



SCS

SBER
CYBER
SECURITY

АНАЛИЗ СИСТЕМЫ ВЫВОДА ДЕНЕЖНЫХ СРЕДСТВ, ПОХИЩЕННЫХ У ГРАЖДАН РФ

Проблемы и меры



Оглавление

Введение	2
1. Дропы	3
2. Организация «бизнеса» по выводу украденных средств	4
3. Ретроспективный анализ проблемы и текущее состояние.....	14
4. Использование дропов в мошеннических схемах.....	19
5. Ответственность за дроперство	25
6. Опыт Сбера по борьбе с дропами	26
7. Меры противодействия дропам на уровне государства	28
Выводы	29

Введение

Количество пользователей банковских карт с каждым годом растет. Мошенники осознали, какие огромные возможности открыты для противозаконного обогащения с помощью современных технологий. Ранее мы раскрыли детали работы одного из крупнейших мошеннических call-центров на территории Украины в г. Бердянск¹. В опубликованном отчете показаны основные этапы телефонного обмана – организация массовых мошеннических звонков, вывод украденных средств, поиск баз с персональными данными для обзвона и т.д. Далее в отдельном расследовании мы раскрыли детали работы SIP-провайдеров, через которых осуществляются звонки гражданам РФ² из мошеннических call-центров. В настоящем отчете рассмотрен этап мошеннической схемы, связанный с выводом похищенных средств через т.н. «дропов»³ и проблемы противодействия ему, в том числе, с учетом опыта Сбера по борьбе с кибермошенничеством.

За последние несколько лет на территории России наблюдается рост числа дистанционных преступлений – телефонного мошенничества, которое реализуется методами социальной инженерии. По данным Банка России, за девять месяцев 2022 года общая сумма денежных средств, похищенных мошенниками у физлиц – клиентов банков, составила свыше 10 млрд рублей. Это более чем на 10% превышает аналогичный показатель предыдущего года.

При этом реальная картина финансовых потерь превышает статистику Банка России в разы – в соответствии со статистикой МВД России и данными экспертов в области кибербезопасности объем мошенничества в РФ оценивается от 55 до 165 млрд рублей в год⁴. За 10 месяцев 2022 г. ущерб гражданам только от дистанционного мошенничества составил более 73 млрд рублей.⁵ По данным Сбера, на социальную инженерию приходится 90% всех финансовых преступлений, из которых 94% — это телефонное мошенничество.

Ранее эксперты оценивали количество звонков из мошеннических call-центров до 100 тыс. в сутки. Однако в 2022 г. Сбер завершил проект по подключению антифрод- систем основных операторов сотовой связи к своей системе транзакционноантифрода, что позволило увидеть всю картину по мошенническим звонкам. Так, в 2022 году мошенники сделали 1,5 млрд попыток позвонить клиентам банков с целью похитить денежные средства.

По экспертной оценке Сбера, на долю Украины приходится до 90% всех call-центров, работающих против граждан РФ, остальные располагаются на территории России и стран СНГ. Общий объем похищенных украинскими call-центрами средств достигал 75 млрд руб. в 2020 году.

В сложившейся геополитической обстановке правоохранительная система нашей страны бессильна в отношении организаторов мошеннических call-центров, т.к. они находятся вне юрисдикции российской правоохранительной системы, а сотрудничество с правоохранительной системой Украины свернуто. Однако обналичивание и вывод

¹ <https://promo.sber.ru/kibrary/assets/berdyansk.pdf>

² https://promo.sber.ru/kibrary/assets/sip_services.pdf

³ Под дропом подразумевается подставное лицо, участвующее в схеме мошенничества, использующее свои либо предоставленные ему карты/счета для обналичивания или транзита похищенных денежных средств. Существует еще термин «дроппер», но в этой статье мы будем использовать дроп.

⁴ <https://www.kommersant.ru/doc/5218254>

⁵ По данным МВД России

похищенных денежных средств происходит через граждан Российской Федерации – «дропов», которых умышленно используют организаторы мошеннических call-центров в преступных целях. Поэтому, не имея возможность пресечь сами атаки телефонных мошенников, системно противодействуя использованию банковской системы Российской Федерации для вывода и обналичивания похищенных денежных средств через дропов или дроп-сервисы, возможно нарушить логистические цепочки мошеннических схем.

По мнению Сбера, это существенно осложнит реализацию мошенничества и позволит снизить объемы потерь граждан Российской Федерации.

1. Дропы

Опыт расследований киберпреступлений Сбером позволяет классифицировать дропов следующим образом:

По типу осведомленности о своей противоправной деятельности:

- **«Неразводные»** – осведомленные о криминальном характере своей деятельности, т.е. действующие умышленно и добровольно. Как правило, разводные дропы самостоятельно ищут организаторов преступных схем, чтобы передать им свои банковские продукты (чаще всего банковские карты). Данная категория дропов является более распространенной и имеет свою специфику. Как правило, данные лица испытывают финансовые ограничения, не имеют стабильной работы и доходов, постоянного места жительства, имеют высокую закредитованность, а также алкогольную или наркотическую зависимость.
- **«Разводные»** – вовлеченные в преступный бизнес неосознанно и используемые организаторами преступной схемы под различными легендами. Такие дропы не понимают, что участвуют в мошеннической схеме. Наиболее распространенный способ привлечения этих граждан в криминальный бизнес – через фиктивное трудоустройство. Например, на сайтах поиска работы размещаются объявления о наборе сотрудников, при оформлении «сотруднику» предлагается выпустить банковскую карту для зачисления зарплаты, подключить к ней телефон «работодателя» и передать карту или реквизиты «бухгалтеру» для оформления. В результате банковская карта со всеми реквизитами доступа к ней оказывается у преступных организаторов схемы.

По типу использования банковских продуктов:

- **«Обнальщики»** – дропы, самостоятельно обналичивающие зачисленные похищенные денежные средства на свои банковские карты или счета в банкоматах или офисах банков. За данную операцию обнальщики получают заранее оговоренное вознаграждение (от 5 до 10%) и передают оставшиеся средства далее по цепочке организатору. В подавляющем большинстве случаев это разводные дропы. Как правило, данный тип дропов несет максимальные риски задержания сотрудниками полиции.
- **«Транзитники»** – дропы-посредники, принимающие перевод похищенных денежных средств на свои карты или счета и переводящие их дальше по цепочке на указанные организатором мошеннической схемы банковские реквизиты. Это делается для сокрытия следов преступления и затруднения

работы правоохранительных органов, с целью успеть обналичить похищенное до блокировки счетов.

- **«Заливщики»** – дропы, получающие от дроповодаб или от других дропов наличные средства и вносящие их на свои карты. Далее средства переводятся по цепочке «транзитному» дропу. Данная манипуляция применяется для создания дополнительных этапов в схеме вывода средств, чтобы максимально затруднить службам безопасности банков и полиции поиск криминальных денежных потоков для их блокировки и последующего возврата.

Ряд преступных групп используют дропов-универсалов, способных выполнять любую задачу в зависимости от конкретной ситуации или команды организатора схемы обналичивания, т.н. «дроповода» (см. рисунок 1).



Рисунок 1. Схема вывода похищенных средств с использованием дропов-универсалов

К примеру, мошенникам необходимо обналичить крупную сумму средств, украденную у жертвы⁷. Для этого клоузеры, обрабатывающие жертву на второй линии call-центра, договариваются с дроп-сервисом о необходимости особого процесса вывода: часть дропов снимает похищенные денежные средства в банкоматах и передает их «дроповоду». Тот организует три дополнительные группы: первая покупает криптовалюту, вторая вносит деньги на т.н. «чистый пластик» (специально изготовленные и ранее не использовавшиеся банковские карты), а третья перевозит крупные суммы наличных в другой регион страны, где осуществляется взнос денежных средств на «чистый пластик» или покупка криптовалюты.

2. Организация «бизнеса» по выводу украденных средств

Типовая схема организации криминального бизнеса достаточно проста – основной организатор дроп-сервиса размещает объявление на одной из специализированных площадок в Darknet (теневых площадках) и привлекает дроповодов, которые

⁶ Подставное лицо, которое осуществляет руководство дропами. Чаще всего является частью более масштабного дроп-сервиса и координирует работу в локальном регионе.

⁷ Рекорд по размеру украденных средств у одной жертвы через телефонное мошенничество – 400 млн. рублей в 2020г., в 2022г. максимальный размер одного хищения 150 млн. рублей.

будут отвечать за подбор, инструктаж и контроль деятельности дропов в отдельно взятом регионе (см. рисунок 2).

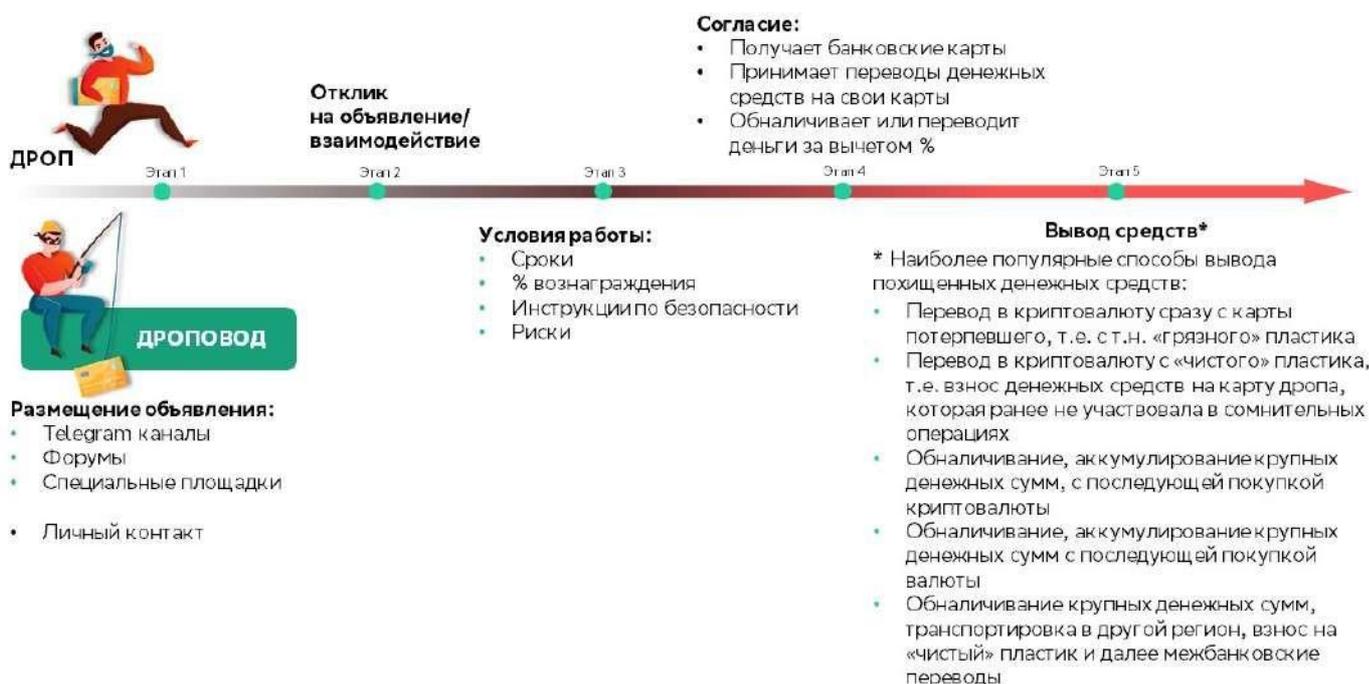


Рисунок 2. Типовая схема привлечения дропов в криминальный бизнес

Для размещения таких объявлений на профильных форумах созданы специализированные разделы, которые обычно называются «Работа/Вакансии» (см. рисунок 3).

