скоординированных действий всех участников финансовой системы. Ведущие российские банки активно внедряют современные системы мониторинга, позволяющие выявлять и блокировать подозрительные операции. Лишь объединенная

стратегия, включающая в себя технологические, правовые и образовательные меры, позволит эффективно противостоять дропперству, сохраняя баланс между безопасностью и доступностью банковских услуг. Решение этой задачи возможно при согласованной работе всех заинтересованных сторон.

#### Список использованных источников:

1. Официальный сайт МВД России. Управление МВД России по липецкой области//Подросток и дроперство [Электронный ресурс]. URL: <https://48.mvd.pf/document/40004687> (дата обращения: 15.04.2025).

2. Дзен. Статья о методах противодействия дропперам [Электронный ресурс]. URL: <https://dzen.ru/a/Z-9ZpluQXHe1MKhX> (дата обращения: 15.04.2025).

3. Ведомости. Банки заблокировали более 700 000 счетов дропперов в 2024 году. [Электронный ресурс]. URL: <https://www.vedomosti.ru/finance/news/2025/04/10/1103593-banki-zablokirovali-bolee> (дата обращения: 15.04.2025).

4. Хабрахабр. Новости о финансовой безопасности [Электронный ресурс]. URL: <https://habr.com/ru/news/810729/> (дата обращения: 10.04.2025).

5. Деловой квартал. Новости банковского сектора [Электронный ресурс]. URL: <https://www.dk.ru/news/237198415> (дата обращения: ).

6. Frank Media. Финансовый мониторинг [Электронный ресурс]. URL: <https://frankmedia.ru/162977> (дата обращения: 10.04.2025).

7. РБК. Финансы: новости [Электронный ресурс]. URL: <https://www.rbc.ru/finances/27/03/2025/67e3cb2f9a7947e06bc1210b> (дата обращения: 21.04.2025).

8. РБК. Финансы: последние новости [Электронный ресурс]. URL: <https://www.rbc.ru/finances/02/04/2025/67ed2b049a794723ea17b2b7> (дата обращения: 16.04.2025).

9. Альфа-Банк. Противодействие мошенничеству [Электронный ресурс]. URL: <https://alfabank.ru/news/t/release/alfa-bank-otmechen-v-sfere-protivodeistviya-moshennichestvu/> (дата обращения: 12.04.2025).

10. Российская газета. Статья "Drop-stop" [Электронный ресурс]. URL: <https://rg.ru/2025/04/28/drop-stop.html> (дата обращения: 04.05.2025).

11. АКБ. Об ответственности за участие в дропперстве [Электронный ресурс]. URL: <https://www.ankb.ru/ob-otvetsvennosti-za-uchastie-v-dropperstve/> (дата обращения: 06.05.2025).

12. КонсультантПлюс. Законодательные акты [Электронный ресурс]. URL: <https://www.consultant.ru/law/hotdocs/89146.html> (дата обращения: 06.05.2025).

13. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025), (ст. 174)

[Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/4dfcfc8807c829f92212ce92efe818c4a707a3ca/](https://www.consultant.ru/document/cons_doc_LAW_10699/4dfcfc8807c829f92212ce92efe818c4a707a3ca/) (дата обращения: 06.05.2025).

14. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025), (ст. 174.1) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/c10431f048782e9c62eccc5a90fc102ac7d0e812/](https://www.consultant.ru/document/cons_doc_LAW_10699/c10431f048782e9c62eccc5a90fc102ac7d0e812/) (дата обращения: 06.05.2025).

15. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025), (ст. 159.3) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/c193654ae5c3bd5b02d92ade18796cd8864ec353/](https://www.consultant.ru/document/cons_doc_LAW_10699/c193654ae5c3bd5b02d92ade18796cd8864ec353/) (дата обращения: 06.05.2025).

16. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025), (ст. 210) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/5649f81c02c8558e22ab26207b2834c0d047d6fb/](https://www.consultant.ru/document/cons_doc_LAW_10699/5649f81c02c8558e22ab26207b2834c0d047d6fb/) (дата обращения: 06.05.2025).

17. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025), (ст. 187) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/539a9a6196cae24f91d30781eced78e28b508617/](https://www.consultant.ru/document/cons_doc_LAW_10699/539a9a6196cae24f91d30781eced78e28b508617/) (дата обращения: 06.05.2025).

18. Адвокатская газета. Проблемы законодательной неопределенности [Электронный ресурс]. URL: <https://www.advgazeta.ru/mneniya/problemy-zakonodatelnoy-neopredelennosti/> (дата обращения: 06.05.2025).

19. Российская газета. Юристы прокомментировали инициативу об уголовных наказаниях для дропперов [Электронный ресурс]. URL: <https://rg.ru/2025/05/02/iuristy-prokommentirovali-iniciativu-ob-ugolovnyh-nakazaniiah-dlia-dropperov.html> (дата обращения: ).

20. РБК. Как осуществлять фрод-мониторинг в реальном времени [Электронный ресурс]. URL: <https://companies.rbc.ru/news/IQVJwKoTJQ/kak-osuschestvlyat-frod-monitoring-v-rezhime-realnogo-vremeni/> (дата обращения: 12.04.2025).

21. Сбербанк. Терминология: дроп [Электронный ресурс]. URL: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/drop> (дата обращения: 10.04.2025).

22. Журнал Уралсиб. Исследования [Электронный ресурс]. URL: <https://journal.uralsib.ru/hse/research/4> (дата обращения: 10.04.2025).

23. Anti-Malware. Новости кибербезопасности [Электронный ресурс]. URL: <https://www.anti-malware.ru/news/2024-08-21-121598/43971> (дата обращения: 12.04.2025).

24. SciLead. Международное сотрудничество в сфере противодействия [Электронный ресурс]. URL: <https://scilead.ru/article/3720-mezhdunarodnoe-sotrudnichestvo-v-sfere-protiv> (дата обращения: 10.05.2025).

25. Коммерсантъ. Банки начали массово блокировать счета дропперов [Электронный ресурс] // Коммерсантъ. – 2025. – URL: <https://www.kommersant.ru/doc/7403445> (дата обращения: 20.04.2025).