Всего мы выделяем около 10 основных теневых площадок для организации дроп-сервиса или поиска такого для своего криминального бизнеса. По понятным причинам данный список нами не публикуется, но вся информация передана правоохранительным органам.

Можно выделить следующие типовые условия при найме дроповодов на данных теневых площадках:

- Наличие у дроповода-кандидата гарантийного депозита в сумме в среднем от 50 тыс. рублей, что говорит о серьезности намерений и является своеобразной страховкой. Есть примеры очень больших сумм депозитов.
- Проведение сделок только через гаранта площадки, т.е. своеобразного третейского судью.
- Желание работать, ответственность, «порядочность».
- Крайне приветствуется наличие собственной и уже действующей сети дропов.

Цвет вакансии: СЕРЫЙ

Временные рамки вакансии: ПОСТОЯННАЯ

География вакансии: ВСЯ РФ

Описание вакансии: Требуется в команду **дроповод**, на постоянную работу, с ручными подконтрольными дропами, с возможностью изготавливать дебет разных банков в хорошем количестве на постоянной основе, с опытом работы и пониманием того, что он делает. Дети и дилетанты - проходите мимо, пожалуйста.

Требования:

- 1) Добросовестность, пунктуальность, ответственность - базовые качества адекватного человека для начала работы
- 2) Стабильный онлайн
- 3) Ручные дропы (именно ручные и подконтрольные дропы, посредники - мимо)
- 4) Символический залог, дабы оттолкнуть бездельников-раздолбаев, халявщиков, и наркоманов, желающих кинуть за 50-100к.

График работы: ежедневно

Оплата: оплата сдельная

Контакты:

- Личные сообщения форума

Более подробно условия и детали работы обсудим с адекватным кандидатом лично.

Рисунок 3. Пример типового объявления о найме дроповодов на теневом форуме

machete1
Серьезный сервис



МЕСТНЫЙ

Регистрация: 06.09.2022
Сообщений: 77
Депозит:
3000000 RUR / 0
GRUSD
Сделок через
ГАРАНТА: 0

Рисунок 4. Пример гаранта с депозитом 3 млн рублей

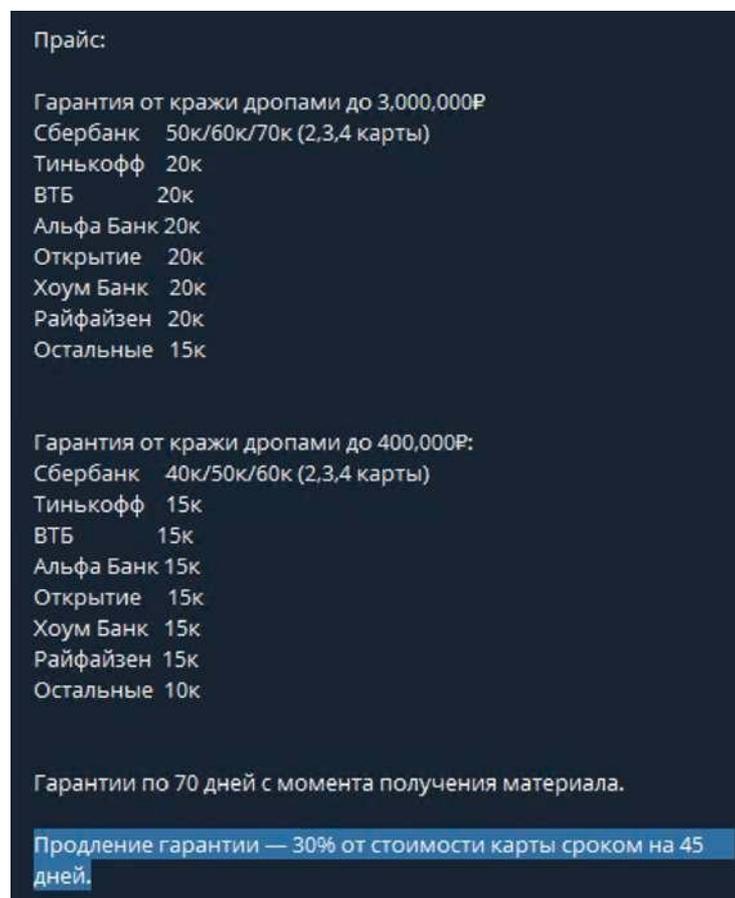


Рисунок 5. Пример гарантии от кражи денежных средств дропами

Зачастую объявления также содержат банальные требования, такие как регион работы и график (см. рисунок 6).

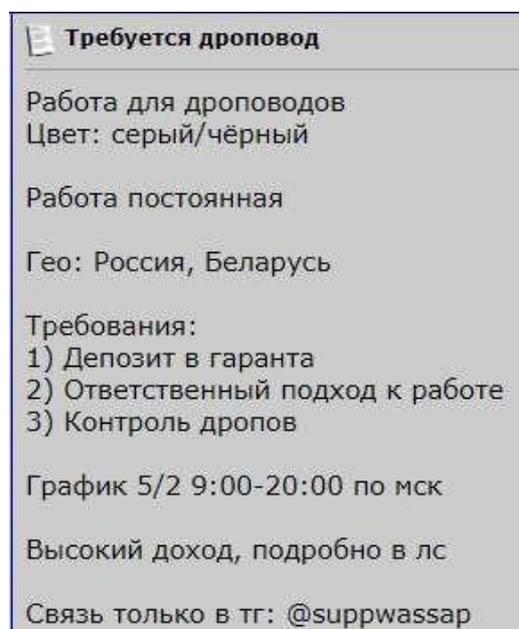


Рисунок 6. Пример типового объявления с деталями о найме дроповодов на теневом форуме

В свою очередь, дроповоды размещают объявления о поиске дропов в свою команду через такие же площадки, социальные сети, личные контакты и пр.

Количество публикуемых объявлений огромно, на скриншоте ниже – лишь малая часть объявлений одной теневой площадки (см. рисунок 7). Всего, по нашим оценкам, количество таких сервисов может достигать в России порядка 3 тыс. шт.

Темы раздела : ПРЕДЛАГАЮ работу (Вакансии)		Опции раздела	Искать в этом разделе
Тема / Автор	Рейтинг	Последнее сообщение	Отв. / Просмотров
Важно: EURO KASSA - Набор нальщиков Россия Заработок от 500 000Р в день! EuroKassa	★★★★★	Сегодня 16:56 от Egoris7	5 / 16,483
Важно: [Черная][Постоянная][Мир] МАСШЕТЕ – набираем нальщиков в команду. До 35% (1 2) machete1	★★★★★	Сегодня 12:40 от Offelia	16 / 2,040
Важно: Нужны нальщики СИМ РФ Obnal Express		https://i.ibb.co/qMtw0Xd/300.png Цвет вакансии: ЧЕРНЫЙ Временные рамки вакансии: ПОСТОЯННАЯ География вакансии: ВСЬ МИР, ЛЮБАЯ СТРАНА	4 / 1,033
Важно: Чёрная Постоянная РФ Ищу дроповодов Obnal Express			3 / 1,360
Важно: [Приму] ИНКАССАТОР, ДРОПОВОД. Нет опыта? Обучим! (1 2 3) LACOSTE_DM		Вчера 14:03 от Offelia	23 / 3,044
Важно: [Приму] Нальщиков Физ Сим РФ (1 2) Vin Diesel		21.11.2022 09:12 от GromnyyGlaz	12 / 4,249
Важно: Белая/постоянная/удаленка Englishman1		18.11.2022 15:01 от Offelia	1 / 307
Важно: Менеджеры по продажам, Серая/Постоянная/Удаленка (1 2) Englishman1		17.11.2022 03:56 от Mozgerse	12 / 1,764
Важно: [Приму] РАБОТА МЕНЕДЖЕРОМ для Девушек! ЗП от 60000р в месяц StoreUA		15.11.2022 17:36 от Offelia	2 / 627
Важно: [Черная][Постоянная][Удаленная] Менеджер по продажам (строительные материалы) Iambada13		02.11.2022 12:52 от kadehal	2 / 2,787
Важно: [Приму] СРОЧНО СОТРУДНИКОВ ВСЕХ СОТОВЫХ ОПЕРАТОРОВ!!! (1 2) CarloGambino\$\$\$		25.10.2022 20:12 от koleso556	18 / 4,953
Важно: Украине! Ищу кураторов колл центров. Creader		18.10.2022 11:22 от Juchka	2 / 2,935
Важно: [Приму] Нальщиков по РФ (1 2 3) Mr. Parker		30.09.2022 11:55 от Mr. Parker	20 / 6,843
Важно: [СЕРЯЯ][ПОСТОЯННАЯ][РОССИЯ]Сотрудник контакта/связного/мегафона (от 10000руб.) (1 2) john2013money		26.09.2022 09:47 от mento1337	11 / 5,329
Важно: [Приму] SIM QIWI Набор нальщиков по РФ. Mr. Parker		28.08.2022 17:11 от bandband	1 / 1,578
Важно: 👀👀👀 DaVinci. Требуются работники всех структур 👀👀👀 (1 2 3 ... Последняя страница) DaVinci	★★★★★	17.07.2022 20:47 от JqUicLPJwaK	38 / 26,170
Важно: [СЕРЯЯ][ПРОЕКТНАЯ][УДАЛЕННАЯ]Набор и обучение - Криптовбиржа - TheProject (1 2) theproject		19.06.2022 01:57 от theproject	10 / 3,050

Рисунок 7. Объявления о найме дропов и дроповодов на теневом форуме

Неразводные дропы, как правило, привлекаются на теневых форумах. Условия из привлечения стандартные: локация работы и процент от сделок. Подразумевается, что люди, которые посещают теневые ресурсы в поисках «работы», уже осведомлены о противоправности своей деятельности, каких-то специфических требований к ним не предъявляется (см. рисунок 8).

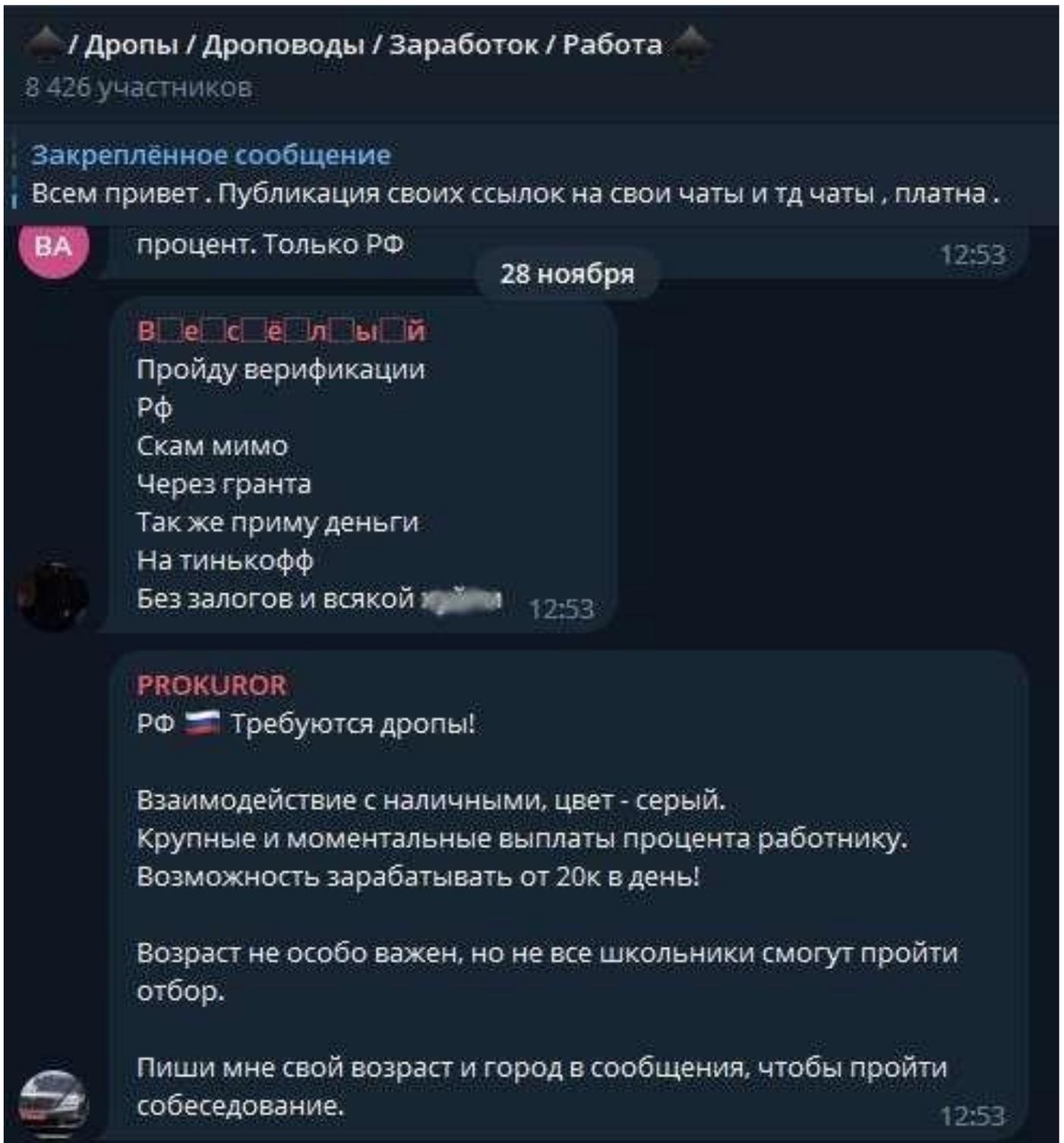


Рисунок 8. Пример объявления о найме дропов в телеграм-канале

К разводным дропам применяются различные схемы обмана. На рисунке 9 приведен пример переписки о поиске дроповода для привлечения в дроп-сервис разводных дропов.

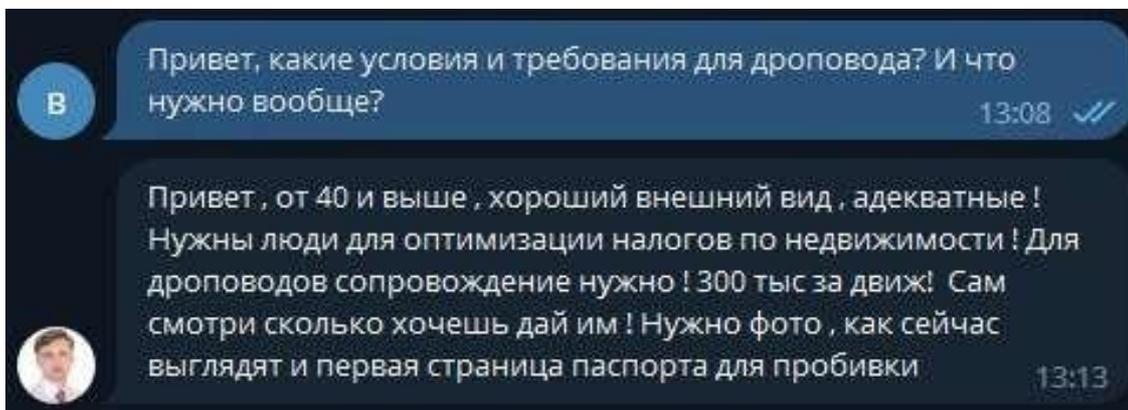


Рисунок 9. Пример переписки о найме дропов в телеграмм. Целевая аудитория – разводные дропы

После того, как команда собрана, дроп-сервис готов к выходу «на рынок» и предложению своих услуг заказчикам мошеннических схем.

Многие сервисы по обналичиванию денежных средств предлагают пакетные услуги, когда клиентам сервиса продаются дебетовые карты дропов вместе с пакетом документов (см. рисунок 10).

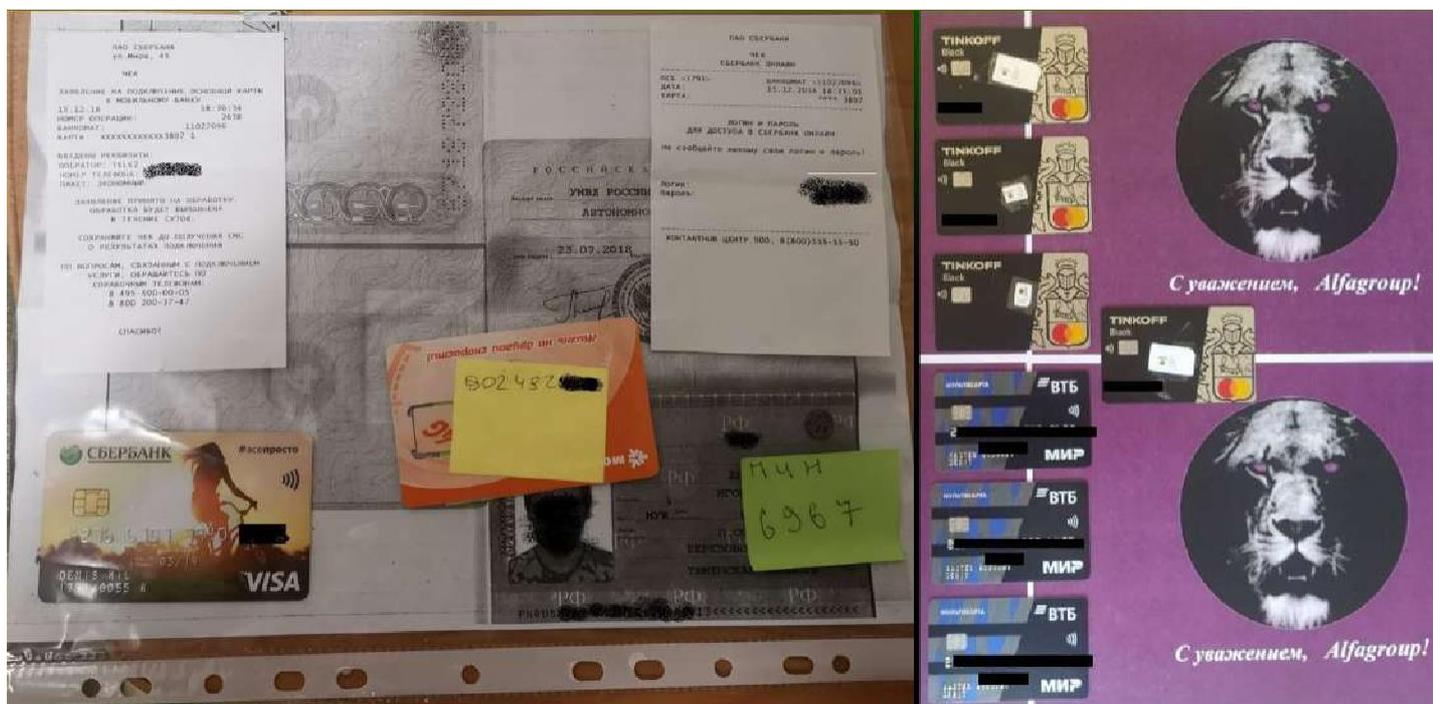


Рисунок 10. Предлагаемые к продаже карты дропов с комплектом документов

Цены на данные услуги можно продемонстрировать на примере карт Сбера. Так, в марте 2021 г. на черном рынке дроп-карт классические карты Сбера предлагались по цене 9 тыс. руб. за штуку, золотые – от 14 тыс., а премиальные – от 18 тыс. руб. В ноябре 2022 г. за классические карты стали просить от 12 тыс. руб., за золотые – от 40 тыс. руб., а стоимость премиальных доходит до 100 тыс. руб. Такой рост обусловлен мероприятиями, проводимыми банком по снижению количества дропов среди своих клиентов. Об этом будет рассказано чуть позже.

За 11 месяцев 2022 года только на одном из самых популярных теневого форумов было создано более 400 объявлений, связанных с продажей и покупкой услуг дропов.

Ассортимент предлагаемых сервисов ничем не ограничивается, в наличии всегда есть карты популярных банков. Но высокая конкуренция среди продавцов вынуждает их вкладываться в рекламу своих услуг и вводить дополнительные услуги по сохранности денежных средств клиентов, к примеру, от кражи их самими дропами. Стоимость рекламы на теневых форумах начинается от 400 тыс. рублей, а страхование от краж средств дропом доходит до 50% от стоимости карт. И это арендная плата, а не разовый платеж.

В целом в дроп-сервисах наибольшей популярностью пользуются банки, которые работают без отделений, т.н. цифровые. Они более лояльны к клиенту и позволяют решить все вопросы дистанционно. Исключение составляет Сбер из-за его универсальности, многообразия продуктов и масштабов. На рисунке 11 представлен своеобразный рейтинг «дроповости» банков, и на стоимость карты прежде всего влияет сложность её получения.

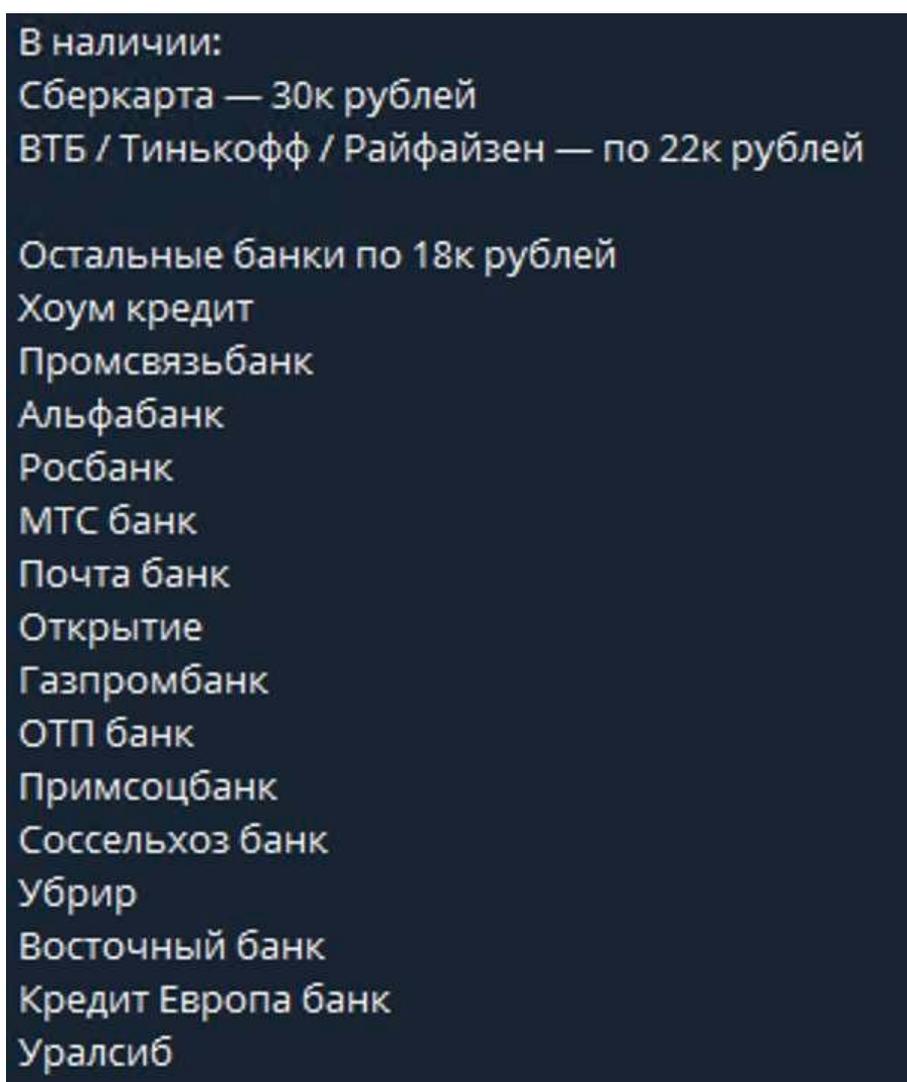


Рисунок 11. Приблизительный рейтинг «дроповости» банков

Существует еще такая услуга, как помощь в выводе средств при блокировке денежных средств банком по 115-ФЗ⁸. По понятным причинам мы не раскрываем подробностей, но и здесь стоимость варьируется от 20 до 30% суммы и при этом никто не дает гарантий. (см. рисунки 12 и 13)

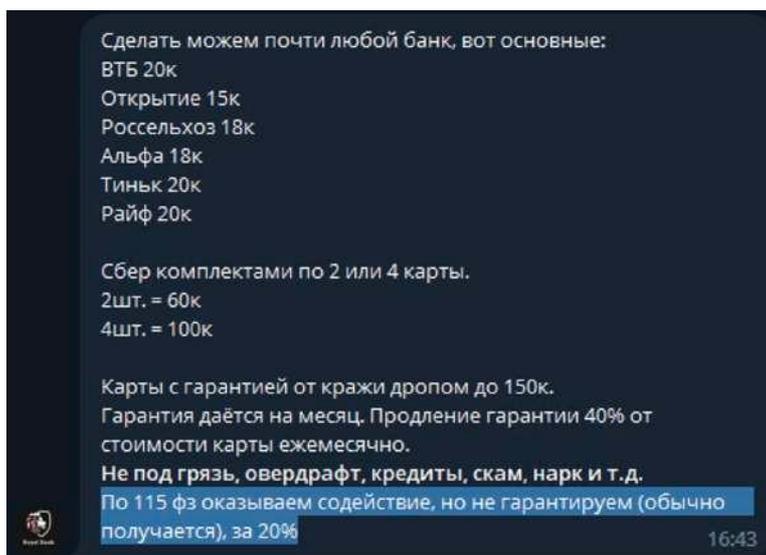


Рисунок 12. Пример условий для помощи в разблокировке средств по 115-ФЗ

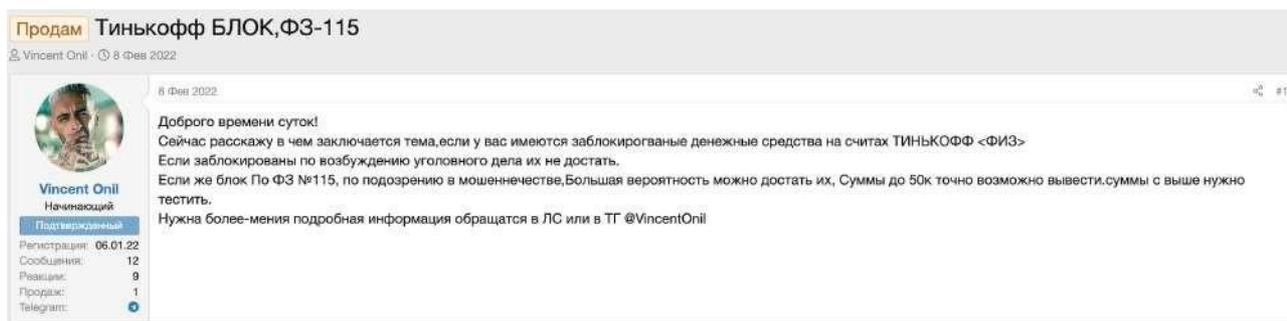


Рисунок 13. Пример объявлений в разблокировке средств по 115-ФЗ

Есть специфические предложения от некоторых продавцов: они предлагают оформить банковские карты, к примеру, на пациентов психоневрологического диспансера или на поддельные ID-карты граждан СНГ, но никаких гарантий при этом не дают.

Жизненный цикл дроп-карты от получения до блокировки может составлять от нескольких часов до двух лет. На продолжительность влияет множество факторов: тип дропа, качество антифрод-систем и процессов банков, скорость обращения потерпевшего, расторопность правоохранительных органов и т.д. Поэтому нередко до момента блокировки через дроп-карту мошенникам удается обналичить денежные средства, украденные у нескольких десятков граждан, а сумма обналиченных средств при этом превышает десятки миллионов рублей.

Отдельно выделяется сегмент т.н. «спящих» дропов: карты такого владельца долгое время не используются, при этом для легализации и обеления последующих операций владелец дроп-карты совершает периодические бытовые

⁸ Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ

платежи или вносит на карту определенную сумму и оформляет подписку на какие-либо сервисы с ежемесячным списание стоимости подписки.

По результатам исследования Сбербанка, дропами чаще становятся молодые мужчины, в основном, проживающие в городах федерального значения или в крупных региональных центрах Поволжья, Урала и Сибири. Более 85% дропов – это россияне, второе место занимают граждане Таджикистана и Узбекистана, а третье – жители Китая и Украины (см. рисунок 14).



Рисунок 14. Среднестатистический портрет дропа

После начала СВО владельцы дроп-сервисов начали активно набирать дропов, используя при этом элементы шантажа и подстраховки. При найме на «работу» у соискателя требуют фото паспорта в развернутом виде и часто лист бумаги с различными политическими лозунгами. Также часто организатор дроп-сервиса требует предоставить видеоролик, на котором будущий дроп не только представляется, но и выкрикивает политические лозунги (см. рисунок 15).

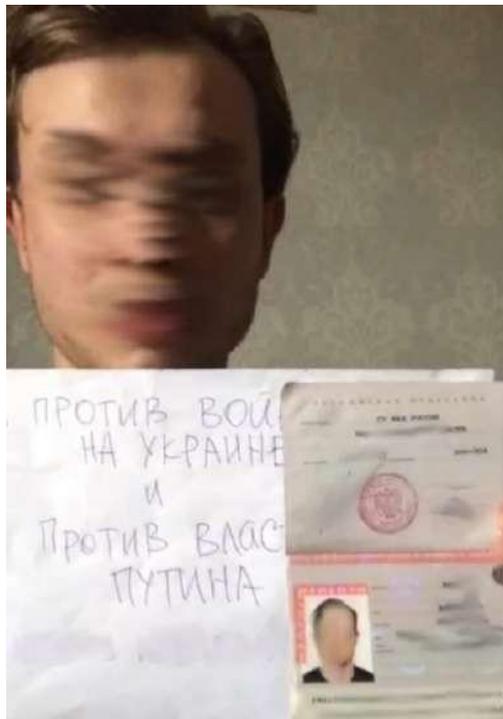


Рисунок 15. Пример скриншота из видео, публикуемого в телеграмм-канале

По данным МВД России, мошенники активно привлекали в качестве дропов не только россиян, но и вынужденных переселенцев с территории Украины.

3. Ретроспективный анализ проблемы и текущее состояние

Исторически в силу экономических условий, острого дефицита качественных западных товаров и откровенной незащищенности онлайн-платежей в западных платежных системах в нашей стране стал развиваться вещевой кардинг – особый вид мошенничества, связанный с покупками в иностранных интернет-магазинах товаров по скомпрометированным банковским картам зарубежных держателей. Эти товары оформлялись на иностранных посредников и пересылались ими в Россию. Тогда впервые появился термин «дроп». К середине 90-х годов, когда схема с вещевым кардингом⁹ стала неактуальной, в интернете стали появляться специализированные площадки («кардшопы»), где продавались данные похищенных или скомпрометированных банковских карт. Их можно было использовать для оплаты своих онлайн-покупок в интернет-магазинах или вывода денежных средств. Особое место на подобных сайтах представляли т.н. «дампы» банковских карт (от англ. «dump» – «свалка») – конфиденциальная информация, записанная на магнитной полосе банковской карты, необходимая для оплаты покупок в магазинах (фактически цифровая копия содержимого карты). Эту информацию злоумышленники получали, копируя данные реальных банковских

⁹ Вещевой кардинг — это способ обналичивания денег со взломанных банковских счетов. Кардер покупает товары, подарочные сертификаты, подписки и услуги, используя чужие банковские реквизиты. Для этого мошенникам нужны только номер карты, дата и трехзначный код (CVC).

карт с помощью специализированного оборудования, скрытно установленного на банкоматах в различных странах (т.н. «скиммеров»¹⁰). Далее дампы необходимо было записать на заготовки, по дизайну похожие на настоящие карты. После чего эти карты были готовы для использования в реальных магазинах. Задачи по обналачиванию средств с карт через магазины взяли на себя дропы, а организацию их работы – дроп-сервисы.

Впечатляюще выглядит история крупнейшей площадки кардеров – CarderPlanet¹¹, которая за 4 года существования прошла путь от небольшого форума единомышленников до маркетплейса с многотысячной аудиторией ежедневного посещения. Одного из организаторов данной площадки спецслужбам удалось задержать в аэропорту Ниццы только в 2017 году.¹²

За короткое время «кардшопы» выросли до размеров полноценных маркетплейсов с большим количеством продавцов. «Кардшопы» предлагали не только карты, но и персональные данные, аккаунты, поддельные документы, скомпрометированные технические учетные записи и др.

Новое развитие функция дропов получила в связи с активным развитием телефонного мошенничества на территории Украины. Тогда организованные преступные группы (далее ОПГ), размещающие инфраструктуру своего бизнеса в этой стране, стали для вывода средств активно привлекать дроп-сервисы, работающие в России. При такой схеме организации даже при ликвидации дроп-сервисов российскими правоохранительными органами невозможно будет дотянуться до украинских заказчиков.

Организация и участие в подобных преступных сообществах для дроп-сервисов – это высокодоходный криминальный бизнес. По сути, предлагается услуга полного цикла, где заказчик (юридическое лицо, мошеннический колл-центр, торговцы оружием, наркотиками и пр.) непосредственно не участвует в обналаживании и выводе денежных средств. Потенциальный доход от такой схемы мог составлять до 20 млрд рублей в 2022 г. Теневые площадки пестрят соответствующими баннерами на главных страницах (см. рисунки 16 и 17).

¹⁰ <https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D0%B4%D0%B8%D0%BD%D0%B3#%D0%A1%D0%BA%D0%B8%D0%BC%D0%BC%D0%B8%D0%BD%D0%B3>

¹¹ CarderPlanet — частное интернет-сообщество, члены которого занимались кардингом (carding — мошенничество с использованием украденных карт, банковских или телефонных, либо их номеров). Ведет свою историю с 1997 года, когда основатели сообщества совершили ряд атак на владельцев кредитных карт и интернет-магазины на территории США. В том же году впервые возникло понятие «кардер» (человек, совершающий незаконные действия с банковскими картами) и начала формироваться иерархия кардерской мафии. Площадка прекратила свою деятельность в 2004 году по инициативе организаторов в связи с преследованием спецслужбами разных стран.

¹² <https://www.forbes.ru/tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kak-sozdavalsya-krupneishii-v-mire-forum-kiber>

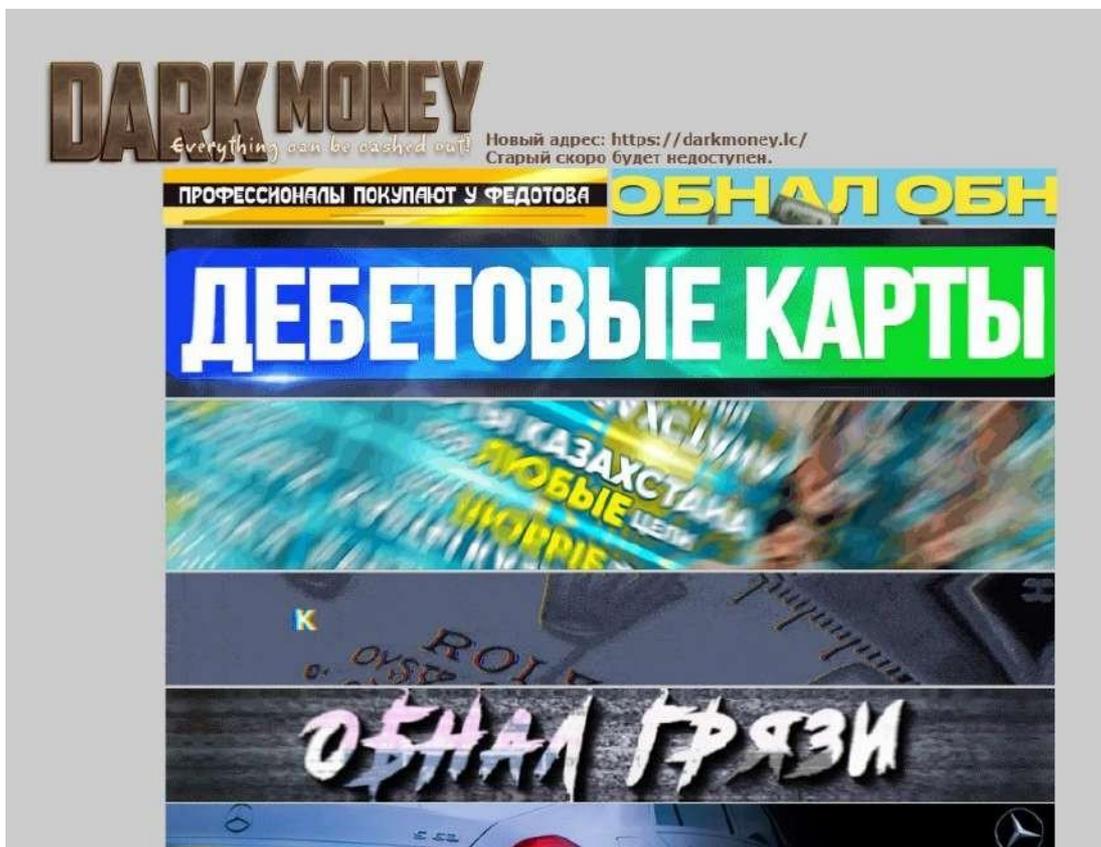


Рисунок 16. Пример объявлений дроп-сервисов

Оплаченная реклама					
Благотворительный фонд DarkMoney		Завели на благотворительность от Artikan	03.11.2012 17:03 ↓	12	592
КАРТЫ НА ВЫМЫШЛЕННЫЕ ДАННЫЕ ТОП - 1 СЕРВИС ДЛЯ ВАС! <ul style="list-style-type: none"> > Банковские карты на вымышленные ФИО, гарантия до конца срока действия! > Карты на ФИО заказчика. > СБЕР/ВТБ/АЛЬФА БАНК/РАЙФАЙЗЕН ТОП БАНКИ. > ОСОБЫЕ условия для обменных сервисов и оптовых клиентов. > Чистка/Обнал денежных средств. 		Карты на вымышленные данные На ваши ФИО! от KARTY.MA	Вчера 19:25 ↓	2	106
Дебетовые карты в Эльбрус: <ul style="list-style-type: none"> - работа с 2013 года - надежные дропы - адекватные цены - ответственное отношение 		Дебетовые карты. Ответственный сервис от elbrus881	Вчера 22:05 ↓	1	47
100BTC.pro - проверенный обмен электронных валют. Депозит 1000000 - 100% гарантия сохранности Ваших средств.		100BTC.pro - ВВОД, ВЫВОД, ОБМЕН: BTC, ETH, USD, qbit, btm, pr24, cash-in, нал в... от 100btc	Сегодня 10:30 ↓	1	487
Vektor T13 Security Services Вопросы анонимности и безопасности в сети, компьютерная криминалистика, бесплатные консультации, платное обучение, готовые продукты и решения.		Отвечаю на ваши вопросы по безопасности и антитексту от klassed1	22.08.2012 20:08 ↓	70	2,180
ОБНАЛ ГРЯЗИ ОТ 13% ГРЯЗЬ БЕЛОЕ СЕРОЕ, мне все равно... Возьмусь за любое. ОБНАЛ ГРЯЗИ ОБНАЛ СИЛМА ОБНАЛ КОЛЦЕНТРОВ ОТ 13% Материал всегда в наличии, работаем без выходных.		Обнал грязных денег от brilliantanta	25.09.2012 00:09 ↓	2	108
pridechange.com - обмен электронных валют (прозрачность: 1) Быстро! Выгодно! Безопасно! это три главных принципа, которыми мы руководствуемся во время проведения сделок.		pridechange.com - обмен электронных валют - BTC - ETH - LTC - XRP -... от PRIDECHANGE	03.11.2012 10:38 ↓	3	73
БРОНСОН И ЕГО ДРУЗЬЯ ОБНАЛИЧАТ СРЕДСТВА Работаем от 20% Всегда в наличии.					

Рисунок 17. Пример объявлений дроп-сервисов

Современные дроп-сервисы — это целая индустрия. Типовая организационная структура таких сервисов представлена на рисунке 18. В этих

«организациях» есть все атрибуты качественной компании, предоставляющей услуги легального сервиса: пакеты клиентских услуг, пошлины и депозиты, рекламные бюджеты, заработная плата «сотрудников», круглосуточная поддержка, личный помощник для постоянных клиентов и многое другое.



Рисунок 18. Организационная структура сервисов по обналичиванию похищенных денежных средств

Если у дропа или дроповода масштабные амбиции, то с небольшими вложениями и наработанной репутацией на теневых площадках он имеет шанс выйти на уровень владельца дроп-сервиса.

На теневых форумах дропам оказывается консультативная поддержка, распространяются скрипты общения с правоохранительными органами и т. д. (см. рисунок 19). Зачастую сообщники задержанных дроповодов нанимают своим «коллегам» дорогостоящих адвокатов.

Поиск: Ключевые слова: **арест, адвокат** Показано с 1 по 14 из 14.
На поиск затрачено 0.04 сек.

Тема / Автор	Просмотров	Раздел
Важно: Как найти хорошего адвоката и вычислить плохого. Пошаговая инструкция. (1 1 2) alin1	16,936	Юридические вопросы безопасности
Важно: Баг: вас приняли, что делать? про общение с полицией, прокурором, адвокатом и судом. (1 1 2 3 ... Последняя страница) Forum services	17.06.2022 20:51 от Forum services 71 68,729	Юридические вопросы безопасности
[Продам] Обманули? Поступили не по весте? Не выполняют долговые обязательства в срок? ILLUMINATE FAMILY	18.08.2021 16:31 от ILLUMINATE FAMILY 0 101	Прочие темы
"История одного обнала" - ищем 3 интересных истории на 60,000 рублей (1 1 2 3 ... Последняя страница) MoneyMusk	14.07.2021 08:51 от iu87ewrh6 44 4,129	Прочие темы
Экстренное уничтожение компьютера - badUSB, USB-киллер DM2019	15.02.2020 16:26 от DM2019 0 639	Безопасность и анонимность
Домашний арест (1 1 2 3 ... Последняя страница) Aresthome	28.01.2019 10:04 от SamRostan 91 8,938	Прочие темы
За рубеж от тюрьмы и сумы: правила экстрадиции (1 1 2) zjudnik	24.10.2017 20:21 от Abriak 11 14,428	Юридические вопросы безопасности
[Вопрос] Проблемы номинального директора ООО (1 1 2 3 ... Последняя страница) Makmanapan	17.06.2017 11:25 от Xristofor 41 9,908	Юридические вопросы безопасности
Платоническая любовь к Darkmoney (1 1 2 3 ... Последняя страница) Forum services	16.05.2017 00:01 от TE6LA 101 13,703	Новости проекта
Важно: Бесплатный курс по юридической безопасности для пользователей darkmoney.is (1 1 2 3 ... Последняя страница) Forum services	17.12.2016 18:34 от CVX 48 35,954	Юридические вопросы безопасности
Идут за дропом по вкам (1 1 2 3 ... Последняя страница) Томск	24.10.2016 15:00 от koly4ka 87 14,318	Юридические вопросы безопасности
Важно: Если вам пришлось бежать. (1 1 2 3) Dante	17.09.2016 07:40 от Лаки 21 37,786	Юридические вопросы безопасности
Хотят впать 174 статью. (1 1 2 3 ... Последняя страница) Kvlm	02.05.2016 15:12 от Энигма 48 9,379	Юридические вопросы безопасности

Рисунок 19. Консультативная поддержка дропов на теневом ресурсе

Как показывает практика, в этой преступной среде консультативная и административная поддержка дропов не носит формального характера. Судя по текстам, их пишут профессиональные юристы, знакомые не понаслышке с уголовным процессом и методами работы правоохранительных органов.

Мы разобрали вышеуказанную тему консультативной поддержки на теневом форуме (см. рисунок 19) и публикуем ключевые выдержки оттуда (авторский слог сохранен):

- *Разговор пойдет о том, о чем никогда не стоит забывать кардеру, да и любому преступнику вообще – как себя вести в первые дни после задержания.*
- *Если коротко, то зашейте себе рот и отрубите руки, когда вас взяли.*
- *Главное продержаться первые три дня, но первый день все равно самый главный.*
- *Если вы будете анализировать альтернативы, предложенные операми, то вы опять проиграете. Делайте скидку на то, что к ночи 80% содержимого вашего мозга будет забито тем, чем захотят опера, и вы будете думать так, как захотят они.*
- *Один из частых трюков, применяемых ими – это ложные альтернативы.*
- *Так что каждое ваше необдуманное слово, каждая роспись в бумагах увеличивает этот срок.*
- *Первыми вы познакомитесь с операми, их задача всеми законными и незаконными способами получить от вас максимум подписанных вами бумаг, а в идеале добиться вашего полного признания и выдачи всех улик.*
- *Другими словами, вас готовят к передаче в другую инстанцию – к следователю.*

- *Самое же главное – то, что вы напишете уже у следователя в первом протоколе, одно неверное слово – и вы будете об этом жалеть всю оставшуюся жизнь.*

Далее идет краткая характеристика сотрудников полиции различных должностей: оперов, экспертов и следователей. Не обошли вниманием и федерального судью.

4. Использование дропов в мошеннических схемах

В основу расследования деятельности мошеннического call-центра в г. Бердянск (Украина) был положен накопленный опыт противодействия мошенничеству Сбера. Отчет опубликован на новом ресурсе Сбера по кибербезопасности «[Кибрарий](#)» и раскрывает детали организации работы типового call-центра.

В частности, в расследовании отмечена роль специальных дроп-сервисов, продающих карты или счета дропов, а также поддерживающих процесс вывода похищенных денежных средств. Бердянский call-центр сотрудничал с несколькими теневыми сервисами, находящимися на торговых площадках DarkMoney и Dublikat.

Вывод денежных средств был организован следующим образом: сотрудники второй линии call-центра в режиме разговора с жертвой заказывали через обнал-сервис подходящую карту «дропа» с необходимым лимитом для вывода средств. Закрепленный за данным call-центром персональный менеджер сервиса в режиме онлайн предоставлял данные и ждал зачисления похищенных у клиента средств. Затем денежные средства обналичивались сотрудниками сервиса. Комиссию в 15-20% забирал сервис, а оставшиеся денежные средства переводились на подконтрольные организаторам call-центра криптокошельки по курсу на текущую дату. При этом злоумышленники активно использовали токенизацию¹³ банковских карт дропов на устройстве жертвы, а также применяли мошенническую схему «самоинкассация», когда дропы вносили похищенные денежные средства через устройства самообслуживания на расчетные счета юридического лица, которые были оформлены, как правило, на подставных лиц.

Это типовые схемы вывода похищенных денежных средств, характерные для всей индустрии отмыwania криминальных доходов. Стремительный рост социальной инженерии в последние годы породил высокий спрос на услуги обналичивания похищенных денежных средств. Это, в свою очередь, сказалось на увеличении количества как теневых дроп-сервисов, так и самих дропов. Спросу также поспособствовали введенные против России санкции – обналить практически все похищенные денежные средства клиентов российских банков можно только на территории России.

Владельцы дроп-сервисов воспользовались сложившейся ситуацией и используют наших сограждан в качестве дропов и, соответственно, банковские карты отечественных кредитно-финансовых учреждений и платежных сервисов. Аналитика Сбера наглядно показывает распределение дропов по всей территории нашей страны, со своеобразными «столицами» (см. рисунок 20).

¹³ Токенизация банковских карт – это технология обмена конфиденциальных данных на специальный цифровой обезличенный токен, иными словами, выпуск в банковском мобильном приложении виртуальной карты, привязанной к действующей пластиковой карте.



Рисунок 20. ТОП-10 регионов РФ по количеству дропов

Известны места концентрации нелегальных сервисов по обналичиванию или переводу похищенных денежных средств в криптовалюту. В Москве это прежде всего Москва-Сити, торговые центры «Горбушкин двор», «Фудсити», «Садовод», автовокзал «Котельники» и торгово-ярмарочный комплекс «Москва». По нашим данным, до 40% теневой наличности сосредоточено именно в Москве.

Отдельно необходимо выделить центры, где аккумулируются похищенные денежные средства в виде наличных, т.н. «денежные хабы». Помимо Москвы, в лидеры также стремится Санкт-Петербург и Ленинградская область. Такая особенность связана с тем, что северная столица является крупным туристическим центром, в котором легко затеряться приезжему. В этом городе еще довольно слабо развито видеонаблюдение и особую роль играет близость к границе с несколькими государствами.¹⁴

¹⁴ По данным Сбера и МВД России



Рисунок 21. Пример одного из ликвидированных сотрудниками полиции дроп-сервисов

Одними из основных инструментов дропов для вывода похищенных денежных средств являются карты российских банков и телефонные номера операторов сотовой связи, которые фактически превратились в самостоятельный платежный инструмент.

Мы провели анализ активности дропов в каждом из указанных инструментов. Ниже представлены результаты, некоторые из них весьма показательны. Так, распределение дропов, которых используют киберпреступные группы, выглядит следующим образом (см. рисунок 22). В силу определенных обстоятельств раскрыть наименования банков мы не можем, поэтому на рисунке указаны условные названия банков (Сбербанк отражен без маскирования).

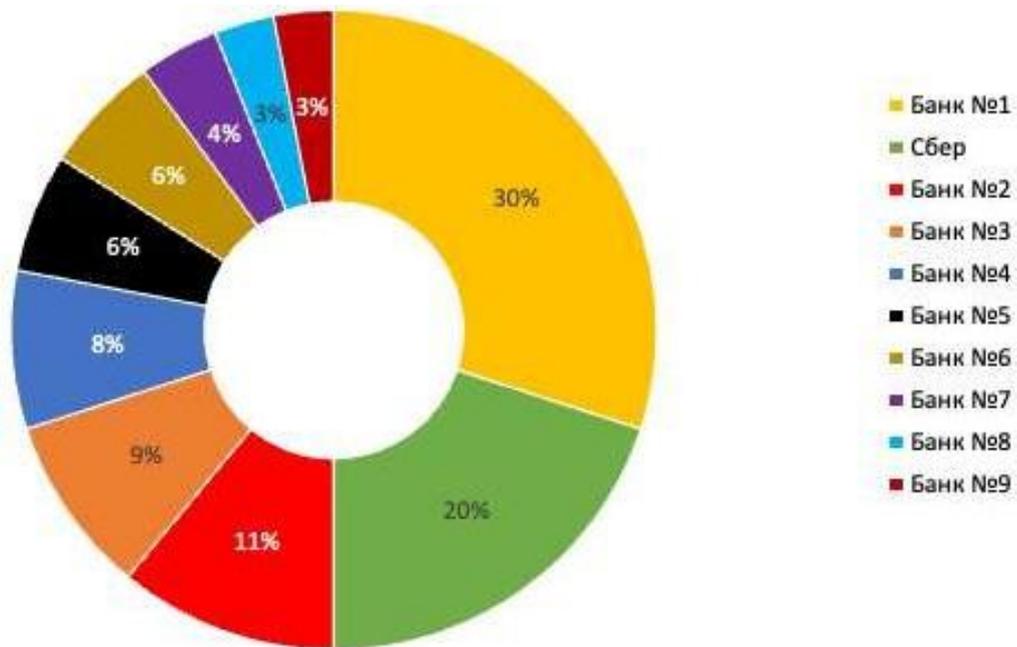


Рисунок 22. Статистика по дропам в абсолютных цифрах по банкам, ТОП-10

Однако, статистика в абсолютных цифрах не дает объективной картины проводимой банками работы по противодействию дроперской активности, т.к. очевидно, что чем больше банк, тем больше будет количество дропов. Корректнее будет взглянуть на эту статистику с учетом размеров клиентской базы.

На рисунке 23 дана оценка статистики, взвешенной относительно размера клиентской базы. По этим данным можно оценить усилия банков по применению рекомендаций ЦБ РФ в части противодействия использованию инфраструктуры банковской системы в противоправных целях (цвета соответствуют цветам на рисунке 22).

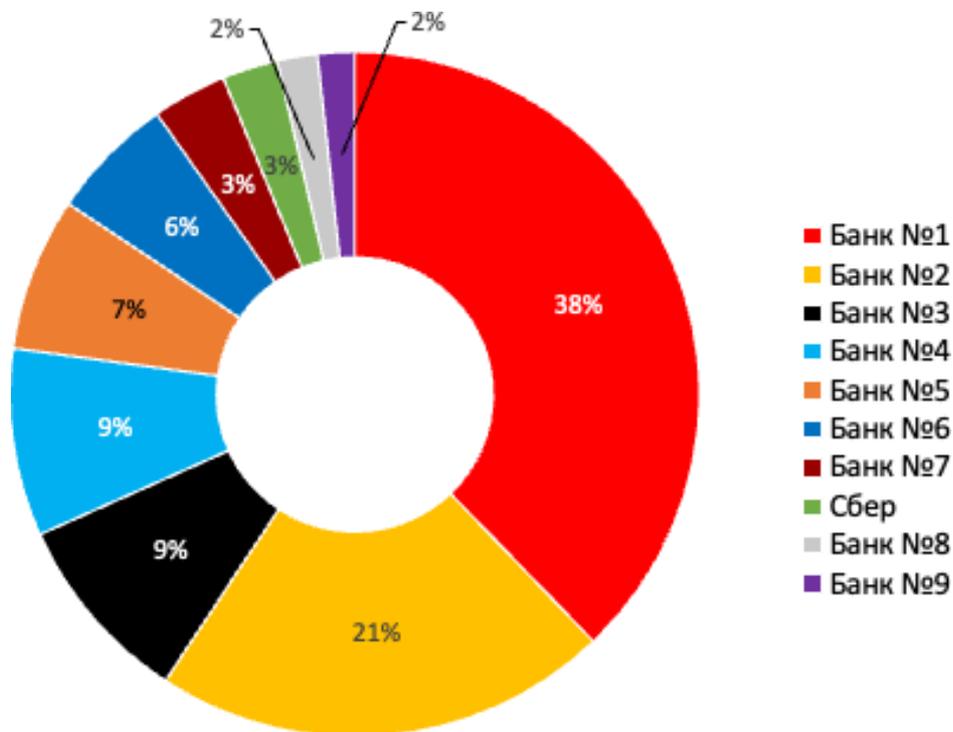


Рисунок 23. Взвешенная статистика распределения дропов по банкам относительно клиентской базы, ТОП-10

Отметим, что лидером по доле дропов в клиентской базе являются цифровые банки, предоставляющие удобные дистанционные сервисы по оформлению и выпуску банковских карт.

Изучив общий показатель активности дропов по банкам, мы решили взглянуть на проблему под другим углом. Последние несколько лет в России безусловным лидером в используемых мошеннических схемах в отношении клиентов банков является социальная инженерия. Но не стоит забывать про фишинг, который активно эксплуатируют мошенники. В этой связи мы решили проанализировать и выделить из общей статистики во взвешенных величинах по банкам две частности: социальная инженерия и фишинг. Результаты представлены на рисунках 24 и 25.

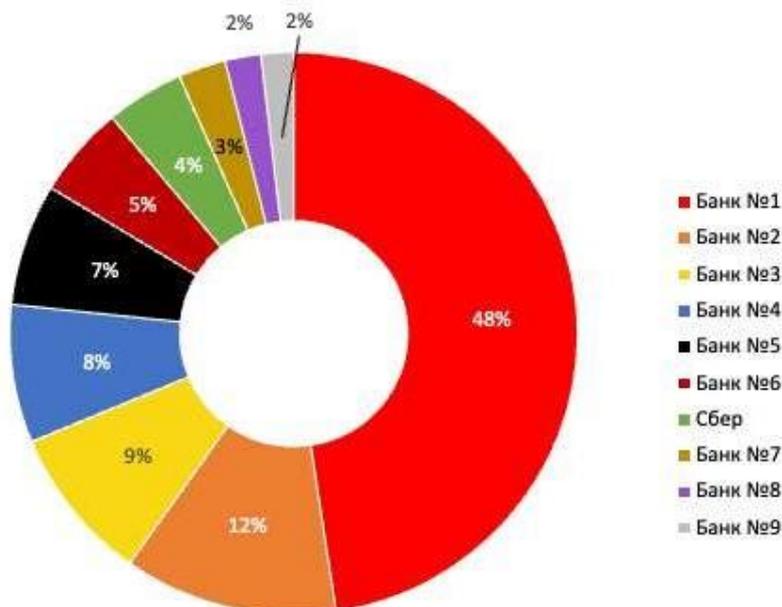


Рисунок 24. Взвешенная статистика по банкам – социальная инженерия

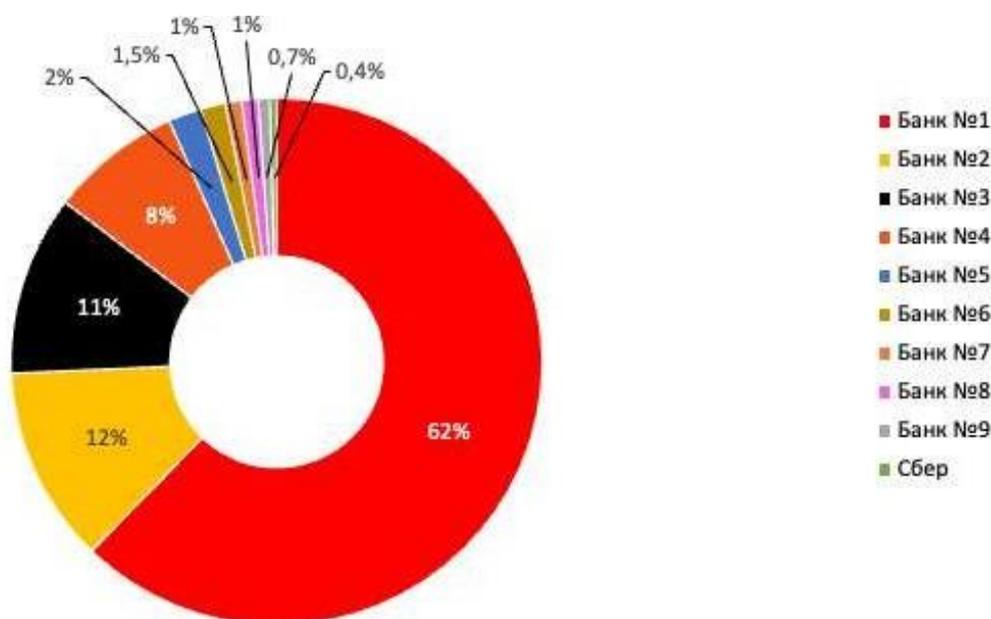


Рисунок 25. Взвешенная статистика по банкам - фишинг

Из рисунков видно, что лидер – банк 1 – в социальной инженерии и фишинге не изменился, но его доля в фишинге выросла до 62%, далее список банков в целом не изменился.

Еще одной интересной деталью является количество банковских карт (продуктов), используемых дропами. Проанализировав профили дропов, мы получили результаты, которые оказались весьма интересными. По статистике 6,3% дропов имеют более 50 карт, почти 53% – от 10 до 50 банковских карт, а максимальное количество карт у одного дропа – 1608 (см. рисунок 26).

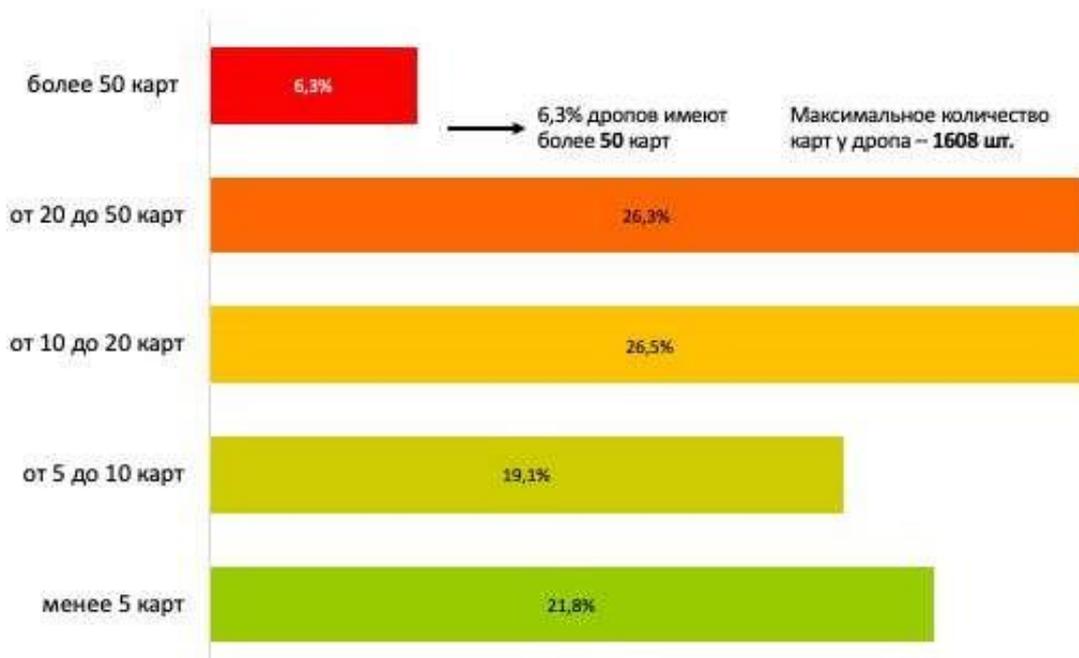


Рисунок 26. Распределение в долях количества карт у дропов

Теперь любопытно взглянуть на статистику по выводу похищенных средств на лицевые счета абонента сотовой связи через операцию пополнения счета мобильного телефона. Статистика приведена в разрезе крупнейших сотовых операторов России. (см. рисунок 27), наименования операторов мы не раскрываем.

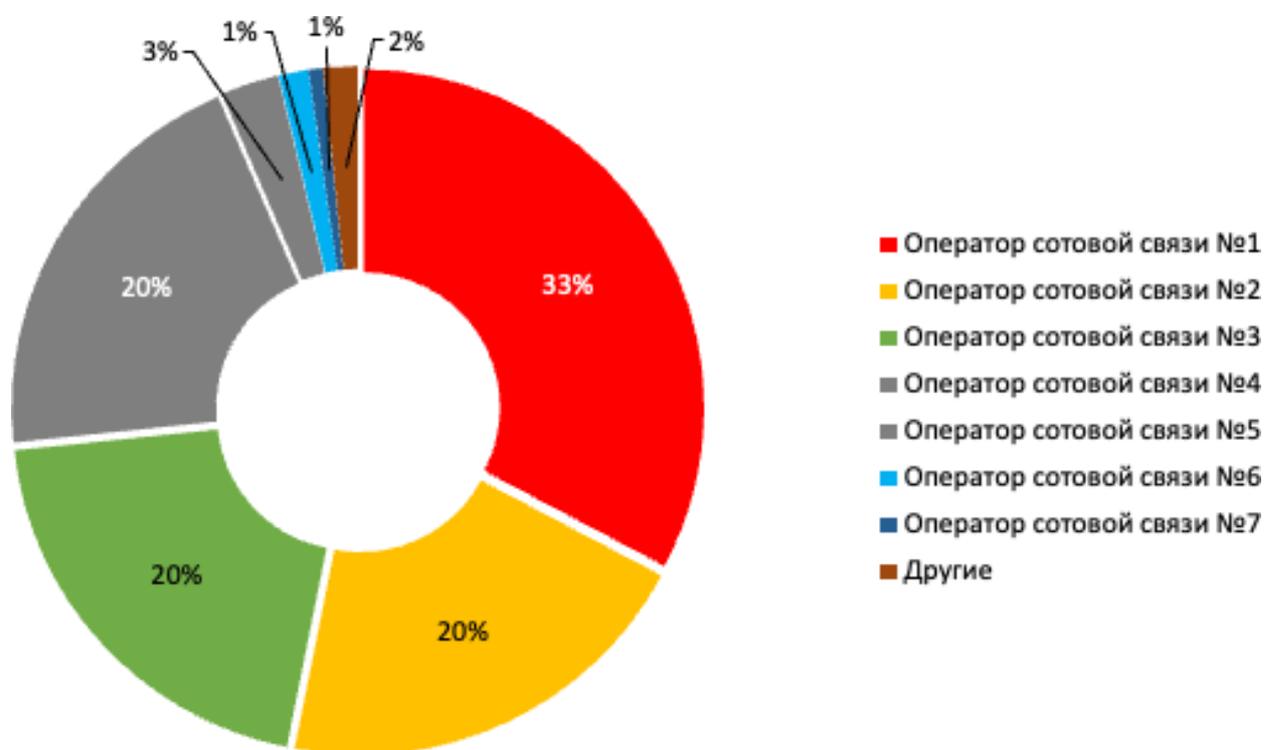


Рисунок 27. Распределение операторов сотовой связи как инструмент вывода похищенных средств

Выделяется один оператор, сервисами которого более активно пользуются мошенники. Вероятно, этому способствует предоставление к счету абонентского номера развитых финансовых сервисов, позволяющих осуществлять дальнейший

быстрый вывод средств с минимальной комиссией.

Подводя итог, можно отметить, что представленная нами аналитика наглядно показывает высокую эффективность предпринимаемых усилий Сбера по противодействию дроперской активности. Мы ставим перед собой амбициозные цели – нулевая толерантность к фроду в целом и к дропам в частности.

5. Ответственность за дроперство

Проблема обналичивания преступного капитала существует во всем мире. В Китае, например, при подозрении на подобную деятельность все счета потенциального дропа незамедлительно блокируются, а в России блокируются только удаленные каналы банковского обслуживания и банковские карты (т.н. электронные средства платежа или «ЭСП»). Примечательно, что в Китае передача банковских карт третьему лицу является уголовно наказуемым правонарушением, за которое можно получить пожизненный срок.

В странах Евросоюза предусмотрены большие штрафы или тюремные сроки до 10 лет лишения свободы за участие в мошеннических схемах или передачу своих банковских карт для этих целей.¹⁵

Стоит также отметить законодательный опыт республики Беларусь, где в 2021 году ввели уголовную ответственность в виде наказания от 3 до 10 лет лишения свободы за передачу реквизитов или продажу своей банковской карты. Но, как показывает практика, не суровость или длительность наказания, а именно принцип его неотвратимости является лучшим фактором сдерживания и профилактики.

В Российской Федерации ситуация выглядит не так позитивно. По статистике МВД России за 10 месяцев 2022 года количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее ИТТ) снизилось на 5,6% по сравнению с аналогичным периодом прошлого года, но количество особо тяжких преступлений в части ИТТ увеличилось на 12%, и при этом количество нераскрытых особо тяжких преступлений увеличилось на 7,5%. Эта статистика говорит о том, что мошенники стали использовать более квалифицированные схемы обмана клиентов банков, что увеличился размер ущерба и предпринимаемых усилий со стороны государства недостаточно. По нашей оценке, к уголовной ответственности привлекается не более 10% дропов, а у органов прокуратуры и суда в регионах практически отсутствует единый подход к правоприменению. При этом важно отметить, что привлечение к уголовной ответственности обналичивающих похищенные средства дропов и их дроповодов не составляет особого труда и успешно реализуется правоохранительными органами при наличии собранной доказательственной базы. Таким образом, современная следственная и судебная практика привлечения дропов к ответственности в РФ нуждается в улучшении.

Сложнее обстоит ситуация с дропами, продавшими свои карты дроповоду или организаторам обнал-сервисов, поскольку за передачу или продажу своей банковской карты третьему лицу до сих пор не предусмотрено административной или

¹⁵ <https://evropakipr.com/istorii/operaciya-warenagent-na-kipre-zaderzhan-glava-mezhdunarodnoy-gruppy-onlayn-moshennikov>
<https://news.rambler.ru/internet/47242585-evropol-arestoval-bolee-sotni-kibermoshennikov-mafiozi/>
<https://xakep.ru/2021/12/02/emma-7/>

уголовной ответственности. Тот факт, что карта будет использоваться для совершения преступлений, всем очевиден. Но, увы, это не доказывает наличие умысла на хищение.

Кроме того, в борьбе с дропами многое зависит от скорости принятия решений правоохранительной системой и сроков проведения оперативно-розыскных и следственных мероприятий.

По данным Сбера, более 80% похищенных денежных средств обналичиваются злоумышленниками в течении первого часа после зачисления на карту/счет дрoпа. В течении 5 часов обналичено или выведено 100% похищенного.

Однако у служб безопасности банков отсутствуют легальные основания наложения каких-либо блокировок на денежные средства, зачисленные на реквизиты дропов. Федеральными законами данное действие разрешается только по основаниям 115-ФЗ, который не подходит под случаи кибермошенничества – злоумышленник при желании может получить заблокированные средства. Поэтому данная проблема требует серьезного переосмысления на уровне МВД и Центрального банка РФ.

6. Опыт Сбера по борьбе с дропами

Согласно требованиям Федерального закона «О национальной платежной системе», кредитные организации обязаны выявлять операции, совершаемые в адрес мошенников, своевременно предупреждать об этом клиентов, а также направлять в Банк России информацию о таких случаях и попытках осуществления переводов.

Со своей стороны, Банк России формирует и ведет базу данных «о случаях и попытках осуществления переводов денежных средств без согласия клиента». В базу данных собирается информация о реквизитах дропов, которую банки обязаны применять при выявлении мошеннических операций. Соответствующие списки с реквизитами регулярно распространяются среди кредитных организаций и содержат более 100 тыс. записей.

Сбор и распространение информации о дропах происходит в рамках созданной ФинЦЕРТ Банка России Автоматизированной системы обработки инцидентов (АСОИ).

Кроме того, регулятор рекомендует банкам блокировать электронные средства платежа мошенников и препятствовать использованию инфраструктуры банковской системы в преступных целях. Также кредитным организациям рекомендуется после предварительного предупреждения отказывать клиентам в приеме от них распоряжений на проведение операции по банковскому счету/вкладу с использованием дистанционных каналов обслуживания в случае выявления сомнительных операций.

Сбер в 2020 году, не ограничиваясь выполнением рекомендаций регулятора, начал активно бороться с клиентами, ведущими дроперскую деятельность с использованием продуктов банка.

В рамках этой работы одновременно с данными из АСОИ в нашей системе фрод-мониторинга объединены все доступные источники о дропах (см. рисунок 28).

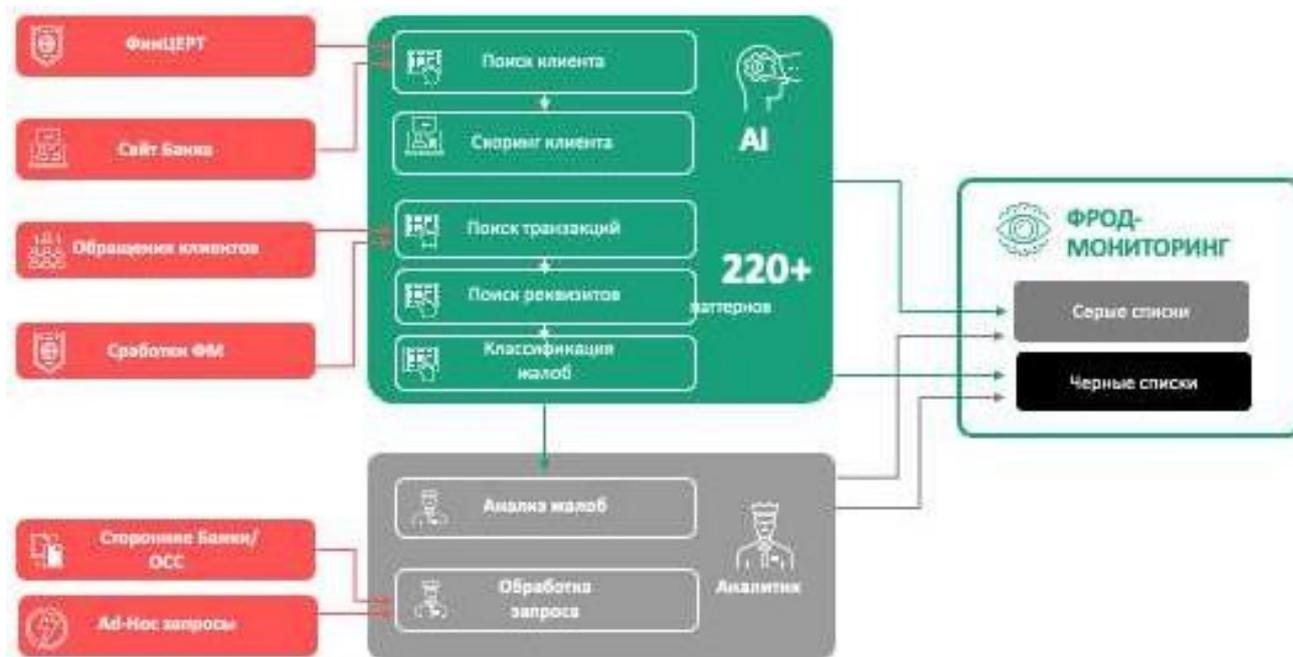


Рисунок 28. Подход Сбера к выявлению дропов

В повседневной деятельности фрод-аналитики используют возможности графовой аналитической платформы фрод-мониторинга. Это позволяет увидеть не просто транзакционную активность карты, но и все связи, поведенческие особенности и ряд других паттернов, характеризующих владельца банковской карты и позволяющих однозначно подтвердить подозрительный профиль клиента или характер использования карты. Данный инструмент дает возможность в короткие сроки выявлять состав и участников дроп-схемы по обналачиванию. Меры реагирования на уровне банка применяются незамедлительно, далее работа выстраивается в тесном взаимодействии с правоохранительными органами.

Процесс совершенствования инструментов Сбера для противодействия кибермошенничеству непрерывен. Разрабатываются собственные программные продукты. Активно используются средства автоматизации, лучшие международные практики в области обеспечения информационной безопасности. В Сбере выстроены сквозные бизнес-процессы, организован производственный алгоритм для проверки операций в режиме 24/7, создан уникальный по своим масштабам и сложности вычислительный комплекс, способный за доли секунды проверить любое событие в системах банка на кибермошенничество. Все перечисленные возможности значительно повышают результативность и компетенции фрод-аналитиков.

В результате банком выявлено уже более 35 тыс. клиентов с признаком дропа, которые поставлены на дополнительный контроль, им также запрещено получать новые карты и другие электронные средства платежа. По оценкам Сбера, всего в России граждан, имеющих признаки дропа, порядка 500 тыс.

В Сбере наработан большой опыт в аналитике цифровых следов и во взаимодействии с правоохранительными органами, в том числе – по борьбе с обналачиванием похищенных денежных средств. В 2022 году в результате совместной работы с МВД России правоохранителями было ликвидировано 70 мошеннических организованных преступных групп, причинивших ущерб гражданам на сумму более 540 млн рублей.

К примеру, 06.07.2022 г. по результатам проведенной сотрудниками Сбера аналитики цифровых следов движения украденных средств были задержаны 4 злоумышленника, причастных к обналичиванию более 10 млн рублей, похищенных в результате телефонного мошенничества. В ходе обыска у подозреваемых было изъято около 380 карт различных банков.

7. Меры противодействия дропам на уровне государства

Массовость данного вида преступлений в России обусловливается прежде всего высоким уровнем организации этих ОПГ, но немаловажную роль также играет недостаточность усилий по борьбе с дропами со стороны государства.

Мошенники имеют благоприятные условия для совершения противоправных деяний в отношении клиентов кредитных организаций. Исправить положение в определенной степени могли бы комплексные меры со стороны государства и бизнеса.

- Прежде всего, необходима организация взаимодействия кредитно-финансовой сферы, правоохранительной системы и операторов сотовой связи с целью оперативного обмена информацией о совершенных преступлениях и проведения блокирующих мероприятий по похищенным денежным средствам клиентов.
- Необходимо внести изменения в действующее уголовное законодательство в части установления ответственности за незаконное предоставление банковских карт, электронных средств платежа и иных банковских продуктов, совершенное их владельцем по аналогии с мировым опытом в этой области.
- Для решения проблемы с использованием звонков с подменных номеров необходимы пересмотр и корректировка требований к оказанию услуг связи на территории РФ, к построению и применению сетей связи, их управлению, защите, порядку пропуска и маршрутизации трафика, порядку взаимодействия сетей связи. Здесь также необходимо усиление контроля.
- Банку России также необходимо разработать для кредитных организаций рекомендации и инструменты, которые можно было бы использовать при оказании помощи клиентам по возврату похищенных денежных средств.
- Необходимо в постоянном и оперативном режиме осуществлять блокировку интернет-ресурсов, где расположены площадки дроп-сервисов. По аналогии с существующей блокировкой интернет-ресурсов, которые нарушают действующее законодательство РФ.

Все эти мероприятия, конечно же, требуют координации деятельности заинтересованных участников: органов власти, правоохранительных органов, кредитных организаций, операторов связи и других структур по борьбе с кибермошенничеством. Одна из первоочередных целей – сделать криминальный обнал экономически невыгодным для мошенников.

Выводы

Масштабы проблемы вывода и обналичивания преступного капитала, массовое вовлечение в криминальный бизнес граждан страны требуют выработки соответствующих мер, которые можно условно разделить на три основных направления:

- социальное: проведение профилактической и просветительской работы, особенно среди молодежи;
- технологическое: совершенствование антифрод-систем, их взаимная интеграция, использование искусственного интеллекта;
- законодательное: необходимость ввести ответственность за передачу банковских карт третьим лицам и ужесточить наказание для дропов.

Отмывание и вывод криминальных доходов уже давно перестали быть проблемой только правоохранительных органов. Необходим комплексный подход, участниками процесса должны стать не только банки и операторы сотовой связи, но и федеральные структуры. Желательно ускорить процесс интеграции МВД России в межбанковский информационный обмен в части предотвращения и раскрытия дистанционных мошенничеств. Первоочередная задача – сделать нерентабельным вывод похищенных денег и, тем самым, отправить на свалку истории целый ряд мошеннических схем.